Volume 4 Number 2 (2026)
July-December 2026
Page: 159-186

E-ISSN: 2987–095X
DOI: 10.37680/JSHEL.v4i2.10577

JSHEL
Journal of Sharia Economic Law

Evidentiary Challenges in Electronic Agreements in Digital Economic Transactions: Reconstructing Legal Certainty and the Protection of the Parties

Nabila Secioria C.G[1], Aditya Maulana Rizky[2]

[1] Muhammadiyah University of Gombong, Indonesia; nabilasecioria@unimugo.ac.id
[2] Muhammadiyah University of Gombong, Indonesia; Aditmauriz@unimugo.ac.id

Received: 23/07/2026 Revised: 15/08/2026 Accepted: 29/08/2026

Abstract

Digital transformation has fundamentally reshaped contractual relationships, particularly in digital economic transactions. Electronic agreements offer efficiency and convenience but also raise evidentiary challenges concerning party authentication, document integrity, electronic signatures, system reliability, and transaction traceability. This study examines the legal position and evidentiary strength of electronic agreements in digital economic transactions. It proposes a reconstruction of evidentiary mechanisms to strengthen legal certainty and protect the parties. Using normative juridical research with statutory, conceptual, and case approaches, the study analyzes Indonesian legal regulations and the development of electronic evidence in civil proceedings. The findings show that Indonesian law recognizes electronic information and electronic documents as legally valid evidence. However, their evidentiary strength depends on establishing the authenticity, integrity, reliability, and traceability of electronic transactions. Accordingly, this study proposes a Four-Parameter Reconstruction Model comprising Authentication, Integrity, System Reliability, and Transaction Traceability. The model provides an integrated framework for verifying the identity and authority of contracting parties, maintaining document integrity, assessing system reliability, and establishing verifiable transaction trails. The study concludes that the model can strengthen evidentiary mechanisms, legal certainty, balanced party protection, trust, and efficiency in the digital economy.

Keywords Electronic Agreements; Electronic Evidence; Digital Economic Transactions; Legal Certainty; Legal Protection

Corresponding Author
Nabila Secioria C.G
Muhammadiyah University of Gombong, Indonesia; nabilasecioria@unimugo.ac.id

1. INTRODUCTION

Digital transformation has fundamentally altered the way economic relationships are established, performed, and documented. Digital transformation has fundamentally altered the formation and performance of contractual relationships, particularly in electronic commerce, where agreements are increasingly concluded without physical interaction between the parties (Siregar, 2025). The growth of e-commerce, digital financial services, and platform-based transactions has shifted contractual practices

Published by Institut Agama Islam Sunan Giri (INSURI), Ponorogo, Indonesia
Accredited Sinta 4

from physical documents and face-to-face interactions toward electronic agreements formed and executed through electronic systems. This transformation offers substantial benefits in transaction speed, accessibility, and efficiency. Still, it also creates new legal challenges regarding the reliability of contractual evidence and the protection of parties in digital transactions. The development of electronic contracting has consequently required legal systems to adapt traditional concepts of contract formation, attribution, authentication, and proof to transactions conducted through digital technologies. At the international level, the development of electronic commerce law has been guided by the principles of non-discrimination, technological neutrality, and functional equivalence, which seek to ensure that electronic communications are not denied legal effect merely because they are in electronic form. (UNCITRAL, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996)

Recent studies indicate that electronic contracts have become an increasingly important legal instrument in Indonesian business and e-commerce transactions. In contrast, questions concerning validity, enforceability, evidentiary value, and legal certainty remain relevant (Vivi Sylvia Purborini, 2026). Recent studies continue to identify uncertainty concerning electronic consent, authentication, evidentiary reliability, and the protection of parties in digital transactions. (Atika Putri Jayanti, 2025)

An electronic agreement is, in essence, a conventional contract concluded electronically. From a juridical perspective, its validity and legal consequences remain governed by the general principles of contract law as outlined in Book III of the Indonesian Civil Code, particularly the requirements of consent, capacity, a certain subject matter, and a lawful cause under Article 1320. At the same time, Law Number 1 of 2024 amending the Electronic Information and Transactions Law recognizes Electronic Information and/or Electronic Documents and their printed forms as valid legal evidence. This recognition represents an important adaptation of Indonesian law to digital economic activities. (A. F. Salsabila, 2024). Nevertheless, the recognition of electronic documents as legally admissible evidence does not automatically resolve the question of their evidentiary weight or reliability. (Danuri, 2019)

At the same time, Law Number 1 of 2024 amending the Electronic Information and Transactions Law recognizes Electronic Information and/or Electronic Documents and their printed forms as valid legal evidence. This recognition represents an important adaptation of Indonesian law to digital economic activities. Nevertheless, the recognition of electronic documents as legally admissible evidence does not automatically resolve the question of their evidentiary weight or reliability. The distinction between legal admissibility and evidentiary strength is particularly important where the opposing party challenges the origin, authenticity, integrity, or reliability of an electronic record. (Roslaili, 2025)

The international development of electronic commerce law similarly demonstrates that legal recognition of electronic communications must be accompanied by rules concerning attribution, reliability, and the functions traditionally performed by written documents and signatures (UNCITRAL, 2001). The central problem has therefore shifted from whether electronic agreements are legally recognizable to how their authenticity, integrity, attribution, and reliability can be established in the event of a dispute. In conventional agreements, physical documents and handwritten signatures have historically served as relatively familiar mechanisms for establishing consent and identifying the contracting parties. In electronic transactions, however, contractual consent may be expressed through electronic signatures, click-based acceptance, electronic correspondence, platform interfaces, biometric authentication, or automated systems. These forms of interaction may complicate the identification of the contracting party and the determination of whether an electronic record accurately reflects the agreement actually reached.

The attribution of an electronic communication is particularly important because the legal effect of an electronic transaction depends upon establishing a sufficient connection between the electronic record and the person or entity alleged to have generated or authorized it. Recent research has identified authentication, identity verification, validity of consent, and evidentiary reliability as continuing challenges to legal certainty in electronic contracts (Rahmawati Sabila, 2025). These challenges are consistent with the broader principle that an electronic signature or authentication method should perform the essential functions of identifying the signatory and indicating approval of the information contained in an electronic communication. The concept of electronic evidence in this study refers to information or documents generated, transmitted, received, or stored through an electronic system that are presented to establish legally relevant facts. Authentication refers to the process of establishing that an electronic record or electronic action can be attributed to the person or entity claimed to have created or performed it.

Integrity refers to the ability to demonstrate that the content of an electronic record has remained complete and has not been altered in an unauthorized manner. Reliability concerns the extent to which the electronic system and processes used to create, store, or transmit the record can be trusted. These concepts are particularly important because the evidentiary value of an electronic agreement depends not merely on the existence of a digital file but also on the circumstances surrounding its creation, authentication, preservation, and presentation before a court (Anike Rasyida Inayah, 2025). From an evidentiary perspective, therefore, an electronic document should not be assessed solely according to its digital form but also according to the reliability of the process through which the information was generated and maintained.

The existing literature has predominantly examined the validity of electronic contracts under conventional contract law, the recognition of electronic documents as evidence, and the protection of consumers or weaker parties in digital transactions. Some studies emphasize the formal validity of electronic contracts under the Indonesian Civil Code and the Electronic Information and Transactions Law. In contrast, others focus on legal certainty and consumer protection in e-commerce transactions (Susanty, 2026). Other research examines the validity and evidentiary value of electronic documents and electronic signatures in Indonesian legal proceedings. Research on biometric-based electronic contracts further demonstrates that technological authentication mechanisms may strengthen security while simultaneously creating new legal questions concerning consent and legal certainty.

Meanwhile, studies concerning smart contracts and digital notarization indicate that technological developments continue to challenge existing legal frameworks concerning contractual validity and evidentiary force (I Nyoman Wahyu Ariartha, 2025). These developments demonstrate that electronic contracting cannot be understood solely by extending conventional contractual concepts to digital environments; rather, the evidentiary characteristics of digital systems must also be considered.

Another strand of research proposes stronger authentication mechanisms to address problems of identity verification and contractual consent. For example, a digital authentication model involving notarial mechanisms has been proposed to strengthen legal certainty in electronic commerce (Andrian Danul Firmansyah, 2026). Such approaches demonstrate that the development of digital contracting requires not only recognition of electronic agreements but also mechanisms to establish the parties' identities and the reliability of the transaction process. At the international level, the development of legal frameworks concerning electronic signatures and identity management likewise reflects the importance of reliable authentication mechanisms in digital transactions. (UNCITRAL, 2002)

At the same time, emerging technologies such as artificial intelligence and automated contracting systems raise additional questions concerning attribution, contractual consent, and legal responsibility (Ery Agus Priyono, 2025). The adoption of the UNCITRAL Model Law on Automated Contracting in 2024 further demonstrates that automated systems and AI-assisted transactions are raising new legal questions regarding attribution and the legal effect of outputs produced by automated processes. (UNCITRAL, 2024)

The development of electronic evidence also demonstrates the importance of maintaining the integrity and reliability of digital records throughout their lifecycle. Unlike conventional documentary evidence, electronic information can be reproduced, transferred, modified, and stored across multiple systems. Consequently, proving the integrity of an electronic agreement may require evidence concerning the processes through which the record was created, transmitted, stored, and retrieved. The reliability of the electronic system is therefore closely connected to the evidentiary value of the record produced by that system. This perspective is consistent with the international approach to electronic signatures, which links the legal effectiveness of an electronic signature to the reliability of the method used in the circumstances in which the electronic communication was generated or communicated (UNCITRAL, 2001). Thus, authentication and integrity cannot be treated as isolated technical characteristics but must be evaluated together with the reliability of the electronic environment in which the transaction occurred.

However, a significant gap remains between the evidentiary dimension of electronic agreements and the economic consequences of legal uncertainty. Existing studies tend to examine contractual validity, electronic signatures, consumer protection, authentication, or technological developments separately. Less attention has been given to how these elements operate collectively as evidentiary parameters in disputes arising from digital economic transactions. The problem is therefore not merely whether electronic documents are admissible as evidence, but whether existing evidentiary mechanisms are sufficiently capable of establishing authenticity, integrity, reliability, and traceability when contractual relationships are disputed. This distinction is important because uncertainty in proving contractual relationships may increase contractual risk, dispute-resolution costs, and barriers to trust in digital transactions. The principles of functional equivalence and technological neutrality suggest that electronic transactions should be capable of performing functions comparable to those performed by conventional documents. However, the practical achievement of such equivalence depends upon the ability to establish the reliability and evidentiary continuity of the electronic record. (UNCITRAL, 1996)

From an economic perspective, evidentiary certainty has implications beyond procedural law. Digital transactions depend upon trust that contractual commitments can be verified and enforced when necessary. When parties are uncertain about the authenticity or integrity of electronic agreements, they may incur additional costs to verify transactions, mitigate risks, or resolve disputes. Consequently, evidentiary law performs not only a procedural function but also an economic function by contributing to the predictability and efficiency of contractual exchanges. The increasing use of digital platforms and automated contractual systems further underscores the importance of reliable, traceable electronic records in supporting complex economic relationships. The development of international legal instruments for electronic communications similarly reflects the broader objective of strengthening legal certainty and facilitating electronic commerce through predictable rules governing electronic contracting.

Against this background, this study aims to examine the legal position and evidentiary strength of electronic agreements in digital economic transactions within the Indonesian legal system; to identify the principal legal and evidentiary challenges relating to authentication, integrity, system reliability, and transaction traceability; and to formulate a reconstructed evidentiary mechanism that strengthens legal certainty and protection of the parties. The novelty of this study lies in the development of a Four-Parameter Evidentiary Reconstruction Model, consisting of Authentication, Integrity, System Reliability, and Transaction Traceability, as an integrated framework for assessing the evidentiary strength of electronic agreements. Unlike previous studies that predominantly examine contractual validity, electronic signatures, authentication, electronic evidence, or technological reliability as separate issues, this study integrates the four parameters into a single evidentiary framework. The proposed model establishes a logical connection between the identity of the parties (Authentication), the preservation of the electronic record (Integrity), the trustworthiness of the electronic environment (System Reliability), and the reconstruction of the transaction history (Transaction Traceability). Accordingly, the study contributes not merely to the recognition of electronic agreements as legally valid evidence but to the reconstruction of the mechanism by which their evidentiary strength can be systematically assessed in civil disputes. The model is expected to provide a conceptual and legal basis for strengthening evidentiary certainty, balancing the protection of contracting parties, and supporting trust and efficiency in the digital economy.

2. METHODS

This study employs normative juridical research to examine the legal and evidentiary challenges surrounding electronic agreements in digital economic transactions within the Indonesian legal system. Normative legal research is appropriate because the study examines law as a system of norms, including legislation, legal principles, legal doctrines, and judicial decisions, rather than through empirical investigation of the behavior of contracting parties (Negara, 2023). The research is directed toward identifying the applicable legal norms, assessing their adequacy in addressing the evidentiary characteristics of electronic agreements, and formulating a prescriptive reconstruction of the evidentiary mechanism. In accordance with the characteristics of normative legal research, the study employs three specific approaches: the statutory, conceptual, and case approaches (Chariansyah, 2026).

The statutory approach is used to examine the legal framework governing electronic agreements and electronic evidence in Indonesia, including the Indonesian Civil Code, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and other relevant legislation concerning electronic signatures, electronic systems, and digital transactions. Through this approach, the study examines the hierarchy, consistency, scope, and adequacy of the applicable legal provisions, particularly those concerning the legal validity of electronic agreements, the recognition of electronic information and electronic documents as evidence, electronic signatures, and the requirements for the integrity and reliability of electronic systems. The statutory approach is employed to identify whether the existing regulatory framework sufficiently accommodates the evidentiary characteristics of contemporary digital transactions.

The conceptual approach is used to examine legal concepts and doctrines relevant to the study, particularly the concepts of electronic agreements, electronic evidence, authentication, integrity, system reliability, transaction traceability, legal certainty, and legal protection. This approach is important because several concepts relevant to electronic evidence are not limited to statutory definitions but have developed through legal doctrine and technological practice. The conceptual analysis is used to construct the normative relationship among the four parameters proposed in this study: Authentication, Integrity, System Reliability, and Transaction Traceability**.** These concepts are subsequently synthesized into an integrated evidentiary framework for assessing the evidentiary strength of electronic agreements. The case approach is employed to examine judicial decisions that demonstrate how electronic evidence has been interpreted, authenticated, and assessed in judicial proceedings.

The case approach focuses on decisions that contain judicial reasoning concerning the admissibility, authenticity, integrity, reliability, or evidentiary value of electronic information or electronic documents. One of the principal decisions examined is Supreme Court Decision Number 1616 K/Pid.Sus/2013, which addresses the validity of electronic evidence under the Electronic Information and Transactions Law and discusses the formal and material requirements that electronic evidence must satisfy. The decision is relevant for examining the judicial treatment of the authenticity and legal validity of electronic evidence.

In addition, the study examines Decision Number 192/Pdt.G/2020/PA. A small quantity of the Bitung Religious Court, which provides a concrete illustration of judicial examination of electronic evidence in a civil proceeding. In that decision, the court considered aspects including availability, integrity, authenticity, security, and accessibility in assessing electronic evidence submitted by the parties. The decision is particularly relevant to this research because the judicial considerations demonstrate that the evidentiary value of electronic records depends not merely on their existence but also on their authenticity, integrity, and the conditions under which the electronic information can be verified. The case approach, therefore, does not merely identify the existence of electronic evidence in judicial proceedings but also analyzes **the** ratio decidendi, evidentiary requirements, and judicial reasoning used to assess such evidence. This approach allows the study to compare judicial practice with the requirements established by legislation and the conceptual framework developed in the study.

Legal materials are systematically classified into primary, secondary, and tertiary categories**.** Primary legal materials consist of authoritative legal sources, including the Indonesian Civil Code, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019 concerning the

Implementation of Electronic Systems and Transactions, regulations governing electronic signatures and electronic system providers, and relevant judicial decisions, particularly Supreme Court Decision Number 1616 K/Pid.Sus/2013 and Decision Number 192/Pdt.G/2020/PA.Bitg. Primary legal materials constitute the main normative basis for determining the legal position and evidentiary requirements of electronic agreements. The classification of legislation and judicial decisions as primary legal materials is consistent with the established methodology of normative legal research.

Secondary legal materials include peer-reviewed journal articles, academic books, legal monographs, scholarly commentaries, research reports, and other academic publications that discuss contract law, electronic agreements, electronic evidence, electronic signatures, digital authentication, digital forensics, legal certainty, and digital economic transactions. These materials are used to interpret, explain, and critically evaluate the primary legal materials and to identify developments in legal doctrine and scholarly debate concerning electronic contracting and electronic evidence.

Tertiary legal materials consist of legal dictionaries, encyclopedias, legal terminology references, bibliographic databases, and authoritative legal databases used to clarify legal concepts and technical terminology, and to provide references to primary and secondary legal materials. Tertiary materials are therefore used as supporting sources rather than as the principal basis for normative conclusions. The collection of legal materials is conducted through library research and document analysis. Relevant legislation, judicial decisions, scholarly publications, and legal references are identified, collected, classified, and examined according to their relevance to the research questions. Judicial decisions are selected based on substantive criteria, namely: (1) the decision contains consideration of electronic information or electronic documents as evidence; (2) the court addresses issues of authenticity, integrity, reliability, accessibility, or attribution; and (3) the decision provides judicial reasoning relevant to the evidentiary assessment of electronic transactions**.** This selection criterion ensures that the case approach is grounded in concrete judicial materials rather than merely on the existence of electronic evidence in court proceedings.

The collected legal materials are analyzed qualitatively and prescriptively through systematic interpretation, conceptual analysis, legal reasoning, and comparison between statutory provisions, judicial considerations, and relevant legal doctrines. The analysis proceeds through four stages: identification of applicable legal norms; examination of judicial reasoning concerning electronic evidence; identification of gaps and inconsistencies in the existing evidentiary framework; and normative reconstruction of the evidentiary mechanism. The results of the analysis are then synthesized into the proposed Four-Parameter Evidentiary Reconstruction Model, consisting of Authentication, Integrity, System Reliability, and Transaction Traceability. Through this methodology, the study seeks not only to describe the existing legal position on electronic agreements but also to formulate a prescriptive evidentiary framework to strengthen legal certainty and provide balanced protection for the parties in digital economic transactions.

3. FINDINGS AND DISCUSSION

The analysis reveals that the Indonesian legal framework has recognized electronic agreements and electronic documents as legally relevant instruments in digital economic transactions. Nevertheless, formal legal recognition does not automatically guarantee strong evidentiary value. An electronic agreement is, in essence, a conventional contract concluded electronically. From a juridical perspective, its validity and legal consequences remain governed by the general principles of contract law as outlined in Book III of the Indonesian Civil Code. (Hayati, 2026)

The principal problems identified in this study concern the authentication of contracting parties, the integrity of electronic records, the reliability of electronic systems, and the traceability of digital transactions. These problems demonstrate that the evidentiary framework for electronic agreements needs to move beyond the question of formal admissibility toward the question of reliability in establishing disputed contractual facts. This finding is consistent with previous scholarship indicating that although electronic evidence has been legally recognized in Indonesia, its probative value remains dependent upon the reliability of the electronic data and the mechanisms through which the data are generated, stored, authenticated, and presented before the court (Anike Rasyida Inayah, 2025). Makarim's analysis, in particular, demonstrates that the recognition of electronic data and electronic signatures must be accompanied by an assessment of their probative value in legal proceedings. (Makarim, 2013)

3.1. Legal Status of Electronic Agreements in Digital Economic Transactions

3.1.1. Electronic Agreements as Legally Binding Contracts

The transformation from conventional contracts to electronic agreements primarily concerns the medium through which consent to a contract is expressed rather than the fundamental requirements of contract formation. Article 1320 of the Indonesian Civil Code continues to set out the basic requirements for contractual validity: consent, legal capacity, a certain subject matter, and a lawful cause. Accordingly, the electronic form of an agreement does not by itself eliminate its contractual validity. This position is consistent with the principle of technological neutrality and functional equivalence developed in international electronic commerce law, particularly through the UNCITRAL Model Law on Electronic Commerce 1996**,** which establishes a framework for recognizing information in electronic form without discriminating against its electronic character (Makarim, 2013). The UNCITRAL Model Law specifically addresses information generated, sent, received, or stored through electronic means and provides a foundation for the legal recognition of electronic communications in commercial transactions.

The Indonesian legal position is also supported by contemporary research demonstrating that electronic contracts may produce binding legal consequences when the substantive requirements of contract law are satisfied. However, the digital environment creates additional issues concerning authentication, consent, attribution, and reliability of electronic records (Susanty, 2026). Although electronic documents, including those authenticated through electronic signatures, are legally recognized as evidence, disputes may still arise in judicial proceedings concerning their evidentiary classification and probative value, particularly whether they should be regarded as having the evidentiary character of an authentic deed or as a private instrument. Recent research confirms that Indonesian law formally recognizes electronic contracts and electronic documents, yet challenges persist regarding authentication, evidentiary reliability, and legal certainty (Hadiyanto, 2025). Article 18, paragraph (1) of the Indonesian Electronic Information and Transactions Law (ITE Law) stipulates that legally valid electronic transactions are binding upon the parties who conclude them. Accordingly, an electronic agreement may have the same legal force as a conventional written agreement, provided it meets the requirements for contractual validity set out in Article 1320 of the Indonesian Civil Code (Hermawan, 2024). Where the subject matter of an agreement is insufficiently clear or ascertainable, the agreement may be considered legally invalid or void (Martinelli, 2024).

This distinction is important because contractual validity and evidentiary strength are not identical concepts**.** An electronic agreement may be legally valid at the moment of formation. However, its evidentiary strength may subsequently become problematic when one party disputes the identity of the signatory, the content of the agreement, or the circumstances under which consent was expressed. Makarim (2013) emphasizes the importance of examining the probative value of electronic evidence rather than merely its electronic form, while identifying evidence and enforcement as continuing challenges to legal certainty in electronic contracts (Inayah, 2025).

3.1.2. Electronic Agreements as Evidence

Law Number 1 of 2024 recognizes Electronic Information and/or Electronic Documents as legally relevant evidence. This development demonstrates the adaptation of Indonesian evidentiary law to digital economic activities. Nevertheless, the existence of legal recognition does not mean that every electronic document automatically possesses the same evidentiary strength. Its probative value depends on whether the document can be authenticated and whether its integrity, reliability, and relationship to the relevant transaction can be demonstrated (Hayati, 2026). The regulatory framework concerning electronic signatures provides an additional evidentiary dimension. Government Regulation Number

71 of 2019 and Minister of Communication and Informatics Regulation Number 11 of 2022 establish a regulatory framework for electronic certification and electronic signature services. Regulation Number 11 of 2022 regulates the organization of electronic certification, supervision of PSrE, and the services associated with electronic certificates. Indonesian PSrEs are authorized, among other things, to verify the identity of prospective owners and/or owners of Electronic Certificates and to provide electronic certification services.

This regulatory structure demonstrates that Indonesian law has moved beyond merely recognizing electronic documents to creating institutional mechanisms that strengthen their evidentiary reliability. In particular, identity verification and electronic certificate validation directly support the Authentication parameter proposed in this study. Electronic signature and certificate mechanisms also contribute to the verification of the integrity of electronic records, while timestamping and preservation mechanisms support the Integrity and Transaction Traceability parameters (as set out in Minister of Communication and Informatics Regulation Number 11 of 2022 concerning the Governance of Electronic Certification). Therefore, the principal legal issue is not simply whether electronic evidence is admissible, but how its probative value should be assessed when the electronic agreement is in dispute**.** This position is consistent with research emphasizing that the legal recognition of electronic contracts does not completely resolve problems concerning evidentiary reliability and legal certainty (Anike Rasyida Inayah, 2025)

3.2. Evidentiary Challenges in Electronic Agreements

3.2.1. Authentication of the Contracting Parties

Authentication constitutes the first fundamental evidentiary challenge. In conventional transactions, identity can generally be established through physical presence, identification documents, and handwritten signatures. Digital transactions, however, frequently occur without direct physical interaction. In the context of digital business, this often creates issues, primarily because the parties' identities are not always clear. For instance, in a marketplace, buyers and sellers might use fake accounts. Therefore, digital platform operators are responsible for ensuring that a user identity verification system is in place to guarantee the validity of agreements made within their systems (Put**ra, 2025)**.

A transaction may be conducted through an account, a password, a one-time password, an electronic signature, biometric authentication, or a click-based agreement mechanism. Consequently, the existence of a digital record does not necessarily establish, by itself, who actually performed the electronic act. The problem becomes particularly significant when a party subsequently denies having agreed. Research on biometric-based electronic contracts demonstrates that biometric authentication may strengthen identification and security. However, Indonesian law has not yet comprehensively regulated biometrics as a form of electronic authentication or electronic signature in contractual relationships (Rahmawati Sabila, 2025). The study further identifies uncertainty concerning the legal status of biometric authentication and the protection of biometric data as important legal issues.

Similarly, research concerning electronic signatures identifies authentication and legal certainty as important issues in digital agreements. Demonstrate that the use of electronic signatures in e-commerce raises questions concerning the legal certainty of digital agreements and their evidentiary consequences (Muhammad Rizky Aji Perdana, 2025). The technical regulatory framework for PSrE provides a more concrete mechanism to address this problem. Minister of Communication and Informatics Regulation Number 11 of 2022 provides that Indonesian PSrE have authority to examine the correctness of the identity of prospective owners and/or owners of Electronic Certificates and to perform functions associated with electronic certification and validation. Therefore, the evidentiary analysis must distinguish between the existence of an electronic transaction and the attribution of that transaction to a particular legal subject**.** This distinction is central because contractual responsibility cannot reasonably be imposed without establishing who actually expressed the relevant consent. Under the Four-Parameter Model, this problem is specifically addressed through Authentication**.**

3.2.2. Integrity of Electronic Documents

The second challenge concerns the integrity of the electronic document. Unlike physical documents, electronic records can be copied, transferred, modified, and stored in multiple systems. Therefore, the mere presentation of a digital file does not necessarily establish that the file represents the original contractual agreement. The relevant legal question is whether the content presented in litigation remains identical to the content accepted by the parties when the agreement was formed. Digital signatures, electronic timestamps, encryption, audit trails, and preservation mechanisms may strengthen the ability to demonstrate document integrity. This principle is consistent with the functional-equivalence approach of the UNCITRAL Model Law on Electronic Commerce 1996, which seeks to ensure that electronic information can perform functions traditionally associated with paper-based information. (UNCITRAL, 1996)

The importance of integrity is also demonstrated by Indonesian judicial practice. In Putusan Pengadilan Agama Bitung Nomor 192/Pdt.G/2020/PA.Bitg**,** the court examined electronic evidence and considered requirements relating to authenticity, integrity, availability, security, accessibility, and the audit trail. This demonstrates that electronic evidence cannot be separated from the process through which it is obtained, maintained, and presented before the court. Thus, technological integrity must be accompanied by evidentiary verifiability. This finding is consistent with research on electronic signatures, which emphasizes that technological authentication mechanisms can provide stronger legal certainty when their technical reliability and legal requirements are simultaneously fulfilled (Muhammad Rizky Aji Perdana, 2025)

3.2.3. Reliability of Electronic Systems

The third challenge concerns the reliability of the electronic system used to create, transmit, process, or store the agreement. An electronic agreement is rarely an isolated document. It is usually generated through an ecosystem involving websites, applications, servers, databases, authentication systems, payment systems, and cloud infrastructure. Consequently, when an electronic agreement becomes the subject of litigation, the relevant evidence may include system-generated transaction records, authentication records, timestamps, payment records, electronic correspondence, access logs, and platform-generated notifications. The evidentiary object in digital transactions is therefore increasingly systemic rather than merely document-based.

This systemic character is consistent with the findings of contemporary research concerning the use of electronic evidence in Indonesian civil proceedings, which identifies the reliability of the electronic system and judicial assessment as important factors affecting the evidentiary value of electronic records. Research on electronic contracts similarly indicates that weak digital infrastructure and incomplete regulatory harmonization may affect legal certainty and enforcement. The Indonesian regulatory framework concerning PSrE further reinforces this systemic dimension. Minister of Communication and Informatics Regulation Number 11 of 2022 regulates the organization and supervision of electronic certification, including electronic certificate management and related certification services. Accordingly, System Reliability should be assessed not only from the appearance of the final electronic document but also from the reliability of the infrastructure that generated, transmitted, authenticated, and preserved it.

3.2.4. Traceability of Digital Transactions

The fourth challenge is transaction traceability. Traceability concerns the ability to reconstruct the sequence of events surrounding the formation and performance of an electronic agreement. In a digital transaction, evidence may need to establish when an offer was submitted, when acceptance occurred, which account performed the relevant action, when payment was made, whether the agreement was subsequently modified, and how the electronic system recorded those events. The importance of traceability is illustrated by judicial consideration of electronic evidence in Indonesia, particularly the emphasis on an audit trail in its examination. An audit trail allows the court to assess how the electronic record was generated and obtained, thereby contributing to the reconstruction of the evidentiary chain. Traceability is also supported by technical mechanisms such as electronic timestamps, electronic delivery records, and preservation services. These mechanisms provide information on the temporal and procedural history of an electronic transaction, thereby strengthening the ability to reconstruct the sequence of digital events. (Minister of Communication and Informatics Regulation Number 11 of 2022 concerning the Governance of Electronic Certification, 2022)

Accordingly, electronic evidence should not be assessed solely as a static document. It should also be evaluated within a chronological chain of digital events. This constitutes the normative basis for the Transaction Traceability parameter proposed in this study.

3.3. Judicial Interpretation and Case Approach

The case approach demonstrates that Indonesian courts have not treated electronic evidence as automatically probative merely because legislation recognizes electronic information as evidence. Judicial practice indicates that electronic evidence remains subject to examination of its authenticity, integrity, relevance, reliability, and the circumstances under which it was obtained and presented. A particularly relevant example is Putusan Pengadilan Agama Bitung Nomor 192/Pdt.G/2020/PA. Bitg. The case involved electronic evidence in the form of screenshots of WhatsApp and Instagram conversations, as well as printed transcripts. The court examined the formal and material aspects of electronic evidence and emphasized considerations relating to availability, integrity, authenticity, security, accessibility, and audit trail. This demonstrates that the court did not assess the evidence solely because it was presented in electronic form; rather, it examined whether the evidence could reliably establish the relevant facts.

The decision is particularly relevant to the Four-Parameter Model. The requirement of authenticity corresponds to Authentication; integrity corresponds directly to Integrity; security and the reliability of the electronic environment relate to System Reliability; while the audit trail corresponds to Transaction Traceability. A second example is Putusan Pengadilan Negeri Donggala Nomor 22/Pdt.G/2021/PN Dgl, decided on 21 February 2022. The case involved printed electronic evidence, including screenshots of online-store transactions and WhatsApp conversations. The Supreme Court's decision directs that printed electronic evidence, including screenshots of online store transactions and WhatsApp conversations, be presented. Subsequent academic analysis of this decision found that the court recognized electronic evidence when formal requirements and material requirements were satisfied, including printing, verification, relevance, and the absence of a successful challenge to authenticity. The study also found that electronic evidence submitted by the defendants was considered sufficient to establish relevant facts, while evidence submitted by the plaintiff lacked sufficient probative value. (HAKIM, 2025)

The two cases demonstrate an important judicial tendency: the electronic nature of evidence does not automatically determine its probative value**.** Instead, the court must examine whether the evidence is sufficiently reliable to establish the disputed facts. This judicial tendency strengthens the argument that Indonesian electronic evidence law should move from formal admissibility toward an integrated assessment of evidentiary reliability.

3.4. Evidentiary Reliability and Legal Certainty

The four challenges identified above demonstrate that electronic evidence has a multidimensional character. Each parameter addresses a different evidentiary question, but the parameters cannot be considered independently.

Table 1. Evidentiary Dimensions of Electronic Agreements and Their Legal Implications

Evidentiary Dimension	Question to Be Established	Relevant Legal/Technical Mechanism	Consequence if Uncertain	Supporting Evidence
Authentication	Who performed or authorized the electronic act?	Electronic Certificate, electronic signature, identity verification, account authentication	Uncertainty regarding identity and attribution	Electronic signature certificate, identity verification, and authentication records
Integrity	Has the content remained complete and unchanged?	Electronic signature, electronic timestamp, preservation, audit trail	Uncertainty regarding contractual terms	Original electronic file, timestamp, hash/audit records
System Reliability	Can the electronic system that generated or stored the record be trusted?	PSrE, security mechanisms, validation systems, system logs	Uncertainty regarding the reliability of system-generated evidence	Server logs, system records, validation records
Transaction Traceability	Can the chronology of the transaction be reconstructed?	Timestamp, transaction logs, audit trail, electronic delivery, and preservation	Uncertainty regarding contractual formation and performance	Transaction history, payment record, access log, notification record

Source: Author's analysis based on Law Number 1 of 2024, Government Regulation Number 71 of 2019, Minister of Communication and Informatics Regulation Number 11 of 2022, UNCITRAL Model Law on Electronic Commerce 1996, *and judicial considerations in Putusan PA Bitung No. 192/Pdt.G/2020/PA.Bitg and Putusan PN Donggala No. 22/Pdt.G/2021/PN Dgl.*

As shown in Table 1, each dimension addresses a different legal problem. However, they cannot be considered independently. A document with strong technical integrity has limited evidentiary value if there is no reliable evidence linking it to the contracting party. Conversely, authentication alone is insufficient if the content of the electronic document cannot be demonstrated to have remained unchanged. Likewise, an authenticated and intact document may still raise questions if the electronic system that generated or stored it cannot be shown to operate reliably. This finding supports an integrated evidentiary approach, in which the four parameters operate cumulatively rather than independently. Such an approach is compatible with the judicial treatment of electronic evidence in Indonesia and with international approaches emphasizing reliability and functional equivalence. (Makarim, 2013)

3.5. Protection of the Parties in Electronic Transactions

Evidentiary uncertainty also affects the protection of contracting parties. Digital economic transactions frequently involve an imbalance in access to information and technological resources. A digital platform or business entity may control system-generated records, while consumers or smaller business actors may possess only limited copies of the transaction. This creates an evidentiary imbalance (Susanty, 2026). The issue becomes particularly significant in standard-form electronic agreements. One party may simply click "agree" without having meaningful control over the contractual terms or the technological system that records the transaction. Research on electronic contracts has similarly identified an imbalance in bargaining power and limitations in authentication as continuing challenges to legal certainty in e-commerce transactions.

Therefore, the evidentiary framework should take into account which party controls the relevant electronic records. This study proposes the following normative principle: Greater Control over Electronic Evidence, Greater Responsibility for Preservation, Accessibility, and Reliability. This principle is particularly relevant where one party controls the platform, database, authentication mechanism, or transaction records. The regulatory framework for PSrE further demonstrates that entities involved in electronic certification are subject to institutional and technical requirements designed to support the reliability of electronic certification services. Accordingly, evidentiary responsibility should not be distributed without considering technological control. A party that controls the system that generates the primary transaction record should bear a greater responsibility for preserving the relevant data and providing a reliable means of verification.

3.6. Implications for the Digital Economy

The evidentiary problem also has an economic dimension. Digital transactions are expected to reduce transaction costs by simplifying communication, reducing geographical barriers, and accelerating contractual processes. However, in the digital era, written evidence is no longer limited to physical documents. However, it may also include electronic documents, transaction process records, digital signatures, and activity logs within a system (Mokosolang, 2023). However, uncertainty regarding the enforceability and evidentiary strength of digital agreements can create additional costs through identity verification, preservation of transaction records, contractual risk mitigation, dispute resolution, and litigation. The relationship can therefore be formulated as:

Evidentiary Dimension	Negative Condition	Legal–Economic Consequence	Positive Condition	Legal–Economic Outcome
Electronic evidence	Uncertain or unreliable	Increased legal risk	Reliable and verifiable	Reduced legal risk
Legal certainty	Low predictability	Greater uncertainty in contractual relationships	High predictability	Greater legal certainty
Transaction costs	Increased costs for verification and dispute resolution	Reduced efficiency	Lower verification and dispute-resolution costs	Increased efficiency
Trust	Reduced confidence between contracting parties	Reluctance to engage in digital transactions	Increased confidence	Greater willingness to transact
Digital economy	Higher uncertainty and transaction barriers	Reduced transaction efficiency	Reliable evidentiary infrastructure	More efficient digital transactions

3.7. Reconstruction of the Electronic Evidence Framework

3.7.1. From Formal Admissibility to Evidentiary Reliability

The central finding of this research is that the existing legal framework has successfully addressed the formal recognition of electronic evidence but has not completely resolved how its reliability should be assessed in a consistent and integrated manner. The question should therefore no longer be limited to: *"Is an electronic document legally recognized as evidence?"* Instead, the more important question is: *"Can* *the electronic document reliably establish the contractual fact that it is intended to prove? "*This distinction is consistent with Makarim's analysis of the probative value of electronic evidence and with more recent research identifying evidentiary reliability and enforcement as continuing challenges in Indonesian electronic contracts. The case approach also supports this shift. The PA Bitung case demonstrates judicial attention to authenticity, integrity, security, accessibility, and audit trail. In contrast, the PN Donggala case demonstrates that electronic evidence remains subject to judicial assessment concerning formal and material requirements.

3.7.2. The Four-Parameter Evidentiary Reconstruction Model

Based on the normative analysis, judicial interpretation, technical regulation, and international comparison, this study proposes a Four-Parameter Evidentiary Reconstruction Model for electronic agreements.

a. Authentication
b. Establishing the identity and attribution of the party performing or authorizing the electronic act.
c. Integrity
d. Establishing that the electronic record remains complete and has not been improperly altered.
e. System Reliability
f. Establishing that the electronic system used to generate, transmit, process, or store the evidence operates reliably and securely.
g. Transaction Traceability
h. Establishing that the sequence of relevant digital events can be reconstructed and verified.

The four parameters should not be interpreted as independent requirements. Rather, they constitute an interconnected evidentiary structure. If authentication is weak, attribution becomes uncertain. If integrity is weak, the contractual content becomes questionable. If system reliability is weak, the electronic record may not be trustworthy. If traceability is weak, the contractual chronology may be impossible to reconstruct. The model, therefore, proposes a cumulative evidentiary assessment**.** The stronger the evidence satisfies the four parameters, the stronger its capacity to establish contractual facts. The model does not necessarily require every electronic agreement to employ the same technological mechanism. Rather, it provides a framework for assessing whether the available evidence is sufficiently reliable in light of the circumstances of the particular transaction.

3.8. Comparison with Previous Research and International Regulation

Previous research has examined electronic contracts from different perspectives and examined the probative value of electronic evidence and electronic signatures within the Indonesian legal framework, providing an important foundation for understanding electronic evidence beyond formal recognition. More recent studies have examined legal certainty in electronic contracts, biometric authentication, electronic signatures, electronic and smart contracts, and e-commerce transactions. (Susanty, 2026)

These studies provide important insights into particular dimensions of electronic contracting. However, the existing literature tends to examine authentication, electronic signatures, contractual validity, evidentiary value, consumer protection, or technological development as relatively separate issues. The present study advances this literature by integrating these dimensions, along with system reliability and transaction traceability, into a single evidentiary reconstruction framework. At the international level, the UNCITRAL Model Law on Electronic Commerce 1996 establishes the principle that information should not be denied legal effect merely because it is contained in a data message. The Model Law is based on principles of technological neutrality and functional equivalence and provides an important conceptual foundation for the legal recognition of electronic transactions.

The European Union provides a more differentiated approach through Regulation (EU) No. 910/2014 (eIDAS). The regulation distinguishes electronic signatures by level of assurance and establishes requirements for the identification of signatories and the detection of subsequent changes to signed data. This demonstrates how technical reliability can be connected with legal consequences and evidentiary confidence. Compared with these international frameworks, Indonesia has established legal recognition of electronic information, electronic documents, and electronic signatures and has developed a PSrE regulatory structure. However, these elements remain distributed across various legal instruments and have not yet been formulated into an integrated judicial evidentiary assessment applicable to electronic agreements in general. The Four-Parameter Model proposed in this study addresses this gap by connecting existing Indonesian legal and technical mechanisms into an integrated framework:

Figure 1. Four-Parameter Evidentiary Model for Electronic Agreements

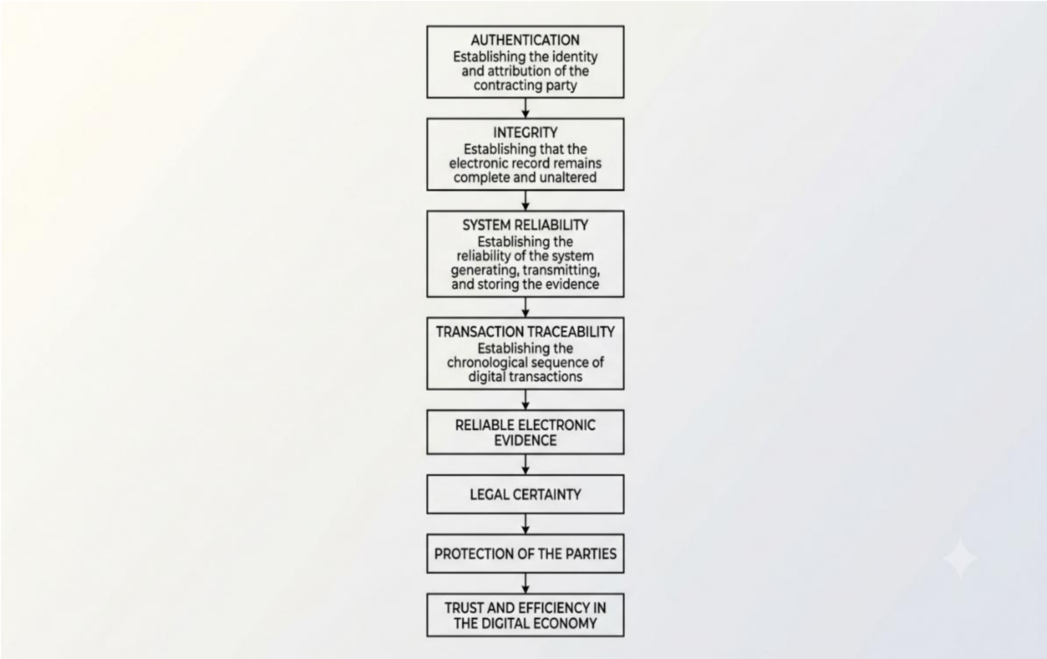


Figure 1 demonstrates that the four parameters constitute an interconnected evidentiary framework rather than independent requirements. Authentication establishes who performed the electronic act, while integrity establishes whether the content of the electronic record remains complete and unaltered. System reliability concerns the trustworthiness of the electronic system through which the record is generated, transmitted, or stored, whereas transaction traceability enables the chronological reconstruction of the contractual process. The fulfillment of these four parameters collectively strengthens the reliability of electronic evidence, which in turn supports legal certainty and balanced protection of the contracting parties. Ultimately, reliable electronic evidence contributes to greater trust and efficiency in digital economic transactions. Thus, the study does not propose the wholesale adoption of foreign regulation. Instead, international instruments provide a comparative reference for reconstructing an Indonesian framework based on the country's existing legal architecture.

3.9. Implications for Indonesian Legal Development

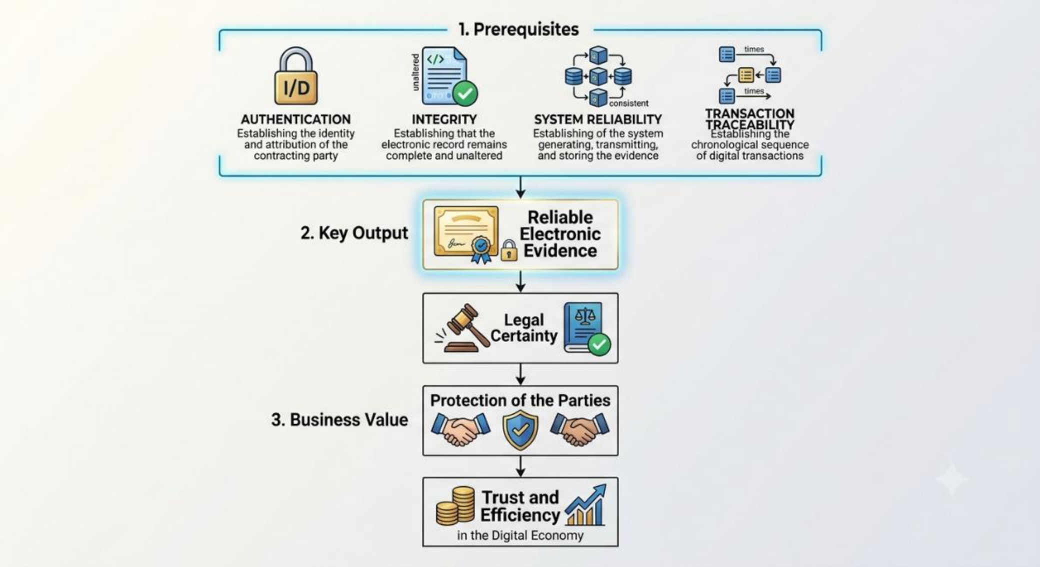
The findings have several implications for the development of Indonesian electronic contract law. An electronic contract cannot be deemed valid merely because it takes place online. It must satisfy both civil law elements and technical requirements pursuant to the provisions of the Electronic Information and Transactions Law (UU ITE) (Setyawati, 2017). It is precisely this combination of legal and technical aspects that guarantees legal certainty in digital transactions (Uu Lukmanul Hakim, 2025). First, the legal framework should provide clearer criteria for assessing the evidentiary reliability of electronic agreements. The existing PSrE framework provides important technical infrastructure for identity verification, electronic certification, validation, and related services. However, the relationship between these technical mechanisms and judicial assessment of evidentiary weight should be further clarified (Minister of Communication and Informatics Regulation No. 11 of 2022). Second, judicial examination should consider not only the electronic document itself but also the technological circumstances surrounding its creation, authentication, storage, transmission, and preservation. The PA Bitung case demonstrates the importance of examining authenticity, integrity, security, accessibility, and audit trail in electronic evidence.

Third, electronic system providers and parties controlling relevant electronic records should maintain adequate transaction records to facilitate verification when disputes arise. This includes authentication records, timestamps, system logs, transaction histories, and preservation records. Fourth, Indonesia may draw comparative lessons from the eIDAS framework concerning the relationship between technical assurance and legal consequences. The European approach demonstrates that the evidentiary confidence attached to an electronic signature can be strengthened by objective requirements concerning identification, control, and detection of subsequent alteration. Finally, legal development should balance technological efficiency with the protection of parties. Digitalization should not reduce a party's ability to establish contractual rights merely because the relevant evidence is stored in a technological system controlled by another party.

3.10. Comparison with Previous Research

The principal contribution of this study becomes clearer when compared with the existing literature. Previous studies generally focus on individual dimensions of electronic contracting, including contractual validity, electronic signatures, biometric authentication, electronic evidence, electronic notarial systems, and consumer protection. The present study advances the literature in three respects. Landasan hukum lain yang memperkuat keberlakuan perjanjian elektronik juga terdapat dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan sistem dan Transaksi Elektronik (PP PSTE) (Zailani, 2026). First, it shifts the analytical focus from formal legal recognition toward evidentiary reliability. Second, it connects judicial interpretation with technical regulation concerning PSrE, electronic signatures, timestamps, validation, and preservation. This regulation governs the responsibilities of electronic system providers, procedures for protecting personal data, and the obligation of digital platform operators to maintain the security and confidentiality of user data. (Hummerson, 2025)

Third, it integrates these elements into the Four-Parameter Evidentiary Reconstruction Model**.** The principal novelty is therefore not the proposition that electronic evidence is legally valid, because that proposition has already been established by Indonesian legislation and previous scholarship. The novelty lies in the systematization of dispersed legal and technical elements into four interconnected parameters for assessing the reliability of electronic agreements. The proposed relationship can therefore be formulated as:

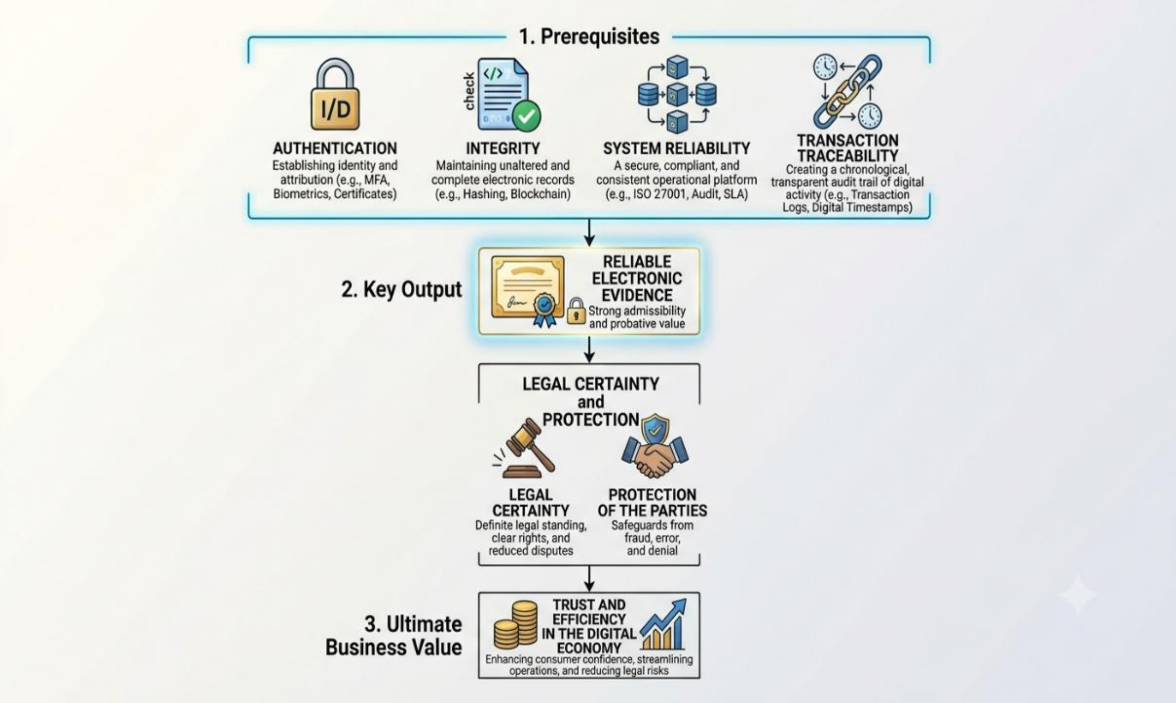


This formulation distinguishes the present study from previous research that examines the individual components of electronic contracting separately.

3.11. Principal Findings

The analysis establishes three principal findings. First, electronic agreements are legally recognizable and capable of producing binding contractual consequences when the requirements of Indonesian contract law and electronic transaction legislation are satisfied. Second, the principal legal challenge has shifted from the validity of electronic agreements to the reliability of electronic evidence, particularly regarding authentication, integrity, system reliability, and transaction traceability. These challenges are reflected both in contemporary scholarship and in judicial treatment of electronic evidence. Third, the existing framework requires a shift from formal admissibility toward integrated evidentiary reliability. The analysis of Indonesian judicial practice, PSrE regulation, and international frameworks demonstrates that the reliability of electronic agreements depends upon several interconnected factors rather than upon electronic form alone.

This study, therefore, proposes the Four-Parameter Evidentiary Reconstruction Model**:**



The model constitutes the principal contribution of this study. It provides a conceptual framework for integrating identity verification, document integrity, electronic-system reliability, and transaction chronology into the assessment of electronic evidence. By connecting these four dimensions, the model seeks to strengthen legal certainty, provide balanced protection for contracting parties, and support trust and efficiency in digital economic transactions.

The analysis reveals that the Indonesian legal framework has recognized electronic agreements and electronic documents as legally relevant instruments in digital economic transactions. Nevertheless, formal recognition does not automatically guarantee strong evidentiary value. The principal problems identified in this study concern the authentication of contracting parties, the integrity of electronic records, the reliability of electronic systems, and the traceability of digital transactions. These problems demonstrate that the evidentiary framework for electronic agreements needs to move beyond the question of admissibility toward the question of reliability in establishing contractual facts. This finding is consistent with recent research indicating that electronic evidence is normatively recognized in Indonesia but continues to encounter difficulties in judicial verification and assessment. (Lahangatubun, 2025)

4. CONCLUSION

This study concludes that while Indonesian law formally recognizes electronic agreements and documents under Article 1320 of the Civil Code and Law No. 1 of 2024 (EIT Law), legal recognition alone does not guarantee strong evidentiary weight in civil disputes. The fundamental challenge in digital economic transactions has shifted from formal legal admissibility to the verification of evidentiary reliability. To resolve this issue, this study formulates the Four-Parameter Evidentiary Reconstruction Model—comprising Authentication, Integrity, System Reliability, and Transaction Traceability—as an integrated framework for legal evaluation. The findings confirm that when these four interconnected parameters are satisfied, electronic records achieve high probative value, thereby establishing legal certainty, protecting contracting parties, and supporting trust and efficiency in the digital economy.

These findings yield important practical and regulatory implications for legal development in Indonesia. For lawmakers and regulators, there is a pressing need to clarify statutory criteria for evaluating the probative weight of digital evidence by formally integrating technical standards—such as Electronic Certification Provider (PSrE) framework, digital timestamps, and cryptographic hashing—into procedural law. For judges and legal practitioners, judicial examination must transition from checking formal admissibility to evaluating the broader technological ecosystem surrounding the evidence. Courts should assess system security, audit trails, and data preservation, while applying the normative principle that platform operators or parties exercising primary control over electronic systems bear a heightened responsibility for maintaining and demonstrating the integrity of digital transaction records.

This study has limitations inherent to its normative juridical approach, as it relies primarily on statutory, conceptual, and case analyses within Indonesian civil law without incorporating empirical field data on private industry practices or direct judicial interviews. Consequently, future research should empirically examine how Indonesian courts apply these four parameters across a broader spectrum of commercial dispute decisions. Further research is recommended to investigate the adaptation and implementation of the Four-Parameter Model within emerging technological paradigms, including smart contracts, decentralized finance, AI-driven automated contracting, and cross-border blockchain-based transactions.

REFERENCES

(UNCITRAL), U. N. (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.* newyork: United Nations.

(UNCITRAL), U. N. (2001). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.* NewYork: United Nations.

(UNCITRAL), U. N. (2002). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.* Newyork: United Nations.

(UNCITRAL), U. N. (2024). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.* NewYork: United Nations.

A. F. Salsabila, R. R. (2024). Pengaruh Revolusi Industri 4.0 Terhadap Hubungan. *Jurnal Pendidikan Dan Ilmu Sosial (Jupendis)*.

Andrian Danul Firmansyah, T. A. (2026). Reconstructing The Role of Notaries in Electronic Commerce: A Notary-Based Digital Authentication Model for Ensuring Legal Certainty in Electronic Contracts. *Journal Customary Law*.

Anike Rasyida Inayah, E. A. (2025). The Principle of Legal Certainty in Electronic Contracts: Challenges of Evidence and Law Enforcement in Indonesia. *International Journal of Social Science and Human Research*.

Anita Mu'min, M. R. (2025). Digitalization of Civil Transactions and Its Implications for Legal Certainty in the Era of Society 5.0. *Edusight International Journal of Multidisciplinary Studies*.

Atika Putri Jayanti, M. K. (2025). Legal Aspects Of Business Contract Planning In The Digital Era. *Jurnal Hukum Sehasen*.

Chariansyah, W. K. (2026). Pendekatan perundang-undangan, konseptual, dan kasus dalam penelitian hukum normatif. *Pendas: Jurnal Ilmiah Pendidikan Dasar*.

Danuri, M. (2019). Perkembangan Dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*.

Ery Agus Priyono, O. O. (2025). Digital Transformation of Contract Law: Legal Certainty and Human Rights Protection in AI-Based Contracts. *Jurnal Suara Hukum*.

Hadiyanto, I. P. (2025). Tinjauan Yuridis Kekuatan Pembuktian Tanda Tangan Elektronik (Digital Signature) dalam Persidangan Hukum Acara Perdata. *Jurnal Ilmiah Fenomena*.

Hakim, A. (2025). Penggunaan Alat Bukti Elektronik dalam Penyelesaian Perkara Perdata di Pengadilan Negeri (Studi Perkara Nomor: 22/Pdt.G/2021/Pn Dgl). *Universitas Muhammadiyah Yogyakarta*.

Hardito Nawaskoro, L. A. (2026). Perlindungan Hukum Para Pihak dalam Perjanjian Elektronik Menurut Hukum Perdata Indonesia. *Journal of Golden Generation Legal Science*.

Hayati, W. (2026). Keabsahan Perjanjian Elektronik Sebagai Akta di Bawah Tangan dalam Perspektif Kuh Perdata dan Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi

Elektronik. *Birokrasi Jurnal Ilmu Hukum dan Tatanegara*.

Hayati, W. (2026). Keabsahan Perjanjian Elektronik Sebagai Akta di Bawah Tangan dalam Perspektif KUH Perdata dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Jurnal Ilmu Hukum dan Tata Negara*.

Hermawan. (2024). Kajian Hukum Penerapan Pasal 1320 KUHPerdata Dalam Kontrak. *Iustitia Omnibus Jurnal Ilmu Hukum*.

Hummerson, R. I. (2025). Tanggung Jawab Penggunaan Data Pribadi Oleh. *Amicus Curiae*.

I Nyoman Wahyu Ariartha, I. M. (2025). Analisis Kepastian Hukum terhadap Kontrak Elektronik dan Smart Contract. *Jurnal Interpretasi Hukum* .

Inayah, A. R. (2025). The Principle of Legal Certainty in Electronic Contracts: Challenges of Evidence and Law Enforcement in Indonesia. *International Journal of Social Science and Human Research*.

Indonesia, M. o. (2022). *Minister of Communication and Informatics Regulation Number 11 of 2022 concerning the Governance of Electronic Certification.* Ministry of Communication and Informatics of the Republic of Indonesia.

Juliani, A. D. (2024). Penyusunan Akta Perjanjian Elektronik dalam Hukum Keperdataan: Peran Notaris dan Tanggung Jawab Hukum. *Officium Notarium*.

Lahangatubun, N. &. (2025). Public Trust and the Legal Validity of Electronic Signatures in Indonesia. *Jurnal Ilmu Hukum Kyadiren*.

Makarim, E. (2013). Electronic evidence and electronic signatures in Indonesia: the probative value of digital evidence. *SAS Open Journal*.

Martinelli, I. (2024). Penggunaan Click-Wrap Agreement Pada E-Commerce. *Jurnal Supremasi*.

Mokosolang, A. A. (2023). Kekuatan Hukum Surat Elektronik Sebagai Alat Bukti Perdata. *Lex Administratum*.

Muhammad Rizky Aji Perdana, R. T. (2025). Validity of Electronic Signatures in Digital Agreements: An Analysis of the Application of the Intellectual Property Law and the Civil Code in E-Commerce Transactions. *Jurnal Mahkamah*.

Muhammad Rizky Aji Perdana, R. T. (2025). Validity of Electronic Signatures in Digital Agreements: An Analysis of the Application of the Intellectual Property Law and the Civil Code in E-Commerce Transactions. *Jurnal Mahkamah*.

Negara, T. A. (2023). Normative Legal Research in Indonesia: Its Origins and Approaches. *Comparative Law Journal (ACLJ)*.

Ni Made Arya Dwi Yusakawati, A. S. (2025). Regulation of Electronic Notarial Deed Creation in Indonesia Based on the Principle of Legal Certainty: Between Opportunities and Challenges. *Jurnal Daulat Hukum*.

Putra, I. N. (2025). Keabsahan Perjanjian Elektronik Dalam Jual Beli. *Journal Media Akademik*.

Rahmawati Sabila, W. W. (2025). Legal Certainty of Biometric-Based Electronic Contracts under Indonesian Contract Law. *Journal Jourisprudentie*.

Roslaili. (2025). Legal Analysis Of The Validity Of Electronic Documents And Signatures As Evidence In Legal Proceedings In Indonesia. *Journal of Law, Policy and Global Development*.

Setyawati, D. A. (2017). Perlindungan Hak Konsumen Dalam Transaksi Elektronik. *Syiah Kuala*.

Siregar, D. (2025). Transforming Civil Procedural Law in the Digital Era: Evidence, Contracts, and Legal Certainty. *Journal of USM Law Review*.

Susanty, A. P. (2026). Legal Certainty in Electronic Contracts for E-Commerce Transactions in Indonesia. *West Science Law and Human Right*s.

Uu Lukmanul Hakim, A. S. (2025). Aspek Hukum Perjanjian Elektronik dalam Bisnis Digital. *Acta Comitas Journal of Hukum Kenotariatan*.

Vivi Sylvia Purborini, S. (2026). Legal Validity of Digital Contracts in Indonesian Business Transactions: A Normative Study of the Civil Code and Electronic Information and Transactions Law. *Sinergi International Journal of Law*.

Zailani. (2026). Eksistensi Nilai-Nilai Syariah Dalam PP 71/2019 Tentang Penyelenggaraan Sistem. *Acta Comitas: Jurnal Hukum Kenotariatan*.