Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions

Fidhela Putri Fadhila
Faculty of Law, Universitas Negeri Gorontalo. Correspondence E-mail: fpagau@gmail.com

Abstract:

The development of blockchain technology and smart contracts opens new opportunities for reforming contract law in Indonesia, particularly in realizing transparency and data integrity in electronic contract transactions. This study aims to analyze the optimization of blockchain in fulfilling the valid requirements of an agreement under Article 1320 of the Indonesian Civil Code (KUHPerdata) and to identify regulatory and technical challenges hindering its implementation. This research employs normative legal research (juridical normative) with statutory, conceptual, and case approaches, including an analysis of Jakarta Barat District Court Decision No. 588/Pdt.G/2020 as well as various related regulations such as the ITE Law, the PDP Law, and sectoral policies. The findings show that blockchain can strengthen the requirement of mutual consent through permanent and transparent recording of changes to the agreement, and reinforce the lawful cause requirement by guaranteeing data integrity through cryptographic hashing and distributed validation. However, implementation still faces regulatory challenges in the form of the absence of a specific law explicitly recognizing smart contracts, as well as technical challenges such as limited scalability, the risk of 51% attacks, and low interoperability. This study concludes that optimizing blockchain requires synergy between adaptive regulatory reform and the development of secure, scalable technical infrastructure, as well as improving the capacity of legal-tech human resources.

Keywords: Blockchain; Contract transparency; Data integrity.

How to cite (Chicago Manual Style):
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

© 2026 – Fidhela Putri Fadhila
Under the license CC BY-SA 4.0

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Introduction

The development of information and communication technology has brought substantial changes to various sectors of life, including civil law. Digital transformation has not only shifted patterns of social and economic interaction but also spurred the emergence of forms of transactions and agreements conducted electronically through digital systems. Within this landscape, blockchain stands out as one of the most prominent technologies due to its ability to provide a secure, transparent, and distributed transaction recording mechanism without requiring a central authority. This characteristic has attracted widespread interest from both business actors and the government as potential users. The existence of blockchain opens new opportunities for reforming legal instruments, especially in creating more accountable transaction models (Aminin 2024). This decentralized system offers a different pattern of interaction compared to conventional mechanisms that have long relied on intermediaries. This transformation creates an urgent need to assess the extent to which national civil law can accommodate these developments, particularly in guaranteeing transparency and data integrity in civil contract transactions.

The use of blockchain in Indonesia is increasing along with the growing need for security and efficiency in data management. This technology is considered capable of providing optimal protection through cryptographic methods that ensure information integrity. However, despite its many advantages, the use of blockchain is not free from technical limitations that demand continuous development. These weaknesses require serious attention so that its utilization does not create new risks for the parties. Blockchain's ability to distribute information without a central authority offers significant added value for users, but on the other hand, progressive technological development also represents an effort to overcome remaining limitations. This context demonstrates the need for in-depth study of blockchain's impact on the national legal system, especially within the framework of electronic agreements that prioritize transparency and data integrity (Apriani et al. 2023).

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Blockchain plays an important role in introducing the concepts of decentralization, transparency, and high-level security in data storage. The working principle of blockchain, which relies on distributed validation, makes transaction data more resistant to manipulation because any change must obtain approval from the majority of nodes in the network. This system offers an alternative to conventional recording mechanisms that are vulnerable to leaks and irregularities. The increasing number of electronic transactions also expands the need for systems that can guarantee data accuracy and validity. Furthermore, the development of smart contracts first introduced by Nick Szabo as an innovation based on Distributed Ledger Technology enriches blockchain's function as an agreement automation instrument (Arsal et al. 2025). This concept describes a mechanism for automatically executing agreements through digital code that runs according to predetermined conditions. The use of smart contracts eliminates the need for a third party as an intermediary in transactions, providing an unalterable record that enhances data reliability. The contract information that has been programmed will automatically execute the parties' obligations. The values of efficiency and transparency make smart contracts relevant in modern transaction systems, yet the integration of this technology raises the need to assess its position within the Indonesian civil law framework (Chairunnas et al. 2024).

The use of smart contracts in the business sector opens up new efficiency opportunities, particularly in buying and selling activities through e-commerce. The ability of digital systems to overcome spatial and temporal barriers makes them a highly adaptive instrument in the modern economy. The execution of transactions through smart contracts must still comply with the provisions of the Indonesian Civil Code (KUHPerdata). Article 1313 of the KUHPerdata stipulates that an agreement is a legal act that creates a binding relationship between the parties. Normatively, the development of blockchain and smart contract technology in electronic transactions should be able to provide legal certainty, security, transparency, and protection for the parties in electronic agreements (Juwita et al. 2025). These provisions are reflected in Article 1320 of the KUHPerdata, which regulates the valid

requirements for an agreement: mutual consent, capacity, a specific subject matter, and a lawful cause. In addition, the Electronic Information and Transactions Law (UU ITE) and Government Regulation Number 71 of 2019 have recognized electronic documents, electronic signatures, and electronic contracts as valid evidence in digital transactions. Thus, blockchain technology through the smart contract system is expected to create a safer, more transparent, and more efficient transaction mechanism because all transaction data is recorded permanently, is difficult to manipulate, and can be executed automatically without the need for a third party (Martinelli et al. 2024).

However, in practice, the use of blockchain technology and smart contracts in Indonesia still faces various legal and technical problems. To date, there is no specific regulation that comprehensively governs the legality of blockchain and smart contracts in Indonesian civil law. The existing regulations are still scattered across several policies such as the ITE Law, Bank Indonesia Regulation (PBI) Number 19/12/2017 concerning Financial Technology Implementation, various regulations of the Financial Services Authority (OJK), and policies of the Commodity Futures Trading Regulatory Agency (Bappebti). This condition creates legal uncertainty in their implementation. In addition, digital transactions remain vulnerable to data misuse, transaction manipulation, and cybercrime. On the other hand, automatically executing smart contracts also raise issues regarding the validity of consent, legal responsibility, and dispute resolution mechanisms in the event of system errors or default (Mawa, n.d.). This condition shows that the development of blockchain technology has not yet been fully matched by the readiness of legal regulations in Indonesia, making the urgency of optimizing blockchain to ensure transparency and data integrity increasingly pressing.

Technical challenges such as scalability are another factor affecting the effectiveness of blockchain use. Public blockchain systems like Bitcoin can only process a small number of transactions per second, a limitation that creates obstacles when transactions are conducted on a large scale. The 51% attack on Bitcoin Gold in 2018 demonstrated the vulnerability of blockchains with inadequate security. The

financial losses caused by that attack illustrate the risk of misuse of computing power (Megawati et al. 2023). This incident provides an important lesson regarding the need for security standardization in blockchain implementation. This situation confirms that the use of technology must still consider the aspect of prudence, while also reinforcing the argument that blockchain optimization involves not only legal aspects but also interrelated technical aspects.

The study of blockchain use in electronic agreements requires supporting case examples to clarify legal issues that arise in practice. One relevant case is the Jakarta Barat District Court Decision Number 588/Pdt.G/2020 between Mr. Amir Salim (Plaintiff) against PT Ecart Webportal Indonesia (Lazada Indonesia) as Defendant. In his lawsuit, the Plaintiff alleged that Lazada's electronic system did not provide adequate protection for the security of consumer accounts and personal data. The Plaintiff argued that the Defendant had committed a tort because the electronic system used was deemed unreliable, insecure, and irresponsible, thereby causing losses to consumers (Simatupang and Iryanti 2024). However, during the trial, Lazada filed an exception regarding the court's jurisdiction based on an arbitration clause in the terms and conditions stipulating that dispute resolution must be conducted through the National Arbitration Agency (BANI). The panel of judges then granted the Defendant's exception and declared that the Jakarta Barat District Court had no authority to hear the case. This case shows that in conventional electronic transaction systems, there are weaknesses in terms of personal data protection and transparency of dispute resolution mechanisms. Users are often bound by standard contracts without having adequate access to the history of changes or independent data verification mechanisms. This serves as an entry point for blockchain to offer solutions through unalterable recording and full transparency of each clause and the history of consent (Algifari and Prasetyo 2025).

Furthermore, the relationship between users and platforms like Lazada constitutes a binding relationship arising from an electronic agreement. When a user registers, an agreement has implicitly been reached regarding the use of services, including the protection of personal data. The data breach case demonstrates the

weakness of conventional electronic transaction systems, particularly in terms of personal data protection. In the context of the Personal Data Protection Law (UU PDP), the use of a person's personal data must be based on the data owner's consent (Ananda and Rinjani 2025). Such consent constitutes a form of "agreement" that aligns with the valid requirements of an agreement under Article 1320 of the KUHPerdata. The PDP Law requires valid consent from the personal data owner, while blockchain can provide a transparent, auditable, and unalterable consent recording mechanism. The integrity of consent data becomes the foundation for fulfilling the requirements of "mutual consent" and "lawful cause" in any digital-based civil contract. Therefore, blockchain optimization is oriented not only toward technical efficiency but also toward strengthening legal certainty and protecting the rights of the parties.

The development of blockchain technology demands a renewal of the legal framework to ensure alignment between digital innovation and civil law provisions. The changing structure of electronic transactions requires attention to aspects of validity, rights protection, and dispute resolution mechanisms. The legal system has a responsibility to ensure that the use of technology does not diminish the values of justice (Hutabarat and Rialdyli 2026). Increasing understanding of the benefits and risks of technology becomes the basis for strengthening regulations. This situation affirms the urgency of this research to assess the legal position of blockchain in the electronic agreement system, specifically how blockchain can be optimized to realize transparency and data integrity in civil contract transactions in Indonesia. Without adequate legal certainty, blockchain's great potential will only become a technological discourse without real impact on improving digital contract governance. Therefore, this research is crucial to bridge the gap between technological progress and the need for legal certainty in Indonesia.

Method

This research employs normative legal research (juridical normative) with a statutory approach, a conceptual approach, and a case approach (Al-Fatih 2023). The

statutory approach is conducted by examining the provisions of Article 1320 of the KUHPerdata, the Electronic Information and Transactions Law (UU ITE), Government Regulation Number 71 of 2019, and other related policies such as PBI Number 19/12/2017 and OJK and Bappebti regulations. The conceptual approach is used to analyze the principles of transparency, data integrity, as well as the concepts of smart contracts and blockchain in relation to contract law theory and contract validity. The case approach is applied through an analysis of Jakarta Barat District Court Decision Number 588/Pdt.G/2020 (Lazada Indonesia) to identify weaknesses in conventional electronic transaction systems and the relevance of blockchain optimization in solving data protection and legal certainty issues. The legal materials used include primary legal materials (legislation and court decisions), secondary legal materials (textbooks, law journals, scholarly articles, and technical documents on blockchain), and tertiary legal materials (legal dictionaries and encyclopedias). Data collection techniques are carried out through library research of legal documents and related literature. Data analysis uses methods of legal interpretation (grammatical, systematic, and teleological) as well as legal reasoning to assess the compatibility between blockchain characteristics and the valid requirements of an agreement, as well as the need for transparency and data integrity in electronic civil contracts in Indonesia.

Optimization of Blockchain in Realizing Transparency and Data Integrity in the Valid Requirements of an Agreement

Transparency and data integrity are two fundamental pillars in any civil contract transaction, especially in the digital era. In the Indonesian civil law system, the validity of an agreement is determined by the fulfillment of objective and subjective requirements as regulated in Article 1320 of the Indonesian Civil Code (KUHPerdata). This article states that an agreement is valid if it meets four requirements: mutual consent of the parties binding themselves; capacity to create an obligation; a specific subject matter; and a lawful cause. The first two requirements are subjective, while the latter two are objective. Among these four

requirements, mutual consent and lawful cause are most directly related to transparency and data integrity (Mufidah and Surur 2025). Mutual consent requires a meeting of minds based on clear and non-misleading information, while lawful cause requires that the performance of the agreement does not violate the law, including provisions on personal data protection. Blockchain technology, through its distributed ledger and smart contract mechanisms, offers an innovative solution to strengthen both requirements simultaneously, while addressing the weaknesses of conventional electronic contract systems that have long been vulnerable to manipulation, lack of transparency, and data integrity violations (Muhaimin, n.d.).

First, regarding the requirement of mutual consent. In conventional electronic contracts, consent is often expressed through simple mechanisms such as clicking an "Agree" button, checking a box on terms and conditions, or similar actions on a digital interface. This practice, although recognized for its validity by Article 18 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments, is actually prone to a lack of transparency. Most users do not read all clauses of standard contracts due to the length of the text and the complexity of legal language (Mulyanto and Purbasari 2024). Furthermore, digital platforms can unilaterally change the terms of the agreement without adequate notice, so that the user's initial consent loses its meaning because the object of the agreement has changed after consent was given. This condition raises a legal question: does consent given without full understanding of frequently changing clauses still satisfy the requirement of "mutual consent" under Article 1320 of the KUHPerdata?

This lack of transparency can be concretely seen in Jakarta Barat District Court Decision Number 588/Pdt.G/2020 between Mr. Amir Salim (Plaintiff) and PT Ecart Webportal Indonesia (Lazada Indonesia). In this case, the user was bound by an arbitration clause in Lazada's standard contract without truly understanding the consequence that disputes must be resolved through the National Arbitration Agency (BANI), not through the district court. The panel of judges granted the defendant's

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

exception and declared the court lacked jurisdiction because the arbitration clause had been electronically agreed upon (Putranto et al. 2024). This case illustrates a legal irony: electronic consent given quickly and without adequate reflection is still formally considered valid by the court, even though the user materially did not have full understanding. This shows that conventional electronic contract systems prioritize formal certainty over substantial transparency, potentially creating injustice for the weaker party (Sirimorok et al. 2025).

Blockchain technology can overcome this structural weakness by recording every version of the agreement permanently in distributed blocks. The distributed ledger mechanism ensures that any change to the terms and conditions must go through a consensus mechanism among the designated parties. Each new version of the agreement is given a timestamp and a unique cryptographic hash, then stored in an immutable blockchain. The parties can access the entire history of changes at any time and anywhere through a transparent interface, thus creating full transparency regarding the object of the agreement. In the context of the mutual consent requirement, blockchain enables an audit trail that shows chronologically when a clause was introduced, when it was changed, and who approved that change (Supriyati et al. 2025). Consent is no longer given blindly to a suddenly changed latest version; instead, users can give their consent gradually and specifically to each material change. This aligns with the principle of informed consent, which is the foundation of a fair contractual relationship. Furthermore, smart contracts computer code running on the blockchain that automatically executes contract clauses allow for a more precise application of the mutual consent requirement. Smart contracts can be programmed so that the execution of obligations only occurs after the parties explicitly provide digital signatures for each predetermined condition, leaving no room for unilateral interpretation (Chic and Bilqisthi 2024).

Second, regarding the requirement of lawful cause. Article 1320 of the KUHPerdata requires that an agreement not conflict with the law, morality, or public order. In modern digital transactions, the scope of "lawful cause" has been expanded

through various laws and regulations, including Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law requires every personal data controller to obtain explicit consent from the data owner, to use the data only for agreed purposes, and to guarantee data security against unauthorized access (Hidayat et al. 2025). Thus, an agreement involving the processing of personal data without valid consent or in a manner that violates data security provisions can be qualified as an agreement that does not meet the lawful cause requirement, thereby being null and void under Article 1335 of the KUHPerdata.

The Lazada Indonesia data breach case, which was the subject matter of Jakarta Barat District Court Decision No. 588/Pdt.G/2020, shows that conventional electronic transaction systems fail to guarantee the integrity of users' personal data. In that case, the plaintiff alleged that Lazada's electronic system did not provide adequate protection for the security of consumer accounts and personal data, resulting in a data breach of user IDs, emails, dates of birth, phone numbers, and other information (Kasim et al. 2025). This failure reflects a fundamental weakness of centralized database systems managed by a single platform authority. In a centralized system, data is vulnerable to single points of failure, cyberattacks, internal misuse, and lack of transparency because users have no independent mechanism to verify whether their data is truly secure and unmanipulated.

Blockchain provides a fundamental solution to the problem of data integrity through cryptographic hashing and distributed validation. Every transaction of data entered into the blockchain, including personal data and contract documents, is encrypted with a cryptographic hash function (e.g., SHA-256) that produces a unique fixed-length string. Each block in the chain contains the hash of the previous block, forming an interconnected chain (Kusumawati 2025). If even one bit of data in a block is changed, the hash of that block changes dramatically and breaks the connection with the subsequent block, so the manipulation is immediately detected by all nodes in the network. Moreover, public (permissionless) blockchains allow every participant to download and verify the entire transaction history without having to trust any

central authority. Thus, data integrity no longer depends on the subjective integrity of the platform, but on an open, publicly auditable mathematical protocol. In the context of the lawful cause requirement, blockchain ensures that agreements are based on legal compliance because every use of personal data is recorded authentically, transparently, and in accordance with the parties' initial consent (Meisinta et al. 2026).

Table 1. Comparison of Fulfillment of Valid Agreement Requirements (Article 1320 KUHPerdata) between Conventional Systems and Blockchain-Based Systems

Aspect / Valid Agreement Requirement	Conventional Electronic Contract System	Blockchain & Smart Contract-Based System
Mutual Consent	- Consent expressed by click/check - Unilateral clause changes without adequate notice - Change history not permanently documented - Users rarely read all clauses	- Consent via digital signature on each version - Each change requires consensus mechanism among parties - Change history stored immutably and publicly accessible - Audit trail allows independent verification
Lawful Cause (including data protection)	- Centralized database vulnerable to breaches and manipulation - Users have no independent verification mechanism - Data violations often not detected in real-time	- Cryptographic hashing and distributed validation ensure data integrity - Every node can verify data authenticity without central authority - Data manipulation immediately detected due to hash change

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Aspect / Valid Agreement Requirement	Conventional Electronic Contract System	Blockchain & Smart Contract-Based System
Capacity & Specific Subject Matter	- Capacity verification depends on user input - Object of agreement (terms and conditions) can change unilaterally	- Smart contract can be programmed to verify capacity via decentralized identity - Subject matter recorded in immutable code
Legal Certainty & Evidence	- Electronic evidence recognized by ITE Law but vulnerable to authenticity disputes - Data changes can occur without trace	- Hash and timestamp evidence recognized as an integral electronic document - Every transaction has an incontestable audit trail

Source: Compiled by the author based on case data and literature, 2026.

The table above systematically shows how blockchain optimizes each valid requirement of an agreement compared to conventional systems. Regarding mutual consent, blockchain eliminates blind consent practices by providing a permanent and transparent history of changes. Regarding lawful cause, blockchain replaces trust in a central authority with distributed cryptographic verification, so data integrity is mathematically guaranteed. Regarding capacity and specific subject matter, smart contracts can be programmed to automate identity verification and ensure that the subject matter of the agreement does not change after consent is given. Regarding legal certainty and evidence, blockchain provides much stronger evidence tools than

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

centralized system logs, because each transaction has a timestamp and hash that anyone can independently verify (Mufrihah and Najmudin 2024).

However, the optimization of blockchain for transparency and data integrity does not automatically replace the role of civil law. This technology functions as a supporting tool that strengthens proof and certainty, not as a substitute for the principle of consensualism, freedom of contract, or substantive justice that lies at the heart of contract law. In other words, blockchain cannot cure defects of consent such as duress, mistake, or fraud regulated under Articles 1321 to 1328 of the KUHPerdata (Purnama 2025). If an agreement is given through a smart contract but occurs due to duress or fraud, the agreement may still be voidable even though the transaction is perfectly recorded on the blockchain. Therefore, civil law remains the normative framework that determines substantive justice, while blockchain acts as a technical infrastructure that strengthens evidentiary integrity and process transparency.

The effectiveness of blockchain also depends heavily on two external factors: first, the parties' understanding of the technological mechanisms used, and second, legal recognition of the digital evidence produced by blockchain. The first factor is important because blockchain is not easily accessible to the general public without education and user-friendly interfaces (Putra 2025). The second factor determines whether blockchain data can be accepted as valid evidence in court. Fortunately, Article 5 paragraph (1) of the ITE Law has recognized electronic information and electronic documents as valid legal evidence, complementing the evidence regulated in Article 1866 of the KUHPerdata. However, this recognition remains general in nature and has not specifically regulated blockchain as a distributed ledger with decentralized characteristics. Therefore, more specific implementing regulations are needed, for example, recognition of blockchain hash evidence as a form of certified electronic signature or as an electronic document that fulfills the elements of integrity and authenticity as regulated in Article 11 of the ITE Law in conjunction with Government Regulation Number 71 of 2019.

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Thus, synergy between technological innovation and an adaptive legal framework is an absolute requirement for realizing transparent and high-integrity civil contracts in Indonesia. Blockchain is not a magic solution, but a highly potential instrument if placed in the right position: as a verification and automation layer that complements, rather than replaces, the well-established principles of contract law. Blockchain optimization must be accompanied by regulatory reform that provides legal certainty, clear technical standards, and dispute resolution mechanisms that accommodate the unique characteristics of this technology. Only with such a holistic approach can Indonesia harness blockchain to enhance transparency and data integrity in civil contract transactions, while maintaining public trust in the national legal system.

Regulatory and Technical Challenges of Blockchain Optimization in the Indonesian Civil Contract Legal System

Although blockchain offers great potential to enhance transparency and data integrity in civil contract transactions as described in the previous section, the implementation of this technology in Indonesia still faces various regulatory and technical challenges. These challenges cannot be ignored because if not systematically addressed, blockchain optimization will remain a normative discourse without real impact on the practice of electronic agreements in the country. Regulatory challenges relate to the absence of a comprehensive and specific legal framework governing blockchain and smart contracts, while technical challenges concern infrastructure limitations, scalability, security, and interoperability between platforms (Aminin 2024). Both types of challenges are closely interrelated because technical weaknesses can give rise to legal issues, and conversely, the absence of clear regulations hinders investment and the development of reliable technical solutions. Therefore, this section will elaborate on these various challenges in depth and offer necessary policy directions so that blockchain can be optimally and responsibly utilized within the Indonesian civil contract legal system.

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Regulatory challenges become the primary obstacle that is most urgent to address. To date, Indonesia does not have a law or regulation at the statutory level that specifically and comprehensively regulates blockchain and smart contracts. The existing regulations are fragmentary, scattered across various legal instruments of different levels and authorities. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments recognize the validity of electronic contracts and electronic signatures but do not explicitly recognize smart contracts as a valid form of automatic agreement (Apriani et al. 2023). Bank Indonesia Regulation Number 19/12/PBI/2017 on Financial Technology Implementation only covers blockchain in the context of payment systems and digital financial services, so it does not apply to general civil contracts outside the financial sector. Meanwhile, various regulations of the Financial Services Authority (OJK) and the Commodity Futures Trading Regulatory Agency (Bappebti) are more oriented toward consumer protection in the financial services and futures trading sectors, without touching the fundamental aspects of contract law. As a result of this fragmentation, serious legal uncertainty arises regarding the position of smart contracts in the national legal system. Can automatic execution by computer code be equated with voluntary performance by the parties as referred to in Article 1234 of the KUHPerdata concerning default? Can technical failures in smart contracts, such as bugs in the code or exploit attacks, be classified as default or as force majeure under Articles 1244 and 1245 of the KUHPerdata? These fundamental questions remain unanswered due to the absence of adequate regulations or jurisprudence.

Regulatory uncertainty also creates serious problems regarding dispute resolution for blockchain-based contracts. In conventional contracts, the parties have the freedom to choose litigation in a district court or arbitration through institutions such as BANI or the National Arbitration Agency of Indonesia. In smart contracts, automatic execution occurs without human intervention based on "if-then" logic that has been programmed. If an execution error occurs, for example, the system transfers a digital asset due to fulfillment of a condition that is wrong because of input error or cyberattack, how can the parties restore the original situation? The principle of

irreversibility in public blockchains is a major obstacle because data already recorded in the blockchain cannot be deleted or changed. The Jakarta Barat District Court Decision Number 588/Pdt.G/2020, as discussed earlier, shows that arbitration clauses in conventional electronic agreements are recognized as valid by the courts. However, in a smart contract, the determination of the dispute resolution institution and the mechanism to "stop" automatic execution have not been standardized. Should the parties insert an emergency stop clause or arbitration clause into the smart contract code? What if that code cannot be changed due to the principle of immutability? Without an adequate legal umbrella, parties harmed by a defective smart contract will have difficulty obtaining justice, or conversely, automatic execution could be used to commit unlawful acts (Arsal et al. 2025).

Table 2. Regulatory and Technical Challenges of Blockchain Optimization in the Indonesian Civil Contract Legal System

Type of Challenge	Specific Aspect	Impact on Blockchain Optimization	Regulatory/Technical Needs
Regulatory	- No specific law on blockchain and smart contracts - Regulations scattered in ITE Law, PBI, OJK, Bappebti	- Legal uncertainty regarding smart contract validity - Difficulty determining legal liability for technical failures - Barrier to investment and innovation	- Drafting specific law or revision of KUHPerdata & ITE Law - Explicit recognition of smart contracts as valid agreements - Rules on technical force majeure and developer liability

Damhil Law Journal
e-ISSN 2808-7143
Fidhela Putri Fadhila, 2026. "Optimization of Blockchain: Realizing Transparency and Data Integrity in Civil Law Contract Transactions" Damhil Law Journal 6 (1): 48-73

Type of Challenge	Specific Aspect	Impact on Blockchain Optimization	Regulatory/Technical Needs
Regulatory	- Dispute resolution mechanism not accommodated	- Automatic execution of smart contract difficult to stop legally - Principle of blockchain immutability conflicts with need for correction	- Mandatory provision of emergency stop or arbitration clause in code - Recognition of court/arbitral awards requiring hard fork or compensation transactions
Regulatory	- Personal data protection not fully synchronized	- Public blockchain is transparent, conflicting with privacy by design principle of PDP Law - Right to erasure difficult to apply on blockchain	- Use of hybrid (permissioned) blockchain for sensitive data - Store only hash on blockchain, actual data off-chain
Technical	- Limited scalability (low transactions per second)	- Public blockchains like Bitcoin/Ethereum unsuitable for	- Development of layer-2 solutions (Lightning Network, Rollups) - Adoption of blockchains

Type of Challenge	Specific Aspect	Impact on Blockchain Optimization	Regulatory/Technical Needs
		large-scale contract transactions - High gas fees	with efficient consensus (PoS, DAG)
Technical	- Security risks of 51% attacks and code exploits	- Significant financial losses as in Bitcoin Gold 2018 case - Smart contract vulnerabilities can be exploited (re-entrancy attack)	- Mandatory standardization of smart contract code audits - Cyber insurance for high-value transactions
Technical	- Low interoperability among blockchain platforms	- Contract data on one blockchain cannot be verified by another blockchain - Obstacles to cross-platform asset or information transfer	- Development of interoperability protocols (Polkadot, Cosmos) - Standardization of contract data format across blockchains

Type of Challenge	Specific Aspect	Impact on Blockchain Optimization	Regulatory/Technical Needs
Technical	- Shortage of human resources proficient in both law and blockchain	- Judges, lawyers, notaries struggle to handle blockchain disputes - Gap between technical and legal understanding	- Massive certification and training programs in legal technology - Collaboration between law and informatics faculties

Source: Compiled by the author based on data from the 2018 Bitcoin Gold case, literature on blockchain scalability, and analysis of the PDP Law, 2026.

The table above systematically summarizes the various regulatory and technical challenges hindering blockchain optimization in Indonesia. On the regulatory side, the absence of a specific law causes legal uncertainty regarding the validity of smart contracts, legal liability, and dispute resolution. On the technical side, limited scalability, security risks, low interoperability, and a scarcity of human resources constitute concrete obstacles that require technological and institutional solutions (Chairunnas et al. 2024). These two groups of challenges cannot be separated because good regulation must be based on adequate technical understanding, while secure technical development requires regulatory certainty.

The most pressing technical challenge is scalability. Public blockchain systems like Bitcoin and Ethereum (before its upgrade to proof-of-stake) can only process around 7 to 15 transactions per second (TPS), far behind conventional payment systems like Visa, which can process thousands of TPS. This limitation creates serious obstacles when blockchain is used for large-scale civil contract transactions,

for example, in e-commerce involving millions of users daily (Juwita et al. 2025). As a result, transaction queues become long and gas fees skyrocket when the network is congested. This condition is inefficient and uneconomical for low-value contracts. Although various layer-2 solutions such as the Lightning Network for Bitcoin and Rollups for Ethereum have been developed, their implementation is still immature, and not all blockchain platforms support them. In addition, the high energy consumption of blockchains using proof-of-work mechanisms (like Bitcoin) also raises environmental concerns that may conflict with Indonesia's commitment to sustainable development.

Security risks are another equally important technical challenge. The 51% attack on the Bitcoin Gold blockchain in 2018 demonstrated that blockchains with inadequate security can be attacked by an actor controlling more than half of the network's computing power. In that attack, the attacker successfully performed double spending and caused financial losses of approximately US$18 million. This incident provides an important lesson that not all blockchains are created equal; smaller and less decentralized blockchains are more vulnerable to attacks. Moreover, vulnerabilities in smart contract code are often exploited, such as the re-entrancy attack that caused a loss of US$60 million in the Decentralized Autonomous Organization (DAO) on the Ethereum network in 2016 (Kusyanti and Trisnawan 2024). In Indonesia, there are no national security standards for smart contracts or a mandatory requirement for independent third-party security audits. As a result, users of blockchain-based contracts in Indonesia face high risks without adequate protection mechanisms (Martinelli et al. 2024).

Another technical challenge is interoperability between blockchains. Currently, there are hundreds of different blockchain platforms, each with protocols, data formats, and consensus mechanisms that are incompatible with one another. A civil contract created on the Ethereum network cannot be directly verified or executed on the Solana or Hyperledger Fabric networks. This inability to communicate between blockchains creates ecosystem fragmentation and hinders cross-platform data and asset exchange. Yet, in modern business practice, parties may use different

blockchains for various purposes (for example, one party uses Ethereum for smart contracts while another party uses a government-owned blockchain). Without interoperability standards, blockchain optimization for civil contract transactions will be limited to closed ecosystems (Mawa, n.d.).

To address these various challenges, concrete and coordinated steps are needed among the government, regulators, industry players, and academics. First, the government should immediately draft specific regulations recognizing smart contracts as valid electronic agreements, as long as they meet the requirements of Article 1320 of the KUHPerdata and the principle of prudence. Such regulations must include provisions on the liability of code developers, mandatory security audits, emergency stop mechanisms that can be integrated into smart contracts, and minimum standards to prevent 51% attacks or code exploits. Second, the development of hybrid (permissioned) blockchains for sensitive civil contract sectors is necessary, so that certain authorities (e.g., notaries or arbitration institutions) still have supervisory access without eliminating the advantages of decentralization. Third, strengthening the capacity of human resources in the field of legal technology, including judges, lawyers, notaries, and academics, is an absolute prerequisite for effective law enforcement in blockchain disputes (Megawati et al. 2023). Certification programs, training, and cross-disciplinary curricula between law faculties and informatics engineering should be vigorously promoted. Fourth, the government should also encourage research and development of a secure, scalable, and interoperable national blockchain infrastructure, for example, by building a public blockchain jointly supervised by the government and private institutions.

Thus, blockchain optimization is not merely a matter of technology adoption, but also of comprehensive legal and institutional reform. Only by simultaneously and integrally addressing the regulatory and technical challenges can Indonesia harness the full potential of blockchain to realize transparency and data integrity in civil contract transactions, while maintaining legal certainty, justice, and protection of the parties' rights. Without serious efforts to overcome these challenges, blockchain will

remain a peripheral technology without significant impact on Indonesia's contract law system, and its great potential will be wasted.

Conclusion

Blockchain technology, through its distributed ledger and smart contract mechanisms, has proven capable of optimizing transparency and data integrity in civil contract transactions in Indonesia, particularly in fulfilling the requirements of mutual consent and lawful cause as regulated under Article 1320 of the KUHPerdata. Blockchain permanently and immutably records every version of an agreement, creating a transparent audit trail so that consent is given based on complete and verifiable information, while simultaneously guaranteeing the integrity of personal data through cryptographic hashing and distributed validation. However, its implementation still faces serious regulatory challenges, namely the absence of a specific law explicitly recognizing smart contracts and governing dispute resolution as well as legal liability for technical failures, in addition to technical challenges such as limited scalability, security risks (51% attacks and code exploits), and low interoperability among platforms. To that end, synergy is required between regulatory reform (drafting a blockchain law, recognizing hash evidence, and establishing smart contract audit standards) and the development of secure, scalable technical infrastructure supported by competent legal-tech human resources. Blockchain optimization will only be realized if an adaptive legal framework and technical readiness go hand in hand, so that Indonesia can utilize this technology to enhance legal certainty, justice, and the protection of the parties in digital contracts.

References

Al-Fatih, Sholahuddin. 2023. *Perkembangan Metode Penelitian Hukum Di Indonesia*. UMMPress. https://books.google.com/books?hl=id&lr=&id=EObiEAAAQBAJ&oi=fnd&pg=PA1&dq=METODE+PENELITIAN+HUKUM&ots=PJKedSYwUv&sig=DoDC383UMZfVB4GCpfjCEJ9sPvA.

Algifari, Muhamad Hafid, and Adit Prasetyo. 2025. "Permasalahan Hukum Dalam Penggunaan Blockhain Untuk Kontrak Cerdas." *Journal of Applied Computing and Digital Information* 1 (01): 15–24.

Aminin, Rista Izza. 2024. "Analisis Implementasi Teknologi Blockchain Dalam Meningkatkan Transparansi, Efisiensi, Dan Keamanan Transaksi Keuangan Perbankan Syariah Indonesia." *Jurnal Hukum Ekonomi Syariah: AICONOMIA* 3 (2): 92–106.

Ananda, Rizky, and Kenzi Katon Rinjani. 2025. "Implementasi Blockchain Untuk Transparansi Dan Keamanan Rantai Pasok Komponen Elektronik." *Journal of Engineering and Technological Science* 1 (1): 16–23.

Apriani, Desy, Nadia Nur Azizah, Nova Ramadhona, and Dhiyah Ayu Rini Kusumawardhani. 2023. "Optimasi Transparansi Data Dalam Rantai Pasokan Melalui Integrasi Teknologi Blockchain." *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi* 2 (1): 1–10.

Arsal, Muryani, Nurfadilah Saleh, Nurwinda Lestari, and Adhelia Paramitha. 2025. "Transformasi Akuntansi Keuangan Melalui Blockchain: Menjamin Keandalan Dan Transparansi Di Era Digital." *Jurnal Akuntansi, Manajemen Dan Ilmu Ekonomi (Jasmien)* 5 (02): 609–20.

Chairunnas, Arnadi, Efendi Sugianto, Rina Pratiwi, Michael Sitorus, and Bambang Cahyono. 2024. "Teknologi Blockchain Dalam Transformasi Keuangan Dan Perbankan: Potensi Dan Tantangan." *Journal of Economic Education and Entrepreneurship Studies* 5 (2): 357–68.

Chic, Sebastian Areen, and Muhammad Fardian Bilqisthi. 2024. "Tantangan Dan Peluang Blockchain Di Era Digital Dalam Bidang Keamanan Data Dan Transaksi Digital." *Journal of Comprehensive Science (JCS)* 3 (11). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=29624738&AN=183397168&h=%2FrP%2FWq6julMDpy9Ml%2BTJuGJmLAOSisxfeuJ3SdaaYJ4shGZvwQFPX12%2FickYEAxUO6ItGvwMxmSWLesSBi8mlQ%3D%3D&crl=c.

Hidayat, Hermawan, Abdul Azis Van Gobel, Roy Marthen Moonti, and Muslim A. Kasim. 2025. "Tinjauan Potensi Dan Tantangan Penerapan Teknologi Blockchain Dalam Sistem Hukum." *Jembatan Hukum: Kajian Ilmu Hukum, Sosial Dan Administrasi Negara* 2 (2): 437–45.

Hutabarat, Hasbullah Maulana Hadi, and Novien Rialdyli. 2026. "Analisis Pengaruh Penerapan Blockchain Terhadap Transparansi Dan Efisiensi Operasional Di

Bank Syariah Indonesia (BSI)." *Wawasan: Jurnal Ilmu Manajemen, Ekonomi Dan Kewirausahaan* 4 (1): 76–84.

Juwita, Zahwa, Febri Yollanda, Mita Azira, and Zul Azmi. 2025. "Penerapan Blockchain Dalam Meningkatkan Keamanan Akuntansi Dan Transparansi Sistem Informasi Akuntansi." *Jurnal Akuntansi Keuangan Dan Perpajakan | E-ISSN: 3063-8208* 1 (3): 339–45.

Kasim, Hariani, Ahmad Muyassar Ibrahim, and Zul Fadli Ahmad. 2025. "Implementasi Teknologi Blockchain Pada Pengelolaan Data Akademik." *Jurnal INSTEK (Informatika Sains Dan Teknologi)* 10 (1): 211–22.

Kusumawati, Evyana Diah. 2025. "Integrasi Teknologi Blockchain Terhadap Transparansi, Akuntabilitas, Dan Efisiensi Dalam Sistem Pengadaan Barang Dan Jasa Di Sektor Maritim." *JURNAL TRANSPORTASI DAN MANAJEMEN MARITIM (TRANSMA)* 1 (2): 87–96.

Kusyanti, Ari, and Primantara Hari Trisnawan. 2024. "Implementasi Teknologi Blockchain Dengan Sistem Smart Contract Pada Klaim Asuransi." *Jurnal Teknologi Informasi Dan Ilmu Komputer* 11 (5): 1105–12.

Martinelli, Imelda, Nabilla Mahva Tsabita, Amanda Fitriani Eka Putri, and Devina Novela. 2024. "Legalitas Dan Efektivitas Penggunaan Teknologi Blockchain Terhadap Smart Contract Pada Perjanjian Bisnis Di Masa Depan." *UNES Law Review* 6 (4): 10761–76.

Mawa, Rizky Maulana. n.d. *Penerapan Teknologi Blockchain Dalam Meningkatkan Transparansi Dan Keamanan Data Siswa*. Accessed June 12, 2026. https://www.researchgate.net/profile/Rizky-Mawa/publication/388960212_PENERAPAN_TEKNOLOGI_BLOCKCHAIN_DALAM_MENINGKATKAN_TRANSPARANSI_DAN_KEAMANAN_DATA_SISWA/links/67ae7af3645ef274a4802161/PENERAPAN-TEKNOLOGI-BLOCKCHAIN-DALAM-MENINGKATKAN-TRANSPARANSI-DAN-KEAMANAN-DATA-SISWA.pdf.

Megawati, Leny, Cecep Wiharma, and Asep Hasanudin. 2023. "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia." *Jurnal Hukum Mimbar Justitia* 9 (2): 410–35.

Meisinta, Ainun, Tessa Icha Ananda, Wike Pebriana, and Gustian Djuanda. 2026. "Blockchain Dan Asuransi Parametrik: Otomatisasi, Privasi & Kepercayaan."

Penerbit Tahta Media. http://tahtamedia.co.id/index.php/issj/article/view/1909.

Mufidah, Muthmainnatun, and Achmad Tubagus Surur. 2025. "Integrasi Blockchain Dan Smart Contracts: Inovasi Dalam Pengelolaan Keuangan Syariah Yang Transparan Dan Efisien." *Sahmiyya: Jurnal Ekonomi Dan Bisnis*, 50–56.

Mufrihah, Wilda Malika, and Nandang Najmudin. 2024. "Transformasi Hukum Dagang Internasional Di Era Teknologi Blockchain Dan Cryptocurrency." *Ikraith-Ekonomika* 7 (3): 382–96.

Muhaimin, Faiq Daffa. n.d. *Pemanfaatan Blockchain Untuk Keamanan Dan Transparansi Data Akademik*. Accessed June 12, 2026. https://www.researchgate.net/profile/Faiq-Muhaimin/publication/388964567_PEMANFAATAN_BLOCKCHAIN_UNTUK_KEAMANAN_DAN_TRANSPARANSI_DATA_AKADEMIK/links/67aebae94c479b26c9dfdae9/PEMANFAATAN-BLOCKCHAIN-UNTUK-KEAMANAN-DAN-TRANSPARANSI-DATA-AKADEMIK.pdf.

Mulyanto, Ferry, and Ayi Purbasari. 2024. "Solusi Arsitektur Berbasis Blockchain Untuk Manajemen Rantai Pasokan Yang Transparan." *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi* 2 (2): 197–206.

Purnama, Sri Intan. 2025. "Blockchain & Sistem Informasi Akuntansi (B-SIA): Tinjauan Sistematis Terhadap Transparansi Dan Keamanan Data." *E-Journal Studia Manajemen* 14 (1): 1–14.

Putra, Ravi Azzura. 2025. "Blockchain Untuk Keamanan Data Dan Pendeteksian Pemalsuan Dalam Rantai Pasok Barang Mewah." https://www.researchgate.net/profile/Ravi-Azzura-Putra/publication/388838303_BLOCKCHAIN_UNTUK_KEAMANAN_DATA_DAN_PENDETEKSIAN_PEMALSUAN_DALAM_RANTAI_PASOK_BARANG_MEWAH/links/67a998518311ce680c5adcab/BLOCKCHAIN-UNTUK-KEAMANAN-DATA-DAN-PENDETEKSIAN-PEMALSUAN-DALAM-RANTAI-PASOK-BARANG-MEWAH.pdf.

Putranto, Muhamad Fajar, Pandi Zulfikar, Mustofa Kamil, and Hasnah Aziz. 2024. "Analisis Penerapan Blockchain Dalam Penyelenggaraan Administrasi Pemerintahan Dan Keuangan Negara Untuk Meningkatkan Kepastian Dan Kepatuhan Hukum: Studi Kasus Di Estonia." *J. PEMANDHU* 5 (2): 103–19.

Simatupang, Thresia Tiatira, and Heni Dwi Iryanti. 2024. "Eksplorasi Potensi Teknologi Blockchain Untuk Meningkatkan Transparansi Rantai Pasok

Pelabuhan Di Indonesia." *Proceeding of National Seminar on Maritime and Interdisciplinary Studies* 3 (1): 125–41. http://e-journal.akpelni.ac.id/index.php/NSMIS/article/view/472.

Sirimorok, Nurdiansyah, Masnur Masnur, Wahyu Arthanugraha, Darul Kaharman, Syahirun Alam, and Muhammad Zainal. 2025. "Simulasi Blockchain Untuk Transparansi Transaksi Pada Akun Game Online." *Jurnal Ilmiah Sistem Informasi* 5 (2): 711–20.

Supriyati, Endang, Mohammad Iqbal, and Tri Listyorini. 2025. "Teknologi Blockchain Dan Aplikasi Terdistribusi: Tinjauan Komprehensif Dan Roadmap Implementasi." *Jurnal Dialektika Informatika (Detika)* 6 (1): 32–38.