IJHESS
International Journal of Health, Economics, and Social Sciences
PUBLISHER:
Universitas Muhammadiyah Palu
ISSN: 2685-6689
SINTA 2

# Analysis of the Application of Information Obligations and Transparency in Consumer Protection of Crypto Asset Investment

**Fajriawati Fajriawati[1]*, Ramlan Ramlan[2], Rizka Syafriana[3]**
[1]Universitas Muhammadiyah Sumatera Utara, Indonesia
[2]Universitas Muhammadiyah Sumatera Utara, Indonesia
[3]Universitas Muhammadiyah Sumatera Utara, Indonesia
***Corresponding author:** Fajriawati Fajriawati. E-mail: fajriawati@umsu.ac.id

## ABSTRACT

Crypto asset investment in Indonesia has expanded rapidly, increasing the importance of information disclosure and transparency. This study examines operators' information obligations and blockchain's potential contribution to transparency. The study employs normative legal research with statutory and conceptual approaches. Primary materials include the Consumer Protection Law, the P2SK Law, Government Regulation Number 49 of 2024, relevant Financial Services Authority (OJK) regulations, and related legal instruments. Materials were collected through library research and analyzed qualitatively through legal interpretation and systematic comparison. The analysis identifies a layered framework combining consumer rights, financial-sector supervision, electronic transaction rules, and sector-specific requirements. Key mechanisms include operator licensing, disclosure of asset characteristics and investment risks, safeguards for consumer funds, governance, risk management, and complaint-resolution channels. However, protection may be limited when consumers use unauthorized or cross-border platforms or cannot interpret complex disclosures. Blockchain, distributed ledgers, and smart contracts can improve transaction traceability and verifiability, but cannot independently establish product quality, legal compliance, or adequate risk disclosure. The study concludes that effective protection requires enforceable disclosure, coordinated supervision, accessible information, and remedies. It recommends that OJK consider cross-border regulatory cooperation, clear authorization requirements for foreign platforms serving Indonesian consumers, risk-based technology supervision, and standardized, understandable risk disclosures.

**Keywords:** Information Disclosure; Transparency; Consumer Protection; Crypto Investment; Financial Services Authority

**ARTICLE IDENTIFIERS**

**ORIGINAL ARTICLE**
**Volume 8 - Issue 4 - 2026**
**Pages 1138-1154**
**DOI: 10.56338/ijhess.v8i4.12029**

**ARTICLE HISTORY**

**Received:** 11 August, 2026
**Revised:** 17 October, 2026
**Accepted:** 28 October, 2026

CC BY-SA 4.0

## INTRODUCTION

Crypto assets have emerged as one of the most sought-after investment instruments in Indonesia over the past decade. The Financial Services Authority (Otoritas Jasa Keuangan/OJK) reported that the value of crypto asset transactions in Indonesia reached IDR 482.23 trillion throughout 2025, amid increasingly stringent supervision of the digital asset industry (Waratmaja & Istiqomah, 2026). The number of crypto investors also reached 21.7 million as of April 2026, exceeding the number of conventional mutual fund investors (Saraswati Harsasi, 2026). This rapid growth demonstrates increasing public interest in crypto asset investments. However, it also raises significant concerns regarding disparities in risk understanding, potential fraudulent activities, and inadequate disclosure of information by crypto asset trading operators. These concerns highlight the importance of establishing an effective consumer protection framework that ensures consumers receive accurate, transparent, and sufficient information before making investment decisions. The digital, decentralized, and highly volatile characteristics of crypto assets can place consumers in a vulnerable position. Unlike conventional investment products that operate within established financial regulatory frameworks, crypto assets in Indonesia were initially supervised as commodities under the futures trading regulatory regime. Consequently, the consumer protection framework developed under this regime may not have fully addressed the preventive dimensions of digital financial asset trading, particularly information transparency, technological security, corporate governance, and risk mitigation (Saputra & Sulistiyono, 2024).

These regulatory challenges may expose consumers to financial losses, market manipulation, and fraudulent activities when the available safeguards do not adequately address the distinctive risks associated with crypto asset investments (Stuart Scott, 2024). From a consumer protection perspective (Fajriawati, 2018) and (Astuti & Gunawan, 2024) emphasize the importance of legal mechanisms that protect parties in weaker bargaining positions within economic relationships. In crypto asset transactions, this protection is particularly relevant because operators generally possess greater access to information concerning trading mechanisms, transaction procedures, platform security, and operational risks than individual consumers. Therefore, imposing clear and enforceable information disclosure obligations is essential to reducing information asymmetry and enabling consumers to make informed investment decisions. A significant regulatory transformation occurred following the enactment of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law), which provides the legal basis for transferring the regulation and supervision of digital financial assets, including crypto assets, from the Commodity Futures Trading Regulatory Agency (*Bappebti*) to OJK (Diva et al., 2026). This transfer was implemented through Government Regulation Number 49 of 2024 and became effective on January 10, 2025. The transition represents an important development in Indonesia's approach to crypto asset consumer protection because it places crypto asset trading within a financial sector supervisory framework that encompasses consumer protection, governance, and risk management.

OJK has emphasized the importance of transparency and consumer protection in maintaining public confidence in the crypto asset industry while balancing regulatory safeguards with the development of financial innovation (Kurniawan Tri Wibowo, 2025). Nevertheless, the effectiveness of this regulatory transition depends not only on the existence of formal rules but also on how information disclosure obligations are implemented by operators and how compliance can be assessed in practice. The information and transparency obligations applicable to crypto asset trading have been further articulated through OJK Regulation Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading, Including Crypto Assets, alongside subsequent regulatory developments, including OJK Regulation Number 23 of 2025 and OJK Regulation Number 30 of 2025 concerning governance and risk management for financial sector technology innovation providers, to the extent applicable to the relevant entities and activities (Nurul Hidayati Indra Ningsih et al., 2025). Another instrument supporting consumer awareness is the publication of official lists of licensed Digital Financial Asset Traders (*Pedagang Aset Keuangan Digital/PAKD*) and registered prospective traders (*Calon Pedagang Aset Keuangan Digital/CPAKD*), which enables the public to verify the regulatory status of trading platforms before conducting transactions (Samsi Ridwan, 2026). As of May 2026, 26 PAKDs had reportedly received official operating licenses in Indonesia (Hardiyanti marzellina, 2022). These regulatory instruments illustrate the importance of preventive supervision, since consumers need to be able to identify authorized operators and understand the legal and financial risks associated with their investment activities before losses occur. This preventive approach is consistent with the argument of (Utomo & Pulungan, 2023) that strengthening preventive supervisory mechanisms is important in complementing enforcement measures taken after violations or losses have occurred.

CC BY-SA 4.0

Despite these regulatory developments, the implementation of information disclosure and transparency obligations continues to face challenges. Indonesia's crypto asset regulatory framework has undergone a significant transition, while questions remain regarding the practical effectiveness of preventive protection mechanisms, including risk disclosure, consumer access to relevant information, and the supervision of trading activities (Lendrawati et al., 2026). The availability of foreign trading platforms that fall outside the effective scope of Indonesian regulatory supervision may further complicate consumer protection, particularly when consumers encounter difficulties verifying platform legitimacy or obtaining effective legal remedies (Habiburrahman Rizapoor, 2024). Furthermore, the formal availability of information does not necessarily mean that consumers can access, understand, and independently verify it. (Muhammad Latifil Ansori et al., 2024)emphasize the importance of legal certainty and fairness in relationships where parties must have adequate information before entering into an agreement. In the context of crypto asset investments, this issue raises a fundamental distinction between regulatory compliance in providing information and the practical ability of consumers to obtain, understand, and verify that information.

Consequently, an assessment of consumer protection requires examining both the legal obligations imposed on operators and the mechanisms through which transparency can be implemented and evaluated. In this context, blockchain technology provides a relevant technological dimension for examining the implementation of transparency in crypto asset trading. Blockchain generally operates through distributed ledger technology (DLT), in which transaction records are maintained and validated across a network according to established consensus mechanisms. Depending on the design of the blockchain, recorded transactions may be publicly accessible and difficult to alter retrospectively without detection. These characteristics can support transaction traceability and the verification of recorded activities, potentially strengthening the availability and integrity of transaction-related information. In addition, smart contracts—programs deployed on a blockchain that execute predefined instructions when specified conditions are met—can facilitate the automatic implementation of certain transaction rules and provide an auditable record of their execution. Such technological characteristics are relevant to the principle of transparency because they may enable consumers and other authorized parties to verify specific transaction records and assess whether certain programmed processes have been executed as intended.

Nevertheless, blockchain transparency should not be equated with the full fulfillment of legal information disclosure obligations. Public blockchain records generally reveal information about on-chain transactions rather than all information material to an investment decision. For example, they may not independently establish the accuracy of an operator's financial statements, the adequacy of its asset reserves, the security of its internal systems, the identity of all relevant counterparties, or the completeness of the risk information provided to consumers. Similarly, smart contracts execute programmed instructions but do not automatically guarantee that the underlying code is correct, that the conditions programmed are fair, or that the information supplied from external sources is accurate. Crypto asset trading platforms may also maintain customer balances and execute transactions through centralized internal databases or off-chain systems, meaning that not all customer activities are necessarily recorded on a public blockchain. Therefore, the contribution of blockchain technology to consumer protection must be assessed in relation to the actual information available, the technical architecture of the platform, and the legal responsibilities of the operator. Blockchain can potentially complement regulatory transparency requirements, but it cannot replace the operator's obligation to provide complete, accurate, understandable, and relevant information to consumers.

The relationship between legal transparency obligations and blockchain-based transaction verification consequently presents an important area for further analysis. Although existing regulatory developments have strengthened the legal framework for crypto asset trading in Indonesia, the extent to which operators implement their information disclosure obligations and the extent to which blockchain mechanisms can support the verification of relevant information require further examination. In particular, the analysis must distinguish between transparency at the technical level, which concerns the accessibility and verifiability of transaction records, and transparency at the legal and consumer protection levels, which concerns the adequacy of information provided to consumers in accordance with applicable requirements. This distinction is necessary to avoid assuming that the technical characteristics of blockchain automatically resolve information asymmetry or eliminate investment risks. Instead, the relevant question is how blockchain-based mechanisms may support, complement, or remain insufficient to fulfill the information obligations imposed on crypto asset trading operators.

Based on these considerations, this study addresses two research questions. First, how are information disclosure obligations implemented by crypto asset trading operators in Indonesia under the applicable legal

CC BY-SA 4.0

and regulatory framework? Second, to what extent can blockchain technology, particularly distributed ledger technology, smart contracts, and the traceability of recorded transactions, support transparency and the fulfillment of information disclosure obligations to consumers? Accordingly, this study aims to analyze the implementation of information disclosure obligations in Indonesian crypto asset investment practices and examine the potential and limitations of blockchain technology in supporting transparency and consumer access to verifiable information. By integrating legal analysis with an examination of the relevant technological mechanisms, this study seeks to clarify the relationship between regulatory obligations and technological transparency and to identify how both dimensions may contribute to more effective consumer protection in Indonesia's crypto asset investment ecosystem.

## METHODS

This study employs a normative legal research method, which conceptualizes law as a set of written norms embodied in legislation and other authoritative legal sources (law in books) (Maharani, 2025). The research uses two approaches: the statute approach and the conceptual approach. The statute approach is employed to examine the relevant legal provisions governing information disclosure and transparency obligations in crypto asset investment, while the conceptual approach is used to analyze the underlying legal principles of consumer protection, transparency, and information asymmetry in the relationship between crypto asset trading operators and consumers. The legal materials consist of primary and secondary legal materials. Primary legal materials include Law Number 8 of 1999 concerning Consumer Protection, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, Government Regulation Number 49 of 2024, OJK Regulation Number 27 of 2024, OJK Regulation Number 23 of 2025, OJK Regulation Number 30 of 2025, and OJK Circular Letter Number 20/SEOJK.07/2024. Secondary legal materials comprise scientific journal articles, books, previous research findings, and relevant publications from reliable sources that provide context for the development and implementation of crypto asset regulations in Indonesia.

Legal materials are collected through library research by identifying, examining, and reviewing relevant legislation, legal literature, and scholarly publications. The collected materials are then classified and systematized according to their legal authority, substantive relevance, and relationship to the research questions (Maharani, 2025). The legal materials are analyzed using descriptive-qualitative analysis through legal interpretation and legal construction. The analysis proceeds through four stages: (1) identifying legal norms governing information disclosure and transparency obligations in crypto asset investment; (2) systematizing these norms according to their legal hierarchy, scope, and interrelationships; (3) interpreting and examining their consistency with consumer protection principles, particularly the principles of transparency, legal certainty, and adequate information disclosure; and (4) formulating conclusions regarding the adequacy of the applicable legal framework and the extent to which its normative provisions address consumer protection challenges in crypto asset investment (Maharani, 2025) and (Peryanto et al., 2025).

## RESULTS

### Regulatory Framework Governing Information and Transparency Obligations in Crypto Asset Trading

The examination and systematization of primary legal materials identify a regulatory framework governing information disclosure and transparency in crypto asset trading in Indonesia. The framework consists of general consumer protection legislation, financial sector legislation, electronic transaction legislation, implementing regulations, and sector-specific regulations governing digital financial asset trading, including crypto assets. At the general legislative level, Law Number 8 of 1999 concerning Consumer Protection establishes consumers' rights to accurate, clear, and honest information regarding the conditions and guarantees of goods and/or services. It also sets out the obligations and responsibilities of business actors in consumer transactions. Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law) provides the legislative basis for restructuring the regulation and supervision of digital financial assets, including crypto assets. This institutional transition is further implemented through Government Regulation Number 49 of 2024 concerning the Transfer of Tasks for the Regulation and Supervision of Digital Financial Assets, Including Crypto Assets and Financial Derivatives.

The legal framework is complemented by Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, which provides a general legal framework for electronic information and transactions. At the sectoral level, OJK Regulation Number 27 of 2024 concerning the

CC BY-SA 4.0

Implementation of Digital Financial Asset Trading, Including Crypto Assets, provides specific provisions governing digital financial asset trading under OJK supervision. Subsequent regulatory developments include OJK Regulation Number 23 of 2025 and OJK Regulation Number 30 of 2025, which address additional regulatory requirements relevant to digital financial asset trading and the governance and risk management of financial sector technology innovation providers, respectively, within their applicable scopes. OJK Circular Letter Number 20/SEOJK.07/2024 is also included in the examination of relevant regulatory materials concerning digital financial asset trading. The regulatory instruments identified in this study are summarized in Table 1.

**Table 1.** Regulatory Framework for Information and Transparency in Crypto Asset Trading

| Regulatory instrument | Regulatory scope relevant to the study |
|---|---|
| Law Number 8 of 1999 concerning Consumer Protection | Consumer rights to accurate, clear, and honest information and the responsibilities of business actors. |
| Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector | Legislative basis for the development and restructuring of financial sector regulation and supervision, including digital financial assets. |
| Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024 | General legal framework for electronic information and transactions. |
| Government Regulation Number 49 of 2024 | Transfer of regulatory and supervisory responsibilities for digital financial assets, including crypto assets, and financial derivatives. |
| OJK Regulation Number 27 of 2024 | Sector-specific framework for the implementation of digital financial asset trading, including crypto assets. |
| OJK Regulation Number 23 of 2025 | Additional regulatory provisions relevant to the governance of digital financial asset trading, subject to the regulation's actual scope. |
| OJK Regulation Number 30 of 2025 | Governance and risk management requirements for financial sector technology innovation providers within the regulation's applicable scope. |
| OJK Circular Letter Number 20/SEOJK.07/2024 | Relevant technical and supervisory provisions identified for examination in relation to digital financial asset trading. |

Source: Systematization of primary legal materials.

The systematization demonstrates that the regulatory framework comprises several interconnected levels. General consumer protection legislation establishes the basis for consumers' information rights, financial sector legislation establishes the institutional framework, electronic transaction legislation provides the broader context for digital transactions, and sector-specific instruments govern the activities of relevant operators. The applicability of each instrument depends on its subject matter, addressees, and operative provisions.

## Forms of Information and Transparency Obligations in Crypto Asset Trading

The examination of the relevant legal materials identifies several forms of regulatory requirements and consumer protection mechanisms associated with information disclosure and transparency in crypto asset trading. These include operator licensing, publication of information regarding authorized operators, disclosure of product characteristics and investment risks, separation of consumer funds, complaint handling and dispute resolution, and governance and risk management requirements. The precise scope of each obligation is determined by the applicable regulatory provisions. First, licensing and verification of operator legality. The regulatory framework establishes authorization requirements for entities conducting regulated digital financial asset trading activities. Information concerning licensed operators, including official lists published by the relevant authority, enables consumers to verify an operator's regulatory status before engaging in transactions. Licensing information therefore constitutes one form of publicly accessible information concerning the legal status of a trading platform.

Second, disclosure of product information and investment risks. The applicable regulatory framework includes requirements concerning information provided in connection with digital financial asset trading. Relevant information may include the characteristics of the crypto asset, transaction procedures, material risks, and other information required under the applicable provisions. The specific disclosure requirements depend on

CC BY-SA 4.0

the relevant legal instrument and the type of activity performed by the operator. Third, separation of consumer funds and operator funds. The regulatory framework also addresses the safeguarding and management of consumer funds through applicable requirements concerning the handling and separation of funds. This mechanism is distinct from information disclosure itself but forms part of the broader regulatory arrangements governing the protection of consumer assets. Its implementation must be assessed against the specific requirements imposed on the relevant operator.

Fourth, complaint handling and dispute resolution. Consumer protection arrangements include mechanisms through which consumers may submit complaints and seek the resolution of disputes arising from the use of digital financial asset trading services. These mechanisms provide channels for addressing problems that occur during or after transactions, subject to the applicable rules and procedures. Fifth, governance and risk management. The relevant regulatory instruments establish governance and risk management requirements within their respective scopes. These requirements concern the organizational and operational arrangements through which regulated entities manage risks associated with their activities. They complement disclosure obligations by addressing the systems and controls that support the operation of digital financial asset trading services. Sixth, additional requirements for activities involving crypto asset derivatives. Where the relevant activities involve digital financial asset derivatives, additional regulatory requirements may apply, including authorization, margin, or collateral arrangements as prescribed by the applicable rules. These requirements are activity-specific and should not be treated as universally applicable to all spot crypto asset transactions. Seventh, consumer education and information accessibility. Consumer education constitutes a relevant component of the b

Roader consumer protection framework. Information accessibility and consumer education are related but distinct: the former concerns whether relevant information is made available, while the latter concerns measures intended to improve consumers' ability to understand digital financial products and their associated risks. The specific obligations of operators and the responsibilities of the regulator must be distinguished according to their respective legal bases. The identified forms of regulatory requirements and protection mechanisms are summarized in Table 2.

**Table 2.** Forms of Information and Transparency Requirements in Crypto Asset Trading

| Form | Regulatory function | Relevant aspect of consumer protection |
|---|---|---|
| Licensing and operator verification | Establishes and communicates the regulatory status of operators. | Enables consumers to check platform legality. |
| Product and risk disclosure | Provides information required for crypto asset trading activities. | Supports informed investment decisions. |
| Separation of consumer funds | Establishes safeguards for the handling of consumer funds. | Helps protect consumer assets against specified operational risks. |
| Complaint handling and dispute resolution | Provides channels for addressing consumer grievances. | Facilitates the handling of disputes and service-related problems. |
| Governance and risk management | Establishes organizational and operational requirements for managing risks. | Supports the controlled operation of trading services. |
| Derivatives-specific requirements | Establishes additional safeguards for regulated derivative activities where applicable. | Addresses risks associated with derivative transactions. |
| Consumer education and information accessibility | Supports access to and understanding of relevant information. | Helps consumers interpret product information and investment risks. |

Source: Systematization of primary legal materials and relevant secondary legal materials.

Based on a conceptual approach, the obligation of information and transparency in crypto asset trading is closely related to the principles of consumer protection, especially the principles of openness, legal certainty, security, and justice. The results of the analysis show that the position of consumers in crypto asset transactions has the potential for information imbalance because organizers have greater control of information regarding technology, product characteristics, transaction mechanisms, and investment risks. In these conditions, information obligations function as an instrument to reduce information asymmetry between organizers and consumers. Consumers need adequate information before making investment choices so that the decisions made are not only based on promotions or potential profits, but also consider the risks inherent in crypto

CC BY-SA 4.0

assets. The findings are in line with the thinking (Fajriawati, 2018) regarding the importance of legal instruments that are able to protect parties who are in a weaker position in economic relations.

### Regulatory Scope and Technological Transparency

The review of the legal materials also identifies a distinction between regulatory obligations imposed on crypto asset trading operators and the technical characteristics of the technologies used to record transactions. The legal framework governs matters such as operator authorization, information disclosure, asset and fund management, governance, and risk management. Blockchain technology, by contrast, provides technical mechanisms for recording and verifying transactions, depending on the architecture and operational arrangements of the system. The technological concepts relevant to this distinction include distributed ledger technology (DLT), smart contracts, and transaction records maintained on public blockchains. DLT concerns the distribution and validation of records across a network. Smart contracts are programs that execute predefined instructions when specified conditions are met. Public blockchain records may enable the inspection and verification of certain on-chain transactions, while cryptographic and consensus mechanisms can make retrospective alteration of confirmed records difficult without detection. These technical characteristics do not, by themselves, establish that an operator has fulfilled every applicable legal information disclosure obligation. In particular, public transaction records do not necessarily contain all information required for consumers to assess product characteristics, investment risks, operator governance, or the handling of customer assets. Furthermore, transactions recorded in an operator's internal systems or other off-chain arrangements may not be fully visible on a public blockchain. Accordingly, the results identify two distinct but potentially complementary dimensions of transparency: regulatory transparency, which concerns the information and disclosures required by law, and technical transparency, which concerns the accessibility, traceability, and verifiability of transaction records.

The relationship between these dimensions provides the basis for further legal analysis of blockchain's potential contribution to consumer protection. In the context of crypto assets, disclosure obligations can be positioned as a legal instrument to reduce information inequality between organizers and consumers. This principle is also related to the view of (Muhammad Latifil Ansori et al., 2024) that certainty and fairness in legal relations require adequate information for the parties before legal relations are formed. In crypto asset transactions, information about the product, risks, legality of the organizer, and dispute resolution mechanism are important parts so that consumers can give their consent consciously. In addition, the results of the study show that preventive supervision has an important position in consumer protection. (Utomo & Pulungan, 2023) emphasizing the importance of optimizing preventive surveillance instruments to prevent community losses from the start. In the context of crypto assets, a preventive approach can be realized through licensing obligations, risk disclosure, consumer education, fund segregation, governance, and risk management of organizers. The results of the descriptive-qualitative analysis show that normatively the legal framework regarding information and transparency of crypto assets has been strengthened. The applicable regulations have regulated aspects of the legality of the organizers, information disclosure, protection of consumer funds, complaints, dispute resolution, governance, and risk management.

Thus, in a nutshell, the obligation of information and transparency has been placed as one of the important instruments in the protection of crypto asset consumers. However, the results of the search for secondary legal materials show that the effectiveness of the implementation of these provisions still faces a number of obstacles. One of the main problems is the character of the regulation which is still in the adjustment stage after the transfer of supervisory authority from Bappebti to the OJK. Changes in the supervisory regime require adjustments not only from the institutional side, but also from the regulator's compliance with the regulatory standards of the financial services sector. The next obstacle has to do with the existence of cross-border platforms and platforms that do not have permissions. Information and consumer protection provisions are easier to apply to organizers under the jurisdiction and supervision of the OJK. On the other hand, for platforms that operate from outside the jurisdiction or do not have a license, the ability of the authority to ensure the fulfillment of information obligations and provide remedies to consumers becomes more limited. The results of the study also show that there is a gap between the normative availability of information and the ability of consumers to understand the information. The level of digital financial literacy is a factor that affects the effectiveness of the principle of transparency. Complete information does not necessarily result in optimal protection if consumers do not have the ability to understand investment risks, asset characteristics, and transaction consequences. Thus, the effectiveness of the principle of transparency is not only determined by

CC BY-SA 4.0

the existence of regulations, but also by the compliance of the organizers, supervisory capacity, jurisdiction reach, information quality, and consumer literacy level.

### Gap between Das Sollen and Das Sein

The results of the study show that there is a gap between legal norms (das sollen) and application in practice (das sein). At the normative level, regulations have built a relatively comprehensive protection mechanism through licensing, information obligations, risk management, fund segregation, complaint mechanisms, and consumer education. However, in practice, this protection has not reached all crypto asset consumers equally. The gap is especially seen in transactions through illegal and cross-border platforms, where information disclosure obligations and consumer protection mechanisms are difficult to implement effectively. In addition, there is still a risk of fraud, market manipulation, cyberattacks, and asset loss due to negligence or lack of consumer understanding of account security and digital assets.

The findings show that the existence of regulations does not automatically guarantee the achievement of consumer protection. It is necessary to strengthen supervision, increase the compliance of organizers, coordinate between institutions, expand public education, and strengthen law enforcement mechanisms against illegal platforms and activities that are detrimental to consumers. Based on the overall results of the analysis, it can be seen that the Indonesian legal framework has provided an increasingly strong basis for the implementation of information and transparency obligations in crypto asset investments. The transfer of supervision to the OJK strengthens the orientation of consumer protection and governance of the digital financial sector. However, the effectiveness of its implementation is still influenced by the issue of regulatory transition, the scope of supervision of cross-border platforms, consumer literacy, business compliance and law enforcement. Therefore, the application of the principle of transparency in crypto asset investment still needs to be continuously strengthened so that consumer protection is not only effective at the normative level, but can also be realized in practice.

## DISCUSSION

### Information Disclosure Obligations as an Instrument of Consumer Protection

The regulatory framework identified in the Results establishes a legal basis for protecting consumers through information disclosure, operator authorization, risk management, and mechanisms for addressing consumer complaints. However, the existence of these regulatory requirements does not automatically ensure that consumers receive adequate protection. Their significance depends on whether the information required by law is sufficiently comprehensive, accessible, understandable, and relevant to investment decisions. Accordingly, the implementation of information obligations should be assessed not merely by the formal availability of information but also by its capacity to address the information imbalance between crypto asset trading operators and consumers. This issue can be explained through Akerlof's theory of information asymmetry, which describes how unequal access to information about product quality can affect market decisions and create opportunities for opportunistic behavior (Tilles et al., 2011). In crypto asset trading, operators may possess more detailed information concerning platform operations, transaction procedures, fees, security arrangements, and the risks associated with particular services than individual consumers. Consumers, meanwhile, may have limited capacity to independently assess the reliability of this information or evaluate the technical and financial characteristics of the assets being traded. This imbalance is particularly significant when investment decisions are influenced by promotional claims, expectations of rapid returns, or incomplete explanations of potential losses.

From this perspective, legal information disclosure obligations serve as an institutional mechanism for reducing information asymmetry. However, the effectiveness of disclosure depends on the quality of the information provided. Information that is technically available but difficult to understand may satisfy a formal disclosure requirement without adequately supporting informed decision-making. Similarly, extensive documentation does not necessarily provide effective protection if material risks are presented ambiguously, important limitations are obscured, or the information is not accessible before a transaction is undertaken. Consequently, substantive transparency requires more than the publication of information. It requires information to be accurate, relevant, sufficiently comprehensive, timely, and understandable to its intended audience. In the context of crypto asset investment, this includes meaningful disclosure of asset characteristics, price volatility, transaction costs, platform security risks, and the procedures available when disputes or service disruptions occur, to the extent required by the applicable regulations. These requirements should enable consumers to evaluate both the potential benefits and the material risks of an investment. This

CC BY-SA 4.0

interpretation is consistent with the consumer protection principles underlying Law Number 8 of 1999 concerning Consumer Protection and the sector-specific regulatory framework discussed in the Results. It also clarifies the relationship between formal legal compliance and substantive consumer protection: the former concerns whether applicable obligations have been fulfilled, whereas the latter concerns whether those obligations provide meaningful safeguards for consumers. The distinction is important because the effectiveness of a disclosure regime cannot be inferred solely from the number of regulations or the volume of information published by an operator.

### Preventive and Repressive Legal Protection

The relationship between information disclosure and consumer protection can also be examined through Philipus M. Hadjon's theory of legal protection, which distinguishes between preventive and repressive protection (Setiawan & Babussalam, 2026). Preventive protection seeks to prevent harm before it occurs, whereas repressive protection concerns the mechanisms available to address violations and resolve disputes after harm has arisen. Within the crypto asset regulatory framework, operator authorization, risk disclosure, governance requirements, and applicable consumer education measures can function as preventive instruments. These mechanisms are intended to reduce the likelihood that consumers enter into transactions without adequate information or that operators conduct regulated activities without satisfying applicable requirements. The availability of official information concerning licensed operators is particularly relevant because consumers need to establish the regulatory status of a platform before deciding whether to use its services. Nevertheless, preventive protection has limitations. A license indicates that an operator has obtained authorization under the applicable regulatory framework; it does not guarantee investment profitability, eliminate market volatility, or establish that every transaction conducted through the platform is free from risk. Similarly, disclosure of investment risks does not eliminate those risks. Its purpose is to ensure that consumers receive the information necessary to assess them before making investment decisions.

Repressive protection complements these preventive measures through complaint handling, dispute resolution, administrative enforcement, and other remedies available under applicable law. These mechanisms become relevant when consumers experience unauthorized transactions, service failures, alleged breaches of contractual obligations, or other losses for which legal remedies may be available. Their effectiveness depends on the availability of accessible complaint channels, the clarity of dispute resolution procedures, the allocation of legal responsibility, and the ability of the relevant authorities to enforce applicable rules. This framework demonstrates that preventive and repressive protection should not be treated as alternatives. Disclosure and supervision may reduce certain risks before transactions occur, while complaint handling and enforcement address problems that preventive measures cannot entirely eliminate. For crypto asset consumers, an effective protection framework therefore requires both adequate information before transactions and accessible mechanisms for seeking remedies when violations occur. The analysis also suggests that the formal existence of complaint procedures is not, by itself, sufficient to establish effective repressive protection. Their practical value depends on whether consumers can identify the responsible operator, preserve relevant transaction records, access the appropriate dispute resolution mechanism, and obtain a remedy under the applicable legal framework. These considerations become more complex when transactions involve unauthorized platforms, foreign operators, or multiple jurisdictions.

### The Legal System and the Gap Between Norms and Implementation

The distinction between regulatory requirements and their practical consequences can be further examined through Lawrence M. Friedman's legal system theory, which identifies legal substance, legal structure, and legal culture as interrelated dimensions of a legal system (Stinchcombe, 1977) and (Flora et al., 2023). This perspective helps explain why the strengthening of formal regulations may not, on its own, eliminate consumer vulnerability in crypto asset investment. The legal substance dimension concerns the rules governing consumer rights, operator obligations, supervision, and available remedies. The regulatory developments identified in the Results demonstrate that Indonesia has established a more specialized framework for digital financial asset trading, including crypto assets. The framework provides a basis for addressing matters such as operator authorization, information disclosure, governance, and risk management. However, the existence of these rules does not establish, without further evidence, that all operators comply with them or that consumers consistently receive effective protection.

The legal structure dimension concerns the institutions responsible for implementing and enforcing the law. In this context, the effectiveness of consumer protection depends on the capacity of the relevant authorities to

CC BY-SA 4.0

supervise regulated operators, identify potential violations, coordinate with other institutions, and take appropriate enforcement measures. The activities of unauthorized or foreign-based platforms may create additional jurisdictional and enforcement challenges where such platforms fall outside the effective reach of domestic supervisory mechanisms. Nevertheless, the extent of these challenges should be assessed using verifiable legal materials and documented cases rather than inferred solely from the existence of cross-border transactions. The legal culture dimension concerns the knowledge, attitudes, and behavior of both consumers and business actors in relation to the law. Consumers need to understand the importance of verifying operator authorization, reviewing material risk disclosures, protecting account credentials, and using available complaint channels. Operators, in turn, must recognize that disclosure is a substantive legal responsibility rather than merely a documentation requirement. Consumer education can support the effective use of available information, but it should not transfer the primary responsibility for regulatory compliance from operators to consumers.

These three dimensions are interdependent. Clear legal rules may have limited practical impact if supervision and enforcement are inadequate. Effective supervision may also fail to produce meaningful consumer protection if disclosure practices remain difficult to understand. Likewise, consumer awareness cannot substitute for compliance by operators or for effective institutional oversight. The distinction between das sollen and das sein is useful in describing this relationship. Das sollen refers to the normative standards prescribed by law, whereas das sein concerns the conditions under which those standards are implemented in practice. The regulatory framework provides a normative basis for transparency and consumer protection, but its practical effectiveness cannot be established solely through an examination of legislation. In a normative legal study, the gap should therefore be framed as an implementation issue identified or indicated by the legal materials and supporting literature, rather than as a quantitatively measured empirical outcome.

The literature cited in this study identifies continuing concerns relating to fraud, phishing, dispute resolution, cross-jurisdictional enforcement, and supervisory capacity (AKERLOF, 1978), (Sukamulya & Kusuma, 2026), (Tlili, 2025). These concerns suggest that legal protection cannot be evaluated exclusively by reference to the completeness of formal rules. However, the extent and prevalence of these problems require further evidence from the underlying studies or other reliable sources. The contribution of the present analysis is therefore to explain how these documented concerns relate to the design and limitations of information disclosure obligations, rather than to claim that the study independently measures their incidence.

## Blockchain Technology and the Limits of Technical Transparency

Blockchain technology introduces an additional dimension to the relationship between legal disclosure obligations and consumer protection. Distributed ledger technology (DLT), smart contracts, and publicly accessible transaction records can support the recording, execution, and verification of certain activities. However, their contribution must be assessed in relation to the specific information that consumers need and the legal responsibilities imposed on trading operators. DLT distributes the maintenance and validation of records across a network according to its technical design and consensus mechanism. In an appropriately designed public blockchain, transaction records can be inspected and independently verified by users with the necessary tools and technical knowledge. Cryptographic mechanisms and consensus processes can also make the retrospective alteration of confirmed records difficult without detection (Yaga et al., 2018). These characteristics may support transaction traceability and provide a technical basis for auditing certain on-chain activities.

From a consumer protection perspective, transaction traceability may help establish whether a particular transaction was recorded, identify the movement of assets between blockchain addresses, and provide evidence relevant to the reconstruction of certain transaction histories (OECD, 2021). However, the interpretation of such records requires caution. A blockchain address does not necessarily reveal the legal identity of its controller, the commercial purpose of a transaction, or the relationship between an address and a particular consumer. Moreover, a publicly visible transaction record does not independently establish whether the underlying activity complied with applicable legal obligations. Smart contracts may provide another mechanism for supporting transparency. These programs execute predefined instructions when specified conditions are met, and their execution may produce records that can be inspected on the relevant blockchain(Yaga et al., 2018).

Smart contracts may provide another mechanism for supporting transparency. These programs execute predefined instructions when specified conditions are met, and their execution may produce records that can be inspected on the relevant blockchain. Where a smart contract governs a transaction or another defined

CC BY-SA 4.0

process, its code and transaction history may allow technical reviewers to examine how particular rules were implemented. This can improve the verifiability of programmed operations and support certain forms of auditability. Nevertheless, smart contracts do not automatically guarantee legal compliance or consumer protection. A contract may execute exactly as programmed while still containing design errors, unintended consequences, or conditions that are unfavorable to consumers. Its execution may also depend on external data supplied through oracles or other systems, the accuracy of which cannot be guaranteed solely by the blockchain. Consequently, technical auditability should not be equated with the fairness, accuracy, or legal adequacy of the underlying transaction (Auer, 2022). The distinction between on-chain and off-chain information is particularly important. A public blockchain may record the transfer of a crypto asset without disclosing the full information needed to evaluate the asset's economic characteristics, the operator's governance, its financial condition, its custody arrangements, or the risks explained to consumers. Similarly, a trading platform may maintain customer balances, internal transaction records, or other operational information in centralized databases. The public blockchain may therefore reveal only part of the activity relevant to a consumer's investment decision.

These limitations establish a distinction between transactional transparency and product-risk transparency. Transactional transparency concerns the ability to inspect and verify particular recorded transactions. Product-risk transparency concerns the disclosure of information necessary to evaluate an asset, the operator, investment risks, fees, and applicable consumer protection mechanisms. Blockchain can support transactional transparency in appropriate circumstances, but it cannot independently fulfill all requirements associated with product-risk transparency. Accordingly, the potential contribution of blockchain to the fulfillment of information obligations under the Financial Services Authority's (OJK) regulatory framework must be assessed on a requirement-by-requirement basis. Where applicable rules require information about a transaction that can be independently verified through a blockchain record, the technology may provide supplementary evidence. Where the required information concerns legal status, risk disclosures, consumer rights, conflicts of interest, or complaint procedures, additional documentation and institutional mechanisms remain necessary.

Blockchain records should therefore be treated as a potential source of verification, not as a substitute for the operator's legal obligation to provide accurate, complete, and understandable information. This distinction is consistent with the regulatory challenges identified by (Bahtiar, 2026) particularly the need to reconcile technological innovation with legal accountability, consumer protection, and the enforcement of existing regulatory frameworks. This analysis also identifies a possible role for regulatory technology (RegTech). Where lawful access, appropriate technical infrastructure, and reliable data are available, traceable transaction records may support supervisory monitoring and the identification of certain transaction patterns. (Auer, 2022) for example, discusses embedded supervision, a framework in which regulatory compliance in decentralized financial markets could be monitored through the market's distributed ledger, potentially reducing the need for intermediaries to collect, verify, and submit certain data.

However, the effectiveness of this approach depends on the reliability of the ledger data, the design of the monitoring framework, and the legal and operational arrangements governing supervisory access and responsibility. Automated monitoring cannot independently determine every question of legal responsibility, and it does not eliminate the need for governance, human oversight, and enforcement. Therefore, blockchain should be understood as a technology that may complement the legal framework for transparency rather than replace it. Its effectiveness depends on whether the information it makes available is relevant to the applicable disclosure requirements, whether consumers or authorized supervisors can interpret and verify that information, and whether the information can be connected to reliable evidence concerning the activities of the regulated operator. In the context of crypto asset consumer protection in Indonesia, blockchain's potential contribution should consequently be evaluated in conjunction with the applicable OJK regulations, the operator's disclosure obligations, and the institutional mechanisms available to verify compliance and address violations.

### Integrating Regulatory Disclosure, Institutional Supervision, and Consumer Understanding

The preceding analysis indicates that the effectiveness of information obligations in crypto asset consumer protection depends on the interaction of three dimensions: normative requirements, institutional implementation, and consumer understanding. These dimensions provide an analytical framework for understanding why the existence of formal disclosure rules and technically traceable transactions may still be insufficient to guarantee meaningful protection. This framework is consistent with (Friedman, 1975) legal system theory, which emphasizes the interrelationship between legal substance, legal structure, and legal

CC BY-SA 4.0

culture in determining how law operates within society. The normative dimension concerns the clarity and scope of the information that operators are legally required to provide. Requirements should be interpreted in accordance with the applicable legislation and regulations, including their respective scopes and addressees. Where different instruments govern consumer rights, operator authorization, electronic transactions, and sector-specific trading activities, their relationship must be examined carefully to identify the obligations that apply to each regulated activity.

In Indonesia, Law Number 8 of 1999 concerning Consumer Protection establishes a general foundation for consumers' information rights, while the regulatory framework governing digital financial asset trading provides more specific requirements applicable to regulated activities. From the perspective of information asymmetry, these obligations are important because consumers may lack the information necessary to assess the quality, characteristics, and risks of a product independently (Akerlof, 1970). Accordingly, regulatory disclosure requirements should provide a legal basis for reducing information disparities between operators and consumers. The institutional dimension concerns the capacity to monitor compliance, verify the accuracy of relevant information, and respond to violations. Operator licensing and official lists can assist consumers in verifying legal status, but they must be accompanied by effective supervisory arrangements and appropriate responses to unauthorized activities.

Similarly, complaint and dispute resolution mechanisms must be sufficiently clear for consumers to identify the appropriate channel when problems arise. This dimension reflects (Friedman, 1975) argument that the effectiveness of legal rules depends not only on their substantive content but also on the institutions responsible for implementing them. It is also consistent with (Setiawan & Babussalam, 2026) distinction between preventive and repressive legal protection: preventive measures seek to reduce the likelihood of harm, whereas repressive mechanisms provide avenues for addressing violations and resolving disputes after harm has occurred. The consumer dimension concerns the practical usability of the information provided. Even where disclosures are legally sufficient, consumers may encounter difficulties understanding technical terminology, complex fee structures, custody arrangements, and the distinction between market risk and platform risk. This makes clarity and accessibility important considerations in the design and implementation of disclosure practices. Such considerations should complement, rather than replace, the operator's legal responsibilities. The relevance of this dimension can be understood through (Tilles et al., 2011) information asymmetry theory: the formal availability of information does not necessarily eliminate information disparities when consumers cannot adequately assess or interpret the information they receive. Therefore, consumer education and understandable risk disclosures should support consumers' ability to make informed decisions without transferring the primary responsibility for compliance from operators to consumers. Blockchain may contribute to this framework by providing verifiable records for particular transactions and supporting certain supervisory processes. However, its contribution is conditional. Distributed ledger technology can support the traceability and verification of recorded transactions, while smart contracts may make the execution of predefined rules auditable under appropriate technical conditions. Furthermore, (Auer, 2022) discusses the potential for integrating certain supervisory functions into distributed ledger systems through embedded supervision. Nevertheless, technical transparency is useful only to the extent that the available records are relevant to the information required, can be reliably interpreted, and can be connected to the legal identity and responsibilities of the relevant parties where necessary. Blockchain records do not independently establish whether an operator has provided adequate risk disclosures, complied with consumer protection requirements, or established effective complaint procedures (OECD, 2021).

Based on this synthesis, several implications follow. First, operators should fulfill applicable disclosure requirements through information that clearly explains material investment risks and relevant service conditions, rather than relying solely on the publication of extensive technical documentation. This approach is consistent with the objective of reducing information asymmetry by enabling consumers to assess relevant product characteristics and risks before making investment decisions (Akerlof, 1970). Second, the regulatory and supervisory framework should distinguish between information that can be verified through transaction records and information that requires separate documentation or disclosure. Blockchain-based verification may complement regulatory supervision, but its use must account for the technical and institutional limitations of distributed ledger systems. Third, complaint handling and dispute resolution should remain integral to consumer protection because neither disclosure nor blockchain verification eliminates the possibility of loss

CC BY-SA 4.0

or misconduct. This follows from the complementary roles of preventive and repressive legal protection described by (Wardah Yuspin & Arief Wicaksono, 2023).

Fourth, consumer education should support informed decision-making without shifting the burden of regulatory compliance onto consumers, while supervisory institutions should continue to ensure that operators fulfill their applicable legal obligations. These implications do not establish that a particular blockchain implementation or supervisory measure has already achieved the intended outcomes. Rather, they identify the legal and institutional conditions under which transparency mechanisms may contribute to more effective consumer protection. In accordance with (Day et al., 2022) legal system theory, the effectiveness of the framework depends on the interaction between the substantive rules governing disclosure, the institutional capacity to supervise and enforce compliance, and the legal culture that shapes how operators and consumers respond to those rules. Accordingly, a more effective approach to crypto asset consumer protection requires the integration of enforceable disclosure obligations, appropriate supervision, accessible information, consumer education, and technological mechanisms that support verification without replacing legal accountability.

## CONCLUSION AND IMPLICATIONS

This study concludes that the normative framework governing information disclosure and transparency in the protection of crypto asset consumers in Indonesia has been strengthened through the interaction of the Consumer Protection Law, the P2SK Law, Government Regulation Number 49 of 2024, OJK Regulation Number 27 of 2024, and subsequent regulatory developments, including OJK Regulation Number 23 of 2025. These instruments establish a legal foundation for consumer protection through operator authorization, information disclosure, risk management, asset protection, and complaint and dispute resolution mechanisms, subject to the scope of each applicable regulation. The analysis demonstrates that information disclosure is not merely an administrative requirement but a substantive instrument for reducing information asymmetry and enabling consumers to make more informed investment decisions. Nevertheless, the existence of a strengthened legal framework does not, by itself, guarantee effective consumer protection. The analysis identifies a potential gap between das sollen and das sein, particularly where consumers engage with unauthorized or cross-border platforms that may fall outside the effective reach of Indonesian supervision. The resulting challenges concern not only the availability of information but also the identification of responsible entities, the enforcement of domestic requirements, the accessibility of legal remedies, and the verification of information provided to consumers. Blockchain technology can support transaction traceability and the verification of certain recorded activities, but it cannot independently establish the accuracy of product disclosures, ensure regulatory compliance, or guarantee effective dispute resolution. Accordingly, consumer protection requires the coordinated operation of substantive legal obligations, institutional supervision, accessible disclosure practices, and enforceable remedies.

## IMPLICATIONS

First, OJK should establish a structured cross-border supervisory cooperation framework. Cooperation with foreign regulators should move beyond general commitments to information exchange and establish operational procedures for handling complaints, verifying operator authorization, investigating suspected violations, and coordinating enforcement actions. Memoranda of understanding or other appropriate cooperation arrangements could specify designated contact points, procedures for urgent information requests, the exchange of supervisory findings, and protocols for preserving relevant digital evidence, subject to applicable laws and confidentiality requirements. Cooperation with the United States Securities and Exchange Commission (SEC) or the Monetary Authority of Singapore (MAS) could be explored where the relevant platform, legal entity, or activity falls within the counterpart regulator's jurisdiction. Such cooperation should not assume that all crypto assets or trading platforms fall within the same regulatory classification in different jurisdictions. Instead, requests and enforcement coordination should be based on the relevant legal mandates and the nature of the activities under investigation. Second, Indonesia should strengthen the domestic authorization and registration requirements applicable to foreign platforms that actively serve Indonesian consumers. Subject to the applicable legislation and OJK's delegated authority, policymakers should consider clarifying when a foreign platform's solicitation, marketing, onboarding, or provision of regulated trading services to Indonesian residents triggers a requirement to obtain the relevant domestic authorization or establish an appropriate locally accountable legal presence. The framework should clearly distinguish

CC BY-SA 4.0

between platforms authorized to serve Indonesian consumers and foreign platforms that are not authorized to conduct the relevant activities in Indonesia. Where local incorporation or representation is legally required, the designated entity should have clearly defined responsibilities for regulatory communications, consumer complaints, compliance with disclosure obligations, and cooperation with lawful supervisory requests. Any such requirement should be established through an appropriate legal instrument rather than imposed solely through informal supervisory guidance.

A proportionate framework should also distinguish between unauthorized platforms actively targeting Indonesian consumers and foreign websites that are merely accessible from Indonesia. Regulatory intervention should be based on legally relevant indicators of market targeting and regulated activity, such as Indonesia-directed marketing, local onboarding arrangements, or other conduct specified by applicable rules. This approach would improve legal certainty and reduce the risk of treating every foreign-accessible service as automatically subject to the same requirements. Third, OJK should consider a cross-border regulatory cooperation and sandbox mechanism for qualifying digital asset activities. A regulatory sandbox could allow OJK and participating foreign regulators to assess selected technological arrangements, cross-border compliance processes, and supervisory tools within a controlled environment. Possible pilot projects include testing procedures for sharing suspicious transaction indicators, verifying licensing information across jurisdictions, reconciling on-chain records with operator disclosures, and coordinating responses to consumer complaints. Participation should be limited to eligible entities and defined activities, with clear entry criteria, consumer safeguards, data protection requirements, reporting obligations, and exit procedures. A sandbox should not be treated as an exemption from applicable licensing requirements or consumer protection obligations unless a lawful and expressly authorized mechanism provides otherwise. Where bilateral participation is impractical, OJK could first implement a domestic pilot and subsequently develop cross-border cooperation protocols based on the pilot's findings.

Fourth, technology-based supervision should be connected to specific regulatory objectives. Rather than adopting blockchain analytics as a general solution, OJK could evaluate tools that support the verification of transaction patterns, the identification of relevant blockchain addresses, and the comparison of available on-chain records with information reported by regulated operators. Such tools should be used only where the data is relevant, access is lawful, and the results can be independently assessed. Supervisory procedures should also recognize the limitations of blockchain analysis, including the difficulty of establishing the legal identity of address controllers and the absence of complete information about off-chain transactions. Human review, documented evidentiary standards, and appropriate procedures for responding to false positives should remain integral to supervisory decision-making. Fifth, disclosure requirements should be operationalized through standardized, layered risk information. OJK could consider developing or refining a standardized disclosure framework that requires regulated operators to present material information in a comparable format. A concise summary could cover the principal investment risks, price volatility, transaction and withdrawal fees, custody arrangements, platform-related risks, relevant conflicts of interest, and available complaint channels, as applicable to the product and service concerned. More detailed technical and legal documentation could be provided through supplementary disclosures. Standardization would help consumers compare operators and products without assuming that a uniform disclosure format eliminates the underlying risks. The framework should be aligned with existing legal requirements and tested for comprehensibility before being applied broadly.

Sixth, consumer protection mechanisms should incorporate measurable implementation indicators. OJK and other competent authorities could evaluate the effectiveness of the framework through indicators such as the time required to process consumer complaints, the completeness and accessibility of required disclosures, the timeliness of responses to supervisory information requests, and the number of substantiated compliance deficiencies addressed. Indicators relating to cross-border cooperation could include the time needed to verify an operator's regulatory status and the proportion of eligible cooperation requests receiving a response within agreed service periods. These measures would allow policymakers to assess implementation more systematically, although the indicators themselves would need to be defined carefully and supported by reliable data. Overall, the policy priority is not simply to increase the volume of regulation or adopt additional technology, but to establish an enforceable framework that connects domestic authorization, cross-border cooperation, meaningful disclosure, supervisory verification, and accessible consumer remedies. International cooperation arrangements, appropriately designed local authorization requirements, controlled regulatory experimentation, and risk-based technology supervision offer complementary pathways for addressing the

CC BY-SA 4.0

jurisdictional limitations of crypto asset regulation. Their implementation should remain consistent with the applicable statutory framework, institutional mandates, proportionality, and due process.

## LIMITATIONS AND FUTURE RESEARCH

This study has several limitations that need to be considered in understanding the results of the study. First, the research focuses more on normative juridical analysis of laws and regulations, secondary legal materials, theories, and previous research so that it has not yet described in depth the experience of consumers in receiving, understanding, and using information provided by crypto asset operators. Second, the study has not conducted empirical measurements of the actual level of compliance of organizers with information and transparency obligations, especially related to the delivery of risk information, asset characteristics, transaction costs, asset security, and complaint mechanisms. Third, the relatively dynamic development of digital financial asset regulations causes research results to potentially require updates if there are changes in regulations, supervisory policies, or OJK institutional developments. Fourth, the study has not comprehensively compared the implementation of crypto asset consumer protection in Indonesia with other jurisdictions that already have a more mature crypto asset regulatory framework. Further research is recommended using a socio-legal approach or empirical research involving consumers, crypto asset operators, regulators, and dispute resolution institutions. The research can measure the level of consumer understanding of risk disclosure documents and analyze the organizers' compliance with the principle of meaningful disclosure. In addition, comparative research with other countries can be conducted to identify best practices in cross-border platform surveillance, blockchain and RegTech utilization, and the harmonization of preventive and repressive consumer protections. Future studies also need to explore the effectiveness of the use of technology in increasing transparency while maintaining the security and protection of consumer data.

## STATEMENTS

**Ethics approval:** This study did not involve human participants, human subjects, personal data, or experimental interventions. The research was conducted using normative legal research methods through the analysis of primary and secondary legal materials, including legislation, regulatory documents, scholarly literature, and previous research. Therefore, formal ethical approval from an institutional ethics committee was not required.

**Funding and Statement:** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The research was conducted using the authors' institutional and personal academic resources.

**Author contributions:** Fajriawati[1] contributed to the conceptualization of the study, formulation of the research problem, analysis of consumer protection principles, and preparation of the initial manuscript. Ramlan[2] contributed to the analysis of the legal and regulatory framework concerning information and transparency in cryptocurrency investment, interpretation of the normative legal findings, and critical revision of the manuscript. Rizka Syafriana[3] contributed to the analysis of information asymmetry, legal protection theory, blockchain transparency, synthesis of previous research, and revision of the manuscript. All authors participated in reviewing and refining the final manuscript and approved the final version for publication.

**Acknowledgements:** The authors would like to express their gratitude to all parties who provided academic support, constructive discussions, and assistance during the preparation of this research. The authors also acknowledge the contribution of the academic and scholarly resources that supported the analysis of consumer protection, information transparency, and cryptocurrency regulation in Indonesia.

**AI disclosure:** The authors declare that artificial intelligence (AI)-based tools were used solely as supporting tools during the preparation of this manuscript, particularly for language editing, grammar checking, organization of ideas, and improving the clarity and readability of the academic text. AI tools were not used to generate research data, conduct data collection, determine research findings, or replace the authors' analytical and scholarly judgment. All arguments, interpretations, legal analyses, conclusions, and references presented in this manuscript remain the responsibility of the authors. The authors have reviewed and verified the content generated or assisted by AI tools to ensure its accuracy, relevance, and consistency with the research objectives and applicable legal framework. The final responsibility for the content and integrity of the manuscript rests entirely with the authors.

CC BY-SA 4.0

## REFERENCES


Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

AKERLOF, G. A. (1978). *15 - THE MARKET FOR "LEMONS": QUALITY UNCERTAINTY AND THE MARKET MECHANISM**The author would especially like to thank Thomas Rothenberg for invaluable comments and inspiration. In addition he is indebted to Roy Radner, Albert Fishlow, Bernard Saffran, Wil* (P. DIAMOND & M. B. T.-U. in E. ROTHSCHILD (eds.); pp. 235–251). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-214850-7.50022-X

Astuti, R. D., & Gunawan, G. (2024). Penanaman Modal Asing dan Penyerapan Tenaga Kerja di Provinsi Jawa Barat. *Jurnal Kebijakan Ekonomi Dan Keuangan*, *2*(2 SE-), 188–193. https://doi.org/10.20885/JKEK.vol2.iss2.art10

Auer, R. (2022). *Embedded Supervision : How to Build Regulation Into Decentralized Finance*. *2*(1), 1–48. https://doi.org/https://doi.org/10.21428/58320208.14a4105d

Bahtiar, M. Y. (2026). *Islamic Contract Architecture for Digital Deferred Payment : A Three-Layer Conceptual Framework for Shariah-Compliant BNPL Regulation*. *2*(2). https://doi.org/https://doi.org/10.67140/jhies.v2i2.19

Day, N., Paas, F., Kervin, L., & Howard, S. J. (2022). A Systematic Scoping Review of Pre-School Self-Regulation Interventions from a Self-Determination Theory Perspective. *International Journal of Environmental Research and Public Health*, *19*(4). https://doi.org/10.3390/ijerph19042454

Diva, I. A., Widnyana, C., Ayu, D., & Sawitri, D. (2026). Transformasi Kewenangan Bank Perekonomian Rakyat Pasca Diberlakukannya Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan (Uup2Sk). *Jurnal Media Akademik (JMA)*, *4*(2), 3031–5220. https://doi.org/https://doi.org/10.62281/m04rk542

Fajriawati. (2018). Analisis Pengaruh Tenaga Kerja Asing Terhadap Pertumbuhan Ekonomi Berdampak Pada Tingkat Pengangguran di Sumatera Utara Analysis of the Effect of Foreign Workers on Economic Growth Affects the Unemployment Rate in North Sumatra. *Ilmu Ekonomi Dan Studi Pembangunan*, *18*(2), 143–150. https://doi.org/https://doi.org/10.30596/ekonomikawan.v18i2.2531

Flora, H. S., Thuong, M. T. H., & Erawati, R. D. (2023). The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System . *Jurnal IUS Kajian Hukum Dan Keadilan*, *11*(1 SE-Articles), 113–125. https://doi.org/10.29303/ius.v11i1.1169

Friedman, L. M. (1975). *The Legal System: A Social Science Perspective*. Russell Sage Foundation. https://books.google.co.id/books?id=pvIWAwAAQBAJ

Habiburrahman Rizapoor. (2024). Fundamentals of Contract Law in Islamic Law and Afghanistan Civil Law. *Journal of Islamic Law and Legal Studies*, *1*(1 SE-Articles), 27–36. https://doi.org/10.70063/sharialex.v1i1.4

Hanung Widjangkoro. (2024). *Upaya hukum terhadap investasi*. *29*, 72–81. https://doi.org/https://doi.org/10.30742/perspektif.v29i2.938

Hardiyanti marzellina. (2022). *Urgensi otonomi desa dalam pengelolaan desa wisata berbasis pembangunan berkelanjutan*. *8*, 2356–4164. https://doi.org/https://doi.org/10.23887/jkh.v8i1.44410

Kurniawan Tri Wibowo. (2025). *Aspek Hukum dalam Dunia Digital*. Sada Kurnia Pustaka. https://books.google.co.id/books?id=MeB2EQAAQBAJ

Lendrawati, N., Hermana, M. A., & Royani, F. (2026). Analisis Perlindungan Bagi Konsumen Dalam Transaksi Digital Menggunakan Transaksi Digital cryptocurrency bitcoin. *JURNAL HUKUM SEHASEN*, *12*(1 SE-Articles). https://doi.org/10.37676/jhs.v12i2.10812

Maharani, C. (2025). Kepastian Hukum Aset Kripto Konsumen pada Perusahaan yang Ditolak Izin Perdagangannya oleh Otoritas Jasa Keuangan. *Krisna Law : Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, *7*(3), 1–22. https://doi.org/10.37893/krisnalaw.v7i3.1252

Muhammad Latifil Ansori, Murni Aisah, Nur Fitriah, & Muhammad Aji Purwanto. (2024). Contracts in the Sharia Context. *Al-Fadilah: Islamic Economics Journal*, *2*(2 SE-Articles), 70–79. https://doi.org/10.61166/fadilah.v2i2.36

Nurul Hidayati Indra Ningsih, S. E. M. M., Misnawati, S. H. M. H., Dr. Muthia Sakti, S. H. M. H., I Wayan Ordiyasa, S. K. M. T., Dadin Solihin, S. H. M. H., Dr. H. Firman Batari, S. H. M. H., Primasari, N. S., Dr. Cut Fadhlan Akhyar, S. H. M. M. M. H., Hilda Yuliastuti S. E, M. M. M. T., Areta Nur Fatimah Azalia, S. E. M. S., & others. (2025). *Hukum Ekonomi Digital: Regulasi Bisnis Di Era Teknologi*. PT. Nawala Gama Education. https://books.google.co.id/books?id=Km9mEQAAQBAJ

OECD, K. D. I. (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*. https://doi.org/https://doi.org/10.1787/8fa190b5-en.

Peryanto, J., Ria Napitupulu, D. W., Saragi, P., Penelitian, A., & Kunci, K. (2025). Perlindungan Hukum Bagi Pengguna Cryptocurrency Menurut UU No. 4 Tahun 2023 Tentang P2SK. Legal Protection for Cryptocurrency Users According to Law No. 4 of 2023 Concerning P2SK. *Jurnal Kolaboratif Sains*, *8*(5), 2432–2446. https://doi.org/10.56338/jks.v8i5.7576

Samsi Ridwan, M. (2026). Perlindungan Hukum Investor Ritel dalam Perdagangan Aset Keuangan Digital Pasca POJK Nomor 23 Tahun 2025. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *4*(2 SE-Articles), 1514–1546. https://doi.org/10.62976/ijijel.v4i2.1829

Saputra, T. T., & Sulistiyono, A. (2024). Upaya Hukum Perlindungan Investor dari Potensi Risiko Investasi Cryptocurrency di Indonesia. *Gema Keadilan; Vol 11, No 1 (2024): Gema KeadilanDO - 10.14710/Gk.2024.22908*. https://doi.org/https://doi.org/10.14710/gk.2024.22908


CC BY-SA 4.0

Saraswati Harsasi. (2026). *REGULASI KEGIATAN USAHA BULION*. Damaro Researchain. https://books.google.co.id/books?id=-jnWEQAAQBAJ

Setiawan, M. D., & Babussalam, A. B. (2026). *PERLINDUNGAN HUKUM ATAS PEMUTUSAN RELASI KERJA DALAM GIG ECONOMY MENURUT TEORI PHILIPUS M . HADJON A . Pendahuluan Transformasi dunia kerja sebagai dampak perkembangan ekonomi digital telah mengubah secara fundamental pola hubungan kerja yang selama ini d*. *8*(April), 59–79. https://doi.org/https://doi.org/10.31949/jpl.v8i1.17501

Stinchcombe, A. L. (1977). Lawrence M. Friedman, The Legal System Donald Black, The Behavior of Law. *Law & Society Review*, *12*(1), 129–131. https://doi.org/DOI: 10.1017/S0023921600024324

Sukamulya, S., & Kusuma, V. T. (2026). Liquidity and Market Microstructure of Tokenized Carbon Assets Trading in Blockchain-Based Voluntary Carbon Markets: A Mean-Centered MMRM with HAC Corrections. *Journal of Risk and Financial Management*, *19*(5). https://doi.org/10.3390/jrfm19050331

Tilles, P. F. C., Ferreira, F. F., Francisco, G., Pereira, C. de B., & Sarti, F. M. (2011). A Markovian model market—Akerlof's lemons and the asymmetry of information. *Physica A: Statistical Mechanics and Its Applications*, *390*(13), 2562–2570. https://doi.org/https://doi.org/10.1016/j.physa.2011.03.007

Tlili, H. (2025). Blockchain and tokenized carbon markets: Empirical evidence on market efficiency and transaction dynamics. *Sustainable Futures*, *10*, 101109. https://doi.org/https://doi.org/10.1016/j.sftr.2025.101109

Utomo, D. K. S., & Pulungan, A. R. (2023). Ekowisata Mangrove dalam Pariwisata Berkelanjutan di Sumatera Utara. *Masyarakat Pariwisata : Journal of Community Services in Tourism*, *4*(2016), 46–60. https://doi.org/10.34013/mp.v4i2.1393

Waratmaja, M., & Istiqomah, M. R. (2026). Peralihan Kewenangan Regulasi Aset Kripto Di Indonesia Dari Bappebti Kepada Otoritas Jasa Keuangan dan Bank Indonesia. *Jurnal Paris Langkis*, *6*(2 SE-), 259–270. https://doi.org/10.37304/parislangkis.v6i2.24700

Wardah Yuspin, & Arief Wicaksono. (2023). *Telaah Yuridis Perlindungan Konsumen Dalam Kegiatan Investasi Aset Kripto Di Indonesia*. *19*, 85–98. https://doi.org/https://doi.org/10.30996/dih.v19i1.7886

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/https://doi.org/10.6028/NIST.IR.8202

CC BY-SA 4.0