Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

Digital Asset Enforcement Reform in Indonesia: A Polycentric Governance Approach

Syamsul Maarif[1*]
[1]The Supreme Court of the Republic of Indonesia and Lecturer at Faculty of Law, Universitas Brawijaya, Indonesia.
*Corresponding author's email: syamsul.maarif@ub.ac.id

Article Information

Received for publication October 31, 2025
Accepted after corrections April 13, 2026

Keywords: Digital Assets Governance; Enforcement and Restitution; Insolvency Reform.

DOI: 10.20961/yustisia.v15i1.110549

Abstract

Digital assets are growing quickly in Indonesia, which has caused a lot of legal and institutional problems, especially when it comes to settling disputes over cryptocurrencies, tokenised assets, and other blockchain-based tools. Despite regulatory recognition, there remains a critical gap between legal frameworks and effective remedies for victims, highlighting the urgency of enforcement reform. This article examines the key legal problems, including regulatory fragmentation, ambiguity in asset classification, cross-border enforcement barriers, limitations in digital forensic capacity, and weak inter-agency coordination. Using a normative-doctrinal method combined with comparative analysis of cases and regulatory developments, this study adopts a polycentric governance approach to assess how administrative, civil, and criminal enforcement pathways interact and where they fail. The findings reveal that enforcement inefficiencies occur across the entire dispute chain, leading to inadequate victim recovery, legal uncertainty, and reduced market trust. This study proposes a sequenced reform framework, including the enactment of a consolidated digital asset law with functional classification, strengthening regulatory authority with asset preservation powers, reforming insolvency law to recognise digital property, establishing standardised forensic and evidentiary protocols, and enhancing cross-border cooperation mechanisms

I. Introduction

The article examines how digital asset disputes are enforced in Indonesia and where the existing framework fails. Digital assets, including cryptocurrencies, tokenised assets, and other ledger-based representations of value, have rapidly gone from fringe experiments into mainstream economic activity (Rodríguez De Las Heras Ballell, 2024). In Indonesia, as in many jurisdictions, the rise of digital asset trading platforms, decentralised finance experiments, and token-based fundraising has created new opportunities for investment, innovation, and financial inclusion. At the same time, it has created a growing volume and variety of disputes (Mulyadi, 2025). Numerous issues

include the loss of customer cash due to exchange failures, fraud and scams, custody and insolvency disputes, AML/CFT problems, smart contract failures, and cross-border fraud that complicates evidence collection and remediation. The resolution of these conflicts and the execution of remedies are significant for market trust, consumer protection, financial stability, and the long-term legitimacy of the digital asset ecosystem.

Despite the necessity of enforcement, five persistent hurdles undermine the efficiency of Indonesia's present enforcement responses to digital asset disputes. The first is the fragmentation of laws and regulations (Berutu et al., 2025). Multiple legal regimes and agencies may have overlapping roles concerning digital assets, such as consumer protection, financial regulation, commodity treatment, and criminal law. This overlap creates uncertainty about the relevant rules and the appropriate enforcement forum (Bahtera et al., 2025). Second, ambiguity in classification. Digital assets are diverse (payment tokens, security-like tokens, utility tokens), and an uncertain legal classification might result in gaps in enforcement and corrective regimes (Iris Ng, 2025). Third, jurisdictional and transnational hurdles, as the cross-border elements complicate evidence collection, asset freezes, and enforcement of foreign orders (Ngozi Samuel Uzougbo et al., 2024; Dwitanti & Puji Simatupang, 2022). The FSB's 2025 thematic review found cross-border cooperation for crypto-asset activities to be "fragmented, inconsistent, and insufficient" across jurisdictions (FSB, 2025). Fourth, technical evidence and forensics, i.e., demonstrating custody, tracing flows, and establishing chain-of-custody for digital evidence require specialised capacity that many enforcement actors lack (Kartono et al., 2024; Fröwis et al., 2020). Fifth, institutional capacity and coordination, because enforcement requires coordinated action by prosecutors, financial intelligence units, regulators, police cyber units, and civil courts, yet coordination is frequently ad hoc or hindered by data-sharing constraints (Rusman & Fakrulloh, 2024; López-Aguilar & Solanas, 2022).

Within this enforcement focus, this article considers civil, criminal, and administrative enforcement pathways (how each pathway functions and where it succeeds or fails); institutional design and inter-agency coordination mechanisms required for effective action; operational capacities; and governance options. The geographic and temporal scope is Indonesia in the current policy moment, drawing on doctrinal analysis, comparative lessons, and case material to provide practical policy paths rather than solely theoretical models.

Prior studies on digital asset legislation and governance in Indonesia found crucial but still fragmented aspects of the regulatory problem. Nitha and Westra (2020) show that the dispute resolution avenues presently available for cryptocurrency cases, including Indonesian Commodity Arbitration Board (hereinafter abbreviated to BAKTI or *Badan Arbitrase Komoditi Indonesia*), Consumer Dispute Settlement Agency (hereinafter abbreviated to BPSK or *Badan Penyelesaian Sengketa Konsumen*), and ordinary litigation, remain constrained by a legal vacuum and do not adequately protect investor losses. Bahtera et al. (2025) likewise argue that crypto-asset investors continue to face

weak legal protection because the regulatory framework remains incomplete, technically underdeveloped, and institutionally unintegrated. In a similar vein, Berutu et al. (2025) find that overlapping authority and the transition from Commodity Futures Trading Regulatory Agency (hereinafter abbreviated to BAPPEBTI or *Badan Pengawas Perdagangan Berjangka Komoditi*) to Indonesia Financial Services Authority (hereinafter abbreviated to OJK or *Otoritas Jasa Keuangan*) have not yet fully resolved fragmentation in supervision and legal certainty. From the enforcement perspective, Nelson et al. (2024) further demonstrate that crypto-related asset recovery is hampered by blockchain tracing difficulties, limited asset-management mechanisms, and the slow pace of cross-border cooperation. Collectively, these studies show that digital asset governance has already been examined through the lenses of legal certainty, investor protection, institutional design, and AML enforcement, and that each of these domains reveals significant weaknesses in the current Indonesian framework.

Nonetheless, the interaction of these flaws throughout the entire dispute enforcement chain remains inadequately examined. Current studies predominantly examine digital assets through distinct regulatory or sectoral lenses. However, they have not comprehensively elucidated the intersections of administrative, civil, and criminal pathways, nor have they addressed the shortcomings across various dispute categories, including exchange insolvency, fraud, custody failure, and cross-border asset dissipation, and the implications of these deficiencies on victim restitution and market actor accountability. They still have not come up with a sequenced reform model that links asset classification, evidentiary standards, insolvency treatment, institutional coordination, and cross-border recovery all in one governance design. This circumstance is especially true in Indonesia now that the OJK has taken over supervision. This work addresses the identified research need. The originality of this article resides in its enforcement-focused methodology for digital asset governance in Indonesia, integrating normative-doctrinal examination and systematic secondary case analysis to identify operational impediments and develop a polycentric, pragmatically ordered reform agenda for legal and institutional transformation.

The article presents four fundamental research questions derived from this diagnosis: What are the primary legal and institutional impediments to the effective enforcement of digital asset disputes in Indonesia? How do enforcement deficiencies vary across different types of disputes (e.g., exchange insolvency, fraud/scams, custody failures, AML violations, smart contract failures)? What operational and capacity investments (technical forensics, training, evidentiary standards, cross-border collaboration) are necessary to implement these models? Additionally, how can Indonesia strategically sequence reforms to ensure that short-term enhancements (quick wins) and long-term structural changes mutually reinforce one another?

The article makes three contributions. First, it provides an empirical mapping of enforcement actors, dispute pathways, and operational bottlenecks specific to the Indonesian context. Second, it develops a typology of enforcement challenges that links dispute categories to enforcement obstacles and remedial shortfalls, enabling targeted policy design. Third, it offers a practical governance roadmap for legal, institutional, and technical reform, sequenced to balance effectiveness, feasibility, and the protection of

fundamental rights. These contributions go beyond general calls for better regulation to deliver concrete, actionable options that acknowledge the political and technical constraints of implementation.

The article proceeds as follows. Section 2 sets out the conceptual and theoretical framework, defining digital assets and classifying dispute types. Section 3 maps the legal and institutional landscape of enforcement actors and pathways. Section 4 presents the methodology. Section 5 analyses case studies illustrating enforcement failures and partial successes. Section 6 identifies and discusses the principal challenges. Section 7 proposes sequenced policy pathways and governance reforms. Section 8 concludes.

This study employs a normative-doctrinal approach complemented by structured secondary-case analysis. The doctrinal strand critically interprets statutes, regulatory instruments, administrative guidance, and judicial decisions to establish what the law prescribes regarding enforcement powers and remedies. The normative strand evaluates those rules against the policy and legal criteria developed in the conceptual framework: effectiveness, timeliness, proportionality, adaptability, and cross-border operability.

Empirical material derives exclusively from secondary sources: legislation and regulatory instruments; regulator circulars and licensing records; prosecutor and court judgments; FATF reports and international agency publications (including IOSCO's 2023 Policy Recommendations and the FSB's 2025 Thematic Review); published forensic and industry reports; and contemporaneous media accounts used for chronology and operational detail. Theory is applied iteratively: regulatory pluralism frames overlapping legal regimes, polycentric governance diagnoses coordination failures, and socio-technical legalism identifies where technical gaps undermine legal remedies.

Cases are selected purposively to illustrate the typology of disputes and enforcement pathways. Selection criteria prioritise variation on three dimensions: (i) dispute type (custodial insolvency, fraud, AML-related cases, smart-contract failures); (ii) institutional pathway engaged (administrative, civil/insolvency, criminal); and (iii) presence of cross-border elements. This purposive sampling enables analytic generalisation to categories of enforcement problems rather than statistical generalisation to all incidents.

Each case is evaluated against four indicators derived from the conceptual framework: (i) the adequacy of the enforcement pathway relative to the dispute type; (ii) the quality, admissibility, and chain-of-custody integrity of digital evidence produced; (iii) the degree of inter-agency coordination among police, prosecutors, regulators, and financial intelligence units; and (iv) the speed and extent of victim restitution or asset recovery.

II. Conceptual and Theoretical Framework

Before outlining the conceptual categories used in this study, the analytical framework must first be grounded in broader socio-legal theory. Niklas Luhmann's Legal System Theory understands law as an autonomous yet cognitively open social

system that stabilises normative expectations through the legal/illegal binary code (Luhmann, 2004). Digital assets introduce new forms of economic communication, technological risk, and transnational interaction that existing legal categories do not fully absorb. When classification, supervisory mandates, and remedial pathways remain fragmented, law loses part of its capacity to reduce complexity and provide predictable expectations (Paterson, 2024). Operationally, this lens is applied in the case analysis to diagnose where regulatory gaps prevent law from performing its complexity-reducing function—specifically, where actors cannot determine which regime applies, which institution has competence, or which remedy is available.

Emile Durkheim's structural functionalism and Talcott Parsons' functionalist theory explain that in complex societies, law performs a restitutive function by coordinating differentiated social roles and preserving integration. Applied to digital assets, these perspectives reveal that the regulatory problem extends beyond isolated statutory gaps to encompass dysfunction across an interconnected institutional field involving market supervisors, financial intelligence bodies, courts, law enforcement, and private platforms. Operationally, this lens diagnoses coordination failures between enforcement actors identified in the case studies and informs the institutional design proposals.

Three domain-specific theoretical lenses further structure the analysis. First, regulatory pluralism recognises that digital asset governance is shaped by overlapping public, private, and market-based norms (Backer, 2016); it frames the mapping of overlapping legal regimes across administrative, civil, and criminal pathways. Second, polycentric governance locates enforcement within a network of nested authorities where multiple actors share responsibilities (Ostrom, 2010; Gunningham & Holley, 2016; Alston et al., 2022); it diagnoses why single-agency solutions are insufficient and why integrated reform and polycentric governance are complementary rather than contradictory. Third, socio-technical legalism understands law and code as mutually constitutive, such that enforceability depends on technical architecture, operational standards, and platform design alongside statutory text (Brown & Marsden, 2013); it explains why technical gaps in blockchain forensics and platform architecture undermine legal remedies.

Digital assets are defined as ledger-represented units of value whose legal nature is determined by their economic function, technological form, and regulatory framing. This includes protocol-governed instruments, tokenized securities, utility tokens, stablecoins, and native payment tokens. Treating digital assets as heterogeneous economic objects rather than a single legal species avoids category errors that produce enforcement gaps (Kochergin, 2022), consistent with international guidance favouring risk-based and activity-based regulation (Perlman, 2019; IOSCO, 2023).

A precise typology of disputes is essential because each class maps onto different evidentiary, procedural, and remedial requirements. The principal categories are: (i) custodial insolvency and exchange failure; (ii) fraud and scams; (iii) AML/CFT-related laundering and illicit financing; (iv) smart contract failures and protocol-level bugs; and (v) cross-border disputes involving extraterritorial evidence and asset recovery.

Operationalising enforcement further requires specification of several legal-technical concepts: *custody* (control over private keys and effective dominion over funds); *provenance* (on-chain and off-chain transaction history); *attribution* (linking pseudonymous addresses to real-world actors); and *evidentiary integrity* (chain of custody for digital forensic artefacts). The landmark *United States v. Sterlingov* (D.D.C. 2024) ruling—the first comprehensive Daubert analysis of blockchain analytics software—illustrates the evidentiary standards enforcement must meet.

Any reform should be evaluated against effectiveness in achieving redress and deterrence; timeliness in preventing dissipation of value; proportionality and protection of fundamental rights; operational feasibility given existing institutional capacities; adaptability to technological change; cross-border operability; and equitable access to remedies.

III. Legal and Institutional Mapping

A. Statutory and Regulatory Frameworks

Indonesia's regulations for digital assets have changed from a focus on commodities under the Commodity Futures Trading Supervisory Agency to a broader financial-asset approach under the Financial Services Authority. In the past, BAPPEBTI considered crypto as tradable commodities and set market rules through Peraturan Bappebti No. 5 of 2019 and its related lists and amendments. Meanwhile, Bank Indonesia has consistently prohibited the use of cryptocurrencies as a means of payment.

Recent administrative and legislative changes have resulted in the transfer of supervisory responsibilities to OJK through POJK No. 27 of 2024. Guidelines for the trading, licensing, governance, and reporting of digital financial assets are established by this rule. Furthermore, it is a step in the direction of incorporating a variety of cryptocurrency activities into the financial regulatory framework (Soerjadi & Kusmiadi, 2024). The simultaneous AML/CFT requirements for virtual asset service providers have been a major focus of Indonesia's financial intelligence unit, as noted in the FATF mutual evaluation. According to (Berutu et al., 2025), this calls for compliance with reporting guidelines and customer due diligence requirements that intersect with specific industry regulations.

However, Bank Indonesia has consistently stated that cryptocurrencies are not legal tender and has prohibited their use for payments in compliance with domestic currency law and related BI regulations. This position promotes monetary sovereignty and lowers the macrofinancial risks connected to tokenized payments. However, it allows for a great deal of investment and trading outside the payments perimeter. This distinction between permissive trading and payment exclusion has long influenced Indonesian policy decisions.

Cryptocurrency's primary perception as an investable asset reduces direct exposure to monetary policy while increasing the need for supervisory coordination to manage market integrity, fraud, and custody risks (Fahira et al., 2024). POJK No. 27 of 2024 marks a substantial shift in that architecture by giving OJK supervisory authority over

a wide class of "digital financial assets" and creating a single set of rules for the trading, licensing, governance, and reporting of digital financial asset operations (Erwanto & Santoso, 2024).

Practically, this reclassification brings crypto activities under prudential-style supervision and consumer-protection mandates, enabling OJK to impose capital, governance and reporting standards that were largely absent under the commodity regime. AML/CFT obligations and financial-intelligence work intersect tightly with these sectoral reforms. Indonesia's financial intelligence unit and the FATF mutual-evaluation process have emphasised the need for VASPs and other market participants to meet customer due-diligence, suspicious-transaction reporting and cross-border cooperation standards — obligations that cut across BAPPEBTI, BI and now OJK responsibilities and that require robust inter-agency coordination and information-sharing protocols. The FATF review in particular highlights both progress and remaining effectiveness gaps, signalling that regulatory reallocation must be accompanied by operational upgrades (supervisory capacity, standardised SAR formats, and public-private liaison mechanisms) to translate rulebooks into enforceable compliance regimes (see Izmi & Siagian, 2024).

B. Organisational Mapping of Enforcement Actors

Enforcement is polycentric and functionally distributed across criminal, prudential, payments, information and intelligence agencies. Enforcement is polycentric and functionally distributed. The Indonesian National Police (Bareskrim Cyber Crime Directorate) handles criminal complaints and seizure operations. The Prosecutor's Office litigates criminal asset recovery and coordinates mutual legal assistance requests. OJK, as the newly empowered prudential supervisor, can conduct onsite examinations, require capital and operational safeguards, and enforce segregation and reporting obligations. Bank Indonesia retains exclusive authority over legal tender and payment systems. Indonesian Financial Transaction Reports and Analysis Center (hereinafter abbreviated to PPATK or *Pusat Pelaporan dan Analisis Transaksi Keuangan*) performs the intelligence function, analysing suspicious transaction reports and operationally linking regulators, prosecutors, and police.

Despite this division of labour, enforcement is frequently constrained by overlapping remits, slow inter-agency procedures, uneven technical capacity for blockchain forensics, and the absence of a supervisor with express restitution powers. These frictions motivate proposals for clearer SOPs, a national coordinating mechanism, accredited forensic units, and stronger public–private investigative linkages.

C. Dispute Pathways

Digital asset disputes follow three overlapping procedural tracks: administrative enforcement against licensed intermediaries; civil litigation and insolvency claims; and criminal prosecutions for fraud, theft, or money laundering. Administrative pathways permit licensing sanctions and supervised remediation but are limited in delivering direct restitution. Civil courts face evidentiary challenges in tracing on-chain flows.

Criminal routes enable freezes and forfeiture but depend on specialist cyber-forensic capacity. Private dispute resolution and platform terms of service supply complementary but uneven remedial options.

D. Cross-Borders Enforcement

Cross-border recovery operates through Indonesia's mutual legal assistance system, but practical difficulties persist. Formal MLA requests proceed through the Ministry of Law and Human Rights and the Attorney General's Office—a process that is typically too slow for urgent digital asset freezes (Wibowo, 2023). The pseudonymous nature of addresses, the use of mixers and cross-chain bridges, and rapid "chain-hopping" permit perpetrators to disperse proceeds in minutes, outrunning MLA processing times (Scorpan, 2021; Prawira & Alamsyah, 2023).

MLATs were not drafted with crypto-specific preservation in mind, and many central authorities lack standardised templates for urgent preservation notices. Comparative studies identify the absence of crypto-tailored MLAT forms and weak mechanisms to convert rapid preservation notices into enforceable domestic restraint as recurring obstacles (Nelson et al., 2024). The Tilburg Law Review's case study of Netherlands cross-border crypto investigations confirms that traditional MLA systems are structurally inadequate for the speed required (Tilburg Law Review, 2024).

E. Indonesia's Financial Technology & Bitcoin Development

Bitcoin (BTC) occupies a dominant and distinctive position within Indonesia's digital-asset ecosystem. Regulator and industry compilations show that BTC consistently ranks among the top traded assets by value on domestic platforms and that the rapid expansion in registered and active crypto accounts has been largely driven by trading in a small set of major tokens, Bitcoin foremost among them. Official and industry sources place Indonesia's crypto investor base in the tens of millions and record a large year-on-year increase in aggregate on-exchange transaction value in 2024, underscoring that disputes over BTC transfers and custody are empirically non-trivial relative to other token classes.

Structurally, Bitcoin trading in Indonesia is concentrated on a handful of licensed trading platforms that combine order-book execution with custodial wallet services; these platforms typically operate hot/cold wallet architectures and present a single-point nexus for execution, custody and settlement. This institutional concentration means that operational failures or contested on-chain movements of BTC produce systemic exposure. A single exchange outage or exploit can generate large numbers of overlapping contractual, tort and insolvency claims (custodial liability, contract performance, conversion and tracing).

The empirical record already shows how BTC-specific incidents crystallise dispute pressures. High-profile security breaches in 2024—most notably the September exploit affecting a major domestic platform, which led to multi-million-dollar losses including dozens of BTC being drained from hot wallets—demonstrate both the scale of potential

BTC misappropriation and the practical difficulties of immediate asset preservation and forensic tracing across on-chain and off-chain venues. Analyses of the exploit and attendant fund flows highlight typical operational vectors (hot-wallet compromise, cascading liquidity freezes) that produce claimant-level harms and complicate recovery, thereby motivating the article's focus on preservation orders, custodial standards and cross-border enforcement of BTC claims.

IV. Case Study

A. Overview of Indonesian Enforcement Actions

Enforcement measures in Indonesia's growing cryptocurrency business have taken place in both the criminal and regulatory domains. Police and prosecutors have handled fraudulent "crypto investment" schemes as general financial crimes, while regulators have acted administratively.

The EDCcash case (2018–21) illustrates criminal enforcement against a large-scale fraud. Indonesian National Police Criminal Investigation Agency for the economic crimes unit arrested the promoter in April 2021, citing 57,000 victims and seizing vehicles, cash, and gold. The JYPRX/SYIPC/LEEDSX case (2025) shows cross-border complexity: Directorate of Cyber Crime dismantled an international online scam promising stock and crypto trading gains. Approximately ninety victims lost Rp105 billion, and six suspects were charged under the Law Number 1 of 2024 on the Electronic Information and Transactions (hereinafter abbreviated to ITE law), fraud provisions (Indonesian Criminal Code Art. 378), and money-laundering statutes. A Malaysian suspect remains on Interpol's wanted list. By contrast, BAPPEBTI's response to the September 2024 Indodax hack was purely administrative: summoning the exchange and "coordinating" to investigate the breach, with no direct restitution mechanism.

Through the lens of regulatory pluralism, these instances show that victims must choose between criminal prosecution and administrative review, with no separate civil framework for digital assets. Polycentric governance theory illustrates the coordination problem: criminal and administrative paths work concurrently without integration, resulting in duplication and delay. Socio-technical legalism explains why the Indodax breach, where quick on-chain transfers rendered seizure orders potentially irrelevant, requires technological preservation capabilities that the current architecture does not give.

B. Judicial Treatment: Decision of the Supreme Court of Indonesia No. 338/PDT/2020/PT SMG

This decision provides a rare Indonesian judicial encounter with "koin virtual digital" as the subject-matter of a commercial agreement. The dispute arose from a 2018 cooperation agreement for digital coin trading that included an express promise to provide land title as security; the pledged mortgage was never effectuated. On appeal, the Semarang court emphasised two doctrinal points: first, the contractual relationship was treated under ordinary civil-law doctrines (breach, restitution) rather than by treating the digital token as legal tender or secured collateral; second, the absence of

clear statutory recognition meant that traditional real-property remedies could not be mechanically transposed onto digital-asset transactions.

The case reveals the evidentiary and remedial gap facing claimants: courts will enforce ordinary contractual obligations where a valid contract and demonstrable loss exist, but they lack settled legal characterisation of crypto as money or collateral—leaving preservation, valuation, and cross-border enforcement questions unresolved without targeted procedural tools.

C. Evidence and Investigative Methods

Enforcement agencies have deployed both blockchain forensics and traditional investigative methods. In the JYPRX case, investigators traced transactions through wallet addresses and communication records, examining WhatsApp conversations revealing victims were prompted to pay fictitious "taxes" to withdraw money, and discovering sixty-seven nominee bank accounts used for laundering. Binance's investigators assisted Bareskrim by locating relevant cryptocurrency wallets, enabling the freezing of approximately US$200,000 in proceeds from a pig-butchering scheme.

For regulatory investigations, forensic alerts and internal security reviews are central. Following the Indodax breach, cybersecurity firm reports showed millions of dollars of ether moving from Indodax wallets, prompting BAPPEBTI to demand a system lockdown and user balance guarantees. Notably, no Indonesian case to date has involved smart-contract failure as a cause of action.

Hence, the result is (i) Enforcement pathways were adequate for straightforward fraud but inadequate for exchange-level custody disputes; (ii) digital evidence quality depended heavily on private-sector cooperation (Binance, cybersecurity firms) rather than public forensic capacity; (iii) inter-agency coordination was achieved through ad hoc channels requiring prolonged coordination; and (iv) victim restitution remained marginal despite successful investigations.

D. Outcomes and Recovery

The EDCcash founder was sentenced to six years' imprisonment (reduced from the ten-year demand); other ring members received two-to-five-year sentences. Investigators froze approximately Rp1.53 billion in suspect accounts. However, actual victim refunds have been minimal. In the Indodax incident, the exchange promised customers that balances were safe, but no legal mechanism existed to reimburse stolen tokens. This pattern—successful prosecution but negligible financial recovery—characterises the remedial inadequacy of current enforcement.

E. Singapore Comparative: TrueCoin LLC v Techteryx Ltd [2024] SGHC 296

The Singapore High Court decision (29 November 2024) provides a comparative reference for cross-border digital asset dispute resolution. The central issue was whether to grant an anti-suit injunction restraining Hong Kong proceedings that threatened to undermine Singapore-seated arbitrations arising from a cross-border stablecoin business transaction.

The Court applied established principles: an anti-suit injunction is appropriate where there is a prima facie breach of a valid arbitration agreement and no compelling countervailing considerations. Finding a prima facie breach, the Court rejected arguments based on comity and foreign-law complexity, concluding that permitting the Hong Kong actions to proceed would defeat the agreed arbitral process.

The decision confirms that clearly drafted arbitration clauses can prevent forum-shopping in crypto disputes, and that anti-suit relief can complement emergency arbitration in preventing asset dissipation. For Indonesia, this illustrates the value of well-designed private dispute-resolution clauses within a polycentric governance framework—an institutional option currently underutilised in Indonesian crypto transactions. Singapore's broader jurisprudence—including ByBit v Ho Kai Xin [2023] SGHC 199 (recognising cryptocurrency as property held on trust) and Cheong v Three Arrows Capital [2024] SGHC 21 (establishing the situs of cryptoassets at the residence of the private-key controller)—further demonstrates how judicial development can fill regulatory gaps that Indonesia's courts will inevitably confront.

V. Discussion: Key Challenges to Effective Digital Asset Governance Enforcement

This section analyses six interconnected challenges, each diagnosed through the theoretical framework and supported by case evidence. To avoid redundancy, each subsection addresses a distinct dimension of the enforcement problem.

A. Fragmented Legal Classification

Effective enforcement requires a functionally oriented classification so that legal duties, remedial powers, and supervisory responsibilities align with economic activity. In practice, however, crypto moved from BAPPEBTI's commodity regime to OJK's remit only with POJK No. 27/2024, while Bank Indonesia retains exclusive control over legal tender and PPATK supplies AML intelligence. The EDCcash and JYPRX cases show how actors exploited definitional ambiguity to evade financial supervision. Comparative frameworks—MiCA's tripartite taxonomy (ARTs, EMTs, other crypto-assets), the UK Law Commission's "third category" of property, and UNIDROIT's control-based Principles on Digital Assets (2023)—illustrate the consolidated approaches that Indonesia's current framework has not yet adopted.

Table 1 below maps dispute types to resolution methods and enforcement challenges across digital asset classes, demonstrating the systemic nature of these gaps.

Asset Type	Common Disputes	Resolution Methods	Enforcement Challenges
Digital assets, private digital currency	Disputes with exchanges, default/tort claims	Civil lawsuits(Articles 1365, 1243 Civil Code), non-litigation (arbitration, mediation), BAPPEBTI supervision	Lack of formalized regulations, trust in broker information
Crypto assets	Exchange failures, fraud, custody, market manipulation	No specific mechanisms; recommends OJK digital dispute resolution, arbitration laws not applied	Absence of mechanisms, legal uncertainty, lack of insurance
Cryptocurrency	Investor-marketplace disputes, fraud	Arbitration (BAKTI), BPSK mediation, litigation, law enforcement	No specific protection for investor losses, legal vacuum
Crypto assets	Money laundering, asset recovery	Penal/non-penal (police, prosecutors), Financial Intelligence Units, Interpol, Indonesian Financial Transaction Reports and Analysis Center (PPATK), Anti-Money Laundering Law	Blockchain tracing, cross-border, lack of asset management mechanisms
Non-fungible tokens (NFTs)	Copyright infringement, ineffective dispute resolution	Courts, arbitration, mediation, regulatory enforcement	Legal loopholes, lack of tech-based oversight, conventional mechanisms
Crypto assets as collateral	Theft/hacking, delisting, loss of collateral	Litigation, non-litigation (negotiation, mediation), fiduciary guarantees	Technical execution, due diligence, asset value fluctuation
Digital investment, cryptocurrency	Fraud, data theft	Courts, regulatory enforcement, compensation, administrative	Lack of comprehensive law, cybercrime risk, regulatory capacity
Non-fungible tokens (NFTs)	Ownership, authenticity, copyright	Courts, arbitration, mediation, conciliation	Legal vacuum, weak cyberspace protection
Non-fungible tokens (NFTs), smart contracts	Smart contract failures, cross-border crime	Courts (evidence), Civil Code, Electronic Information and Transactions Law	No regulation, technical complexity, cross-border
Crypto assets	Institutional overlap, regulatory compliance	Regulatory enforcement, administrative, OJK/BAPPEBTI	Fragmented framework, limited tech oversight

There are a lot of problems with exchange failures and custody breakdowns, fraud and marketplace misconduct, questions of ownership and authenticity (particularly for NFTs), smart-contract failures, hacking/theft, and money laundering. The remedies used are different and often not planned ahead of time. They include civil lawsuits (for

investor loss claims), arbitration/mediation, regulatory oversight and administrative actions, and criminal investigations when fraud or cybercrime is suspected. However, the table makes it clear that these ways of fixing things often run into systemic problems, like a lack of tailored regulations and clear legal categories, limits on evidence and blockchain tracing, a lack of insurance or formal recovery mechanisms, fragmentation among supervisors, and cross-border enforcement issues. As a result, many disputes either move slowly or get lost in enforcement gaps.

B. Evidentiary and Technical Gaps

The conceptual framework identified custody, provenance, attribution, and evidentiary integrity as core enforcement concepts. The cases expose a persistent gap between this ideal and operational reality. Prosecutors and courts face difficulties proving constructive control, linking pseudonymous addresses to natural persons, and preserving volatile evidence before assets move across chains. The Indodax breach illustrates how rapid on-chain transfers render seizure orders moot unless preservation is immediate and coordinated.

Internationally, the *Sterlingov* ruling (D.D.C. 2024) established that Chainalysis Reactor's clustering methodology satisfies all four Daubert factors for admissibility—but no comparable evidentiary standard exists in Indonesian law. Fröwis et al. (2020) document the risks that CoinJoin and other obfuscation techniques pose to forensic reliability. Indonesian enforcement actors require both validated toolchains and express statutory guidance on the admissibility of blockchain-derived evidence.

C. Institutional Coordination Failures

Polycentric governance theory expects nested authorities to coordinate through shared protocols. Indonesian practice remains uneven. Cyber Crime Directorate, the Prosecutor's Office, PPATK, OJK, and Bank Indonesia have complementary roles but often act through ad hoc channels, producing duplication and delay. The JYPRX investigation—dependent on prolonged banking traces and international leads—exemplifies how sequential rather than parallel inter-agency action slows both criminal proceedings and asset preservation. The FATF's 2023 mutual evaluation acknowledged Indonesia's risk awareness but identified operational frictions in time-sensitive cooperation (FATF, 2023).

D. Cross-Border Operational Limits

The case material confirms that perpetrators and custody chains routinely traverse national borders. One JYPRX suspect is sought via Interpol and MLA channels. Formal mutual legal assistance is too slow for digital assets that can be moved and mixed within hours. Indonesia lacks standardised, fast crypto-specific MLAT templates and provisional freeze mechanisms tailored to virtual assets. The FSB's 2025 thematic review and IOSCO's 2025 implementation review both confirm this as a global problem, not unique to Indonesia, but one that disproportionately affects jurisdictions with less developed cross-border enforcement infrastructure.

E. Remedial Inadequacy

A central normative yardstick is whether remedies deliver timely redress. The cases show a persistent shortfall. Courts have convicted perpetrators but victim restitution has been marginal because current instruments do not translate forensic success into prompt asset return. Administrative powers enable suspension or fines, yet regulators lack express authority to compel reimbursement or mandate insurance. Comparative evidence from the FTX bankruptcy—where the estate recovered approximately US$7 billion and customers with claims under US$50,000 received roughly 118 per cent of petition-date values—demonstrates that well-designed insolvency frameworks can achieve substantial recovery even in complex crypto failures (Lipson & Skeel, 2025). Indonesia's insolvency framework does not yet accommodate digital property.

F. Political Economy and Regulatory Incentives

Exchanges and financial firms resist costly custody or capital rules. Regulators balance market growth with consumer protection, leading to incremental rather than transformative reform. Limited forensic and prosecutorial resources concentrate attention on high-profile fraud rather than systemic improvements. POJK No. 27/2024 shifts institutional incentives by giving OJK a stronger supervisory role, but the new rules will only improve enforcement with investments in capacity, clearer remedial powers, and transparent safeguards against conflicts of interest.

VI. Pathways for Digital Assets Governance Reform

Following Luhmann, law must derive complexity into legally intelligible categories and procedures while remaining open to technological change. Indonesia's current framework has not yet performed that function. The findings reveal that digital asset actors do not always know which regime applies, which institution has competence, or which remedy can realistically secure recovery.

This systemic deficit also has a social and institutional dimension. Durkheim's theory explains that law preserves social solidarity by coordinating differentiated roles; Parsons understands law as an integrative mechanism enabling adaptation without losing normative order. The findings show that Indonesia's digital asset disputes reflect dysfunction across an interconnected field—OJK, Bank Indonesia, PPATK, police cyber units, prosecutors, courts, insolvency mechanisms, and private platforms. When these institutions lack procedural integration, common evidentiary standards, or timely coordination, law cannot perform its restitutive and integrative functions.

Accordingly, the reform pathway rests on three interdependent pillars. First, a *functionally oriented legal classification and consolidated legal base* answers the Luhmannian need for legal coherence. Second, a *remedial architecture* composed of administrative redress, insolvency adaptation, and civil recovery tools restores the Durkheimian

restitutive function of law. Third, an *operational governance framework* based on lead-agency coordination, accredited forensic capacity, and expedited international cooperation answers the Parsonian requirement that differentiated institutions be integrated into an adaptive and stable legal order.

A. Asset Classification and Consolidated Legal Base

A consolidated digital-asset statute (or integrated amendments to POJK, BI, AML, and capital-markets law) should adopt a functional taxonomy—payment tokens, investment/security-like tokens, utility tokens, stablecoins, and protocol-native instruments—so that prudential, consumer-protection, and AML/CFT obligations follow economic function. Drawing on the EU's MiCA framework and the UNIDROIT Principles on Digital Assets and Private Law (2023), the consolidated statute should operationalise the taxonomy through: (i) a public registry and dynamic "permitted-list" mechanism; (ii) modular licensing categories with harmonised minimum capital and governance requirements; and (iii) mandated custody standards distinguishing hot-wallet operational balances from cold-storage segregation.

Transparency tools should function as regulatory instruments. "Proof-of-reserves" disclosures must be complemented by periodic attested financial statements, independent attestations of off-chain liabilities, and continuous monitoring APIs. The statute should resolve cross-cutting questions about property, custody, and insolvency ex ante—including whether token holdings on an exchange are proprietary client property or contractual claims, and the priority ranking among creditors in a digital-asset insolvency. Emergency powers—to appoint technical custodians, to issue swift preservation notices, and to require immediate cold-wallet freezes subject to judicial oversight—should be embedded.

Institutionally, the statute should mandate inter-agency protocols: statutory obligations for information-sharing between the prudential supervisor, central bank, PPATK, and criminal authorities; standardised SAR formats for VASPs; and fast-track MLAT templates.

B. Administrative Redress

Administrative redress should be redesigned for speed and direct victim remediation. The reform should: (a) empower regulators to require interim custodial arrangements and order escrowed disbursement where fiduciary breaches are credibly alleged; (b) create a regulator-managed emergency remediation fund financed by industry levies or mandatory insurance; and (c) establish expedited administrative adjudication with defined evidentiary rules for digital artefacts.

C. Insolvency Reform

Insolvency law must be adapted to on-chain assets. The reforms should establish: (i) rebuttable presumptions that tokens in designated client accounts are proprietary client property, and that custodian-controlled wallets give rise to constructive-trust presumptions over on-chain balances; (ii) expedited preservation orders authorising

wallet freezes, withdrawal suspensions, and reconciliation requirements; (iii) statutory roles for technical custodians empowered to operate on-chain; (iv) creditors' committees including certified blockchain forensic advisors; (v) calibrated avoidance and clawback rules with safe harbours for bona fide transfers; (vi) standardised token valuation methodologies; and (vii) cross-border recognition provisions including model clauses for foreign insolvency orders and foreign technical custodian appointments.

The comparative experience of FTX's Chapter 11 proceedings—where the bankruptcy court effectively functioned as a crypto market regulator (Yadav & Stark, 2024)—demonstrates both the necessity and the feasibility of insolvency frameworks adapted to digital assets. Japan's decade-long Mt. Gox civil rehabilitation process, by contrast, illustrates the costs of inadequate statutory tools (Steele & Morishita, 2020).

D. Institutional Design and Coordination

A lead-agency model should be formalised through the appointment of a national coordinator for digital asset enforcement, establishing explicit operational protocols linking police cyber units, prosecutors, PPATK, OJK, Bank Indonesia, and specialist judicial chambers. The coordinator should maintain SOPs for preservation notices, a secure evidence-sharing platform, and quick-reference templates for international cooperation. Multi-disciplinary rapid-response teams should be created, trained in chain-of-custody for blockchain artefacts and empowered to issue administrative preservation requests.

E. Evidentiary Standards

Legislatures or courts should adopt statutory guidance clarifying: (a) the legal effect of cryptographic hashes and blockchain timestamps as prima facie provenance markers; (b) required elements of admissible chain-of-custody affidavits for on-chain and off-chain records; and (c) standards for expert testimony about attribution, including disclosure of tool versioning and validation evidence.

An accreditation regime for forensic providers and tools should cover personnel certification, laboratory security, and toolchain validation. Licensed VASPs should be required to expose standardised preservation and evidence interfaces: machine-readable SAR templates, API endpoints for emergency preservation requests, and encrypted export formats. Standardised chain-of-custody artefacts should include cryptographic snapshots, metadata describing extraction parameters, transaction graphs in common interchange format, and human-readable narratives linking technical output to legal theory.

F. Cross-Border Cooperation

Cross-border cooperation should employ a two-track approach: (1) fast-track operational agreements (MOUs or regulatory cooperation agreements) for emergency preservation and evidence sharing; and (2) binding mutual-assistance instruments

(crypto-specific MLAT templates, provisional-freeze recognition clauses, and enforceable recognition of foreign technical custodian appointments).

Governments should agree on a minimal evidence package accompanying emergency preservation requests and adopt a common preservation order template. National registries of regulated VASPs with 24/7 points of contact, coupled with API-based emergency-preservation endpoints, should permit authenticated preservation requests that platforms can implement immediately. Model statutory language permitting provisional recognition of foreign technical custodians should reduce the time to preserve on-chain assets.

VII. Conclusion

This study has demonstrated that Indonesia's digital-asset enforcement challenges constitute a single systemic problem: a persistent misalignment between rapidly evolving ledger-based technologies and the legal-institutional framework. The consequence is that timely restitution and effective deterrence remain elusive, victims incur unrecovered losses, and market confidence is weakened.

Three main findings emerge. First, legal fragmentation and classification ambiguity—compounded by the incomplete transition from BAPPEBTI to OJK—permit actors to exploit regulatory boundaries and deprive victims of clear enforcement pathways. Second, institutional coordination failures, evidentiary deficits, and slow cross-border processes transform otherwise recoverable incidents into permanent losses. Third, current remedial mechanisms do not lead to the successful investigation and prosecution of meaningful victim restitution. The sequenced reform agenda proposed, from comprising a consolidated statute with functional classification, empowered administrative redress, adapted insolvency rules, accredited forensic standards, and expedited international cooperation, addresses these interconnected failures as components of a coherent governance design rather than isolated regulatory fixes. If Indonesia combines clear legal foundations with appropriate procedural powers, credible technical capacity, and pre-negotiated international cooperation mechanisms, enforcement can become a visible public good—protecting consumers, restoring market trust, and supporting legitimate technological development.

References:

Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2022). Blockchain Networks as Constitutional and Competitive Polycentric Orders. *Journal of Institutional Economics*, *18*(5), 707–723. https://doi.org/10.1017/S174413742100093X

Backer, L. C. (2016). Governance polycentrism or regulated self-regulation. In K. Blome et al. (Eds.), *Contested Regime Collisions* (1st ed., pp. 198–225). Cambridge University Press. https://doi.org/10.1017/CBO9781316411230.009

Bahtera, H. R. A., Setiono, J., & Fadri, I. (2025). Legal Protection for Crypto Asset Investors in Indonesia Within an Incomprehensive Regulatory Framework. *Jurnal Greenation Sosial Dan Politik*, *3*(3), 521–529. https://doi.org/10.38035/jgsp.v3i3.433

Berutu, J. R., Yuhelson, Y., & Prasetyo, D. A. (2025). Regulatory Shifts and Legal Certainty in Cryptocurrency Trading. *Asian Journal of Social and Humanities*, *3*(9), 1687–1693. https://doi.org/10.59888/ajosh.v3i9.578

Brown, I. & Marsden, C. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*. MIT Press.

Dwitanti, A. I., & Puji Simatupang, D. (2022). Tax Imposition and Legal Enforcement on the Digital Asset of NFT. *Unram Law Review*, *6*(2). https://doi.org/10.29303/ulrev.v6i2.250

Erwanto, E., & Santoso, A. P. A. (2024). Study of Crypto Currency in Indonesia. *JISIP*, *8*(3), 1527. https://doi.org/10.58258/jisip.v8i3.6870

European Union. (2023). Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). *Official Journal of the European Union*, L 150, 40–205.

Fahira, S. H., Daimah, D., & Mu'amar, I. (2024). Cryptocurrency Regulation in Indonesia. *Indonesian Cyber Law Review*, *1*(1), 1–12. https://doi.org/10.59261/iclr.v1i1.3

Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs.

Financial Action Task Force (FATF). (2023). Indonesia: Mutual Evaluation Report. Paris: FATF.

Financial Action Task Force (FATF). (2024). Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (5th Update).

Financial Action Task Force (FATF). (2025). Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (6th Update).

Financial Stability Board (FSB). (2023). Global Regulatory Framework for Crypto-asset Activities. Basel: FSB.

Financial Stability Board (FSB). (2025). Thematic Review on FSB Global Regulatory Framework for Crypto-asset Activities. Basel: FSB.

Fröwis, M., Gottschalk, T., Haslhofer, B., Rückert, C., & Pesch, P. (2020). Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations. *Forensic Science International: Digital Investigation*, *33*, 200902. https://doi.org/10.1016/j.fsidi.2019.200902

Gunningham, N., & Holley, C. (2016). Next-Generation Environmental Regulation. *Annual Review of Law and Social Science*, *12*(1), 273–293. https://doi.org/10.1146/annurev-lawsocsci-110615-084651

IOSCO. (2023). Policy Recommendations for Crypto and Digital Asset Markets: Final Report. Madrid: IOSCO.

Iris Ng, Y. K. (2025). The Legal Recognition and Regulation of Digital Assets. *Highlights in Business, Economics and Management*, *52*, 52–61. https://doi.org/10.54097/ybywwm42

Izmi, N., & Siagian, A. W. (2024). Technological Innovation of the Crypto-Asset Financial Sector in Indonesia after Law Number 4 of 2023. *The International Journal of Financial Systems*, *2*(1), 1–28. https://doi.org/10.61459/ijfs.v2i1.34

Kartono, K., Susanti, N. S., Soewita, S., Salim, A., & Imron, A. (2024). Legal Ambiguity in Handling Cryptocurrency Evidence. *Interdiciplinary Journal and Hummanity (INJURITY)*, *3*(11), 768–776. https://doi.org/10.58631/injurity.v3i11.1307

Kochergin, D. (2022). Crypto-assets: Economic Nature, Classification and Regulation. *International Organisations Research Journal*, *17*(3), 75–130. https://doi.org/10.17323/1996-7845-2022-03-04

Kokorin, I. (2023). The Anatomy of Crypto Failures and Investor Protection under MiCAR. *Capital Markets Law Journal*, *18*(4), 500–525. https://doi.org/10.1093/cmlj/kmad019

Law Commission of England and Wales. (2023). *Digital Assets: Final Report* (Law Com No. 412). London: Law Commission.

Lipson, J. C., & Skeel, D. A. (2025). FTX'd: Conflicting Public and Private Interests in Chapter 11. *Stanford Law Review*, *77*, 369.

López-Aguilar, P., & Solanas, A. (2022). Cross-Border Exchange of Digital Evidence Using Blockchain. In *Applications in Electronics Pervading Industry, Environment and Society* (Vol. 866, pp. 132–138). Springer. https://doi.org/10.1007/978-3-030-95498-7_19

Luhmann, N. (2004). *Law as a Social System*. Oxford University Press. https://doi.org/10.1093/oso/9780198262381.001.0001

Mulyadi, D. (2025). Legal Analysis of Trading in the Digital Age. *Ipso Jure*, *2*(7), 77–88. https://doi.org/10.62872/mwftad66

Nelson, F. M., Prosperiani, M. D., Ramadhan, C. R., & Andini, P. P. (2024). Cracking the Code: Investigating the Hunt for Crypto Assets in Money Laundering Cases in Indonesia. *Journal of Indonesian Legal Studies*, *9*(1), 89–130. https://doi.org/10.15294/jils.vol9i1.4534

Ngozi Samuel Uzougbo, Ikegwu, C. G., & Adewusi, A. O. (2024). International Enforcement of Cryptocurrency Laws. *Magna Scientia Advanced Research and Reviews*, *11*(1), 068–083. https://doi.org/10.30574/msarr.2024.11.1.0075

Noor, A., Arifin, Moh., & Astuti, D. P. W. (2023). Crypto Assets and Regulation: Taxonomy and Framework. *JED*, *8*(3), 303–315. https://doi.org/10.26618/jed.v8i3.10886

Ostrom, E. (2010). Beyond Markets and States: Polycentric Governance of Complex Economic Systems. *American Economic Review*, *100*(3), 641–672. https://doi.org/10.1257/aer.100.3.641

Paterson, J. (2024). Decentralised Finance, Regulation, and Systems Theory. *Oñati Socio-Legal Series*, *14*(5), 1296–1314. https://doi.org/10.35295/osls.iisl.1916

Perlman, L. (2019). A Model Crypto-Asset Regulatory Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3370679

Prawira, M. Y., & Alamsyah, F. (2023). The Implementation of Mutual Legal Assistance between Indonesia and Switzerland. *Indonesian Comparative Law Review*, *5*(2), 58–74. https://doi.org/10.18196/iclr.v5i2.17435

Remolina, N., Gurrea-Martínez, A., & Liu, D. (forthcoming). The Treatment of Digital Assets in Insolvency. In *Oxford Handbook of Digital Assets and the Law*. Oxford University Press. SSRN: https://ssrn.com/abstract=4915592

Rodríguez De Las Heras Ballell, T. (2024). The Emergence of Principles and Best Practices on Digital Assets. *European Journal of Risk Regulation*, 1–12. https://doi.org/10.1017/err.2024.55

Rusman, R., & Fakrulloh, Z. A. (2024). Reform of Law Enforcement to Strengthen the Legal System in Eradicating Money Laundering Through Cryptocurrency. *Journal of Social Research*, *4*(1), 1–15. https://doi.org/10.55324/josr.v4i1.2332

Scorpan, A. (2021). Reflections on Legal Deficiencies Affecting Mutual Legal Assistance in Criminal Asset Recovery. *Administrarea Publica*, *3*(111), 136–142. https://doi.org/10.52327/1813-8489.2021.3(111).15

Soerjadi, D. F., & Kusmiadi, R. (2024). Transition of Crypto Asset Supervision from Bappebti to OJK. *Action Research Literate*, *8*(11), 3322–3327. https://doi.org/10.46799/arl.v8i11.2531

Steele, S., & Morishita, T. (2020). Lessons from Mt Gox: Practical Considerations for a Virtual Currency Insolvency. In D. W. Arner et al. (Eds.), *Research Handbook on Asian Financial Law* (p. 479). Edward Elgar.

UNIDROIT. (2023). *Principles on Digital Assets and Private Law*. Rome: UNIDROIT.

Werbach, K. D. (2016). Trustless Trust. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2844409

Wibowo, A. (2023). Barriers and Solutions to Cross-Border Asset Recovery. *Journal of Money Laundering Control*, *26*(4), 739–750. https://doi.org/10.1108/JMLC-01-2022-0022

Yadav, Y., & Stark, R. J. (2024). The Bankruptcy Court as Crypto Market Regulator. *Southern California Law Review*, *96*(6).