JOURNAL
AXIOMA LEX PRIMA

OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

Civil Liability of Crypto-Asset Custodians for Consumer Asset Losses after OJK Supervisory Transfer

Yasin Ali
Fakultas Hukum, Universitas Bhayangkara Jakarta Raya, Indonesia
Correspondence: aliyasinlaw@gmail.com

Keywords:
crypto-asset custody; consumer asset loss; civil liability; OJK; asset segregation; operational resilience

ABSTRACT
This study examined the civil liability of crypto-asset custodians for consumer asset losses after supervision was transferred to the Financial Services Authority. Normative legal research used statutory, conceptual, and comparative approaches. The study found that OJK Regulation Number 27 of 2024, as amended by Regulation Number 23 of 2025, imposes direct responsibility for assets lost in custody, while Law Number 4 of 2026 classifies centralized custodians as Crypto-Asset Financial Services Institutions. Attribution within multi-entity custody chains, evidentiary asymmetry, valuation, insolvency segregation, and mass compensation nevertheless remain insufficiently regulated. The proposed control-based and layered recovery model applies a rebuttable presumption against the entity controlling private keys, joint and several liability when operators cannot locate the loss, in-kind restitution, mandatory insurance, an industry compensation fund, real-time reconciliation, and bankruptcy-remote treatment of identifiable consumer assets.

Keywords:
crypto-asset custody; consumer asset loss; civil liability; OJK; asset segregation; operational resilience

ABSTRACT
This study examined the civil liability of crypto-asset custodians for consumer asset losses after supervision was transferred to the Financial Services Authority. Normative legal research used statutory, conceptual, and comparative approaches. The study found that OJK Regulation Number 27 of 2024, as amended by Regulation Number 23 of 2025, imposes direct responsibility for assets lost in custody, while Law Number 4 of 2026 classifies centralized custodians as Crypto-Asset Financial Services Institutions. Attribution within multi-entity custody chains, evidentiary asymmetry, valuation, insolvency segregation, and mass compensation nevertheless remain insufficiently regulated. The proposed control-based and layered recovery model applies a rebuttable presumption against the entity controlling private keys, joint and several liability when operators cannot locate the loss, in-kind restitution, mandatory insurance, an industry compensation fund, real-time reconciliation, and bankruptcy-remote treatment of identifiable consumer assets.

JOURNAL
AXIOMA LEX PRIMA
OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

A. Introduction

Crypto-asset trading in Indonesia has developed into a financial-services activity involving a substantial consumer base. In May 2026, the Financial Services Authority recorded 22.40 million consumer accounts and monthly crypto-asset transactions of IDR 23.01 trillion.[1] Throughout 2025, the value of crypto-asset transactions reached IDR 482.23 trillion.[2] This scale of participation expands opportunities in the digital economy while increasing consumer exposure to losses arising from cyberattacks, failures in private-key management, erroneous transfers, internal misuse, asset commingling, and operator insolvency. Custody losses possess distinctive characteristics because crypto assets are not held as physical objects. Economic control depends on private keys, wallet infrastructure, balance records, and the operator's ability to demonstrate the connection between internal ledgers and assets recorded on a blockchain network.

An institutional change occurred when the regulation and supervision of digital financial assets, including crypto assets, were fully transferred from the Commodity Futures Trading Regulatory Agency to OJK on January 10, 2025.[3] The transfer implemented the mandate of the Financial Sector Development and Strengthening Law and Government Regulation Number 49 of 2024.[4] OJK subsequently applied OJK Regulation Number 27 of 2024, as amended by OJK Regulation Number 23 of 2025, as the operating framework for digital financial asset trading.[5] The new regime shifts the legal orientation from commodity supervision to financial-sector supervision, integrating governance, cyber resilience, business conduct, and consumer protection.

---

[1] Otoritas Jasa Keuangan, "Resiliensi dan Kinerja Intermediasi Sektor Jasa Keuangan Terjaga, Mendukung Pertumbuhan Ekonomi Nasional," June 2026 Board of Commissioners Meeting press release, July 7, 2026, reporting 22.40 million consumer accounts and crypto-asset transactions of IDR 23.01 trillion in May 2026.

[2] Otoritas Jasa Keuangan, "Pembukaan Bulan Literasi Kripto 2026," press release, April 7, 2026, reporting crypto-asset transactions of IDR 482.23 trillion during 2025.

[3] Otoritas Jasa Keuangan, Badan Pengawas Perdagangan Berjangka Komoditi, and Bank Indonesia, "Bappebti Kemendag Alihkan Tugas Pengaturan dan Pengawasan Aset Keuangan Digital termasuk Aset Kripto serta Derivatif Keuangan kepada OJK dan BI," joint press release, January 10, 2025.

[4] Indonesia, Government Regulation Number 49 of 2024 on the Transfer of Regulatory and Supervisory Duties over Digital Financial Assets, Including Crypto Assets and Financial Derivatives.

[5] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024 on the Operation of Digital Financial Asset Trading, Including Crypto Assets, as amended by OJK Regulation Number 23 of 2025.

The transfer received a clearer statutory basis through Law Number 4 of 2026. Article 221A classifies a centralized crypto-asset custody operator as a Crypto-Asset Financial Services Institution and requires it to obtain an OJK business licence.[6] This status matters because a custodian can no longer be understood merely as a storage-technology provider. It is a financial-services business entrusted with control over facilities holding consumer assets, verification of transfers, maintenance of records, and assurance that assets remain available when consumers request withdrawal. This position generates a standard of prudence higher than that applicable to an ordinary technology provider.

International scholarship indicates that custody risk cannot be resolved through contractual consent alone. An empirical study of 110 custody providers in 48 jurisdictions identified significant differences in asset-segregation clauses, insolvency protection, limitations of liability, third-party use, and forum selection.[7] Other scholarship distinguishes institutional resilience from asset resilience. A custodian may satisfy organisational requirements while consumers remain unprotected when asset rights, estate segregation, and return mechanisms upon business failure are not clearly defined.[8] Empirical evidence concerning centralised European exchanges also reveals a tendency to use terms and conditions to transfer security risks and restrict liability toward users.[9]

Crypto-company failures demonstrate the consequences of uncertainty between consumer rights and intermediary control. Levitin explains that consumers frequently bear unpriced credit risk because assets delivered to a platform may enter the debtor's estate when the contract does not create effective proprietary segregation.[10] Kokorin links crypto-company failures to deficient governance, use

---

[6] Indonesia, Law Number 4 of 2026 amending Law Number 4 of 2023 on Financial Sector Development and Strengthening, State Gazette of the Republic of Indonesia 2026 Number 62, Supplement to the State Gazette Number 7180, art. 221A.

[7] Dirk A. Zetzsche and Areti Nikolakopoulou, "Crypto Custody: An Empirical Assessment," *Journal of Financial Regulation* 11, no. 1 (2025): 73–97, https://doi.org/10.1093/jfr/fjaf004.

[8] Dirk A. Zetzsche, Julia Sinnig, and Areti Nikolakopoulou, "Crypto Custody," *Capital Markets Law Journal* 19, no. 3 (2024): 207–229, https://doi.org/10.1093/cmlj/kmae010.

[9] Marilyne Ordekian, Ingolf Becker, Tyler Moore, and Marie Vasek, "Raising the Bar: Assessing Historical Cryptocurrency Exchange Practices in Light of the EU's MiCA and DORA Regulation," *Computer Law & Security Review* 59 (2025): 106227, https://doi.org/10.1016/j.clsr.2025.106227.

[10] Adam J. Levitin, "Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency," *Texas Law Review* 101, no. 4 (2023): 877–954.

OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

of consumer assets, related-party transactions, and weak insolvency protection.[11] These findings confirm that an asset loss does not always take the form of an on-chain theft. It may consist of a balance shortfall, suspended withdrawal, loss of access, unauthorised transfer, or inclusion of consumer assets in bankruptcy proceedings.

Indonesian studies preceding the supervisory transfer generally assessed consumer protection through the Consumer Protection Law and Bappebti regulations.[12] Studies addressing the transfer to OJK have focused primarily on institutional authority, legal certainty for industry actors, and regulatory harmonisation.[13] Other scholarship stresses the urgency of integrated digital-asset regulation but does not formulate standards for attributing loss to a custodian or a recovery design for missing assets.[14] Recent insolvency literature identifies the uncertain status and enforcement difficulties of crypto assets, yet it does not connect asset segregation with the specific liability of Crypto-Asset Financial Services Institutions after Law Number 4 of 2026.[15]

The research gap concerns the absence of an integrated construction combining four normative layers: the custodian-specific duties under OJK regulations, the liability of Crypto-Asset Financial Services Institutions under Law Number 4 of 2026, financial-sector consumer protection, and general civil-liability rules. The problem is material because consumers normally interact with a trader through an application while most assets are held by a separate custodian. When a loss occurs, consumers may be unable to prove which entity controlled the wallet, when the failure arose, and whether the system failure caused the reduction in assets.

---

[11] Ilya Kokorin, "The Anatomy of Crypto Failures and Investor Protection under MiCAR," *Capital Markets Law Journal* 18, no. 4 (2023): 500–525, https://doi.org/10.1093/cmlj/kmad019.

[12] Wardah Yuspin and Arief Wicaksono, "Telaah Yuridis Perlindungan Konsumen dalam Kegiatan Investasi Aset Kripto di Indonesia," *DiH: Jurnal Ilmu Hukum* 19, no. 1 (2023): 85–98, https://doi.org/10.30996/dih.v19i1.7886.

[13] Beni Darmawan Hidayat and Muhamad Hasan Sebyar, "Implikasi Hukum Perpindahan Pengawasan Aset Kripto dari Bappebti ke OJK terhadap Pelaku Industri dan Investor," *Hakim: Jurnal Ilmu Hukum dan Sosial* 2, no. 4 (2024): 888–899, https://doi.org/10.51903/hakim.v2i4.2206.

[14] Francisca Romana Nanik Alfiani, "The Urgency of Comprehensive and Integrated Digital Asset Regulation," *Journal of Social Science* 5, no. 1 (2024): 90–102, https://doi.org/10.46799/jss.v5i1.764.

[15] S. Hullu and M. Huda, "Analisis Yuridis terhadap Penanganan Aset Digital (Crypto) dalam Kepailitan Perusahaan di Indonesia," *Jurnal Ilmu Hukum, Humaniora dan Politik* 6, no. 4 (2026): 3092–3104, https://doi.org/10.38035/jihhp.v6i4.8458.

This article addresses two questions. First, how should the civil liability of a crypto-asset custodian for consumer asset losses be constructed after supervision was transferred to OJK? Second, what liability model can secure consumer recovery when the loss arises within a chain of control involving a trader, custodian, clearing institution, and technology provider? The novelty lies in a control-based liability and layered recovery model. It treats control over private keys and infrastructure as the basis for a rebuttable presumption of liability, imposes joint and several liability when operators cannot establish attribution, prioritises restitution in the same type and quantity of asset, and combines insurance, an industry compensation fund, and bankruptcy-remote segregation.

B. Research Method

This study used normative legal research with a prescriptive orientation. The statutory approach examined the Financial Sector Development and Strengthening Law as amended by Law Number 4 of 2026, OJK Regulation Number 27 of 2024 as amended by OJK Regulation Number 23 of 2025, OJK Regulation Number 22 of 2023, the Consumer Protection Law, the Indonesian Civil Code, and the Bankruptcy Law. The conceptual approach distinguished regulatory responsibility, contractual liability, tort liability, liability for other persons, and asset segregation. The comparative approach considered Regulation (EU) 2023/1114 on Markets in Crypto-Assets and Regulation (EU) 2022/2554 on digital operational resilience.

Primary legal materials consisted of legislation and official OJK documents. Secondary legal materials comprised national and international journal articles on crypto custody, consumer protection, crypto-company failures, operational resilience, and insolvency. The materials were collected through document study. The analysis systematically identified the entity controlling the asset, the breached duty, the form of fault, causal connection, allocation of the evidentiary burden, type of loss, and recovery mechanism. The findings were then compared with international standards to formulate a liability model suited to Indonesia's crypto-asset trading structure.

JOURNAL
AXIOMA LEX PRIMA
OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

C. Discussion

1. Construction of Custodian Liability after the Transfer of Supervision to OJK

a. Repositioning the Custodian as a Crypto-Asset Financial Services Institution

The term custodian in this article refers to a centralised crypto-asset custody operator under Article 221A(1)(d) of Law Number 4 of 2026. OJK regulations use the term Custody Facility Operator. The terminological difference does not alter its principal functions of holding, maintaining, recording, monitoring, and delivering digital financial assets placed by a trader. This arrangement differs from self-custody because consumers do not directly control the private keys. The custodian controls the infrastructure determining whether assets can be transferred, frozen, recovered, or withdrawn.

Following amendment, Article 40 of OJK Regulation Number 27 of 2024 requires a custodian to own, possess, and control custody facilities with layered security, update security systems, verify incoming and outgoing assets, maintain separate records for each trader, issue custody receipts, preserve assets, and implement risk mitigation.[16] The phrase own, possess, and control strengthens the link between technical authority and legal liability. A custodian should not escape liability by asserting reliance on a vendor when the design, selection, and supervision of that vendor remain under its control.

OJK Regulation Number 23 of 2025 also requires a custodian to maintain equity equal to at least 80 per cent of paid-up capital.[17] This requirement strengthens institutional loss-bearing capacity but does not constitute a readily available fund for replacing consumer assets. Equity may be tied to operational assets and may decline after a major incident. Prudential capital requirements must be distinguished from compensation mechanisms so that consumers do not treat licensing and minimum capital as a full guarantee of all assets.

[16] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024 as amended by OJK Regulation Number 23 of 2025, art. 40(1)(a)–(m), (5), (6), and (9).
[17] Otoritas Jasa Keuangan, OJK Regulation Number 23 of 2025, art. I(45), inserting art. 39A into OJK Regulation Number 27 of 2024.

The technical-security standards in Article 41 cover offline and online storage, protection of key-management devices, multi-party authorisation, multi-factor authentication, and access restrictions.[18] These duties form a standard of care for assessing fault. Assessment cannot stop at the existence of written policies. The custodian must prove implementation, testing, updates, access logging, incident response, and recovery. A failure in any of these elements may indicate negligence when causally connected to the loss.

Indonesia's custody structure separates trading functions from asset control. Consumer balances are recorded by the trader, custodian, and clearing institution, and all three must exchange information in real time.[19] A trader may self-custody no more than 30 per cent of consumer assets, while the balance must be placed with a custodian.[20] This design reduces concentrated risk at the trader level but creates an evidentiary chain. Consumers view their balances through the trader's application, while on-chain assets may reside in a custodian wallet. Inconsistent records among the three institutions may generate disputes over where the loss occurred and which entity must pay first.

b. Specific and General Bases of Civil Liability

The most direct basis of liability appears in Article 40(1)(l) and Article 92(2) of OJK Regulation Number 27 of 2024. A custodian must assume responsibility for losses of consumer assets held in custody and maintain the security of assets under its control.[21] This is a specific rule because it connects liability to loss and to the custody relationship. The wording does not require the consumer to prove a particular form of fault at the outset. Its structure can be read as a limited obligation of result: assets recorded as belonging to consumers must remain available unless the custodian proves a legally valid ground of exoneration.

Law Number 4 of 2026 broadens that basis. Article 221A(11) provides that a Crypto-Asset Financial Services Institution is liable for consumer losses caused

[18] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024, art. 41, concerning custody standards, key security, layered authorisation, and access control.
[19] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024, art. 90(5)–(7).
[20] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024, art. 91(1)–(7).
[21] Otoritas Jasa Keuangan, OJK Regulation Number 27 of 2024, art. 92.

JOURNAL
AXIOMA LEX PRIMA
OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

by fault, negligence, conduct contrary to financial-sector rules, or breach of contract by controllers, shareholders, directors, commissioners, employees, equivalent officers, and third parties representing or acting for the institution.[22] The rule overcomes formal separation between the corporate entity and technical actors. A custodian cannot avoid liability merely because the incident was committed by an employee, data-centre provider, wallet developer, or security administrator working for its benefit.

Article 221A(12) adds personal liability for principal parties proven to have committed unlawful acts causing losses to the Crypto-Asset Financial Services Institution.[23] The rule primarily protects the institution from misconduct by its managers and controllers, yet it indirectly strengthens consumer recovery because the institution may seek recourse against those parties. OJK regulations also provide that controllers and beneficial owners share responsibility when violations or losses result from management fault. The two rules should be applied consistently so that personal liability does not replace the institution's primary obligation to consumers.

OJK Regulation Number 22 of 2023 reinforces protection by making a financial-services business liable for losses resulting from fault, negligence, violations of financial-sector law, or breach of contract by its organs, employees, and third parties acting for its benefit.[24] The business may be released if it proves the consumer's involvement or fault. This structure shifts the evidentiary burden. Consumers must still establish loss and a service relationship, while the institution controlling operational information must prove that the loss arose from consumer conduct or from a circumstance genuinely beyond its control.

General private-law grounds remain relevant. When the consumer is a party to the custody contract, failure to return assets may constitute breach of contract under Articles 1239 and 1243 of the Indonesian Civil Code, with damages covering costs, losses, and interest under Article 1246.[25] When the contract exists only between a trader and a custodian, the consumer may rely on statutory duties, tort,

---

[22] Indonesia, Law Number 4 of 2026, art. 221A(11).
[23] Indonesia, Law Number 4 of 2026, art. 221A(12).
[24] Otoritas Jasa Keuangan, OJK Regulation Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector, art. 10.
[25] Indonesian Civil Code, arts. 1239, 1243, and 1246.

JOURNAL
AXIOMA LEX PRIMA
OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

or a third-party-beneficiary stipulation if the contractual structure satisfies Article 1317.[26] Articles 1365, 1366, and 1367 provide bases for unlawful acts, negligence, and acts committed by persons under another party's responsibility.[27]

The existence of specific statutory duties means that standard-form clauses cannot remove minimum obligations. A clause assigning every cyberattack, key loss, or vendor failure to the consumer conflicts with the duties to protect and assume responsibility for assets held in custody. Article 18 of the Consumer Protection Law prohibits clauses transferring a business operator's liability and clauses subjecting consumers to unilateral rules.[28] Contractual freedom may govern claims procedures, operational limits, or risk allocation only to the extent that it does not reduce rights granted by legislation and OJK regulations.

Table 1. Matrix of Liability Rules and Recovery Gaps

Instrument	Core Rule	Recovery Gap Requiring Reform
Law No. 4 of 2026	Crypto-Asset Financial Services Institutions are liable for consumer losses caused by fault, negligence, regulatory violations, or breach of contract.	The law does not specify the measure of restitution, a direct claims procedure, or the allocation of the evidentiary burden.
OJK Regulation No. 27 of 2024 as amended by OJK Regulation No. 23 of 2025	Custodians must maintain security, separate records, and assume responsibility for losses of assets held in custody.	Loss, exculpation standards, and joint and several liability among operators remain undefined.
OJK Regulation No. 22 of 2023	Financial services businesses are liable for losses caused by their organs, employees, and third parties unless consumer fault is established.	No specific technical evidentiary standard exists for private keys, wallets, and blockchain reconciliation.
Indonesian Civil Code and Consumer Protection Law	They provide contractual liability, tort liability, vicarious liability, and a prohibition on exoneration clauses.	Contractual privity, price volatility, and omnibus-wallet structures complicate application.
Bankruptcy Law	It regulates the bankruptcy estate and creditors generally.	It does not expressly exclude segregated consumer crypto assets from a custodian's bankruptcy estate.

Source: Author's analysis of applicable legislation, 2026.

The matrix shows that liability rules exist at statutory and OJK-regulation levels, but the operation of recovery still depends on interpretation. The clearest gap concerns the relationship between security obligations and private-law consequences when assets cannot be returned. Regulatory reform must convert general duties into claims procedures that can be implemented and judicially tested.

[26] Indonesian Civil Code, art. 1317.
[27] Indonesian Civil Code, arts. 1365, 1366, and 1367.
[28] Indonesia, Law Number 8 of 1999 on Consumer Protection, art. 18.

c. Attribution of Loss, Fault, and the Evidentiary Burden

Loss should be interpreted by reference to economic function, rather than confined to the disappearance of tokens from a wallet address. Consumer assets are lost when the quantity that should be available cannot be returned, is transferred without authorisation, becomes inaccessible because a private key is destroyed, or cannot be withdrawn because of an asset shortfall. A narrow interpretation recognising only outbound blockchain transactions would disregard ledger failures, key destruction, unjustified internal freezes, and reconciliation failures.

The first element a consumer must prove is the recorded entitlement or balance. Evidence may include transaction history, the trader's balance report, clearing records, a custody receipt, and blockchain data. Once a discrepancy arises between ownership records and deliverable assets, the technical evidentiary burden should shift to the entity controlling the infrastructure. The custodian holds access logs, wallet policies, key-rotation records, authentication configurations, vendor relationships, and incident-response records. Requiring consumers to prove every technical element would create an informational inequality that ordinary civil procedure cannot cure.

A control-based presumption of liability is not absolute liability without defences. A custodian may rebut the presumption by proving that the loss resulted from intentional conduct or gross negligence by the consumer, that the asset never entered the custodian's system, or that an external event could not have been prevented despite compliance with every reasonable standard. Exonerating evidence must include technical compliance, audit results, a chronology, resilience tests, authentication logs, and recovery measures. A general statement that a hack occurred is insufficient because cyberattack risk is the principal reason for requiring layered security.

Force majeure cannot be applied automatically. It requires an event beyond the debtor's power that could not reasonably have been anticipated and cannot be attributed to the debtor. Exploitation of a known vulnerability, failure to install updates, key storage without divided authorisation, or uncontrolled employee access remains within the sphere of fault. DORA treats information-technology risk management, resilience testing, incident reporting, and third-party oversight as continuous duties of financial institutions.[29] That approach is relevant when deciding whether an incident genuinely exceeded the custodian's reasonable control.

Liability for third parties should follow the principle that outsourcing does not transfer duties to consumers. Law Number 4 of 2026 expressly includes third parties representing or acting for a Crypto-Asset Financial Services Institution. A custodian may seek contractual recourse against a vendor, but consumers should not have to pursue a vendor they did not select. This standard accords with IOSCO recommendations concerning client-asset management, disclosure of custody arrangements, and operational-risk controls for crypto service providers.[30]

d. The Liability Relationship between Traders and Custodians

A trader also bears responsibility for consumer assets under its own custody. Article 91 limits that portion to a maximum of 30 per cent, while the remainder must be held by a custodian. The percentage allocation is not always visible to consumers and may change with liquidity requirements. When a loss occurs, the trader may claim that the assets were held by the custodian while the custodian alleges that the trader's records are inaccurate. Such internal disputes should not delay consumer recovery.

The trader has the direct consumer relationship, manages the transaction interface, presents account balances, and transmits withdrawal instructions. The custodian controls most assets and processes transfers. Their functions are interdependent. When a consumer proves a balance and non-delivery, the trader and custodian should be jointly and severally liable if they cannot establish the precise location of the assets and the stage at which the loss occurred. Joint and several liability gives both institutions an incentive to maintain auditable reconciliation and prevents their coordination failure from being imposed on consumers.

---

[29] European Parliament and Council, Regulation (EU) 2022/2554 of December 14, 2022 on Digital Operational Resilience for the Financial Sector, OJ L 333, December 27, 2022.

[30] International Organization of Securities Commissions, *Policy Recommendations for Crypto and Digital Asset Markets*, Final Report FR11/23 (Madrid: IOSCO, November 2023), recommendations 12–16.

Joint and several liability does not eliminate final allocation. After compensating the consumer, the trader and custodian may seek contribution or recourse based on custody records, transfer logs, degree of fault, and operational agreements. This approach separates two issues often conflated: the consumer's right to prompt recovery and the final allocation of burdens among operators. The separation is consistent with financial-sector consumer protection, which prioritises fulfilment of consumer rights without foreclosing internal settlement mechanisms.

The dispute-resolution route begins with a complaint to the financial-services business. If no settlement is achieved, the consumer may use the Financial Services Sector Alternative Dispute Resolution Institution or file a claim before a court.[31] OJK may conduct market-conduct supervision, examinations, specific-action orders, and administrative sanctions. Administrative sanctions do not automatically compensate losses. A judgment or settlement should determine the quantity of assets, the time for return, consequences of delay, and responsibility for evidentiary costs.

2. A Liability Model to Secure Recovery of Consumer Asset Losses

a. Normative Gaps in Consumer Recovery

The Indonesian framework establishes custodian liability but does not resolve all private-law consequences. The first gap concerns the measure of recovery. Crypto assets fluctuate rapidly, so cash compensation based on value at the date of loss may disadvantage consumers when prices rise before payment. Conversely, valuation at the date of judgment may overcompensate when prices fall or when part of the asset has already been returned. Current regulation does not determine the valuation date, price source, treatment of forks, airdrops, staking rewards, or transaction fees.

The second gap concerns asset segregation in bankruptcy. OJK regulations require consumer assets to be separated from custodian assets in accounting and records. Accounting segregation is important but does not necessarily establish exclusion from the bankruptcy estate. An omnibus wallet may contain assets

[31] Otoritas Jasa Keuangan, OJK Regulation Number 22 of 2023, provisions on complaint services and dispute resolution through the Financial Services Sector Alternative Dispute Resolution Institution.

belonging to many consumers, and proprietary status depends on reconciliation with internal records. Insolvency scholarship demonstrates that consumer outcomes depend on the classification of the legal relationship, the form of control, and recognition of proprietary rights in crypto assets.[32] Indonesia's Bankruptcy Law does not specifically exclude consumer crypto assets from a custodian's bankruptcy estate.[33]

The third gap concerns the source of payment when a large-scale loss exceeds the custodian's capital. OJK regulations require risk mitigation and permit cooperation with insurers, but they do not prescribe minimum coverage, mandatory insured risks, payment priorities, or procedures when an insurer rejects a claim. Capital and equity cannot substitute for liquid compensation instruments. Without mandatory insurance or an industry fund, consumer rights may amount only to claims against an institution unable to pay.

The fourth gap concerns reserve transparency. Proof of on-chain assets is insufficient without proof of aggregate liabilities to consumers. A custodian may show a substantial wallet balance, while the public cannot determine whether the assets are encumbered, lent, or inadequate relative to recorded liabilities. Financial-statement audits may also detect transfers only after the reporting date. Reconciliation must combine proof of assets, proof of liabilities, key-control verification, and withdrawal testing.

The fifth gap concerns direct consumer access to the custodian. The principal contracts often exist between the trader and consumer and between the trader and custodian. When a custodian holds assets for consumers, the right to bring a direct claim should be explicit rather than dependent on third-party-beneficiary doctrine. Law Number 4 of 2026 recognises the liability of Crypto-Asset Financial Services Institutions toward consumers, but implementing rules should define the direct-claim procedure, minimum evidence, and settlement period.

[32] Dominik Skauradszun, "Crypto Custodians in Financial Distress," *International Insolvency Review* 33, no. 1 (2024): 71–95, https://doi.org/10.1002/iir.1521.
[33] Indonesia, Law Number 37 of 2004 on Bankruptcy and Suspension of Debt Payment Obligations.

b. Lessons from MiCA and Operational Resilience

MiCA requires custody service providers to conclude agreements with clients, maintain position registers, apply custody policies, segregate client assets, facilitate the exercise of rights, and return assets or means of access as soon as possible. Article 75 also imposes liability for the loss of assets or means of access resulting from an incident attributable to the provider, capped at the market value of the assets at the time of loss.[34] The attribution formula permits a defence but requires a clear connection between the incident and the custody function.

MiCA's strength lies in connecting organisational duties, recordkeeping, segregation, and liability. Its valuation cap at the time of loss is less satisfactory when the consumer is substantively entitled to receive the same number of tokens. Zetzsche, Sinnig, and Nikolakopoulou argue that MiCA is stronger on institutional resilience than asset protection when related parties fail or private-law issues arise.[35] Indonesia should therefore supplement prudential rules with rules on property rights, insolvency, and in-kind recovery.

DORA complements MiCA through information-technology risk governance, incident classification, resilience testing, third-party risk management, and business continuity. Ordekian and colleagues found that exchange practices before these standards took effect remained deficient in custody, cybersecurity, and liability clauses.[36] The experience shows that compliance cannot be assessed solely through written policies. OJK requires evidence-based supervision, loss-scenario testing, and evaluation of withdrawal-recovery capacity.

IOSCO recommendations likewise emphasise client-asset segregation, disclosure of custody arrangements, accurate reconciliation, risk management, and insolvency protection. International consensus is moving toward the application of financial-services principles to crypto intermediaries while recognising their technological characteristics.[37] Indonesia can adopt these standards functionally. It

---

[34] European Parliament and Council, Regulation (EU) 2023/1114 of May 31, 2023 on Markets in Crypto-Assets, art. 75, OJ L 150, June 9, 2023.
[35] Zetzsche, Sinnig, and Nikolakopoulou, "Crypto Custody," 207–229.
[36] Ordekian et al., "Raising the Bar," 106227.
[37] Douglas W. Arner, Dirk A. Zetzsche, Ross P. Buckley, and Jamieson M. Kirkwood, "The Financialisation of Crypto: Designing an International Regulatory Consensus," *Computer Law & Security Review* 53 (2024): 105970, https://doi.org/10.1016/j.clsr.2024.105970.

need not reproduce the entire European Union structure, but any entity controlling keys, wallets, and transfers should bear duties proportionate to that control.

c. Control-Based Liability and Layered Recovery Model

The proposed model begins from the principle that technical control must carry legal liability. At the first stage, consumers need only establish the account identity, recorded quantity of assets, and non-delivery or balance discrepancy. That evidence creates a presumption against the entity controlling private keys or wallet infrastructure. The trader, custodian, and clearing institution must disclose relevant records identifying the asset location, transfer time, and authorising party. Refusal or inability to produce records should support an adverse inference against the party controlling the evidence.

At the second stage, liability is allocated according to actual control. The custodian is liable for assets within its wallets or custody facilities, including losses caused by employees and vendors. The trader is liable for assets it retains, erroneous instructions, and balance representations. The clearing institution is liable when verification or reconciliation failure causes the loss. When inconsistent records prevent a precise allocation, all three institutions should be jointly and severally liable to the consumer and resolve contribution after payment.

At the third stage, recovery should restore the consumer's position. The custodian should deliver the same type and quantity of asset together with benefits directly attached during the loss period, provided those benefits can be calculated and legally belong to the consumer. Cash should be used when in-kind restitution is impossible or selected by the consumer. Valuation should apply the more protective value between the date of loss and the date of payment, accounting for partial recovery to prevent overcompensation. Transaction costs, tracing expenses, and proven direct losses may be added.

At the fourth stage, payment resources should operate in layers. The first layer consists of the custodian's assets and capital. The second consists of mandatory insurance covering external theft, internal misuse, key failure, and operational error. The third consists of an industry compensation fund financed by risk-based contributions from Crypto-Asset Financial Services Institutions. The

OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

industry fund should be used only after institutional and insurance obligations are enforced, preserving market discipline. OJK should determine a minimum compensation limit per consumer and may increase it according to the risk profile and assets under custody.

At the fifth stage, segregation should become bankruptcy remote. Regulation should state that consumer assets identifiable through records and reconciliation do not form part of the bankruptcy estate of a custodian or trader. The receiver should return those assets directly after verification rather than treat consumers as unsecured creditors. If an omnibus wallet has a shortfall, the remaining assets should be distributed proportionately without extinguishing damages claims against the operator and responsible persons. This approach reduces the credit risk concealed within custody services.[38]

At the sixth stage, supervision should use real-time three-way reconciliation among the trader, custodian, and clearing institution. Reconciliation should include proof of consumer liabilities, verification of wallet control, mapping of hot and cold wallets, and an independent audit of withdrawal capability. OJK may prescribe reporting formats through a circular and use its authority to establish special regulatory and supervisory policies for Crypto-Asset Financial Services Institutions.[39] Public information need not disclose personal data or security-sensitive details, but it should show asset-coverage ratios, audit results, material incidents, and recovery status.

d. Regulatory and Enforcement Reformulation

The first reform concerns the definition of loss. OJK regulations should define loss as any circumstance in which assets recorded as belonging to a consumer cannot be delivered in the required type and quantity because of a balance reduction, unauthorised transfer, loss of access, key destruction, asset shortfall, or transfer into the control of an unauthorised party. This definition prevents operators from limiting loss to external theft.

---

[38] Levitin, "Not Your Keys, Not Your Coins," 877–954.
[39] Indonesia, Law Number 4 of 2026, art. 221C.

OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

The second reform concerns evidence. OJK regulations should provide that proof of balance and non-delivery creates a presumption of liability against the entity controlling the asset. Operators must provide a chronology, forensic findings, audited logs, and evidence of compliance. Consumers remain responsible when they are proven to have disclosed credentials, ignored clear warnings, or authorised the transaction. Contributory fault may be allocated proportionately, but only on individualised evidence.

The third reform concerns joint and several liability among operators unable to establish the location and cause of the loss. The rule should protect consumers externally while inter-operator contracts govern contribution. OJK should also prohibit clauses limiting liability below the value of assets held or releasing an operator from vendor failure. Empirical research on custody terms shows that, without mandatory standards, consumers possess weak bargaining power and commonly accept clauses that do not protect their rights.[40]

The fourth reform concerns minimum insurance and a compensation fund. Premiums and contributions may be based on assets under custody, the proportion held in online wallets, audit results, previous incidents, vendor concentration, and governance quality. The scheme should control moral hazard through deductibles, recourse against wrongdoers, and sanctions for inaccurate reporting. Use of the compensation fund does not extinguish claims against controllers or principal parties committing unlawful acts.

The fifth reform concerns resolution and bankruptcy protection. Specific provisions should be included in amendments to the Bankruptcy Law or in financial-sector rules supported by statutory authority. At minimum, the rules should recognise consumer assets as separate property, establish a direct right of return, grant the receiver access to keys and records, and maintain minimum operations for withdrawals. This approach is preferable to reliance on accounting segregation because crypto-asset existence depends on the combination of technical control and legal recognition.

[40] Zetzsche and Nikolakopoulou, "Crypto Custody: An Empirical Assessment," 73–97.

The sixth reform concerns coordinated enforcement. OJK should address prudential and market-conduct violations, law-enforcement agencies should investigate theft and manipulation, the Financial Services Sector Alternative Dispute Resolution Institution should resolve private disputes, and courts should award damages and collective remedies. Data exchange must protect digital-evidence integrity, consumer confidentiality, and defence rights. Integrated handling prevents consumers from being required to repeat the same proof before multiple institutions. Anti-money-laundering and counter-terrorist-financing standards must continue to apply so that recovery does not facilitate laundering of criminal proceeds.[41]

The model does not remove market risk. Price decreases caused by investment decisions remain the consumer's risk absent misrepresentation or manipulation. Custodian liability is confined to losses connected with control, custody, transfer, recordkeeping, and return of assets. This boundary balances consumer protection and industry sustainability. Excessively broad liability would turn custodians into guarantors of investment value, while excessively narrow liability would disregard the trust underlying the transfer of asset control.

D. Conclusion

The transfer of supervision to OJK has repositioned crypto-asset custodians as Crypto-Asset Financial Services Institutions carrying prudential duties and direct civil liability toward consumers. OJK Regulation Number 27 of 2024, as amended by OJK Regulation Number 23 of 2025, requires security, segregated records, and responsibility for losses of assets held in custody. Law Number 4 of 2026 reinforces institutional liability for fault, negligence, regulatory violations, and contractual breaches committed by organs, employees, and third parties. These rules must be read together with OJK consumer-protection regulation, the Indonesian Civil Code, and the prohibition of exoneration clauses. Unresolved issues concern attribution, evidentiary burdens, trader-custodian relationships, valuation of recovery, compensation resources, and the status of assets in bankruptcy. OJK should

[41] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris: FATF, 2021).

establish a control-based liability and layered recovery model through a presumption against controllers of keys and infrastructure, joint and several liability when inter-operator records cannot locate the loss, restitution in the same type and quantity of asset, mandatory insurance, an industry compensation fund, three-way reconciliation, and bankruptcy-remote segregation. This framework provides an enforceable recovery route without making custodians guarantors of market risk.

References

Alfiani, Francisca Romana Nanik. "The Urgency of Comprehensive and Integrated Digital Asset Regulation." *Journal of Social Science* 5, no. 1 (2024): 90–102. https://doi.org/10.46799/jss.v5i1.764.

Arner, Douglas W., Dirk A. Zetzsche, Ross P. Buckley, and Jamieson M. Kirkwood. "The Financialisation of Crypto: Designing an International Regulatory Consensus." *Computer Law & Security Review* 53 (2024): 105970. https://doi.org/10.1016/j.clsr.2024.105970.

Dachi, Fitri Natasha, and Urbanisasi. "Tanggung Jawab Perdata dalam Transaksi Crypto Asset: Kajian terhadap Risiko Kerugian Investor." *Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora* 3, no. 2 (2025): 69–79. https://doi.org/10.55606/jurrish.v3i2.5638.

European Parliament and Council. Regulation (EU) 2022/2554 of December 14, 2022 on Digital Operational Resilience for the Financial Sector. OJ L 333, December 27, 2022.

European Parliament and Council. Regulation (EU) 2023/1114 of May 31, 2023 on Markets in Crypto-Assets. OJ L 150, June 9, 2023.

Fahmi, A. B. "Crypto Regulation and Anti-Money Laundering in Indonesia." *Jurnal Pembangunan Hukum Indonesia* 7, no. 3 (2025): 514–541.

Financial Action Task Force. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF, 2021.

Hidayat, Beni Darmawan, and Muhamad Hasan Sebyar. "Implikasi Hukum Perpindahan Pengawasan Aset Kripto dari Bappebti ke OJK terhadap Pelaku Industri dan Investor." *Hakim: Jurnal Ilmu Hukum dan Sosial* 2, no. 4 (2024): 888–899. https://doi.org/10.51903/hakim.v2i4.2206.

Hullu, S., and M. Huda. "Analisis Yuridis terhadap Penanganan Aset Digital (Crypto) dalam Kepailitan Perusahaan di Indonesia." *Jurnal Ilmu Hukum, Humaniora dan Politik* 6, no. 4 (2026): 3092–3104. https://doi.org/10.38035/jihhp.v6i4.8458.

Indonesia. Indonesian Civil Code.

Indonesia. Law Number 8 of 1999 on Consumer Protection.

Indonesia. Law Number 37 of 2004 on Bankruptcy and Suspension of Debt Payment Obligations.

JOURNAL
AXIOMA LEX PRIMA
OPEN ACCESS
Volume 1 No 1 Tahun 2026
ISSN: xxxx-xxxx (Online)

Indonesia. Law Number 4 of 2023 on Financial Sector Development and Strengthening, as amended by Law Number 4 of 2026.

Indonesia. Government Regulation Number 49 of 2024 on the Transfer of Regulatory and Supervisory Duties over Digital Financial Assets, Including Crypto Assets and Financial Derivatives.

International Organization of Securities Commissions. *Policy Recommendations for Crypto and Digital Asset Markets*. Final Report FR11/23. Madrid: IOSCO, 2023.

Kokorin, Ilya. “The Anatomy of Crypto Failures and Investor Protection under MiCAR.” *Capital Markets Law Journal* 18, no. 4 (2023): 500–525. https://doi.org/10.1093/cmlj/kmad019.

Levitin, Adam J. “Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency.” *Texas Law Review* 101, no. 4 (2023): 877–954.

Ordekian, Marilyne, Ingolf Becker, Tyler Moore, and Marie Vasek. “Raising the Bar: Assessing Historical Cryptocurrency Exchange Practices in Light of the EU’s MiCA and DORA Regulation.” *Computer Law & Security Review* 59 (2025): 106227. https://doi.org/10.1016/j.clsr.2025.106227.

Otoritas Jasa Keuangan. OJK Regulation Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector.

Otoritas Jasa Keuangan. OJK Regulation Number 27 of 2024 on the Operation of Digital Financial Asset Trading, Including Crypto Assets.

Otoritas Jasa Keuangan. OJK Regulation Number 23 of 2025 amending OJK Regulation Number 27 of 2024.

Otoritas Jasa Keuangan. OJK Circular Letter Number 20/SEOJK.07/2024 on the Operation of Digital Financial Asset Trading, Including Crypto Assets.

Skauradszun, Dominik. “Crypto Custodians in Financial Distress.” *International Insolvency Review* 33, no. 1 (2024): 71–95. https://doi.org/10.1002/iir.1521.

Yuspin, Wardah, and Arief Wicaksono. “Telaah Yuridis Perlindungan Konsumen dalam Kegiatan Investasi Aset Kripto di Indonesia.” *DiH: Jurnal Ilmu Hukum* 19, no. 1 (2023): 85–98. https://doi.org/10.30996/dih.v19i1.7886.

Zetzsche, Dirk A., and Areti Nikolakopoulou. “Crypto Custody: An Empirical Assessment.” *Journal of Financial Regulation* 11, no. 1 (2025): 73–97. https://doi.org/10.1093/jfr/fjaf004.

Zetzsche, Dirk A., Julia Sinnig, and Areti Nikolakopoulou. “Crypto Custody.” *Capital Markets Law Journal* 19, no. 3 (2024): 207–229. https://doi.org/10.1093/cmlj/kmae010.