

Legal Certainty of Smart Contracts: The Validity of Evidence for Blockchain-Based Agreements in Civil Procedure Law

Noviya Anis*
Jambi University, Jambi, Indonesia

Abstract. *The rapid global adoption of blockchain technology has given rise to smart contracts, self-executing digital agreements that automatically perform contractual obligations once predetermined conditions encoded in the distributed ledger are satisfied. While these instruments promise efficiency, transparency, and reduced transaction costs, they raise fundamental questions of legal certainty, particularly concerning their validity as agreements and their admissibility as evidence in civil litigation. This study examines the legal certainty of smart contracts by analyzing the extent to which blockchain-based agreements satisfy the validity requirements of civil law and constitute legitimate evidence under civil procedure law, with particular attention to the Indonesian legal system. Using a normative juridical method combined with statutory and comparative approaches, the study analyzes primary, secondary, and tertiary legal materials. The findings indicate that smart contracts can generally satisfy the substantive requirements of contract formation, yet their evidentiary treatment remains fragmented across jurisdictions due to differing conceptions of authenticity, integrity, and evidentiary weight. Comparative analysis reveals divergent regulatory responses, ranging from explicit statutory recognition to reliance on general electronic evidence doctrines. The study proposes a framework of formal validity, authentication mechanisms, and judicial assessment guidelines to strengthen legal certainty for blockchain-based evidence in civil procedure, and recommends supplementary technical regulation for the Indonesian judiciary.*

Keywords: Smart Contract; Blockchain; Legal Certainty; Electronic Evidence; Civil Procedure Law

Received: 12 14, 2025 | **Revised:** 01 05, 2026 | **Accepted:** 01 23, 2026 | **Published Online:** 01 28, 2026

Correspondence:

Noviya Anis
anisnoviyanoviya@gmail.com



1. Introduction

The proliferation of blockchain technology over the past decade has fundamentally transformed the way contractual relationships are formed, recorded, and enforced. Among its most consequential applications is the smart contract, a self-executing computer protocol that automatically implements the terms of an agreement once predefined conditions encoded within the blockchain are satisfied.¹ Unlike conventional agreements that depend on the continuing willingness of the parties or the intervention of a third party for performance, smart contracts operate autonomously, immutably, and transparently across a distributed ledger, thereby narrowing much of the discretion traditionally exercised by contracting parties and courts alike.² This technological innovation has been rapidly adopted across commercial

¹Rahman (2024).

²Dwivedi, Pattanaik, Deval, Dixit, Norta, & Draheim (2021).

sectors, including supply chain management, financial services, insurance, and cross-border trade, owing to its capacity to reduce transaction costs, minimize counterparty risk, and streamline the resolution of commercial contract disputes.³

In Indonesia, the growth of digital commerce, peer-to-peer financing platforms, and cryptocurrency-based transactions has created increasing practical demand for self-executing contractual instruments, even though no dedicated statute currently governs the formation, performance, or evidentiary treatment of smart contracts. Businesses and individuals engaging in blockchain-based transactions therefore operate within a regulatory environment where the enforceability of their agreements, and the weight that a court will attach to the underlying blockchain data if a dispute arises, cannot be predicted with confidence. This uncertainty is compounded by the transnational character of many blockchain networks, which frequently involve nodes, validators, and counterparties located outside Indonesian jurisdiction, raising additional questions of applicable law and cross-border judicial cooperation that existing civil procedure doctrine was not designed to address.

Despite these advantages, the deployment of smart contracts has outpaced the development of legal frameworks capable of accommodating their distinctive technical characteristics. Civil law systems, including Indonesia's, have historically constructed their doctrines of contract validity around the assumption of deliberate human agency expressed through negotiation, signature, or conduct.⁴ The Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata/KUHPerdata) requires that a valid agreement satisfy four cumulative conditions under Article 1320: the consent of the parties who bind themselves, the capacity to enter into an agreement, a certain object, and a lawful cause.⁵ The extent to which self-executing code, rather than a continuously expressed act of will, can be said to embody the requisite consent of the parties remains a matter of ongoing scholarly and judicial contention, and Indonesian commentators have only recently begun to articulate criteria for assessing conformity between coded logic and the civil code's consent requirement.⁶ Comparable uncertainty exists in numerous jurisdictions: Polish civil procedure has struggled to reconcile blockchain-generated data with conventional standards of documentary proof;⁷ Kazakh legislation continues to debate the civil law qualification of smart contracts alongside their evidentiary function in judicial proceedings;⁸ and courts in the United States have only recently begun to articulate the evidentiary significance of blockchain records within existing rules of procedure.⁹

³Absi, Mulyati, & Suakanto (2026).

⁴Sudarto (2025).

⁵Wilson, Hutapea, & Sulistiyono (2024).

⁶Sari (2026).

⁷Kaczmarek-Templin (2023).

⁸Otebaliyeva, Shaimukhanova, Erzhanova, & Adibayeva (2026).

⁹Wang, Wu, & Ma (2024).

The second, and arguably more pressing, dimension of legal uncertainty concerns the evidentiary status of blockchain-based agreements once a dispute reaches litigation. Civil procedure law, both in Indonesia and in comparative jurisdictions, traditionally recognizes a closed or semi-closed catalogue of evidence comprising written documents, witness testimony, presumptions, admissions, and oaths.¹⁰ The admission of electronic evidence, including blockchain records, is generally accommodated through specific legislation such as Indonesia's Law No. 19 of 2016 on Electronic Information and Transactions (UU ITE), which recognizes electronic information and electronic documents as valid extensions of documentary evidence provided that their authenticity and integrity can be demonstrated.¹¹ However, the cryptographic architecture of blockchain, characterized by pseudonymous participants, decentralized custody, and algorithmic immutability, complicates the conventional evidentiary requirements of authentication and chain of custody.¹² Although blockchain's tamper-resistant design is frequently cited as a guarantee of evidentiary reliability, scholars caution that immutability alone does not equate to legal authenticity, particularly where the underlying data entered into the ledger may itself be erroneous, fraudulent, or disputed prior to its recording.¹³

Efforts to resolve these tensions have produced markedly different regulatory responses across jurisdictions. Some countries have moved toward explicit recognition of blockchain-based records within existing evidentiary institutions, exemplified by frameworks in Brazil that extend notarial functions to blockchain infrastructure,¹⁴ while others continue to rely on judicial interpretation of general electronic evidence provisions, often resulting in inconsistent evidentiary outcomes from one case to the next.¹⁵ Indonesian scholarship has likewise begun to interrogate whether existing civil procedural instruments, principally the *Herzien Inlandsch Reglement* (HIR) and the UU ITE, are adequate to address blockchain-specific evidentiary questions, or whether supplementary regulation is required to accommodate the technology's distinct evidentiary profile.¹⁶ Recent studies further indicate that Indonesian legal practitioners and judges frequently lack the technical literacy necessary to assess the probative weight of blockchain data, creating a practical gap between statutory recognition and judicial application.¹⁷

Prior scholarship on smart contracts and blockchain evidence has tended to proceed along two largely separate tracks. The first strand addresses the substantive civil law validity of smart contracts, examining whether self-executing code can satisfy the formation requirements of an enforceable agreement, and proposing doctrinal adjustments to

¹⁰Latifah Soroinda & Soroinda Nasution (2022).

¹¹Wulandari & Priyono (2025).

¹²Santamaría, Tobarra, Pastor-Vargas, & Robles-Gómez (2023).

¹³Efimova, Sizemova, & Chirkov (2021).

¹⁴Menezes, De Araújo, & Nishijima (2023).

¹⁵Pulatov (2025).

¹⁶Alvian, Harianja, & Satya (2026).

¹⁷Lubis & Purba (2024).

accommodate algorithmic consent and automated performance.¹⁸ The second strand, drawn predominantly from digital forensics and computer science literature, focuses on the technical mechanisms by which blockchain systems preserve the integrity and chain of custody of digital evidence, including cryptographic hashing, distributed consensus, and smart-contract-based evidence management frameworks.¹⁹ While both strands offer valuable insights, they rarely intersect: doctrinal studies of contract validity seldom engage with the procedural mechanics of evidentiary admission, while technical studies of blockchain evidence management rarely address the doctrinal standards of proof recognized under civil procedure law.²⁰ Comparative doctrinal studies spanning civil law and common law jurisdictions confirm that this fragmentation is not unique to Indonesia but reflects a broader global unevenness in how legal systems reconcile automated performance with established rules of contract formation and proof.²¹

The novelty of this study lies in its integration of these two strands into a single analytical framework specifically oriented toward civil procedure law. Rather than treating the validity of smart contracts and the admissibility of blockchain evidence as separate inquiries, this research examines how the technical characteristics of blockchain-based agreements, namely immutability, pseudonymity, decentralization, and algorithmic execution, interact with the formal and material evidentiary standards imposed by civil procedure law, and how this interaction shapes the legal certainty available to litigants and judges. By synthesizing comparative regulatory experience from multiple jurisdictions alongside Indonesia's own evidentiary doctrine, this study constructs a framework of criteria, comprising formal validity, authentication mechanisms, and judicial assessment guidelines, intended to guide the evaluation of blockchain-based evidence in civil disputes. This integrative approach distinguishes the present study from previous research, which has generally examined either the substantive validity of smart contracts or the technical reliability of blockchain evidence, but not the intersection of the two within the specific procedural architecture of civil evidence law.

Given the accelerating use of smart contracts in commercial practice and the corresponding absence of settled evidentiary doctrine, the question of legal certainty is not merely theoretical. It bears directly on the capacity of civil courts to adjudicate disputes arising from blockchain-based transactions in a predictable, consistent, and technically sound manner. This study accordingly seeks to answer two central questions: first, to what extent do smart contracts satisfy the substantive validity requirements of civil law; and second, how should blockchain-based data be evaluated as evidence within the formal and material standards of civil procedure law, drawing on comparative practice to inform recommendations for the

¹⁸Eshonkulov (2025).

¹⁹Philip & Saravanaguru (2022).

²⁰Kaya, Konca, & Kiyak (2026).

²¹Maydanyk (2024).

Indonesian legal system. Answering these questions is a necessary precondition for building public and judicial confidence in blockchain-based commerce, without which the technology's efficiency gains risk being offset by unresolved litigation costs and inconsistent adjudication.

2. Research Methods

This study employs a normative juridical (*yuridis normatif*) method, which examines law as a coherent system of norms, principles, and doctrines rather than as a social phenomenon to be measured empirically. The research relies on three complementary approaches: a statute approach, examining the relevant primary legal materials, including the Indonesian Civil Code (KUHPerdata), the *Herzien Inlandsch Reglement* (HIR), and Law No. 19 of 2016 on Electronic Information and Transactions (UU ITE); a comparative approach, analyzing regulatory and judicial practice in Poland, Kazakhstan, Brazil, Malaysia, and the United States; and a conceptual approach, drawing on doctrinal literature concerning contract formation and evidentiary theory. Secondary legal materials consist of books, peer-reviewed journal articles, and legal commentaries, while tertiary materials include legal dictionaries and academic databases used to verify terminology and cross-check citation accuracy. Data were collected through library and document research and analyzed using a qualitative descriptive-analytical technique, in which legal materials are systematically classified, compared, and interpreted to identify normative gaps between existing civil procedure doctrine and the technical characteristics of blockchain-based smart contracts, culminating in the construction of the proposed framework of legal certainty.

3. Result and Discussion

3.1 The Legal Nature and Validity of Smart Contracts under Civil Law

Under Indonesian civil law, the validity of any agreement, including a smart contract, is measured against the four cumulative requirements of Article 1320 of the KUHPerdata: the consent of the parties who bind themselves, the capacity to enter into an agreement, a certain object, and a lawful cause.²² Analysis of smart contract architecture suggests that the requirements of a certain object and a lawful cause are generally capable of being satisfied, since the terms encoded within the contract are typically definite and quantifiable, and the underlying transaction, whether the transfer of digital assets, execution of a payment, or performance of a service, is ordinarily lawful.²³ The more contested requirements are consent and capacity. Because a smart contract executes automatically once predetermined conditions are met, questions arise as to whether the parties' consent is genuinely present at the moment of execution, or whether it is merely presumed from the parties' initial act of deploying or

²²Wilson, Hutapea, & Sulistiyono (2024).

²³Absi, Mulyati, & Suakanto (2026).

interacting with the code.²⁴ Several scholars argue that consent can be satisfied at the point of code deployment or digital signature, provided the parties possessed adequate understanding of the code's operative logic at that time, a position broadly consistent with the principle of freedom of contract under Article 1338 of the KUHPerdata.²⁵ Others caution that the opacity of code to non-technical parties may undermine the quality of consent, particularly where standard-form smart contracts are deployed without meaningful negotiation, a concern echoed in consumer protection scholarship examining blockchain-based e-commerce transactions.²⁶

Comparative practice illustrates a spectrum of doctrinal responses to this tension. Regional scholarship examining dispute resolution and public policy across the ASEAN+6 region generally treats smart contracts as legally neutral instruments, that is, technical mechanisms for performing obligations that remain governed by the general civil law of the underlying jurisdiction rather than as an entirely distinct category of contract.²⁷ Central Asian scholarship has approached the same question from the standpoint of legal qualification, cautioning that treating source code as self-sufficient evidence of agreement risks displacing the courts' traditional role in interpreting the parties' true intention where the coded terms are ambiguous or incomplete.²⁸ Indonesian scholarship has converged on a comparable view, holding that smart contracts are not inherently invalid under the KUHPerdata, but that their conformity with the Civil Code depends heavily on the manner in which consent is documented and communicated prior to code deployment, and on whether the parties retain a meaningful opportunity to review the contractual logic before it becomes irrevocable.²⁹

A related but distinct question concerns the capacity of Indonesian civil law. Article 1330 of the KUHPerdata restricts contractual capacity to persons who are of legal age and not placed under guardianship, a standard premised on the assumption that a human party can be identified and evaluated at the moment of contracting.³⁰ Blockchain networks, however, frequently permit participation through pseudonymous wallet addresses, meaning that a counterparty's legal capacity, and at times even legal personality, cannot be verified from the transaction record alone. This creates a structural tension between the technology's design and a doctrinal requirement that was conceived for a world of identifiable, physically present contracting parties. Where capacity cannot be independently verified, the burden shifts to the party seeking to enforce the smart contract to establish, through supplementary evidence, that its counterparty possessed the requisite legal capacity at the time the agreement was concluded, a burden that conventional written contracts rarely impose because signatories are typically identified by name and accompanying identification documents.

²⁴Sari (2026).

²⁵Sari (2026).

²⁶Tresnawati & Fatmawati (2021).

²⁷Goh (2022); Sinitsyn, Diakonova, & Chursina (2021).

²⁸Pulatov (2025); Eshonkulov (2025).

²⁹Alvian, Harianja, & Satya (2026).

³⁰Wilson, Hutapea, & Sulistiyono (2024).

3.2 Blockchain Data as Electronic Evidence in Civil Procedure Law

Even where a smart contract satisfies the substantive requirements of contract validity, its function as evidence in civil litigation depends on separate procedural criteria. Indonesian civil procedure law recognizes five categories of evidence under Article 164 of the HIR and Article 1866 of the KUHP: written evidence, witness testimony, presumptions, admissions, and oaths.³¹ Electronic records, including blockchain data, are accommodated within the category of written evidence through Law No. 19 of 2016 on Electronic Information and Transactions, which extends legal recognition to electronic information and electronic documents provided their authenticity, integrity, and accessibility can be demonstrated.³² The practical application of this provision to blockchain-based smart contracts, however, raises distinct challenges. Because blockchain records are distributed across a decentralized network rather than held by a single custodian, conventional chain-of-custody procedures, which presume a linear and traceable transfer of evidence from one identifiable party to another, must be reconceived to account for consensus-based verification across multiple nodes.³³

Technical solutions proposed in the digital forensics literature offer partial responses to this challenge. Blockchain-based chain-of-custody frameworks, for instance, employ smart contracts themselves to timestamp and cryptographically seal each transfer of evidentiary custody, thereby producing an auditable and tamper-evident record that can be independently verified by the court.³⁴ Comparable frameworks have been developed for digital evidence management in vehicular accident investigations, demonstrating the feasibility of using blockchain infrastructure not merely as the subject matter of a dispute but as a mechanism for preserving the evidentiary record itself throughout the litigation process.³⁵ Nonetheless, these frameworks presuppose a level of technical literacy among judges, court officials, and legal practitioners that is not yet uniformly present in Indonesian judicial practice, where recent studies indicate a persistent gap between the statutory recognition of electronic evidence and its practical evaluation in the courtroom.³⁶ Comparative experience in the United States illustrates that even where courts are willing to recognize blockchain evidence, its evidentiary weight is often reduced by unresolved questions of authentication and expert qualification, requiring courts to develop new evidentiary standards specific to distributed ledger technology on a case-by-case basis.³⁷

³¹Latifah Soroinda & Soroinda Nasution (2022).

³²Wulandari & Priyono (2025).

³³Santamaría, Tobarra, Pastor-Vargas, & Robles-Gómez (2023).

³⁴Santamaría, Tobarra, Pastor-Vargas, & Robles-Gómez (2023).

³⁵Philip & Saravanaguru (2022).

³⁶Lubis & Purba (2024).

³⁷Wang, Wu, & Ma (2024).

3.3 Comparative Practices: Divergent Approaches to Evidentiary Weight

A comparative review of jurisdictional responses reveals considerable divergence in how blockchain-based agreements and their associated data are treated as evidence in civil proceedings. Table 1 summarizes the principal legal basis and evidentiary orientation adopted in six jurisdictions examined in this study.

Jurisdiction	Primary Legal Basis	Evidentiary Orientation	Key Challenge
Indonesia	UU ITE (Law No. 19/2016 jo. No. 11/2008); HIR; KUHPperdata	General electronic evidence doctrine; no smart-contract-specific rule	Judicial technical literacy gap; unresolved authentication standards
Poland	EU electronic-evidence framework (eIDAS) and Civil Procedure Code	General documentary evidence doctrine applied case-by-case	Absence of smart-contract-specific evidentiary rules
Kazakhstan	Civil Code and emerging digital-asset legislation	Civil law qualification debated; evidentiary use extends to criminal proceedings	Unsettled qualification of smart contracts as instruments or technical tools
Brazil	Civil law notarial framework extended to blockchain	Blockchain records treated as functionally equivalent to notarized instruments	Integrating blockchain infrastructure with existing notarial institutions
Malaysia	Electronic signature and conveyancing regulations	Attestation-based recognition once authentication protocols are met	Remote/video-based attestation and identity verification
United States	State-level blockchain statutes and evolving case law	Judicially developed evidentiary standards, not yet codified nationally	Fragmented, jurisdiction-specific case law; expert qualification requirements

The comparative data in Table 1 indicate that jurisdictions vary not only in the specificity of their statutory frameworks but also in the underlying evidentiary philosophy applied to blockchain data. Brazil and Malaysia have extended existing notarial or attestation frameworks to accommodate electronic and blockchain-based instruments, effectively treating blockchain records as functionally equivalent to notarized documents once specific

authentication protocols are satisfied.³⁸ By contrast, Poland and Kazakhstan continue to apply general electronic evidence doctrines without smart-contract-specific provisions, leaving courts to determine evidentiary weight on a case-by-case basis and often requiring expert testimony to establish the technical reliability of the blockchain record.³⁹ The United States exhibits an intermediate position, in which judicial precedent has begun to articulate blockchain-specific evidentiary standards without corresponding statutory codification, resulting in a body of case law that remains fragmented across jurisdictions.⁴⁰ Indonesia's current framework most closely resembles the Polish and Kazakh model: general recognition of electronic evidence exists under the UU ITE, but no specific statutory or judicial guidance addresses the unique evidentiary characteristics of blockchain-based smart contracts.⁴¹

This divergence carries practical consequences for litigants engaged in cross-border blockchain transactions. A party relying on blockchain-recorded performance to prove a contractual claim in an Indonesian court cannot presently predict whether the evidence will be assessed under the relatively permissive documentary standard applied to conventional electronic records, or subjected to a heightened evidentiary burden akin to that observed in United States case law, where courts have sometimes required independent expert corroboration of a blockchain's technical integrity before assigning it evidentiary weight.⁴² The absence of a settled position within Indonesian jurisprudence means that outcomes may vary significantly depending on the individual judge's technical familiarity and willingness to admit expert testimony, undermining the predictability that civil procedure law is meant to secure for commercial actors.

3.4 Toward a Framework of Legal Certainty for Blockchain-Based Evidence

The preceding analysis suggests that legal certainty for blockchain-based agreements in civil procedure law cannot be achieved through reliance on general electronic evidence doctrine alone. Three elements are proposed as the foundation of a more coherent framework. First, formal validity requires that the parties' consent be demonstrably established prior to the automated execution of contractual terms, whether through digital signature, verifiable identity credentials, or documented agreement to the code's operative logic, thereby satisfying Article 1320 of the KUHPerdata notwithstanding the automated nature of performance.⁴³ Second, authentication mechanisms should be developed to verify the integrity of blockchain data at the point of judicial submission, drawing on cryptographic hash verification and distributed consensus records, supplemented where necessary by expert witness testimony as recognized

³⁸Menezes, De Araújo, & Nishijima (2023); Wong, Muhamad, Durovic, Azmi, Abu Bakar, & Thomas (2022).

³⁹Kaczmarek-Templin (2023); Otebaliyeva, Shaimukhanova, Erzhanova, & Adibayeva (2026).

⁴⁰Wang, Wu, & Ma (2024).

⁴¹Alvian, Harianja, & Satya (2026).

⁴²Wang, Wu, & Ma (2024).

⁴³Wilson, Hutapea, & Sulistiyono (2024).

under Article 154 of the HIR.⁴⁴ Third, judicial assessment guidelines are needed to standardize how courts evaluate the probative weight of blockchain-based evidence, including protocols for assessing the reliability of the underlying blockchain network, the qualifications required of technical expert witnesses, and the treatment of pseudonymous transaction data in establishing the identity of contracting parties.⁴⁵

These proposed elements respond directly to the gaps identified in comparative practice. Where jurisdictions such as Brazil have achieved a measure of legal certainty by integrating blockchain records into existing notarial frameworks, Indonesia's evidentiary architecture would benefit from a similarly structured integration, situating blockchain-based evidence within, rather than outside, its existing procedural categories, while supplementing the UU ITE with technical guidelines issued through Supreme Court regulation (Peraturan Mahkamah Agung) to standardize judicial practice.⁴⁶ Absent such measures, the evidentiary treatment of smart contracts in Indonesian civil litigation is likely to remain inconsistent, dependent on the technical literacy of individual judges and the persuasiveness of expert testimony presented by the parties, rather than on settled and predictable legal standards.⁴⁷

The proposed framework also carries implications for legal practice beyond adjudication. Notaries, legal counsel, and compliance officers structuring blockchain-based transactions would benefit from standardized documentation practices that record the parties' consent and identity verification prior to code deployment, thereby pre-empting later disputes over formal validity. Financial technology providers operating smart-contract platforms in Indonesia could likewise be required, through sectoral regulation, to maintain auditable records of contracting parties' identities and to retain technical logs sufficient to satisfy future authentication requests from courts. Such preventive measures would reduce reliance on after-the-fact expert reconstruction of blockchain transactions, which is often costly and, given the shortage of judicially recognized blockchain forensic experts in Indonesia, not always readily available to litigants of ordinary means. Ultimately, legal certainty in this field depends on the coordinated action of legislators, the judiciary, and industry participants, rather than on doctrinal clarification alone

4. Conclusion

This study demonstrates that the legal certainty of smart contracts within civil procedure law depends on the resolution of two distinct but interrelated issues: the substantive validity of smart contracts as agreements under civil law, and the evidentiary treatment of blockchain-based data within the procedural standards of civil litigation. The analysis indicates that smart contracts can generally satisfy the substantive requirements of Article 1320 of the KUHPerdata,

⁴⁴Philip & Saravanaguru (2022).

⁴⁵Kaya, Konca, & Kiyak (2026).

⁴⁶Menezes, De Araújo, & Nishijima (2023).

⁴⁷Lubis & Purba (2024).

provided that adequate consent and verifiable capacity are established prior to automated execution. The evidentiary status of blockchain data, however, remains unsettled both in Indonesia and in comparative jurisdictions, owing to the absence of specific statutory or judicial guidance addressing blockchain's decentralized custody, pseudonymity, and cryptographic verification methods. Comparative analysis reveals that jurisdictions integrating blockchain records into existing notarial or documentary evidence frameworks, rather than treating them as an entirely novel category of evidence, have achieved greater consistency in judicial outcomes. This study accordingly recommends that Indonesian civil procedure law be supplemented with technical guidelines, potentially through Supreme Court regulation, establishing authentication protocols, expert witness standards, and judicial assessment criteria for blockchain-based evidence, thereby strengthening legal certainty for parties engaging in blockchain-based agreements and reducing the litigation risk currently associated with this emerging form of contracting evolving systems, and that even the European Union's more advanced regulatory apparatus remains incomplete following the 2025 withdrawal of its proposed AI Liability Directive. The article accordingly proposes a risk-tiered accountability framework combining strict liability for high-risk AI operators, reversed evidentiary burdens modeled on the EU's revised Product Liability Directive, mandatory insurance mechanisms, and a principled allocation of responsibility among developers, operators, and users based on control and benefit rather than mere causal proximity. For Indonesia specifically, the recommended path is a targeted *lex specialis* regulation on AI civil liability that supplements, rather than replaces, Articles 1365 and 1367 of the Civil Code, thereby closing the practical evidentiary gap facing victims of algorithmic harm without prematurely committing the legal system to unresolved questions of AI subjecthood. Future research should examine how Indonesian courts interpret Article 1367 in early AI-related disputes as they arise, and should further explore the design of sector-specific insurance pools for high-risk AI applications in healthcare and financial technology.

References

- Absi, W. Z., Mulyati, R., & Suakanto, S. (2026). Integration of blockchain-based smart contracts in the resolution of commercial contract disputes. *Journal of Legal and Cultural Analytics*. <https://doi.org/10.55927/jlca.v5i1.16233>
- Alvian, S., Harianja, H., & Satya, A. M. (2026). Smart contract integration in Indonesian law: Legal certainty and data protection in the digital age. *Perspektif Hukum*. <https://doi.org/10.30649/ph.v26i1.446>
- Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally enforceable smart-contract languages. *ACM Computing Surveys*, 54(5), 1–34. <https://doi.org/10.1145/3453475>
- Efimova, L., Sizemova, O., & Chirkov, A. (2021). Smart contracts: Between freedom and strict legal regulation. *Information & Communications Technology Law*, 30(3), 333–353. <https://doi.org/10.1080/13600834.2021.1889759>

- Eshonkulov, J. (2025). The role of smart contracts in civil law and issues of legal regulation. *Uzbek Journal of Law and Digital Policy*. <https://doi.org/10.59022/ujldp.294>
- Goh, G. R. D. E. (2022). Smart contract disputes and public policy in the ASEAN+6 region. *Digital Law Journal*, 3(4), 32–70. <https://doi.org/10.38044/2686-9136-2022-3-4-32-70>
- Kaczmarek-Templin, B. (2023). Smart contract – Problems with taking evidence in Polish civil proceedings in the light of European regulations. *Bratislava Law Review*, 7(1). <https://doi.org/10.46282/blr.2023.7.1.308>
- Kaya, S., Konca, N. K., & Kiyak, E. (2026). The evidentiary value of blockchain in civil litigation: Comparative insights and future directions. *Frontiers in Blockchain*, 9. <https://doi.org/10.3389/fbloc.2026.1783805>
- Latifah Soroina, D., & Soroina Nasution, A. A. R. (2022). Kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata. *Jurnal Hukum & Pembangunan*, 52(2), 384–405. <https://doi.org/10.21143/jhp.vol52.no2.3344>
- Lubis, F., & Purba, S. R. (2024). Analisis kritik pembuktian elektronik dalam hukum acara perdata: Tantangan dan prospek di era digital. *Judge: Jurnal Hukum*, 5(2), 39–47. <https://doi.org/10.54209/judge.v5i02.570>
- Maydanyk, R. (2024). Smart contract on a crypto assets in the civil law and common law jurisdictions: Implementation of best practices. *Open Journal for Legal Studies*. <https://doi.org/10.32591/coas.ojls.0702.01015m>
- Menezes, L. D., De Araújo, L. V., & Nishijima, M. (2023). Blockchain and smart contract architecture for notaries services under civil law: A Brazilian experience. *International Journal of Information Security*, 22, 1–12. <https://doi.org/10.1007/s10207-023-00673-3>
- Otebaliyeva, K., Shaimukhanova, Z. T., Erzhanova, Z., & Adibayeva, A. (2026). Smart contracts in Kazakh legislation: Problems of civil law qualification and evidence in criminal proceedings. *Eurasian Scientific Journal of Law*. <https://doi.org/10.46914/2959-4197-2026-1-2-268-282>
- Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, 34(7), 4031–4046. <https://doi.org/10.1016/j.jksuci.2022.06.001>
- Pulatov, T. (2025). Smart contracts in the civil law system: Problems of legal qualification. *Uzbek Journal of Law and Digital Policy*. <https://doi.org/10.59022/ujldp.298>
- Rahman, S. (2024). Smart contracts: The blockchain revolution in contract law. *International Journal for Multidisciplinary Research*. <https://doi.org/10.36948/ijfmr.2024.v06i03.23553>
- Santamaría, P., Tobarra, L., Pastor-Vargas, R., & Robles-Gómez, A. (2023). Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study. *Smart Cities*, 6(2), 678–694. <https://doi.org/10.3390/smartcities6020034>
- Sari, I. P. (2026). Legal certainty in the conformity of smart contracts with the Indonesian civil code. *Priviet Social Sciences Journal*. <https://doi.org/10.55942/pssj.v6i2.1574>
- Sinitsyn, S., Diakonova, M., & Chursina, T. (2021). Smart-contracts in the digital economy: Contractual regulation and dispute resolution. *Digital Law Journal*, 2(4), 40–50. <https://doi.org/10.38044/2686-9136-2021-2-4-40-50>



- Sudarto, S. (2025). Smart contracts from a civil law perspective: Validity and implementation in Indonesia. *Jurnal Ilmiah Hukum Dirgantara*. <https://doi.org/10.35968/jihd.v15i2.1444>
- Tresnawati, T., & Fatmawati, A. M. (2021). Blockchain-based smart contract: Advancing digital consumer protection and preventing private international law e-commerce cases. *Yustisia Jurnal Hukum*. <https://doi.org/10.20961/yustisia.v10i3.54891>
- Wang, X., Wu, Y., & Ma, Z. (2024). Blockchain in the courtroom: Exploring its evidentiary significance and procedural implications in U.S. judicial processes. *Frontiers in Blockchain*, 7. <https://doi.org/10.3389/fbloc.2024.1306058>
- Wilson, K., Hutapea, H., & Sulistiyono, A. (2024). Keabsahan smart contract dengan teknologi blockchain menurut Kitab Undang-Undang Hukum Perdata. *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*. <https://doi.org/10.62383/aliansi.v1i3.177>
- Wong, H. S., Muhamad, M. M., Durovic, M., Azmi, I. M. A. G., Abu Bakar, N., & Thomas, R. (2022). Electronic signature and attestation in conveyancing practice: A Malaysian legal perspective. *F1000Research*, 10, 1088. <https://doi.org/10.12688/f1000research.73548.3>
- Wulandari, A. H., & Priyono, E. (2025). Validity of electronic contracts as evidence in the settlement of civil disputes. *International Journal of Social Science and Human Research*, 8(7). <https://doi.org/10.47191/ijsshr/v8-i7-48>