PERSPEKTIF HUKUM

Volume 26 Issue 1 Mei 2026

SMART CONTRACT INTEGRATION IN INDONESIAN LAW: LEGAL CERTAINTY AND DATA PROTECTION IN THE DIGITAL AGE

Syahban Alvian Hamonangan Harianja [1]✉, Mujiburrohman[2], Adhika Mahindra Satya[3]

[1] Master of Law, Faculty of Law, Universitas Airlangga, Surabaya, Indonesia, Email: syahban.alvian.hamonangan-2024@fh.unair.ac.id
[2] Master of Law, Faculty of Law, Universitas Airlangga, Surabaya, Indonesia, Email: mujiburrohman-2024@fh.unair.ac.id
[3] Master of Law, Faculty of Law, Universitas Airlangga, Surabaya, Indonesia, Email: adhika.mahin.satya-2024@fh.unair.ac.id

✉ corresponding email: syahban.alvian.hamonangan-2024@fh.unair.ac.id

Article

Keywords:
Smart Contract, Contract Validity, Legal Certainty, Data Protection

Article History
Received: Oct 02, 2025;
Reviewed: May 10, 2026;
Accepted: May 16, 2026;
Published: May 19, 2026;

Abstract

Indonesia's digital economy ecosystem shows an increase in the adoption of blockchain and smart contracts. However, the Civil Code, the Electronic Information and Transactions Law, and the Personal Data Protection Law do not explicitly anticipate contracts executed by code, creating a legal vacuum in terms of definition, validity, technical standards, and governance of accountability. This study aims to (1) analyze the position and validity of smart contracts in Indonesia's civil law system; and (2) analyze legal liability and personal data protection in an immutable and decentralized ecosystem. The method employed is normative legal research, utilizing a legislative, conceptual, and comparative approach, with reference to European Union practices. The results show that the recognition of electronic information or documents and electronic

signatures provides a legal basis; however, the absence of clear definitions and minimum clauses weakens contractual certainty, especially in cross-border transactions. Blockchain records have high evidential value as long as reliability parameters accompany them. In the realm of personal data, the tension between data subject rights and immutability can be bridged through privacy by design/default, data minimization at the on-chain layer (off-chain identity), crypto-erasure options, and zero-knowledge proofs, with role mapping of controllers and processors based on functions and data protection impact assessment obligations. Recommendations include legal recognition of smart contracts along with mandatory clauses (choice of law/forum, ADR/ODR levels, escrow/circuit breaker), pre-deployment code audits, change management, and hybrid on-chain/off-chain dispute architecture, as well as the adoption of elements of EU practice (built-in legal/jurisdictional rules and minimum technical safeguards).

Copyright (c) 2025 All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions. Author(s) retain copyrights under the licence of Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).
https://doi.org/10.30649/ph.v26i1.446

Introduction

The ongoing digital transformation has reached a new milestone with the advent of distributed ledger technology or blockchain.[1] Initially designed to facilitate cryptocurrency transactions, blockchain has developed into a multifunctional digital architecture influencing business operations and governance systems alike.[2] Within Indonesia,

[1] Pratiksha Alhat, "Blockchain Technology," *International Journal of Scientific Research in Engineering and Management* 08, no. 04 (April 2024): 1–5, https://doi.org/10.55041/IJSREM30694.

[2] Marsela Thanasi-Boçe and Julian Hoxha, "Blockchain for Sustainable Development: A Systematic Review," *Sustainability* 17, no. 11 (May 2025): 1–38, https://doi.org/10.3390/su17114848.

the utilization of blockchain has significantly altered the landscape of the digital economy.[3] Among its prominent innovations is the smart contract, a self-executing computer program residing on the blockchain that performs designated tasks when predefined criteria are satisfied.[4] However, this disruptive innovation poses fundamental challenges to Indonesia's civil law framework, which is based on the Civil Code.[5] Under the *wils-theorie* and *uitings-theorie*, a contract attains legal validity only when the parties possess a sincere will and deliberately express their mutual agreement.

Smart contracts exhibit fundamental attributes analogous to traditional legal instruments, primarily due to their capacity for autonomous execution and enforcement of contractual stipulations through codified logic.[6] This principle boils down to the adage "code is law," which asserts that the code itself is the law, even though users do not always understand the substance of the agreement embedded in it.[7]

This theoretical tension manifests at Indonesia's normative level, exposing the inadequacy of its existing contractual framework. Article

---

[3] Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia," *Jurnal Studi Kebijakan Publik* 2, no. 1 (May 2023): 55–68, https://doi.org/10.21787/jskp.2.2023.55-68.

[4] Farhan Abel Septian Rachmadani and Sinta Dewi Rosadi, "Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia," *Jurnal Sains Sosio Humaniora* 5, no. 1 (June 2021): 650–64, https://doi.org/10.22437/jssh.v5i1.14838.

[5] Sakirman, Ma'ruf Akib, and Wahyudi Umar, "Kepastian Hukum Smart Contract Dalam Perspektif Hukum Perdata," *Rewang Rencang: Jurnal Hukum Lex Generalis* 5, no. 10 (2024): 1–11.

[6] Fabio Bassan and Maddalena Rabitti, "From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation," *Computer Law & Security Review* 55 (November 2024): 1–25, https://doi.org/10.1016/j.clsr.2024.106035.

[7] Cristina Argelich Comelles, "Smart Contracts o Code Is Law," *InDret* 2 (October 2020): 1–41, https://doi.org/10.31009/InDret.2020.i2.01.

1320 of the Civil Code stipulates the prerequisites for a valid agreement, which was never envisioned to accommodate consensus mechanisms codified into machine language. Furthermore, while Article 1338 establishes the binding nature of agreements (*pacta sunt servanda*), its absolute application is explicitly moderated by the overriding principle of good faith (*goede trouw*) in contractual execution.[8] This requisite for good faith introduces a subjective, flexible standard fundamentally at odds with the deterministic and automated enforcement of smart contracts.[9]

Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law), recognises electronic information, electronic documents, electronic signatures, and electronic agents as part of Indonesia's digital legal framework. However, the ITE Law has not yet provided an explicit legal construction for smart contracts as autonomous and self-executing contractual entities. At the same time, the immutable nature of blockchain technology creates an operational conflict with Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law), which grants data subjects several rights over their personal data, including the right to rectify and erase personal data. This tension demonstrates the need for a more adaptive legal framework that can reconcile the certainty of code-based execution with the protection of fundamental data subject rights. Viewed through Hadjon's theory of legal protection, this condition

[8] Jabalnur et al., "Perjanjian Di Bawah Tangan Ditinjau Dari Asas Pacta Sunt Servanda," *Halu Oleo Legal Research* 6, no. 2 (2024): 247–57, https://doi.org/10.33772/holresch.v6i2.848.

[9] Yudi Setiawan et al., "Pelaksanaan Pasal 1338 Ayat (1) (3) KUHPdt Tentang Kebebasan Berkontrak dan Itikad Baik dalam Pembiayaan Kendaraan Bermotor," Journal Kompilasi Hukum 5, no. 1 (2020): 154–74, https://doi.org/10.29303/jkh.v5i1.5.

reflects weaknesses in both preventive and repressive legal safeguards.[10] While Rahardjo's progressive law theory underscores the need for adaptive and human-centered legal reform.[11]

Previous legal scholarship has begun to map the complexities of smart contracts. Research by Inola Kadly, et.al., entitled: "Keabsahan Blockchain-Smart Contract dalam Transaksi Elektronik: Indonesia, Amerika dan Singapura", confirming that smart contracts can be read as electronic contracts based on Article 1320 of the Civil Code and the ITE Law. However, this study has not sufficiently addressed the post-execution legal consequences of smart contracts, particularly when code execution produces outcomes that differ from the parties' actual intent.[12]

Research by Willion Lim, et.al., entitled: "Smart Contracts: Validitas Hukum dan Tantangan di Masa Depan Indonesia", confirms that smart contracts are blockchain-based innovations that automatically execute agreements with the advantages of transparency, efficiency, and reduced transaction costs. Nevertheless, the study mainly emphasizes validity and future challenges, without constructing a comprehensive liability model for data protection failures in decentralized environments.[13]

---

[10] Edy Purwito, "Konsep Perlindungan Hukum Konsumen Dan Tanggung Jawab Hukum Pelaku Usaha Terhadap Produk Gula Pasir Kadaluarsa Di Kota Surabaya," *Jurnal Magister Ilmu Hukum* 13, no. 1 (June 2023): 114, https://doi.org/10.56943/dekrit.v13n1.152.

[11] Mardona Siregar, "Teori Hukum Progresif Dalam Konsep Negara Hukum Indonesia," *Muhammadiyah Law Review* 8, no. 2 (August 2024): 10, https://doi.org/10.24127/mlr.v8i2.3567.

[12] Eureka Inola Kadly et al., "Keabsahan Blockchain-Smart Contract dalam Transaksi Elektronik: Indonesia, Amerika dan Singapura," Jurnal Sains Sosio Humaniora 5, no. 1 (2021): 199–212.

[13] Willion Lim, Steven Angkasa, and Alexander Danelo Putra Wibowo, "Smart Contracts: Validitas Hukum Dan Tantangan Di Masa Depan Indonesia," *Jurnal Kewarganegaraan* 8, no. 1 (June 2024): 829–38, https://doi.org/10.31316/jk.v8i1.6410.

Research conducted by Shafaq Naheed Khan et.al., entitled: "Blockchain Smart Contracts: Applications, Challenges, and Future Trends", emphasise that there are two major trends in smart contracts, namely improvement (programming language, formal verification, performance, security, privacy) and cross-sector utilisation (finance, health, IoT, supply chain, philanthropy). Although this study provides a broad technological mapping of smart contract development, it does not specifically examine the doctrinal implications of smart contracts within Indonesia's civil law and data protection regime.[14]

The existing literature has not yet provided an integrated legal framework that simultaneously explains the contractual validity of smart contracts, their evidentiary value, the allocation of liability among decentralized actors, and the protection of personal data within an immutable blockchain architecture. This gap becomes more significant in Indonesia following the shift of crypto-asset regulatory and supervisory authority from the Commodity Futures Trading Regulatory Agency (hereinafter referred to as Bappebti) to the Financial Services Authority (hereinafter referred to as OJK). This regulatory transition requires a more comprehensive legal approach that does not merely treat crypto assets as tradable commodities, but also addresses consumer protection, financial innovation, systemic risk mitigation, data protection, and legal accountability in decentralized digital ecosystems. The novelty of this research lies in its construction of an adaptive legal model for smart contracts in Indonesia by integrating four dimensions: contractual validity under Article 1320 of the Civil Code, evidentiary recognition under the ITE Law, PDP Law, and dispute resolution mechanisms for code-based contractual failures.

---

[14] Shafaq Naheed Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends," *Peer-to-Peer Networking and Applications* 14, no. 5 (September 2021): 2901–25, https://doi.org/10.1007/s12083-021-01127-0.

This study examines the jurisprudential complexities of implementing smart contracts within the Indonesian legal system. Based on the research problems outlined above, this study has two main objectives: (1) to analyse the position, validity, and legal implications of smart contracts under Indonesian civil law, particularly in relation to the four requirements of Article 1320 of the Civil Code and the fundamental principles of contract law; and (2) to formulate a legal liability model, personal data protection framework, and dispute resolution mechanism for autonomous and immutable smart contract ecosystems, in order to balance the legal certainty offered by technological innovation with substantive justice and the protection of the fundamental rights of the parties.

Method

This research is normative legal research that applies statutory, conceptual, and comparative approaches. The statutory approach is used to examine relevant Indonesian legal instruments, particularly the Civil Code, Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 and Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and relevant regulations issued by the OJK. The conceptual approach is used to analyse legal concepts and doctrines relevant to smart contracts, including freedom of contract, pacta sunt servanda, good faith, the theory of will, the theory of statement, legal protection theory, progressive law theory, privacy by design, data minimisation, and accountability in decentralized digital ecosystems. The comparative approach is applied by examining

selected European Union legal frameworks and practices relating to data protection, controller–processor responsibility, smart contract governance, and dispute resolution, in order to identify regulatory models that may be adapted to the Indonesian legal context.

The legal materials used in this research consist of primary and secondary legal materials, collected through library research. Primary legal materials include statutes, government regulations, and sectoral regulations, while secondary legal materials include books, peer-reviewed journal articles, legal commentaries, conference proceedings, and other scholarly publications. These materials are analysed using descriptive-analytical and prescriptive methods to explain the current legal position of smart contracts in Indonesia and to formulate an adaptive legal framework that ensures contractual certainty, data protection, liability allocation, and effective dispute resolution in autonomous smart contract ecosystems.

Result and Discussion

A. Legal Position, Contractual Validity, and Evidentiary Value of Smart Contracts in Indonesian Civil Law

1. Blockchain Adoption and the Need for a Legal Framework

Indonesia's digital economy ecosystem is undergoing rapid transformation thanks to blockchain technology and crypto assets. Blockchain adoption has become a central legal and regulatory concern.[15] Throughout 2024, the total value of cryptocurrency transactions in Indonesia reached IDR 556.53 trillion,[16] signaling

[15] Tegar Dwi Fajriatama et al., "Penerapan Teknologi Blockchain Dalam Transformasi Keuangan Sebagai Tantangan Dan Peluang Di Era Digital," *EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi* 4, no. 3 (March 2025): 4799–807, https://doi.org/10.56799/ekoma.v4i3.6464.

[16] Sapto Andika Candra, *Melonjak, Transaksi Aset Kripto Sepanjang 2024 Capai Rp556,53 Triliun*, December 31, 2024, https://news.ddtc.co.id/berita/nasional/1807916/melonjak-transaksi-aset-kripto-sepanjang-2024-capai-rp55653-triliun.

widespread adoption across various segments of society and increased digital literacy as an important part of the future financial landscape. The legal framework for contracts in Indonesia (Civil Code/BW) is designed for agreements based on human will, not for autonomous code-based instruments.

Law No. 11 of 2008, in conjunction with Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE Law), does contain a definition of "electronic contract" in Article 1, point 17. However, the formulation is comprehensive and does not explicitly consider the characteristics of *smart contracts*, which are *self-executing*. There is a dogmatic tension when *smart contracts* are viewed through the perspective of the Theory of Will (*wilstheorie*) and the Theory of Expression (*uitingstheorie*), where deterministic execution by code tends to reflect objective statements. Conversely, the subjective will of the parties, especially in relation to defects of will such as *dwang* (coercion), *dwaling* (mistake), or *bedrog* (fraud), may not be accommodated in lines of code that are not easily accessible or understandable to users. Therefore, acceptance of the results of "code execution" cannot be equated with legal consensus, and must still be interpreted within the framework of the principle of good faith and *pacta sunt servanda* (Article 1338 of the Civil Code).

The mandate of Law No. 4 of 2023 concerning P2SK transfers the regulation and supervision of digital financial assets, including *cryptocurrency*, from Bappebti to OJK. This transfer is further regulated through POJK No. 3 of 2024 concerning the Application of Financial Sector Technology Innovation. The paradigm shift from "traded commodities" to "ITSK (Financial Sector Technology Innovation)-based financial products/services" necessitates a new focus on consumer protection, system stability, and risk mitigation, rather than solely on trading aspects.

From the perspective of Philipus M. Hadjon's Theory of Legal Protection, the need for more precise regulation of smart contracts is part of preventive protection. Rahardjo's Progressive Legal Framework

reinforces this humanistic orientation: the law should not be subject to technological determinism ("code is law") but must guarantee substantive justice and protection for the weaker party. Without a clear normative basis for smart contracts, developers and businesses face the risk of product cancellation or agreement invalidity. On the other hand, investors and millions of users lose confidence in protection during disputes or losses due to code defects. This regulatory gap weakens both market confidence and legal certainty.

2. Smart Contract Validity under Article 1320 of the Civil Code

From the perspective of Philipus M. Hadjon's Theory of Legal Protection, the need for more precise regulation of smart contracts is part of preventive protection. Rahardjo's Progressive Legal Framework reinforces this humanistic orientation: the law should not be subject to technological determinism ("code is law") but must guarantee substantive justice and protection for the weaker party. Without a clear normative basis for smart contracts, developers and businesses face the risk of product cancellation or agreement invalidity. On the other hand, investors and millions of users lose confidence in protection during disputes or losses due to code defects. This regulatory gap weakens both market confidence and legal certainty.

Article 1320 of the Burgerlijk Wetboek (Civil Code) stipulates four cumulative conditions that must be met by the parties in agreeing. The provisions of Article 1320 of the Civil Code form the basis for Article 46 paragraph (2) of Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), which states that an Electronic Contract is valid if it meets the four conditions above.

The following is an analysis of the fulfilment of these requirements of Article 1320 of the Burgerlijk Wetboek (Civil Code) in the context of smart contracts:

a. Agreement

An agreement refers to the expression of intent by the parties until mutual consent is reached. The expression of intent can be expressed verbally or through behavior or other means related to the parties' intentions.[17] In a smart contract, an agreement occurs between the parties mediated using private cryptographic keys.[18] To agree to a smart contract, users must click the "Agree" button in the application and then sign the transaction with their private key.[19] The Information, Technology, and Electronics Law regulates electronic signatures. However, from a civil law perspective, a valid agreement must be free from defects of consent (*wilsgebreken*), which include coercion (*dwang*), error (*dwaling*), and fraud (*bedrog*).[20]

The content of a smart contract agreement is presented as source code displayed on the application screen. Users do not have technical access to read, understand, or verify the code in the programming language; they can only interact through a simple interface based on the code's functionality.[21] This condition gives rise to the potential for misrepresentation. Users may agree to something different from what the code executes, which could be a bug or a hidden feature in the code. So, even though procedurally there appears to be an agreement, substantively the agreement is flawed and could lead to cancellation.

---

[17] Salim H.S., *Hukum Kontrak, Teori & Tekriik Penyusunan Kontrak* (Jakarta: Sinar Grafika, 2008).

[18] Korintus Wilson Horas Hutapea and Adi Sulistiyono, "Keabsahan Smart Contract Dengan Teknologi Blockchain Menurut Kitab Undang-Undang Hukum Perdata," *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 1, no. 3 (April 2024): 86–94, https://doi.org/10.62383/aliansi.v1i3.177.

[19] Mehmet Aydar et al., "Private Key Encryption and Recovery in Blockchain," version 2, preprint, arXiv, 2019, https://doi.org/10.48550/ARXIV.1907.04156.

[20] Sumriyah, "Cacat Kehendak (Wilsgebreken) Sebagai Upaya Pembatalan Perjanjian Dalam Persepektif Hukum Perdata," *Simposium Hukum Indonesia* 1, no. 1 (2019): 662–70.

[21] Christian Delgado-von-Eitzen et al., "Ethereum Blockchain Interconnectivity for Dynamic and Privacy-Preserving Access Control," *IEEE Access* 13 (2025): 112918–31, https://doi.org/10.1109/ACCESS.2025.3584429.

b. Competence

Article 1330 of the Civil Code states that parties who are not competent to make agreements are minors and those under guardianship. The legal consequence of an agreement made by an incompetent party is that it can be canceled (*vernietigbaar*).[22] In smart contracts related to blockchain, the identities of the parties in a transaction are represented solely by wallet addresses, which are a series of alphanumeric characters that provide no information about the age, status, or legal capacity of the owner.[23]

There is no built-in mechanism in blockchain technology to verify identity or age, so minors or legally incompetent persons can create or execute smart contracts without supervision.[24] Indonesian civil law requires an identity verification mechanism to ensure that the capacity requirement is met.[25] Therefore, there is a need to integrate a centralized identity solution for *Know YourCustomer* (KYC) verification in decentralized applications (*dApps)* operating in Indonesia.

c. A Specific Matter

Smart contracts have an advantage over conventional contracts in fulfilling specific elements. All clauses of the agreement, along with

---

[22] Ananda Bunga Neesya et al., "Tinjauan Yuridis Terhadap Syarat Keabsahan Perjanjian Dalam Hukum Kontrak Indonesia," *Causa: Jurnal Hukum Dan Kewarganegaraan* 14, no. 9 (2025): 31–40, https://doi.org/10.6679/ynwg9575.

[23] Saurabh Suratkar, Mahesh Shirole, and Sunil Bhirud, "Cryptocurrency Wallet: A Review," *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, September 28, 2020, 1–7, https://doi.org/10.1109/ICCCSP49186.2020.9315193.

[24] Yile Hong et al., "SNFM: Scalable Node Feature Modeling in Smart Contracts for Vulnerability Detection through Graph-Based Approaches," *2025 IEEE Global Blockchain Conference (GBC)*, June 20, 2025, 1–6, https://doi.org/10.1109/GBC60041.2025.11134470.

[25] Rahadian Kadafi, Rahmadi Indra, and Iwan Rachmad, "Kepastian Hukum Pembuatan Akta Perjanjian Kredit Digital Oleh Notaris," *JURNAL RECHTENS* 14, no. 1 (2025): 171–95, https://doi.org/10.56013/rechtens.v14i1.4200.

the rights and obligations of the parties, are defined with mathematical precision and logic as expressed in code, ensuring that the parameters of "specific matters" are fulfilled with a very high degree of certainty.[26]

d. Lawful Cause

According to Article 1320 of the Civil Code, the last requisite for a valid contract is the existence of a lawful cause, its purpose must not contravene legislation, moral norms, or public order. Failure to satisfy this condition results in the agreement being *void ab initio*. While the underlying smart contract code is technologically neutral, it remains susceptible to exploitation for illicit ends.[27] Smart contracts running on distributed global networks are a very difficult task. Although this requirement remains legally valid, its enforcement in the innovative contract ecosystem faces significant technical obstacles.

3. Smart Contracts as Valid Electronic Evidence According to the Electronic Information and Transactions Law and Civil Procedure Law

The evidentiary implications of smart contracts are significant, as they create a permanent, immutable performance record on a distributed ledger.[28] Indonesia's ITE Law supports this characteristic; Article 5, paragraph (1) grants electronic documents the standing of

---

[26] Judy Yueh Ling Song and Esther Tan, "Beyond Traditional Contracts: The Legal Recognition and Challenges of Smart Contracts in Malaysia and Singapore," *Journal of Law, Market & Innovation* 3, no. 3 (November 2024): 323–57, 4MB, https://doi.org/10.13135/2785-7867/11334.

[27] Ghassan Adhab Atiyah, Ahmed Ismael Ibrahim, and Ahmed Abdulkhudhur Jasim, "Enforcement of Smart Contracts in Cross-Jurisdictional Transactions," *International Journal of Law and Management*, ahead of print, November 29, 2024, https://doi.org/10.1108/IJLMA-06-2024-0220.

[28] Laila Alfina Mayasari Rizqi and Dedi Farera Prasetya, "Urgensi Penggunaan Smart Contract Dalam Transaksi Jual Beli Di E-Commerce," *Jurnal Hukum Lex Generalis* 3, no. 4 (April 2022): 327–38, https://doi.org/10.56370/jhlg.v3i4.247.

valid legal evidence (save for specific exceptions). Consequently, smart contracts are legally recognized as evidence of electronic agreements. This position is further substantiated by Article 6 of the ITE Law, which legitimizes electronic signatures and stamps, thereby underpinning the formal validity of all digital agreements in the Indonesian legal system.

Every intelligent contract interaction is documented chronologically with time-stamping and verified through network consensus, making transaction records difficult to falsify.[29] These characteristics make blockchain a highly reliable source of evidence. However, linking on-chain records to legal identities still needs off-chain verification.[30]

The transparency and reliability of blockchain evidence are very high, but contextual interpretation in the legal realm is still necessary. Although electronic evidence from smart contracts has been legally recognized as valid, there are practical challenges related to its readability and understanding by judges.[31] Smart contracts are written as code that is not as easy to understand as traditional legal contracts.[32] Article 11 of the ITE Law has opened up the possibility of using expert testimony, but the limited number of blockchain forensic experts in Indonesia is an obstacle. Therefore, strengthening the capacity of

---

[29] Zaleha Fauziah et al., "Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review," *Aptisi Transactions on Technopreneurship (ATT)* 2, no. 2 (August 2020): 160–66, https://doi.org/10.34306/att.v2i2.97.

[30] Zelin Su, "Evidentiary Value and Evidentiary Status of Blockchain Evidence," *The International Journal of Evidence & Proof* 29, no. 1 (January 2025): 58–76, https://doi.org/10.1177/13657127241238020.

[31] Muhammad Syafiq and Siti Nur Syifa, "Analisis Penggunaan Blockchain Untuk Meningkatkan Transparansi Dan Keamanan Data Pada Pembuktian Perceraian Di Pengadilan Agama," *Journal of Innovative and Creativity (Joecy)* 5, no. 2 (June 2025): 9662–72, https://doi.org/10.31004/joecy.v5i2.978.

[32] Adam Muko, "Kajian Smart Contract Dalam Perspektif Hukum Positif Di Indonesia," *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik* 2, no. 2 (January 2024): 13–24, https://doi.org/10.59581/doktrin.v2i2.2517.

judges and advocates in digital literacy is a crucial step to ensure the effectiveness of evidence.

B. Data Protection, Legal Liability, and Dispute Resolution in Immutable Smart Contract Ecosystems

1. The Dialectic of the Principle of Blockchain Immutability and Data Subject Rights as Regulated in the Personal Data Protection Law

Indonesia's digital economy ecosystem is undergoing rapid transformation thanks to blockchain technology and crypto assets. Blockchain adoption has become a central legal and regulatory concern.[33] Throughout 2024, the total value of cryptocurrency transactions in Indonesia reached IDR 556.53 trillion,[34] signaling widespread adoption across various segments of society and increased digital literacy as an important part of the future financial landscape. The legal framework for contracts in Indonesia (Civil Code/BW) is designed for agreements based on human will, not for autonomous code-based instruments.

The application of blockchain technology in smart contract transactions raises profound techno-legal dilemmas when juxtaposed with the regulatory framework for personal data protection.[35] Law No. 27 of 2022 on PDP establishes a comprehensive regime that grants individuals fundamental rights to control their personal data, including the right to rectify and erase data. This framework

---

[33] Fajriatama et al., "Penerapan Teknologi Blockchain Dalam Transformasi Keuangan Sebagai Tantangan Dan Peluang Di Era Digital."

[34] Candra, *Melonjak, Transaksi Aset Kripto Sepanjang 2024 Capai Rp556,53 Triliun*.

[35] Masripa Siti Zahra et al., "Integrasi Metadata Dan Teknologi Blockchain: Implikasi Hukum Terhadap Perikatan Di Indonesia," *Journal Customary Law* 2, no. 2 (April 2025): 10, https://doi.org/10.47134/jcl.v2i2.3951.

encounters structural incompatibility with the architectural principle of blockchain, which is immutable.

This tension stems from a fundamental incompatibility between blockchain's immutable by design architecture and the statutory rights conferred upon data subjects by the PDP Law.[36] Immutability is the foundation of blockchain security and integrity, ensuring that recorded transaction data cannot be altered, modified, or deleted, thereby fostering trust in a system that operates without a central authority. Conversely, the PDP Law explicitly confers upon data subjects the "right to rectification" (to correct erroneous data) and the "right to erasure" (to delete personal information), a concept analogous to the "right to be forgotten". These statutory rights fundamentally presuppose a data architecture that permits modification and deletion.[37] Reviewed from Hadji's Legal Protection Theory, this contradiction reflects the inadequacy of current legal guarantees. The inherently immutable architecture of blockchain prevents the exercise of legally guaranteed rights, leaving data subjects without effective remedies. This reflects both preventive and repressive failures of protection.

To overcome this dichotomy, a privacy by design approach is needed that integrates compliance mechanisms at the technology architecture level. Three main techno-legal models have emerged as attempts to mitigate this contradiction:

a. Off-Chain Storage

---

[36] Janaka Ishan Senarathna, "The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency and Security," preprint, Computer Science and Mathematics, April 22, 2025, https://doi.org/10.20944/preprints202504.1814.v1.

[37] Kurdi Kurdi and Joko Cahyono, "Perlindungan Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (December 2024): 330–39, https://doi.org/10.31289/juncto.v6i2.5443.

Personal data is stored externally (off-chain) while the blockchain only retains cryptographic hashes or pointers. This allows modification or deletion on external servers without compromising ledger integrity, consistent with the European Data Protection Board (EDPB) recommendations.[38]

b. Cryptographic Erasure (Crypto-Shredding)

Data remains encrypted on-chain, but "deletion" occurs by permanently destroying the decryption keys, rendering data inaccessible and effectively anonymized.[39]

c. Zero-Knowledge Proofs (ZKPs)

These mechanisms allow the verification of a statement's accuracy without disclosing the underlying data, embodying the principles of data minimization and privacy by default to prevent excessive processing from the outset.[40]

2. Legal Liability for Personal Data Breaches in Smart Contracts through the Identification of Data Controllers and Processors

The law should construct legal liability for personal data breaches in smart contracts by identifying the function of each actor within the blockchain ecosystem. Regulators should not treat protocol developers, dApp providers, oracle providers, wallet providers, infrastructure operators, validators, and governance participants

---

[38] Mongetro Goint, Cyrille Bertelle, and Claude Duvallet, "Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems," *Mathematics* 11, no. 7 (March 2023): 1592, https://doi.org/10.3390/math11071592.

[39] Dola Ramalinda, Jayadi, and Agung Rachmat Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," *Journal of International Multidisciplinary Research* 2, no. 6 (June 2024): 665–71, https://doi.org/10.62504/jimr679.

[40] Cristina Vilchez Moya et al., "Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain," *Applied Sciences* 13, no. 9 (April 2023): 5552, https://doi.org/10.3390/app13095552.

uniformly, because each actor may determine different purposes, means, and security measures in data processing. Therefore, the legal framework should adopt a functional approach to classify whether each party acts as a data controller, data processor, joint controller, or merely a technical participant in the network. This approach enables the law to allocate liability proportionally for code defects, security failures, improper on-chain data storage, or the absence of privacy-by-design mechanisms. Based on this framework, this section formulates a liability model under Indonesia's PDP Law. It uses the European Union's GDPR as a comparative reference to develop a clearer accountability structure in smart contract ecosystems.

a. Legal Liability for Personal Data Leaks in Smart Contracts in Indonesia

The PDP Law adopts a similar distinction of roles, placing the primary obligation on data controllers to ensure the legality, accuracy, security, and transparency of processing. This is accompanied by the obligation to notify data subjects of any failure to protect their data within a specified time limit.[41] Challenges arise when this regime is applied to smart contracts running on public blockchains. Determining the locus of responsibility becomes complicated because key roles are distributed among various actors, including protocol developers, dApp interface providers, infrastructure partners, oracle providers, wallet managers, and node operators. Therefore, the assessment must shift from the formal label of the entity to a substantive functional analysis. If a smart contract is developed,

[41] Predderics Hockop Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital Di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)," *Jurnal Esensi Hukum* 6, no. 2 (2025): 105–24, https://doi.org/10.35586/jsh.v6i2.412.

operated, and monetized by an entity, that entity should be positioned as the controller of the specified data flow.[42]

Decentralized autonomous organization (DAO) governance mechanisms in protocol management enable parties that set the objectives and processing methods, including the core development team, multisig signers, or token holders who approve the parameters, to become the de facto joint controllers. Meanwhile, dApp providers, oracles, and computing partners acting on the controllers' instructions function as processors.[43]

The framework of Hadjon's Theory of Legal Protection, the preventive dimension requires transparent and accountable derivative regulations, as well as a privacy-by-design obligation for every smart contract that processes personal data. Minimum security standards (strong encryption, key management, independent code auditing, vulnerability testing, and/or formal verification before deployment). The obligation of off-chain processing for identity data and the prohibition of embedding personal data in plaintext on the on-chain layer, the use of self-sovereign identity and verifiable credentials for dKYC that verifies attributes (such as age/competence) without expanding the data trail, and accountability mapping that documents "who did what" along the technical chain. The repressive dimension requires effective recovery channels, including individual compensation rights, the possibility of class actions, the processing of cessation orders, proportional administrative fines, and the

---

[42] Ivan Franko and Tsudzenko Y, "Assessment of the Efficiency of Using Smart Contracts for Intelligent Analysis of User Actions in Social Networks," *Artificial Intelligence* 29, no. AI.2024.29(4) (December 2024): 36–40, https://doi.org/10.15407/jai2024.04.036.

[43] Asma Alawadi et al., "Decentralized Autonomous Organizations (DAOs): Stewardship Talks but Agency Walks," *Journal of Business Research* 178 (May 2024): 114672, https://doi.org/10.1016/j.jbusres.2024.114672.

strengthening of dispute resolution relevant to the on-chain ecosystem.[44]

Drawing on the practice of smart contracts in Indonesian data-exchange platforms, this approach fits a model in which automated execution directly involves the processing of identity, location, cultivation, ecological, market, and transaction data. In this context, the law should determine legal responsibility based on the actual role of each party, not merely on its formal status. A platform provider or smart contract operator that determines the purpose and flow of data processing should act as a data controller. In contrast, parties that only process data based on instructions should act as processors. This functional approach prevents the automated nature of smart contracts from obscuring accountability when data misuse, system failure, or breach of contractual obligations occurs.[45]

This overall design prevents a legal vacuum due to unclear role attribution, aligns the principles of certainty, utility, and fairness, and ensures that the characteristics of immutability and decentralization do not compromise fundamental rights to personal data. Ultimately, strengthening the derivative regulations of the PDP Law that explicitly regulate the *blockchain* data architecture pattern, role qualifications in protocol governance, the validity of *crypto-erasure* solutions, and incident reporting standards to authorities and data subjects will be key to ensuring that the preventive and repressive protection taught by Prof. Hadjon can run effectively in the Indonesian *smart contract* landscape.

---

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

[45] Ninis Nugraheni, Nikmah Mentari, and Belgis Shafira, "The Study of Smart Contract in the Hara Platform under the Law of Contract in Indonesia," *Scholars International Journal of Law, Crime and Justice* 5, no. 7 (July 2022): 273–85, https://doi.org/10.36348/sijlcj.2022.v05i07.005.

b. Legal Liability for Personal Data Breaches in Smart Contracts in the European Union

The framework of the *General Data Protection Regulation* (GDPR) in the European Union places responsibility based on the functional distinction between controllers and processors, supported by the principles of accountability, data protection by design and default, processing security obligations, and breach notification mechanisms.[46] The regulation mandates processors to adopt suitable technical and organisational safeguards to protect data.[47] If both contribute to a breach, the GDPR recognises joint liability and gives data subjects the right to claim compensation.

In the context of smart contracts, parties' responsibilities are identified using a function-oriented approach that evaluates their actual roles in the contractual process. Protocol developers and/or governance token holders who have substantive authority in setting processing parameters and controlling code updates are generally positioned as de facto data controllers.[48] Providers of *dApp* interfaces that manage telemetry, analytics, or *user logs* may also be considered controllers because they determine the flow of data being processed. Conversely, *oracle* providers and infrastructure partners tend to be classified as data processors when acting on the instructions of a controller. As for validators or node operators on public networks, they do not work "on behalf" of a specific controller, so their legal

---

[46] Muhammad Akbar Eka Pradana and Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative: Journal Of Social Science Research* 4, no. 4 (n.d.): 3412–25, https://doi.org/10.31004/innovative.v4i4.13476.

[47] Agnes Juliet Gonie, Christine J. J. G Goni, and Jolanda M. Korua, "Tinjauan Hukum Kebocoran Data Pribadi Terhadap Kepercayaan Konsumen Di Industri Finansial Teknologi (Fintech)," *Lex Administratum* 13, no. 3 (2025): 1–12.

[48] Shipra, *Smart Contracts in DeFi: The Backbone of Decentralization*, n.d., accessed September 29, 2025, https://www.solulab.com/smart-contracts-in-defi/.

status cannot be automatically determined. However, this should be further examined based on their specific functions and the context of their role in processing.

Data breaches trigger the application of GDPR standards, which require immediate notification, an assessment of the potential risks to the rights and freedoms of data subjects, followed by the implementation of quantifiable corrective measures.[49] The immutable nature of blockchain, which makes physical *on-chain* deletion impractical, shifts the focus of compliance to architectural designs that minimize data usage from the outset. Examples include storing personal data *off-chain* only as *on-chain* hash references, implementing end-to-end encryption with strong key management, or utilizing *zero-knowledge proofs* for attribute verification without disclosure.[50]

The GDPR connects the rule of law with the rule of code by limiting personal data storage in immutable layers, requiring DPIAs for high-risk processing, regulating controller–processor agreements, and enforcing proportionate sanctions. With this framework, decentralised and deterministic smart contracts can still be placed within an accountability structure, encouraging the application of the principle of prevention through design and ensuring the availability of recovery efforts in the event of a breach.

3. Resolving Disputes Arising from Code Defects in Smart Contracts

Dispute resolution for smart contract failures should address the tension between the certainty of automated code execution and the

---

[49] Rizki Alamsyah and Sidi Ahyar Wiraguna, "Dilema Media Massa Di Era Digital: Antara Perlindungan Data Pribadi Dan Kebebasan Pers Dalam UU PDP," *Media Hukum Indonesia (MHI)* 2, no. 6 (May 2025): 107–16, https://doi.org/10.5281/ZENODO.15486207.

[50] Dev Thakkar, Suraj Sabale, and Aayushka Waghmare, "Exploring the Efficiency of Off-Chain vs. On-Chain Transactions in Blockchain Network," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10, no. 3 (May 2024): 40–44, https://doi.org/10.32628/CSEIT24102126.

need to protect substantive justice for the parties. Smart contracts may execute automatically, but their execution can still produce legally problematic outcomes when the code contains bugs, security vulnerabilities, hidden functions, or instructions that do not reflect the parties' actual intention. Therefore, the law should not treat code execution as an absolute and final outcome that is immune from legal review. Instead, the legal framework should provide mechanisms that allow parties to challenge, suspend, correct, or seek compensation for losses arising from defective code or failed execution. Based on this framework, this section examines dispute resolution for smart contract failures in Indonesia. It compares it with the European Union approach, particularly in relation to litigation, alternative dispute resolution, online dispute resolution, and preventive technical safeguards such as auditability, access control, and emergency interruption mechanisms.

a. Smart Contract Dispute Resolution in Indonesia

Blockchain's immutability renders deployed code effectively unpatchable, meaning logical flaws or security vulnerabilities can be exploited without recourse, causing significant losses. This operational rigidity translates directly into a normative conflict within contract law. The principle of pacta sunt servanda (the agreement must be kept) compels adherence to the automated execution. However, the principle of justice demands that the outcome reflect the parties' bona fide intentions, which the flawed code may fail to do. Therefore, any dispute resolution mechanism must be crafted to mediate between the certainty of code execution and the equitable demands of substantive justice.

Resolving disputes through litigation in court faces serious obstacles in smart contract cases. The main obstacles include high technical complexity, high costs, slow processes, issues of cross-border

jurisdiction, and the anonymity of the parties. [51] This situation encourages the use of Alternative Dispute Resolution (ADR), particularly digital arbitration and mediation, as a more suitable solution. The on-chain arbitration model shows the potential for fast and efficient dispute resolution, with decisions made by a virtual jury panel and automatically enforceable through smart contracts.[52]

The architecture for dispute resolution through hybrid arbitration is designed to combine the speed of digital mechanisms with formal legal legitimacy.[53] This process takes place in two stages. The first stage is *on-chain arbitration*, which serves to delay, freeze, or correct the execution of contracts related to digital assets. The second stage involves ratifying the arbitration results into a ruling by an arbitration institution that has executive power under national law.[54] Thus, the efficiency of dispute resolution in the digital space gains the support of positive legal legitimacy. The effectiveness of this mechanism relies on the existence of a smart legal contract that explicitly includes dispute resolution clauses, such as the chosen forum, applicable law, multi-tier dispute resolution procedures, and safety instruments like escrow or circuit breakers.

Legal Protection Framework Hadjon positions dispute resolution design as an instrument that contains both preventive and repressive legal protection. Preventive protection is realised through

---

[51] Zainudin, "The Urgency of Reforming Indonesian Civil Law in the Digital Era," *Jurnal Tana Mana* 6, no. 2 (2025): 187–98, https://doi.org/10.33648/jtm.v6i2.1051.

[52] Riikka Koulu, "Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement," *SCRIPTed* 13, no. 1 (May 2016): 40–69, https://doi.org/10.2966/scrip.130116.40.

[53] Leny Megawati, Cecep Wiharma, and Asep Hasanudin, "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia," *Jurnal Hukum Mimbar Justitia* 9, no. 2 (December 2023): 410, https://doi.org/10.35194/jhmj.v9i2.3856.

[54] Husnul Khatimah Khatimah, "Penyelesaian Sengketa Smart Contract Dalam Tekhnologi Blockchain," *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 2, no. 9 (2024): 240–57.

code audit obligations, the application of minimum-security standards, and the formulation of dispute clauses from the outset of the contract to minimise potential losses. Repressive protection is achieved through effective recovery mechanisms, such as digital arbitration, litigation, or compensation, so that legal subjects still have access to justice even in the event of a technological system failure. The integration of these two approaches ensures that the resolution of disputes stemming from code errors or failed smart contract executions enhances legal certainty while simultaneously safeguarding justice and fundamental human rights in the context of a rapidly decentralising digital ecosystem.

b. Smart Contract Dispute Resolution in the European Union

In the European Union, disputes relating to smart contracts are resolved through the established legal framework of agreements and international civil law. Generally, the parties explicitly include clauses on the choice of law and choice of forum so that the legal authority and competent court can be immediately determined in the event of a dispute.[55] If such clauses are not included, the Rome I Regulation is applied to determine the applicable law based on the closest connection to the contract in question. Under this framework, disputes arising from failure of execution or code defects are still resolved through positive law, even if the contract is blockchain-based.

Litigation continues to be available within the European Union; however, its role is increasingly complemented by promoting Alternative Dispute Resolution (ADR) and Online Dispute Resolution (ODR), particularly in business-to-consumer transactions.[56]

---

[55] Fatihani Baso et al., "Overview of Smart Contract: Legality and Enforceability," *Dialogia Iuridica* 16, no. 1 (November 2024): 096–111, https://doi.org/10.28932/di.v16i1.10024.

[56] Fandi Iskandar Sopang and Andi Maysarah, "Penyelesaian Sengketa Transaksi Bisnis Di Era Digital Secara Online (Online Dispute Resolution)," *Jurnal Bisnis Net* 7, no. 1 (2024): 155–63.

The ADR Directive and ODR Regulation establish cross-border online platforms that allow consumers to settle disputes electronically faster and more cost-effectively. Although not initially designed for the Web3 environment, these mechanisms can be adapted to address contractual disputes arising from smart contracts, including transaction failure or data misuse by digital service providers.

The latest development comes through the EU Data Act, which introduces minimum technical requirements for smart contracts used for data sharing. This regulation requires smart contracts to have secure termination/interruption capabilities, verifiable audit trails, access controls, and compliance with underlying data agreements. These requirements indirectly serve as a dispute prevention mechanism, as bugs or code defects can be anticipated through pause or emergency kill switch features. In addition, contract auditability facilitates the verification process if disputes proceed to legal resolution. Thus, the European Union's approach to smart contract disputes rests on three layers: legal certainty through choice of law and choice of forum instruments, efficiency and accessibility through ADR/ODR mechanisms, and technical prevention through regulations that require security and auditability functions in smart contracts. This combination allows disputes arising from bugs or execution failures to be resolved within a framework of legal certainty while ensuring substantive justice for the parties.

Conclusion

The research conclusion affirms that the legal status of smart contracts within the Indonesian legal system remains in a state of significant juridical ambiguity. The positive framework recognizes electronic information/documents and electronic signatures, but does not yet provide definitions, validity requirements, minimum technical standards, or governance and accountability mechanisms that specifically regulate contracts executed by code. This normative vacuum has an impact on three main areas: (i) contractual certainty,

especially in cross-border transactions and when choice of law and forum clauses are not included; (ii) personal data protection due to the tension between blockchain immutability and data subject rights; and (iii) effectiveness of dispute resolution and evidence, because the quality of on-chain evidence has not been fully institutionalized in judicial practice and the blockchain forensic capacity of law enforcement agencies still needs to be improved.

The essentials include establishing an operational definition of smart contracts and their status in contract law; minimum clause requirements (choice of law, choice of forum, ADR/ODR tiers, and mechanisms for delaying execution through escrow or circuit breakers); standardization of on-chain evidence with clear reliability parameters; mandatory formal audits or verification prior to deployment and code change governance; and improved technical capacity of courts and dispute resolution institutions. In the realm of data protection, an accountability-based approach needs to be positively reinforced through privacy by design/default, data minimization at the on-chain layer (identities stored off-chain with hashes/pointers on the chain), crypto-erasure options in limited circumstances, role mapping of controllers and processors based on function, and mandatory impact assessments for high-risk scenarios. In line with EU practices, Indonesia also needs to adopt cross-border reference elements, built-in rules for determining the most relevant law and jurisdiction when clauses are absent, integration of ADR/ODR for access to digital disputes, and minimum technical requirements for smart contracts that process or share data.

References

Books

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

H.S., Salim. *Hukum Kontrak, Teori & Tekriik Penyusunan Kontrak*. Jakarta: Sinar Grafika, 2008.

Journals

Alamsyah, Rizki, and Sidi Ahyar Wiraguna. "Dilema Media Massa Di Era Digital: Antara Perlindungan Data Pribadi Dan Kebebasan Pers Dalam UU PDP." *Media Hukum Indonesia (MHI)* 2, no. 6 (May 2025): 107–16. https://doi.org/10.5281/ZENODO.15486207.

Alawadi, Asma, Nada Kakabadse, Andrew Kakabadse, and Sam Zuckerbraun. "Decentralized Autonomous Organizations (DAOs): Stewardship Talks but Agency Walks." *Journal of Business Research* 178 (May 2024): 114672. https://doi.org/10.1016/j.jbusres.2024.114672.

Alhat, Pratiksha. "Blockchain Technology." *International Journal of Scientific Research in Engineering and Management* 08, no. 04 (April 2024): 1–5. https://doi.org/10.55041/IJSREM30694.

Atiyah, Ghassan Adhab, Ahmed Ismael Ibrahim, and Ahmed Abdulkhudhur Jasim. "Enforcement of Smart Contracts in Cross-Jurisdictional Transactions." *International Journal of Law and Management*, ahead of print, November 29, 2024. https://doi.org/10.1108/IJLMA-06-2024-0220.

Aydar, Mehmet, Salih Cemil Cetin, Serkan Ayvaz, and Betul Aygun. "Private Key Encryption and Recovery in Blockchain." Version 2. Preprint, arXiv, 2019. https://doi.org/10.48550/ARXIV.1907.04156.

Baso, Fatihani, Dzakiyah Ulya Yusuf, Andi Novita Mudriani Djaoe, Iswandi Iswandi, and Anisa Ramadhany. "Overview of Smart Contract: Legality and Enforceability." *Dialogia Iuridica* 16, no. 1 (November 2024): 096–111. https://doi.org/10.28932/di.v16i1.10024.

Bassan, Fabio, and Maddalena Rabitti. "From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation." *Computer Law & Security Review* 55 (November 2024): 1–25. https://doi.org/10.1016/j.clsr.2024.106035.

Candra, Sapto Andika. *Melonjak, Transaksi Aset Kripto Sepanjang 2024 Capai Rp556,53 Triliun*. December 31, 2024. https://news.ddtc.co.id/berita/nasional/1807916/melonjak-transaksi-aset-kripto-sepanjang-2024-capai-rp55653-triliun.

Comelles, Cristina Argelich. "Smart Contracts o Code Is Law." *InDret* 2 (October 2020): 1–41. https://doi.org/10.31009/InDret.2020.i2.01.

Delgado-von-Eitzen, Christian, Manuel José Fernández-Iglesias, Luis Anido-Rifón, and Martín Llamas-Nistal. "Ethereum Blockchain

Interconnectivity for Dynamic and Privacy-Preserving Access Control." *IEEE Access* 13 (2025): 112918–31. https://doi.org/10.1109/ACCESS.2025.3584429.

Fajriatama, Tegar Dwi, Muhammad Rama Rizaldi, Nurmala Dewi Rahmawati, Nadira Aisha Amidia, Siti Nurazizah, Nafisah Dwi Yuliarida, and Muhammad Daffa Jauza Fikri. "Penerapan Teknologi Blockchain Dalam Transformasi Keuangan Sebagai Tantangan Dan Peluang Di Era Digital." *EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi* 4, no. 3 (March 2025): 4799–807. https://doi.org/10.56799/ekoma.v4i3.6464.

Fauziah, Zaleha, Haznah Latifah, Xavier Omar, Alfiah Khoirunisa, and Shofiyul Millah. "Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review." *Aptisi Transactions on Technopreneurship (ATT)* 2, no. 2 (August 2020): 160–66. https://doi.org/10.34306/att.v2i2.97.

Franko, Ivan, and Tsudzenko Y. "Assessment of the Efficiency of Using Smart Contracts for Intelligent Analysis of User Actions in Social Networks." *Artificial Intelligence* 29, no. AI.2024.29(4) (December 2024): 36–40. https://doi.org/10.15407/jai2024.04.036.

Goint, Mongetro, Cyrille Bertelle, and Claude Duvallet. "Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems." *Mathematics* 11, no. 7 (March 2023): 1592. https://doi.org/10.3390/math11071592.

Gonie, Agnes Juliet, Christine J. J. G Goni, and Jolanda M. Korua. "Tinjauan Hukum Kebocoran Data Pribadi Terhadap Kepercayaan Konsumen Di Industri Finansial Teknologi (Fintech)." *Lex Administratum* 13, no. 3 (2025): 1–12.

Hong, Yile, Xiangfu Liu, Jiahui Huang, Tongqi Chen, Teng Huang, and Yan Pang. "SNFM: Scalable Node Feature Modeling in Smart Contracts for Vulnerability Detection through Graph-Based Approaches." *2025 IEEE Global Blockchain Conference (GBC)*, June 20, 2025, 1–6. https://doi.org/10.1109/GBC60041.2025.11134470.

Hutapea, Korintus Wilson Horas, and Adi Sulistiyono. "Keabsahan Smart Contract Dengan Teknologi Blockchain Menurut Kitab Undang-Undang Hukum Perdata." *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 1, no. 3 (April 2024): 86–94. https://doi.org/10.62383/aliansi.v1i3.177.

Jabalnur, Ruliah, Oheo Kaimuddin Haris, Deity Yuningsih,

Zahrowati, and Muh Hasrul La Aci. "Perjanjian Di Bawah Tangan Ditinjau Dari Asas Pacta Sunt Servanda." *Halu Oleo Legal Research* 6, no. 2 (2024): 247–57. https://doi.org/10.33772/holresch.v6i2.848.

Kadafi, Rahadian, Rahmadi Indra, and Iwan Rachmad. "Kepastian Hukum Pembuatan Akta Perjanjian Kredit Digital Oleh Notaris." *JURNAL RECHTENS* 14, no. 1 (2025): 171–95. https://doi.org/10.56013/rechtens.v14i1.4200.

Kadly, Eureka Inola, Sinta Dewi Rosadi, and Elisatris Gultom. "Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura." *Jurnal Sains Sosio Humaniora* 5, no. 1 (June 2021): 199–212.

Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." *Peer-to-Peer Networking and Applications* 14, no. 5 (September 2021): 2901–25. https://doi.org/10.1007/s12083-021-01127-0.

Khatimah, Husnul Khatimah. "Penyelesaian Sengketa Smart Contract Dalam Tekhnologi Blockchain." *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora* 2, no. 9 (2024): 240–57.

Koulu, Riikka. "Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement." *SCRIPTed* 13, no. 1 (May 2016): 40–69. https://doi.org/10.2966/scrip.130116.40.

Kurdi, Kurdi, and Joko Cahyono. "Perlindungan Data Pribadi Di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *JUNCTO: Jurnal Ilmiah Hukum* 6, no. 2 (December 2024): 330–39. https://doi.org/10.31289/juncto.v6i2.5443.

Lim, Willion, Steven Angkasa, and Alexander Danelo Putra Wibowo. "Smart Contracts: Validitas Hukum Dan Tantangan Di Masa Depan Indonesia." *Jurnal Kewarganegaraan* 8, no. 1 (June 2024): 829–38. https://doi.org/10.31316/jk.v8i1.6410.

Megawati, Leny, Cecep Wiharma, and Asep Hasanudin. "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia." *Jurnal Hukum Mimbar Justitia* 9, no. 2 (December 2023): 410. https://doi.org/10.35194/jhmj.v9i2.3856.

Moya, Cristina Vilchez, Juan Ramón Bermejo Higuera, Javier Bermejo Higuera, and Juan Antonio Sicilia Montalvo. "Implementation and Security Test of Zero-Knowledge Protocols on SSI

Blockchain." *Applied Sciences* 13, no. 9 (April 2023): 5552. https://doi.org/10.3390/app13095552.

Muko, Adam. "Kajian Smart Contract Dalam Perspektif Hukum Positif Di Indonesia." *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik* 2, no. 2 (January 2024): 13–24. https://doi.org/10.59581/doktrin.v2i2.2517.

Neesya, Ananda Bunga, Fedya Batara Trisya Sukmana, Suci Aulia, Vega Febriana, and Nandang Kusnadi. "Tinjauan Yuridis Terhadap Syarat Keabsahan Perjanjian Dalam Hukum Kontrak Indonesia." *Causa: Jurnal Hukum Dan Kewarganegaraan* 14, no. 9 (2025): 31–40. https://doi.org/10.6679/ynwg9575.

Nugraheni, Ninis, Nikmah Mentari, and Belgis Shafira. "The Study of Smart Contract in the Hara Platform under the Law of Contract in Indonesia." *Scholars International Journal of Law, Crime and Justice* 5, no. 7 (July 2022): 273–85. https://doi.org/10.36348/sijlcj.2022.v05i07.005.

Pradana, Muhammad Akbar Eka, and Horadin Saragih. "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya." *Innovative: Journal Of Social Science Research* 4, no. 4 (n.d.): 3412–25. https://doi.org/10.31004/innovative.v4i4.13476.

Purwito, Edy. "Konsep Perlindungan Hukum Konsumen Dan Tanggung Jawab Hukum Pelaku Usaha Terhadap Produk Gula Pasir Kadaluarsa Di Kota Surabaya." *Jurnal Magister Ilmu Hukum* 13, no. 1 (June 2023): 114. https://doi.org/10.56943/dekrit.v13n1.152.

Rachmadani, Farhan Abel Septian, and Sinta Dewi Rosadi. "Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia." *Jurnal Sains Sosio Humaniora* 5, no. 1 (June 2021): 650–64. https://doi.org/10.22437/jssh.v5i1.14838.

Ramalinda, Dola, Jayadi, and Agung Rachmat Raharja. "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi." *Journal of International Multidisciplinary Research* 2, no. 6 (June 2024): 665–71. https://doi.org/10.62504/jimr679.

Rizqi, Laila Alfina Mayasari, and Dedi Farera Prasetya. "Urgensi Penggunaan Smart Contract Dalam Transaksi Jual Beli Di E-Commerce." *Jurnal Hukum Lex Generalis* 3, no. 4 (April 2022): 327–38. https://doi.org/10.56370/jhlg.v3i4.247.

Sakirman, Ma'ruf Akib, and Wahyudi Umar. "Kepastian Hukum Smart Contract Dalam Perspektif Hukum Perdata." *Rewang Rencang: Jurnal Hukum Lex Generalis* 5, no. 10 (2024): 1–11.

Senarathna, Janaka Ishan. "The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency and Security." Preprint, Computer Science and Mathematics, April 22, 2025. https://doi.org/10.20944/preprints202504.1814.v1.

Setiawan, Yudi, Budi Sutrisno, and Ari Hakim Budiawan Firdaus. "Pelaksanaan Pasal 1338 Ayat (1) (3) KUHPdt Tentang Kebebasan Berkontrak Dan Itikad Baik Dalam Pembiayaan Kendaraan Bermotor." *Journal Kompilasi Hukum* 5, no. 1 (June 2020): 154–74. https://doi.org/10.29303/jkh.v5i1.5.

Simanjuntak, Predderics Hockop. "Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital Di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi Dan General Data Protection Regulation (GDPR)." *Jurnal Esensi Hukum* 6, no. 2 (2025): 105–24. https://doi.org/10.35586/jsh.v6i2.412.

Siregar, Mardona. "Teori Hukum Progresif Dalam Konsep Negara Hukum Indonesia." *Muhammadiyah Law Review* 8, no. 2 (August 2024): 10. https://doi.org/10.24127/mlr.v8i2.3567.

Song, Judy Yueh Ling, and Esther Tan. "Beyond Traditional Contracts: The Legal Recognition and Challenges of Smart Contracts in Malaysia and Singapore." *Journal of Law, Market & Innovation* 3, no. 3 (November 2024): 323–57. 4MB. https://doi.org/10.13135/2785-7867/11334.

Sopang, Fandi Iskandar, and Andi Maysarah. "Penyelesaian Sengketa Transaksi Bisnis Di Era Digital Secara Online (Online Dispute Resolution)." *Jurnal Bisnis Net* 7, no. 1 (2024): 155–63.

Su, Zelin. "Evidentiary Value and Evidentiary Status of Blockchain Evidence." *The International Journal of Evidence & Proof* 29, no. 1 (January 2025): 58–76. https://doi.org/10.1177/13657127241238020.

Sumriyah. "Cacat Kehendak (Wilsgebreken) Sebagai Upaya Pembatalan Perjanjian Dalam Persepektif Hukum Perdata." *Simposium Hukum Indonesia* 1, no. 1 (2019): 662–70.

Suratkar, Saurabh, Mahesh Shirole, and Sunil Bhirud. "Cryptocurrency Wallet: A Review." *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, September 28, 2020, 1–7. https://doi.org/10.1109/ICCCSP49186.2020.9315193.

Suryawijaya, Tito Wira Eka. "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia." *Jurnal Studi Kebijakan Publik* 2, no. 1 (May 2023): 55–68. https://doi.org/10.21787/jskp.2.2023.55-68.

Syafiq, Muhammad, and Siti Nur Syifa. "Analisis Penggunaan Blockchain Untuk Meningkatkan Transparansi Dan Keamanan Data Pada Pembuktian Perceraian Di Pengadilan Agama." *Journal of Innovative and Creativity (Joecy)* 5, no. 2 (June 2025): 9662–72. https://doi.org/10.31004/joecy.v5i2.978.

Thakkar, Dev, Suraj Sabale, and Aayushka Waghmare. "Exploring the Efficiency of Off-Chain vs. On-Chain Transactions in Blockchain Network." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 10, no. 3 (May 2024): 40–44. https://doi.org/10.32628/CSEIT24102126.

Thanasi-Boçe, Marsela, and Julian Hoxha. "Blockchain for Sustainable Development: A Systematic Review." *Sustainability* 17, no. 11 (May 2025): 1–38. https://doi.org/10.3390/su17114848.

Zahra, Masripa Siti, Nurmala, Sinta Solihah, and Anita Kamilah. "Integrasi Metadata Dan Teknologi Blockchain: Implikasi Hukum Terhadap Perikatan Di Indonesia." *Journal Customary Law* 2, no. 2 (April 2025): 10. https://doi.org/10.47134/jcl.v2i2.3951.

Zainudin. "The Urgency of Reforming Indonesian Civil Law in the Digital Era." *Jurnal Tana Mana* 6, no. 2 (2025): 187–98. https://doi.org/10.33648/jtm.v6i2.1051.

Website

Shipra. *Smart Contracts in DeFi: The Backbone of Decentralization*. n.d. Accessed September 29, 2025. https://www.solulab.com/smart-contracts-in-defi/.