

The Legal Vacancy of Consumer Protection in Smart Contract Execution: A Substantive Justice Approach

Totok Catur Wismo Malaicanto

Faculty of Law, Universitas Borobudur, Indonesia, E-mail: kkptotok@gmail.com

Abstract. *The Web3 digital economic transformation presents smart contracts that operate autonomously and decentralized based on the doctrine of "Code is Law." The immutable nature of these algorithms creates a legal paradox because it eliminates the obligation of good faith and cripples consumer protection, especially when virtual defaults occur, such as the practice of Rug Pull. This normative legal research aims to analyze the legal gaps in the Consumer Protection Law (UUPK), the ITE Law, and the PDP Law, and formulate a reconstruction of protection based on substantive justice. The research results show that agreements in smart contracts are vulnerable to defects of will (wilsgebrek), and the architecture that rejects refunds is a form of obfuscation by code that is null and void according to Article 18 of Law No. 8 of 1999. The immutable nature also conflicts with the right to data deletion in the Personal Data Protection Law. As crypto oversight shifts to the Financial Services Authority (OJK), problem solving demands a Fairness-by-Design approach. This research recommends mandatory Smart Contract Escrow, integrated Online Dispute Resolution (ODR), and the implementation of off-chain storage. This architectural imposition is justified by the Government's authority in Article 40A of Law No. 1 of 2024 for the sake of a fair digital ecosystem.*

Keywords: *Consumer Protection; Financial Services Authority; Obfuscation by Code; Smart Contract; Virtual Default.*

1. Introduction

The global economy is currently undergoing radical disruption as a result of the rapid development of information and communication technology. The digital economy, previously dominated by centralized platform architecture (Web2)—such as e-commerce platforms and the gig economy—is now slowly shifting toward a decentralized ecosystem (Web3) driven by Distributed Ledger Technology (DLT), or blockchain. Historically, blockchain technology was initially designed exclusively to facilitate cryptocurrency transactions, enabling them to operate without a central authority. However, over time, this technology has mutated into a far more complex financial and commercial infrastructure, one of the most crucial innovations being smart contracts.

Smart contract It is essentially a computer algorithm protocol designed to automatically verify, monitor, and execute the rights and obligations of parties according to pre-coded "if-then" conditional logic. This innovation offers absolute efficiency by eliminating the need for intermediaries or third parties (such as banks, notaries, or intermediary platform providers), reducing transaction costs, and facilitating instantaneous execution across geographic jurisdictions.

In practice, smart contract implementation is no longer just a theoretical discourse but has been adopted in various sectors of the digital economy. Globally, this technology is applied in Decentralized Finance (DeFi) platforms like Aave and Compound, which autonomously execute loans and provide liquidity without the need for credit bureaus or traditional banks. Furthermore, smart contracts are used as automated escrow systems in real estate transactions, supply chain management, and even cross-border remittances, where funds are held and only released by the system once the remittance conditions have been met.

In Indonesia, smart contract adoption has begun to be implemented on a commercial scale and in pilot projects. A concrete example of this application is the use of blockchain-smart contracts to facilitate the secure recording and transactions of Non-Fungible Tokens (NFTs) by corporations such as PT. Saga Riung Investama. Furthermore, the implementation of this technology has also begun to penetrate the traditional capital market sector through asset tokenization initiatives on the Indonesia Stock Exchange (IDX). This widespread implementation demonstrates that smart contracts have effectively bound the financial rights and obligations of people across various sectors.

However, despite their technological efficiency and widespread implementation, smart contracts are simultaneously fundamentally disrupting the conventional contractual legal order, particularly in terms of consumer protection. Contract law in Indonesia, rooted in the Civil Code (*Burgerlijk Wetboek* or *KUHPerdata*), is a 19th-century Dutch legal legacy that was ontologically designed to regulate physical transactions and conventional agreements between individuals.

The fundamental characteristic of smart contracts rests on the "Code is Law" doctrine, which assumes that a sequence of programming codes is the absolute manifestation of the will of the parties. Once a smart contract is deployed onto a blockchain network and executed, it becomes immutable (absolute, unable to be changed, prevented, or deleted). This mechanical execution greatly upholds the principle of *Pacta Sunt Servanda* (a binding agreement as law). Unfortunately, this creates a fatal legal anomaly: algorithmic machines are oblivious to emergencies and lack the conscience to accommodate the principle of good faith (*goede trouw*) as required by Article 1338 of the Civil Code.

This legal anomaly has a direct impact on the loss of equal bargaining power between developers on the one hand and consumers (retail users) on the other. According to Law No. 8 of 1999 concerning Consumer Protection (UUPK), consumer rights protection is based on justice, balance, and legal certainty. Article 18 of the UUPK expressly prohibits businesses from including standard clauses that shift responsibility or refuse to refund consumers' money.

In the smart contract ecosystem, these standard, prohibitive clauses mutate into what's known as "obfuscation by code." Unfair clauses no longer exist as passive text written on paper, but instead become algorithmic functions that actively and instantly execute losses without the consumer's knowledge. Extreme manifestations of this practice are seen in the ability of code functions to unilaterally freeze assets, shift absolute liability in the event of a network hack, and modify contract logic without consent (as occurred in the Parity Wallet hack). At the same time, conventional courts lose their enforceability when confronted with the immutable nature of blockchain architecture, which precludes the intervention of external legal decisions.

Furthermore, electronic consent provided by consumers to enter into smart contracts (for example, by clicking an agreement or signing a cryptographic transaction) is highly susceptible to being classified as consent containing a defective will (*wilsgebreken*). Extreme information asymmetry regarding programming languages often results in consumers being misled (*dwaling*) or even potentially becoming victims of abuse of circumstances (*misbruik van omstandigheden*). In addition to the impasse in contract law and the Consumer Protection Law, the immutable architecture of smart contracts also directly conflicts with the privacy law regime, namely Law No. 27 of 2022 concerning Personal Data Protection (PDP Law).

The urgency of this legal anomaly becomes even more undeniable when examining the concrete manifestations of virtual breach of contract that have claimed many victims in the digital economy sector. Indonesia's platform economy, projected to reach a transaction value of Rp500 trillion by 2025, has become fertile ground for complex electronic contract disputes. One crucial empirical precedent is the transaction dispute on the e-commerce platform Tokopedia, which was heard at the Jakarta Commercial Court in 2025. In this case, the breach of contract occurred in the form of delayed and failed delivery of goods, caused purely by system overload and an error in the automated warehouse algorithm during the 11.11 promotion period. The court ruled in favor of the consumer for Rp50 million in damages and affirmed joint and several liability between the seller and the platform. This case clearly demonstrates that algorithmic failure can result in real financial losses, requiring a redefinition of the conventional concept of breach of contract.

Furthermore, in the context of decentralized architectures or more immutable smart contracts, consumer vulnerabilities are brutally manifested through hacking and code manipulation incidents. The most monumental example of the dangers of unilateral modification clauses and code obfuscation is the Parity Wallet incident. In that incident, the developer discovered a flaw in the algorithm's functionality that allowed for unilateral mid-process modification of the contract's logic, ultimately resulting in mass asset freezes without user consent. Due to the inherently immutable nature of smart contracts, consumers whose funds are locked and harmed lack legal remedies like those in conventional courts, placing the "Code is Law" doctrine as a shield that legitimizes machine-driven exploitation.

Furthermore, the imbalance in bargaining power caused by algorithms has also spread to digital wallets and the gig economy. Cases such as overcharging on GoPay, which triggered oversight and administrative sanctions from the Financial Services Authority (OJK), and unilateral tariff determination driven by global positioning (GPS) algorithms in ride-hailing apps like Gojek, highlight the lack of transparency in machine-driven decision-making. This phenomenon confirms that default in the digital era is no longer limited to human error but has evolved into a systemic algorithmic failure that exploits consumer information asymmetries. This series of real-life cases demonstrates that the Civil Code (*Burgerlijk Wetboek*), designed for physical transactions, is beginning to experience a deficit in its grip if the protection architecture is not immediately injected directly into the code (*Fairness-by-Design*).

In response to these complex dynamics, an institutional paradigm shift has occurred in Indonesia. Since January 2025, the regulatory and supervisory authority for digital and crypto financial assets has officially shifted from the Commodity Futures Trading Regulatory Agency (Bappebti) to the Financial Services Authority (OJK), implemented through POJK No. 27 of 2024. This transition is not merely an administrative change, but rather a philosophical legal transformation, with the OJK holding a holistic mandate centered on consumer protection. When analyzed using Legal Protection Theory and Progressive Legal Theory, current legal instruments suffer from "ontological blindness" when passively applied to blockchain technology. Therefore, this research focuses on reconstructing consumer protection in digital contract execution through a substantive justice approach with a *Fairness-by-Design* dimension, so that justice can be injected directly into the smart contract algorithm architecture.

2. Research Methods

2.1. Type of Research

This study employs doctrinal legal research. Normative legal research positions law as a system of interrelated written norms, principles, and dogmas. This type of research was chosen because the primary focus of the study is the anomalies and legal vacuums that occur within Indonesian positive law when confronted with the decentralized and autonomous characteristics of smart contracts. The analysis focuses on synchronizing laws and regulations and discovering new legal principles to address the dynamics of virtual breach of contract in the digital economy ecosystem.

2.2. Research Approach

In order to obtain a sharp and comprehensive analytical knife, this research collaborates three problem approaches at once, namely:

1. Statute Approach:

This approach is carried out by holistically and systematically examining the hierarchy of positive regulations in Indonesia that directly relate to the research object. The regulations analyzed in depth include the Civil Code (KUHPerdata), specifically Book III on Contracts; Law No. 8 of 1999 concerning Consumer Protection (UUPK); Law No. 1 of 2024 concerning the Second Amendment to the ITE Law; Law No. 27 of 2022 concerning Personal Data Protection (UU PDP); and Financial Services Authority Regulation (POJK) Number 27 of 2024.

2. Conceptual Approach:

This approach is used to examine the doctrines and views of legal scholars developing within the fields of contract law, consumer protection, and digital technology. Concepts critically analyzed include the "Code is Law" doctrine, the obfuscation-by-code doctrine, the Theory of Legal Protection, and the application of Fairness-by-Design to find a balance between machine automation and the principle of good faith.

3. Comparative Approach:

This approach is used to compare the legal regulatory framework and consumer protection governance practices in other jurisdictions. This research specifically refers to the legal framework in the European Union, such as the principles in the Digital Fairness Act (DFA), the protection of data subjects' rights in the General Data Protection Regulation (GDPR), and cross-border online dispute resolution (ODR), to identify relevant regulatory adoption models for implementation in Indonesia.

2.3. Sources of Legal Materials

In line with the type of normative legal research, the data used comes from library research which is classified into three types of legal materials:

1. Primary Legal Materials:

It is an authoritative and binding legal material, consisting of the 1945 Constitution of the Republic of Indonesia; the main legal instruments (Civil Code, UUPK, ITE Law, and PDP Law); as well as sectoral regulations such as POJK No. 27/2024 and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

2. Secondary Legal Materials:

This material provides explanations of primary legal materials, including literature, academic papers, dissertations, conference proceedings, and national and international indexed scientific journal articles that focus on the study of smart contracts, blockchain, and consumer protection in the digital era.

3. Tertiary Legal Materials:

In the form of supporting legal materials that provide guidance and explanations of primary and secondary legal materials, such as the Legal Dictionary, the Big Indonesian Dictionary (KBBI), a glossary of cyber law terms, and an encyclopedia.

2.4. Techniques for Collecting and Analyzing Legal Materials

All legal materials were collected through comprehensive literature review and document searches, both from online legal databases and printed literature. After data collection, the legal materials were verified, classified, and analyzed using qualitative techniques with a descriptive-prescriptive approach. Descriptive analysis was used to map the legal vacuum and current operational challenges of smart contracts. Prescriptive analysis was applied to provide legal arguments, theoretical justification, and formulate dispute resolution reconstruction models (such as Escrow obligations and Decentralized Arbitration) to provide equitable consumer protection in the platform economy ecosystem.

3. Results and Discussion

3.1. Legal Analysis of Smart Contracts: Clash of Consensualism Principles and Defective Will

From a civil perspective, smart contracts are a digital transformation of agreements subject to Book III of the Civil Code. Formally, this protocol fulfills the four requirements for a valid agreement as stipulated in Article 1320 of the Civil Code: (1) Agreement through private key authentication; (2) Digital wallet ownership; (3) Specific objects via "If-Then" logic parameters; and (4) Lawful cause.

However, absolute adherence to the *Pacta Sunt Servanda* principle creates a paradox because it eliminates the Principle of Good Faith (Article 1338 paragraph 3 of the Civil Code). Furthermore, the consent given by consumers when clicking or signing cryptographic transactions is highly susceptible to being categorized as flawed will (*wilsgebrek*). Lack of understanding by ordinary consumers regarding smart contract programming languages leads to *dwaling* (misleading/mistaking) regarding the substance of the contract. Furthermore, the severe information asymmetry between developers and consumers opens up opportunities for *misbruik van omstandigheden* (abuse of circumstances).

From a procedural legal perspective, the existence of smart contracts is strongly legitimized through Article 5 paragraph (1) of the ITE Law, which establishes electronic information as valid legal evidence. Every interaction is documented chronologically with time stamping. However, the main challenge shifts to the litigation process. Smart contracts, which consist of lines of code, are difficult for conventional judges to read, so courts often require digital forensic experts.

3.2. The Form of "Obfuscation by Code" and the Implications of the Legal Vacancy of the UUPK

Positive consumer protection law in Indonesia has reached a deadlock when dealing with smart contract algorithms. The Consumer Protection Law strictly prohibits business actors from creating Standard Clauses that state the transfer of responsibility or the right to refuse the return of money (refunds) through Article 18 paragraph (1) letters a and c.

In smart contracts, these standard clauses transform into obfuscation by code, where the unfair clause is no longer passive text but rather an active, hidden algorithmic function. This manifests in three extreme forms:

1. Function of Unilateral Asset Freeze: The code allows developers to unilaterally freeze consumer funds in digital wallets in the event of a dispute.
2. Code Disclaimer Clause: Terms and conditions that force consumers to bear all financial losses due to bugs or hacks in the smart contract system.
3. Unilateral Modification Clause: The ability of developers to change the business logic of contracts (such as the Parity Wallet hack incident) without user consent.

Such clauses/codes are de jure null and void under Article 18 paragraph (3) of the Consumer Protection Law. Unfortunately, the absence of an intermediary authority in the blockchain means that a court's decision to annul a clause cannot be forcibly injected into an algorithmic system that has already been executed.

3.3. Mapping Legal Responsibilities and Conflicts with the Personal Data Protection Law

The immutable nature of blockchain creates a structural conflict with Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law guarantees data subjects the right to erase their personal data (the right to erasure). Blockchain architecture technically prevents the exercise of this constitutional right.

To establish legal liability, the data protection regime requires a functional classification between Data Controllers and Data Processors. In a decentralized ecosystem, determining who is responsible becomes complex. However, legally, developer entities or Decentralized Autonomous Organization (DAO) governance holders who determine the purposes and methods of data processing (such as multisig holders) should be qualified as Joint Controllers. Meanwhile, Decentralized Application (dApp) providers or node operators (validators) who simply execute instructions are considered Data Processors.

3.4. Virtual Breach of Contract and the OJK Authority

The development of the platform economy, valued at hundreds of trillions of rupiah, has given rise to a phenomenon known as Virtual Breach of Contract. This breach of contract does not always involve individual broken promises, but rather systemic algorithm failures, manipulation of fake reviews, and even force majeure cyberattacks (such as DDoS attacks) that lead to the failure of goods/services distribution. In this context, platform providers and smart contract developers can be held jointly and severally liable under Articles 1365 and 1367 of the Civil Code if their algorithmic systems fail to execute their obligations properly.

The shift in authority from Bappebti to the Financial Services Authority (OJK) as of January 2025 provides a broader mandate regarding governance and consumer protection. The OJK has new protection instruments in collaboration with Law No. 1 of 2024 (Revised ITE Law):

1. Article 28 paragraph (1) of the ITE Law: Criminalize developers who distribute fake project whitepapers that result in material losses for consumers.
2. Article 18A paragraph (1) of the ITE Law: Bypassing the jurisdictional immunity of foreign developers by forcing them to comply with Indonesian law if their services target users from Indonesian jurisdictions.

3.5. Protection Reconstruction: Fairness-by-Design, Escrow, and ODR

In response to the aforementioned impasse, legal instruments must adopt a protective framework that is instilled from the system design phase, borrowing from the European Union's concept of Fairness-by-Design. This reconstruction includes:

1. **Escrow Smart Contract Obligations:** The OJK must require developers to design code with a time-lock feature. Consumer crypto funds will be temporarily held (automated escrow) and cannot be disbursed by the developer until the product or service has been verified and delivered.
2. **Integrated Online Dispute Resolution (ODR):** Just as its effectiveness on e-commerce platforms has been proven to reduce the burden on the courts by up to 70%, the smart contract ecosystem must provide a digital ODR facility in the form of Decentralized Arbitration. Settlement is conducted using a Multi-Signature Wallet, where the arbitrator has access to "force" the algorithm to return funds in the event of a virtual contract breach.
3. **Off-Chain Storage Implementation:** To comply with the right to data deletion in the PDP Law, consumer personal data must not be stored directly within the blockchain network, but rather on an external server (off-chain), while the blockchain only stores its cryptographic hash value.

This legal-by-design architecture enforcement model is fully justified by Article 40A of Law No. 1 of 2024. This article affirms the Government's attributive authority to order Electronic System Providers to make system adjustments or add software features to create a fair and secure digital ecosystem.

3.6. Conceptual and Comparative Review: EU Regulation Adoption Model for Indonesia

In formulating an adaptive consumer protection model in Indonesia, a conceptual and comparative approach that references the European Union legal framework provides a very comprehensive foundation. Three key EU regulatory instruments are highly relevant for adaptation to Indonesia's smart contract ecosystem and positive law:

1. **Fairness by Design Principles in the Digital Fairness Act (DFA)**The European Union is currently finalizing the Digital Fairness Act (DFA), which focuses on protecting consumers from manipulative digital interface designs (dark patterns), addictive design, and unfair personalization practices. The DFA's conceptual approach is based on design-based regulation and ecosystem-based regulation. As a model for adoption in Indonesia, the Financial Services Authority (OJK) and the Ministry of Communication and Information Technology can mandate the Fairness by Design principle for smart contract developers. Under this principle, fairness is not only regulated on paper but must be embedded directly into the code architecture. For example, adopting the obligation to provide an "easy cancellation facility" or the right to refuse personalization through a standard, consumer-friendly privacy button to prevent financial losses due to unilateral contract extensions.
2. **Protection of Data Subject Rights through the General Data Protection Regulation (GDPR)**The immutable nature of smart contracts significantly conflicts with data subjects' rights, particularly the right to be forgotten or erased, which are guaranteed by both the GDPR and Indonesia's Personal Data Protection Law (PDP Law). The EU's

GDPR conceptual framework resolves this tension by defining functional responsibility boundaries. Protocol developers or Decentralized Autonomous Organization (DAO) governance holders are positioned as Data Controllers, while derivative service providers (oracles) act as Data Processors. For implementation in Indonesia, the PDP Law could adopt this European-style privacy-by-design solution by prohibiting the storage of raw personal data on the blockchain. Mandatory technical solutions include: off-chain storage, crypto-shredding, and the use of Zero-Knowledge Proofs (ZKPs), which allow systems to verify data without exposing consumers' true identities to the public network.

3. Cross-Border Online Dispute Resolution (ODR) The emergence of virtual breaches of contract, where code fails to execute its obligations properly, necessitates the establishment of a rapid, cross-jurisdictional dispute resolution framework. In the European Union, consumer rights disputes related to smart contracts are efficiently managed through Alternative Dispute Resolution (ADR) mechanisms and Online Dispute Resolution (ODR) platforms, which reduce the costs and time of conventional litigation. This model is highly relevant for implementation in Indonesia. Integration of the ODR system, based on UNCITRAL standards, can be adopted by granting technical authority to the Consumer Dispute Resolution Agency (BPSK) to mediate disputes on e-commerce platforms and crypto exchanges. Furthermore, adopting the principles of the EU Data Act, Indonesia needs to require that every operating smart contract have an emergency kill switch (circuit breaker) and a third-party verifiable audit trail. This ensures that if a dispute is brought to the ODR platform, the smart contract can be paused to preserve consumer assets.

The legal basis for the state to enforce the above architecture rests on Article 40A of Law No. 1 of 2024 (Revised ITE Law). This article grants the government attributive authority to order Electronic System Providers to adjust their systems or add specific software features to create a fair, accountable, and secure digital ecosystem.

4. Conclusion

Based on the legal and comparative analysis that has been described, three main conclusions can be drawn:

1. The formal status of smart contracts is valid and binding, like electronic agreements, based on Article 1320 of the Civil Code and Article 5 paragraph (1) of the ITE Law. However, absolute adherence to algorithms creates a paradox that paralyzes the principle of good faith (*goede trouw*). This results in electronic consent given by consumers being highly susceptible to defects in will (*wilsgebreken*), particularly in the form of error (*dwaling*) and abuse of circumstances due to the asymmetry of programming language information.

2. The immutable and self-executing characteristics of smart contracts create a fatal legal vacuum in the Consumer Protection Law and the Personal Data Protection Law. Standard clauses that prohibit them transform into code obfuscation—such as unilateral asset freezing and automatic refund denial—which are technically difficult to overturn by conventional court decisions. Furthermore, the permanent nature of blockchain data directly conflicts with the right to data erasure guaranteed in the Personal Data Protection Law.

3. With the transfer of crypto regulatory authority to the Financial Services Authority (OJK) as of January 2025, consumer protection instruments can no longer rely solely on a repressive approach. Facing the dynamics of virtual defaults, Indonesia is pressing for the adoption of Fairness by Design and Privacy by Design models that align with the European Union's Digital Fairness Act (DFA) and GDPR standards. Fairness must be embedded within the algorithm's architecture through mandatory Smart Contract Escrow features, cross-border Online Dispute Resolution (ODR) mechanisms based on multi-signature wallets, and off-chain data storage. In order to address the legal vacuum and build a fair digital economic ecosystem, the following recommendations are suggested:

1. For Regulators (OJK and Ministry of Communication and Information):

Immediately formulate an OJK Regulation (POJK) derived from POJK No. 27 of 2024 that specifically regulates smart contract operational standards. This regulation must include a "blacklist" of exploitative algorithmic code functions, mandate the implementation of Smart Contract Escrow, and require developers to conduct code audits (smart contract audits) through a certified independent institution before launching to the public.

2. For Developers (Web3 Developers and Entities):

To create a truly technically secure and legally protected Escrow Smart Contract, its design must not rely solely on lines of code but must combine technical risk mitigation with legal compliance. Furthermore, developers are required to comply with the Privacy-by-Design Act by adopting a Privacy-by-Design architecture. Consumer personal data must not be stored on-chain, but must instead use an external server (off-chain storage) or implement a mechanism for permanently destroying decryption keys (crypto-shredding) to facilitate consumer erasure rights.

3. For the Judicial Body and BPSK:

The Supreme Court and the Consumer Dispute Resolution Agency (BPSK) are recommended to immediately integrate a robust Online Dispute Resolution (ODR) system. Furthermore, judicial institutions should begin fostering collaboration with blockchain forensic experts to comprehensively interpret smart contract evidence in addressing virtual defaults.

5. References

Journals:

- Baso, F., Yusuf, D. U., Djaoe, A. N. M., Iswandi, I., & Ramadhany, A. (2024). The overview of smart contract: Legality and enforceability. *Dialogia Iuridica*, 16(1), 96–111.
- Dewi, D. C., Amelia, D., Pratama, F. R., Shidiq, F., & Ferdansyah, F. (2024). Tanda Tangan Elektronik sebagai Solusi Hukum Perikatan dalam Era Digital di Indonesia. *Letterlijk*, 1(2), 145–156.
- Fior, M. (2024). Towards a New Era of Digital Payments: Blockchain, Global Standards and the Future of Finance. *Crypto Valley Research Journal* 2024.

- Forbes, L. (2023). Consumer Protection In the Face of Smart Contracts. *Loyola Consumer Law Review*, 34(1), 45.
- Girsang, F. H. S., Sijabat, C. R., & Rahmadanti, S. M. (2025). Analysis of Consumer Legal Protection Against Unfair Clauses in Smart Contracts in Indonesia. *Jurnal Hukum*, Volume VI, Nomor 1.
- Harianja, S. A. H., Mujiburrohman, & Satya, A. M. (2026). Smart Contract Integration in Indonesian Law: Legal Certainty and Data Protection in the Digital Age. *Perspektif Hukum*, 26(1), 34-65.
- Kadly, E. I., Rosadi, S. D., & Gultom, E. (2021). Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. *Jurnal Sains Sosio Humaniora*, 5(1), 199–212.
- Kępczyński, P., & Napieralska, A. (2024). Smart Contracts in Financial Security: A Legal Analysis in the Context of Traditional Finance and DeFi. *Crypto Valley Research Journal 2024*.
- Levi, S. D., & Lipton, A. B. (2022). An Introduction to Smart Contracts and Their Potential and Inherent Limitations. *Harvard Law School Forum on Corporate Governance*.
- Lim, W., Angkasa, S., & Wibowo, A. D. P. (2024). Smart contracts: Validitas hukum dan tantangan di masa depan Indonesia. *Jurnal Kewarganegaraan*, 8(1), 829–837.
- Pendang, S. R. (2025). The Doctrine of Unlawful Acts in E-Commerce Consumer Protection. *Journal of Law and Economics*, 4(2), 193–201.
- Saputri, F. A. (2024). Regulating the use of smart contract in Indonesia. *Jurnal Hukum dan Keadilan*, 1(2), 42–50.
- Tanchangya, T., Sarker, T., Rahman, J., Islam, M. S., Islam, N., & Siddiqi, K. O. (2025). Mapping Blockchain Applications in FinTech: A Systematic Review of Eleven Key Domains. *Information*, 16(769).
- Wahyuni, H. A., Naili, Y. T., & Ruhtiani, M. (2023). Penggunaan smart contract pada transaksi e-commerce dalam perspektif hukum perdata di Indonesia. *Jurnal Hukum In Concreto*, 2(1), 1–11.
- Widjaja, G. (2026). The Evolution of Contract Law in the Digital Age: The Challenges of Electronic Contracts, Virtual Breaches of Contract, and Consumer Protection in the Platform Economy. *International Journal of Financial Economics (IJEFE)*, 2(10), 141-151.

Books:

- Busch, C., Fletcher, A., & Ledger, M. (2026). *Towards an EU Consumer Law Fit for the Digital Age Report*. Centre on Regulation in Europe (CERRE).
- De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

Hadjon, Philipus M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: Bina Ilmu.

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Rahardjo, Satjipto. (2009). *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing.

Subekti. (2005). *Hukum Perjanjian*. Jakarta: Intermasa.

Regulation:

Civil Code (Burgerlijk Wetboek).

Financial Services Authority Regulation Number 27 of 2024 concerning the Implementation of Digital Financial Asset Trading, Including Crypto Assets.

Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions.

Law No. 27 of 2022 concerning Personal Data Protection.

Law No. 4 of 2023 concerning the Development and Strengthening of the Financial Sector.

Law No. 8 of 1999 concerning Consumer Protection (State Gazette of the Republic of Indonesia 1999 Number 42).

The 1945 Constitution of the Republic of Indonesia.