

Blockchain as Electronic Evidence in the Indonesian Legal System: An Analysis of Legal Certainty in Crypto Asset Disputes

Olfriady Letunggamu^{1*}, Rahmat Dwi Putranto²

IBLAM School of Law, Jakarta, Indonesia

*Corresponding Author: Oscoberlin@gmail.com

ABSTRACT

Keywords:

Blockchain; electronic evidence; legal certainty; crypto assets.

Article Info

Received:

08/04/2026

Revised:

19/04/2026

Accepted:

21/05/2026

Published:

31/05/2026

This study examines the legal position and evidentiary value of blockchain-based records within the Indonesian legal system and their implications for legal certainty in crypto-asset disputes. Although Indonesian law recognizes electronic information and electronic documents as admissible evidence, the existing framework does not specifically regulate the authentication, verification, submission, and assessment of blockchain-based evidence in judicial proceedings. This study employs normative legal research using statutory, conceptual, comparative, and case approaches to analyze relevant legislation, legal doctrines, and court decisions concerning electronic evidence and crypto-asset disputes. The findings indicate that blockchain records possess strong technical characteristics of authenticity, integrity, traceability, and resistance to unauthorized alteration through cryptographic verification, timestamps, and distributed consensus. However, technical reliability does not automatically establish legal admissibility or evidentiary weight. In judicial practice, blockchain-based evidence may require supporting verification through digital forensic expertise, chain-of-custody documentation, and evidence linking blockchain addresses to the relevant legal subjects. The absence of specific procedural standards creates uncertainty in the authentication and assessment of blockchain evidence and may lead to inconsistent judicial treatment. This study proposes the development of specific judicial guidelines, particularly through a Supreme Court Regulation (PERMA), establishing standards for submission, authentication, technical verification, and judicial assessment of blockchain-based evidence. Such a framework would strengthen legal certainty while maintaining procedural fairness and compatibility with personal data protection requirements.



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)



How to cite: Letunggamu, O., & Putranto, R. D. (2026). Blockchain as Electronic Evidence in the Indonesian Legal System: An Analysis of Legal Certainty in Crypto Asset Disputes. *International Journal of Educational Review, Law And Social Sciences (IJERLAS)*, 6(3), 365–379. <https://doi.org/10.54443/ijerlas.v6i3.5265>

Introduction

The social changes brought about by advances in information and communication technology in the 21st century have created a major revolution in human life. These developments have not only impacted the economic and social spheres but also had fundamental consequences for national legal systems (Arinanto, 2021). The ongoing digital transformation worldwide has required every country, including Indonesia, to adapt its legal system to meet the challenges posed by technological innovations such as big data, artificial intelligence, and especially blockchain technology. Blockchain technology is a significant innovation first introduced by Satoshi Nakamoto in his 2008 paper, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2017). In this paper, Nakamoto introduced the concept of a decentralized network capable of recording every transaction into interconnected, immutable blocks of data (Tapscott et al., 1998). Each block has a unique hash that guarantees the authenticity and integrity of the data without the need for a central authority or traditional financial institutions.

Initially, blockchain was used as the primary infrastructure for cryptocurrencies like Bitcoin, Ethereum, and Litecoin, but its development has expanded into various sectors, including government, logistics, healthcare, education, and even the legal system (Akgyray, 2019). In the legal field, blockchain is beginning

to be considered as a tool to increase transparency, the reliability of digital evidence, and the efficiency of judicial administration processes (Fauzi, 2020) . In the context of Indonesian law, the development of blockchain technology presents an interesting legal dilemma. On the one hand, this technology presents significant opportunities for reforming the evidentiary system and increasing legal transparency. However, on the other hand, the absence of a clear and comprehensive regulatory framework creates legal uncertainty, both in the context of evidence and the resolution of disputes involving crypto assets. The Indonesian legal system, which still relies on the classical legal paradigm, often lags behind in responding to technological changes (Atmasasmita, 2020) . Procedural law principles, which have relied on conventional evidence (written evidence, witnesses, and experts), have not fully accommodated the digital evidence generated by blockchain systems (Harahap, 2020) . Yet, blockchain's fundamental properties of authenticity, transparency, and immutability make it highly potential for strengthening the integrity of evidence in court (Tapscott et al., 1998) . Conceptually, the law of evidence is a crucial component of the procedural law system, defining the methods and tools used to convince judges of the truth of a legal event (Mulyadi, 2022) . In Indonesian civil and criminal procedural law, the recognized evidence is still limited, as stipulated in Article 1866 of the Civil Code and Article 184 of the Criminal Procedure Code. However, developments have shown that electronic evidence has become an unavoidable necessity.

Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended by Law Number 1 of 2024, has recognized electronic information and/or electronic documents as valid legal evidence (Article 5 paragraph (1)). However, the ITE Law does not explicitly regulate blockchain as a source of electronic evidence. There are no provisions regarding how data stored in a blockchain ledger is verified, who is authorized to assess its authenticity, and what the chain of custody procedure is in the judicial system (Fadilah, Deny Susanto, 2025) . Blockchain offers inherent advantages in terms of data authenticity and integrity. Every transaction recorded on the blockchain network is accompanied by a unique timestamp and hash code (Siregar et al., 2025) . The slightest change to the data will alter the entire hash structure, making it easier to detect data manipulation. Thus, blockchain can technically function as a source of verifiable electronic evidence without the need to rely on a single party (trustless verification). In Indonesian judicial practice, judges still lack formal assessment standards for blockchain evidence. In a number of cybercrime cases or digital asset disputes, evidence sourced from blockchain is often considered only as additional evidence or clues (Kobis, 2017) . This occurs because the legal system of evidence in Indonesia still emphasizes a formalistic approach and has not yet adopted a comprehensive digital forensics framework (Rahardjo, 2019) .

This situation raises serious problems regarding the implementation of the principle of legal certainty as regulated in Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Without legal certainty regarding the position of blockchain evidence, digital transaction actors do not have a guarantee of legal protection and enforcement of justice. Beyond the issue of proof, blockchain development is also closely related to the phenomenon of crypto assets (cryptocurrencies). Crypto assets are a direct result of the implementation of blockchain technology, enabling the transfer of value without traditional financial institutions (Zakiri, 2025) . In Indonesia, crypto assets have been recognized as tradable digital commodities under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti, 2024) . However, this recognition is limited to the trading aspect and has not yet addressed the legal status of crypto assets in civil law or procedural law. According to Bappebti data from 2024, the number of crypto asset users in Indonesia reached more than 17.6 million people with a transaction value of IDR 149 trillion (Bappebti, 2024) . This rapid growth has been accompanied by the emergence of various disputes, both between users and platform providers and between investors (OJK Institute, 2024) . Most of these disputes relate to the loss of digital balances, breach of contract, or system errors that cause losses.

One case that set an important precedent is the South Jakarta District Court Decision Number 605/Pdt.G/2022/PN Jkt.Sel and the DKI Jakarta High Court Decision Number 483/Pdt/2023/PT DKI (Supreme Court of the Republic of Indonesia, 2023) . In this case, the panel of judges acknowledged that crypto assets have economic value and can be the object of civil disputes, even though it is not explicitly regulated in the Civil Code. This decision demonstrates a progressive step by the judiciary in applying the principle of substance over form, namely assessing the economic nature of a transaction rather than solely its legal form (Muhammad et al., 2021) . Problems arose when the evidence of crypto transactions submitted by the plaintiff sourced from the blockchain system was not fully accepted as valid evidence (OJK Institute, 2024) . The panel of judges in their consideration stated that the digital evidence still requires confirmation

from an authorized third party, such as an IT forensic expert or an electronic certification body (Muhammad Syafiq, 2025) . This means that even though courts are starting to recognize the existence of crypto assets, the validity of blockchain evidence is still legally questionable. This uncertainty raises broader issues. Blockchain operates on the principle of immutability, meaning that any recorded data cannot be deleted. However, this principle may conflict with the provisions of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), specifically Article 16, which regulates the right to erase personal data. Therefore, a potential conflict arises between the principle of privacy protection and the need for digital evidence (Wahyudi Djafar, 2023) . Through Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK), supervision of crypto assets has been transferred from Bappebti to the Financial Services Authority (OJK). This shift creates normative tension between the two state institutions because their implementing regulations are not yet fully integrated. The OJK emphasizes consumer protection and financial system stability, while Bappebti focuses on futures trading mechanisms. It can be argued that the Indonesian legal system currently faces two major challenges simultaneously:

1. How to ensure the recognition and validity of blockchain evidence in court, and
2. How to ensure legal certainty in resolving crypto asset disputes based on blockchain technology.

The law's lag behind technological developments is nothing new. According to Roscoe Pound, law has always served as a tool of social engineering, adapting norms to societal dynamics. However, when social change moves faster than the law's ability to adapt, a legal gap emerges that can hinder justice. In the blockchain context, this legal gap is evident in the lack of digital evidence standards and clear legal accountability mechanisms (Bhattacharjee et al., 2025) . To address this, procedural law reform is imperative. Recognition of blockchain evidence requires not only normative amendments but also a renewal of the legal paradigm. The evidentiary system, which currently emphasizes formality and the hierarchy of evidence, needs to be shifted to a more flexible system based on technological trust (Malaheksa et al., 2025) . Countries such as Estonia, Singapore, and the European Union have provided concrete examples of how the law can adapt to blockchain. Estonia uses blockchain to manage state archives and public documents through the KSI Blockchain, which is legally recognized as an authentic source of government data. The European Union, through Regulation (EU) No. 910/2014 (eIDAS), has also classified blockchain as part of legitimate trust services.

Indonesia could adopt a similar approach by issuing a Supreme Court Regulation (PERMA) on Blockchain-Based Electronic Evidence, or even drafting a Digital Procedural Law Bill that comprehensively regulates procedures for evidence collection, data verification, and storage of electronic evidence. Furthermore, it is necessary to improve the competence of law enforcement officials in the fields of digital forensics and technology law to bridge the gap between legal norms and their implementation capabilities. From the above description, it is clear that the relationship between blockchain evidence and legal certainty in court is a strategic issue in the development of national law in the digital era. The recognition of blockchain-based evidence is not merely a technical issue, but concerns the integrity of the judicial system and the protection of citizens' legal rights. This research is highly relevant because:

1. There is a legal vacuum in the governance of blockchain evidence;
2. There is inconsistency in judicial practice in assessing digital evidence;
3. There is a conflict of norms between the law of evidence, civil law, and personal data protection; and
4. There is an urgent need to formulate a procedural law model that is adaptive to technological developments.

This research is expected to provide conceptual and practical contributions to the establishment of an Indonesian digital evidence legal system that guarantees justice, certainty, and legal benefits in facing the era of global digital transformation. Based on the background explanation above, the formulation of the research problem is: What is the position and strength of blockchain technology-based data evidence in the Indonesian evidence legal system? How is the principle of legal certainty applied by the courts in resolving crypto asset disputes in Indonesia? What are the normative and technical obstacles faced in implementing blockchain as electronic evidence and the basis for resolving digital disputes in Indonesia? What is the ideal procedural law and regulatory model that can guarantee the validity of blockchain evidence while protecting legal certainty for the parties in court?

Method

This research employs a normative legal research method (doctrinal legal research), focusing on the analysis of positive legal norms, legal principles, doctrines, and court decisions relevant to the issue under study. Normative legal research aims to identify consistency, coherence, and alignment between prevailing norms and social and technological developments (Marzuki, 2017). In the context of this research, a normative approach is used to examine the position of blockchain technology as electronic evidence in the Indonesian legal system and its implications for the principle of legal certainty.

The approaches used include a statutory approach, a conceptual approach, and a case approach. The statutory approach is carried out by examining various regulations related to electronic evidence and crypto assets, including the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Financial Sector Development and Strengthening Law. The conceptual approach is used to analyze the theory of legal certainty as proposed by Radbruch (1961), the responsive legal theory of (Nonet, P., & Selznick, 1978), and the progressive legal theory of (Rahardjo, 2019) as a basis for evaluating the adaptability of the legal system to the development of blockchain technology.

Furthermore, a case-based approach is employed through an analysis of court decisions related to crypto asset disputes and electronic evidence. The jurisprudential analysis aims to identify patterns of judges' considerations in accepting or evaluating blockchain-based evidence. This approach is crucial because in the Indonesian legal system, court decisions play a significant role in shaping legal practice, particularly when there are gaps or ambiguities in norms (the IRAC method in decision analysis; see Marzuki, 2017). The legal sources used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and court decisions; secondary legal materials include textbooks, scientific journal articles, and legal doctrines relevant to electronic evidence and blockchain (Fauzi, 2020), while tertiary legal materials include legal dictionaries and legal encyclopedias that support the clarification of technical terms. The analysis was conducted qualitatively using grammatical, systematic, and teleological interpretation methods to obtain prescriptive and comprehensive legal arguments (Marzuki, 2017).

Results and Discussion

The Position and Power of Evidence of Blockchain Technology in the Indonesian Legal System

The development of information technology has transformed many social and economic institutions, including the evidence system in courts. Among the new technologies that have had the greatest impact on electronic evidence are: Blockchain, a distributed ledger technology (DLT) that offers a permanent, verifiable, and tamper-resistant mechanism for recording transactions. This technology presents a new possibility for the practice of proof: evidence that is not just a digital record, but a record that has the properties of a physical record: immutability, timestamped provenance, and cryptographic linkage so that the feasibility and strength of the evidence need to be examined within the framework of national procedural law. In answering questions about the status and validity of blockchain evidence, analysis must be conducted at three levels: (1) the normative basis (positive law and principles of evidence), (2) the technical characteristics of blockchain relevant to the law of evidence, and (3) judicial acceptance and existing judicial practice. These three levels are interrelated: norms define the legal space for the use of electronic evidence; technical features determine whether evidence meets legal requirements; and judicial practice shows how norms and technology interact in concrete decisions.

Normatively, the initial position of blockchain-based evidence in Indonesia is determined by the provisions regarding electronic evidence in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its revisions. The ITE Law affirms that electronic information and/or electronic documents, as well as their printouts, constitute valid legal evidence in judicial proceedings; this provision essentially opens the door for various forms of digital recordings to be recognized as evidence as long as they meet the requirements for system reliability. Updates and interpretations of these norms through amendments to laws and judicial guidelines then determine the boundaries of practice; however, it is important to note that the text of the ITE Law is general and does not specify verification mechanisms for specific technologies such as DLT or blockchain (Fauzi, 2020). Consequently, while a formal legal basis already exists for electronic evidence, the specificity of blockchain requires normative interpretation and the development of technical guidelines to ensure clarity and consistency before judges.

Theoretically, the law of evidence focuses on three main criteria that make evidence admissible and have weight: authenticity, integrity, and relevance to disputed facts. Evidence that meets these three

elements will more easily convince the judge, thus contributing to the judge's belief in the material truth of an event (Harahap, 2020). Blockchain, based on its technological characteristics, shows the potential to meet the criteria of authenticity and integrity: each transaction is given hash, recorded on the block with timestamp, and validated through a consensus mechanism so that retrospective changes will be detected through discrepancies hash (Tapscott et al., 1998). Therefore, at a conceptual level, blockchain can be viewed as a powerful source of evidence, but, it is important to emphasize, this power is technical and must be bridged to the legal realm through verification mechanisms that can be understood and trusted by the judicial authorities. To understand the technical contribution of blockchain to proof, a brief explanation of the relevant components is necessary: (1) hash function as a digital fingerprint; (2) Merkle tree which aggregates transactions; (3) timestamping which records the recording time; (4) digital signature (public/private key) which links the owner's identity to the transaction; and (5) distributed consensus which guarantees that the record has been approved by the validator network. This combination produces proofs that are difficult to forge or alter without a trace (Nakamoto, 2017). From a proof-of-fact perspective, two important points emerge: first, on-chain proofs provide objective trace about the timing and content of the transaction; second, such evidence does not automatically answer the question of substantive ownership when the legal relationship governing ownership (e.g., service contracts, custodial arrangements) exists. Off-chain. This means that the ledger is able to prove that 'something happened at time T', but it does not necessarily answer who is legally responsible unless there is an additional legal link that connects the private key or account to a specific legal subject (Marzuki, 2017).

In national judicial practice, there are early signs of acceptance of digital evidence related to crypto assets and electronic transactions. Decisions at the district and appellate court levels have begun to accept electronic records from platforms or digital transaction records as evidence (Kumar et al., 2023). However, in many decisions, judges tend to require corroboration of the evidence through testimony from digital forensic experts, affidavits from platform operators, or chain-of-custody documentation explaining how the data was retrieved (Lilik Mulyadi, 2021). This attitude reflects a duality: courts accept the possibility of digital evidence but still require verification of the retrieval process and its technical validity. In practice, this has resulted in the operational position that blockchain evidence can carry high weight if (a) it is presented with forensic metadata (tx hash, block number, snapshot from a block explorer), (b) accompanied by a statement of authenticity from an independent extractor/custodian, and (c) if its material relevance to the claim is clear and demonstrable (Widiana Purnawan, 2025).

The issue of assessing blockchain evidence is not only technical but also normative: should the legal system provide presumptive authenticity (assumption of rebuttable authenticity) against verified on-chain records? Some advanced jurisdictions including Singapore through Evidence (Amendment) Act 2018 and Estonia through its national arrangements has pursued the option of providing some sort of presumption or at least guidelines that facilitate the admissibility of DLT evidence in court. Such an approach can expedite litigation and reduce the initial burden of proof for the plaintiff; however, it must be balanced with fairness mechanisms to provide the opposing party with the opportunity to challenge the evidence, for example through re-examination by an independent expert. In the Indonesian context, the adoption of such a principle needs to be calibrated with the state of national forensic capacity and the protection of the parties' procedural rights.

There are several substantive legal issues that are critical to the acceptance of blockchain evidence. First, the issue The relationship between private keys and legal entities. Although digital signatures technically link transactions to public keys, the legal relationship between public keys and personal or legal entity identities is often not recorded on-chain; identification often occurs through off-chain processes (know-your-customer (KYC), contracts, registration). Therefore, proving ownership or executing orders solely by relying on on-chain evidence requires adequate identification evidence (OJK Institute, 2024). Second, the issue Chain-of-custody: Although data in the ledger is immutable, copies of evidence presented in court (e.g., screenshots, export files) can be manipulated; the process of collecting, packaging, and storing such evidence must be procedural and documented so that the court can assess the authenticity of the copies submitted.

Third, the issue **Privacy and data subject rights**: some transactions contain personal data protected by the Personal Data Protection Act—the conflict between the blockchain immutability principle and the right to erasure demands technical solutions (e.g., off-chain storage with on-chain pointers, redaction protocols) and clear legal policies (Rosadi, 2020). From a practical evidentiary perspective, the role of digital

forensics experts is crucial. Experts not only explain technical matters but also explain the verification methodology used (e.g., the use of independent nodes, the read-only snapshot process, Merkle root verification, cross-checking with a public block explorer) so that judges can assess whether the procedures used have maintained the integrity of the evidence. To prevent the expert's role from becoming a source of excessive subjectivity, nationally recognized competency standards, certifications, and guidelines for digital forensic methods are needed. This effort requires collaboration between judicial institutions and technical bodies such as BSSN, BRIN, or academic institutions. From a legal perspective, many countries have taken proactive stances that can be instructive for Indonesia. Singapore, through changes to its legislation, has lowered barriers to the admissibility of DLT evidence by establishing provisions that make it easier for courts to assess on-chain evidence; the European Union, through its eIDAS framework and EBSI initiative, is promoting the interoperability and standardization of cross-border digital evidence; and Estonia is practicing the use of blockchain for public data, demonstrating how legal and technical infrastructure can complement each other to provide evidentiary strength (Akgiray, 2019). The key lesson is: successful legal recognition of blockchain evidence is not simply a matter of recognizing the ledger as valid data, but also of building an ecosystem: technical standards, verification bodies, privacy policies, and judicial guidelines.

Given all these potentials and constraints, how do we formulate the appropriate legal position in Indonesia? Normatively, a pragmatic step is to recognize that blockchain evidence deserves to be treated as **authentic electronic documents** when: (1) the method of extraction and submission of evidence follows forensically sound principles; (2) technical metadata that guarantees integrity (tx hash, block number, merkle root, timestamp) is included; (3) there is an affidavit or certificate of authenticity from the extractor or an independent verification agency; and (4) the opposing party is given the opportunity to test and challenge the evidence through re-examination or counter-expert. This concept allows for practical and fair recognition: it gives medium-high weight to blockchain evidence without compromising the counterparty's processual rights.

Finally, from the perspective of the social function of law, the recognition and utilization of blockchain evidence can strengthen legal objectives: ensuring certainty, providing substantive justice, and increasing the efficiency of law enforcement. When properly regulated and verified, DLT evidence contributes to the transparency and accountability of digital economic transactions. However, reaching this point requires legal and technical commitment: the formulation of judicial guidelines (e.g., the Supreme Court Regulation on DLT-based electronic evidence), the development of national forensic capacity, harmonization with the PDP Law and sector regulations (e.g., OJK/Bappebti regarding digital assets), and intensive training for judges and law enforcement officials. Without these proactive measures, the technology's potential will remain locked in the technical realm, without providing the certainty required for legal practice.

Procedural Law Regulations Regarding the Validity of Blockchain Evidence in Court

The digital transformation that has engulfed nearly every sector of life requires Indonesian procedural law to adapt to new realities. In the context of evidence, there is an urgent need to regulate the validity of evidence sourced from digital systems, particularly blockchain. Indonesian procedural law, both criminal and civil, is fundamentally rooted in the conventional evidentiary paradigm, where physical documents and human testimony are the primary sources of formal truth. Developments in information technology, particularly distributed ledger technology, are challenging this classical structure by introducing new forms of evidence that are difficult to understand within traditional legal systems.

Normatively, Indonesian procedural law has not specifically regulated evidence derived from blockchain systems. The Criminal Procedure Code (KUHAP) and Civil Procedure Code (HIR/RBg) still use classical categories of evidence, such as witness statements, letters, instructions, and confessions (Subekti, 2009). Electronic documents were only recognized as evidence after the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, particularly Law Number 1 of 2024, which affirms the legality of electronic information and documents. However, this recognition is general in nature and does not specify the type of electronic system used, including the validation mechanism for blockchain-based data.

In principle, the Indonesian procedural legal system adheres to the principle of due process of law, namely that every evidentiary process must be conducted legally, fairly, and provide an equal opportunity to all parties to prove the truth of their case (Mertokusumo, 2002). Therefore, even though digital evidence has been recognized, without technical regulations governing how to present it in court, confusion often

occurs in practice. Judges, prosecutors, and advocates do not have uniform guidelines for assessing evidence sourced from distributed ledger systems such as blockchain. As a result, the admissibility of evidence often depends on the judge's subjective assessment of the reliability of the technology and the expert testimony presented.

In practice, there is a tendency for evidence sourced from blockchain to be accepted with limited scope, provided it is first verified by an information technology expert or independent institution. This is evident in the South Jakarta District Court Decision Number 605/Pdt.G/2022 and the Jakarta High Court Decision Number 483/Pdt/2023, which accepted blockchain crypto asset transaction records as valid electronic evidence. However, in their deliberations, the panel of judges still required technical validation to ensure that the submitted data truly originated from the blockchain system and was unaltered. Thus, it can be said that *de facto*, blockchain has been recognized as a source of evidence, but *de jure*, it still awaits more detailed regulations in procedural law. According to Philippe Nonet and Philip Selznick, a legal system that is rigid and unresponsive to social and technological developments is called repressive law (Nonet, P., & Selznick, 1978). In contrast, a legal system that is open to change is called responsive law, which strives to adapt norms to the needs of modern society. In the Indonesian context, this view aligns with Romli Atmasasmita's thinking, who emphasized that national law must be adaptive to technological developments and must balance legal certainty with social justice (Atmasasmita, 2020). Thus, updating procedural law to accommodate blockchain evidence is not an option, but rather an urgent legal necessity.

Concrete steps towards responsive procedural law can begin with the establishment of a Supreme Court Regulation (PERMA) as a technical guideline regarding the procedures for proving blockchain-based electronic evidence. Such a regulation has legal legitimacy, because the Supreme Court has the authority to issue regulations to fill legal gaps and ensure uniformity in judicial practice. In the context of blockchain evidence, PERMA can regulate several important matters: (1) the operational definition of "blockchain evidence," (2) procedures for submitting evidence in court, (3) the obligation to include verification metadata such as hash values, timestamps, and transaction IDs, (4) criteria for the reliability of the electronic system used, and (5) the role of digital forensic experts in conducting independent verification. The issuance of this PERMA is also in line with the spirit of judicial modernization initiated by the Supreme Court through the Electronic Court System (e-Court) under PERMA Number 3 of 2018 and PERMA Number 1 of 2019 concerning Electronic Case Administration and Court Trials. Through this PERMA, the Supreme Court has opened up space for the digitization of the litigation process. However, the e-Court system is limited to case administration and has not yet addressed aspects of blockchain-based evidence. Therefore, the issuance of new guidelines regarding blockchain evidence could be a logical continuation of this innovation, while also affirming the judicial institution's commitment to adapting to the era of digital transformation.

On the other hand, a national digital verification agency is also needed to guarantee the reliability of blockchain evidence. This agency could take the form of a Digital Forensic Verification Center (DFVC) under the coordination of the Supreme Court or the National Cyber and Crypto Agency (BSSN). The primary function of this agency is to verify the authenticity and integrity of blockchain data submitted to court, issue digital authentication certificates, and provide technical recommendations to judges. With such an agency, the evidentiary process can be more objective, efficient, and standardized, thereby reducing reliance on subjective expert testimony. Institutionally, synergy between the Supreme Court, the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information Technology (Kominfo), the Financial Services Authority (OJK), and the Commodity Futures Trading Regulatory Agency (Bappebti) is crucial (OJK Institute, 2024). These institutions have distinct but interconnected authorities in overseeing digital activities, crypto assets, and data security. Without proper coordination, regulations regarding blockchain evidence can overlap and be ineffective. Therefore, the establishment of a cross-agency Blockchain Legal Framework Task Force is a strategic step to develop legal standards, technical procedures, and national certification for digital evidence.

From a comparative perspective, Singapore is an example of a country that has successfully integrated blockchain evidence into its procedural legal system through the Evidence (Amendment) Act 2018, which grants authentic status to distributed ledger technology (DLT)-based electronic records. The law even provides a rebuttable presumption of authenticity, meaning evidence is considered valid until proven otherwise. This approach saves judicial time and resources without sacrificing procedural fairness. In the European Union, through Regulation (EU) No. 910/2014 or the eIDAS Regulation, digital records and

electronic signatures verified through blockchain have cross-border evidentiary force (European Union, Regulation, 2014) . Meanwhile, Estonia has gone further by implementing the KSI Blockchain Act 2019, which recognizes blockchain as a legal infrastructure for public documents.

Practice in these countries demonstrates that recognizing blockchain evidence does not always require new legislation. Technical regulations at the level of court rules or judicial practice directions are sufficient to provide certainty to judges in accepting blockchain evidence. Indonesia could adopt a similar approach by issuing a Supreme Court Circular (PERMA) or Supreme Court Circular Letter (SEMA) on procedures for digital evidence. However, reforming procedural law will not be effective without strengthening the human resources (HR) capacity of the judiciary. Many judges and prosecutors in Indonesia lack a thorough understanding of how blockchain works, including the mechanisms of hash verification, smart contracts, and digital signatures. Therefore, ongoing training programs for law enforcement officials are needed in collaboration with academia, industry, and international institutions such as the OECD or UNODC, which already have modules on digital evidence.

From a legal theory perspective, updating procedural law to regulate blockchain evidence is a concrete manifestation of progressive legal theory as developed by Satjipto Rahardjo, who asserts that law must be a tool for achieving substantive justice, not merely a static normative device (Rahardjo, 2019) . Procedural law should not limit itself to old forms and formalities, but must serve the primary purpose of law, namely protecting truth and justice. Thus, the formation of digital procedural law that is adaptive to blockchain reflects the evolution of law moving from a legal-formal paradigm to a substantive and responsive paradigm. Finally, a normative draft of Indonesian digital procedural law is needed that expressly recognizes the validity of blockchain evidence by taking into account three layers of dimensions:

1. The normative dimension, namely the formation of PERMA or technical regulations that provide an explicit legal basis for the acceptance of blockchain evidence.
2. Institutional dimension, namely the establishment of DFVC as a national digital verification institution.
3. The technical-procedural dimension, namely the preparation of standards for the collection, storage, and verification of blockchain evidence that comply with forensically sound and chain of custody principles.

Three dimensions form an integral whole that will ensure that blockchain evidence is legally accepted, objectively assessed, and fairly regulated within the Indonesian justice system.

Implications of Blockchain Use for Legal Certainty in Crypto Asset Disputes in Court

The development of blockchain technology not only brings innovation in the digital economy and finance, but also raises new challenges in the legal system, particularly in the context of legal certainty . Legal certainty is one of the main pillars of a state based on law (*rechtsstaat*) as emphasized in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia. This principle implies that all actions of the government and citizens must be based on legal norms that are clear, predictable, and consistent in their application. In the context of crypto asset disputes, legal certainty is a vital element because it concerns the legitimacy of ownership, the validity of transactions, and legal protection for parties transacting in the digital world.

The use of blockchain technology in crypto asset transactions brings a new dimension to the concept of proof and law enforcement. Blockchain systems are decentralized , not dependent on a single authority, and all transactions are recorded in a publicly verifiable distributed ledger (Tapscott et al., 1998) . Technically, this characteristic creates a trustless system , a system that enables trust without the need for intermediaries (Wright, 2018) . However, from a legal perspective, a system without a central authority creates ambiguity regarding who is responsible in the event of violations, fraud, or loss of digital assets. This is where the paradox arises between the decentralized nature of technology and the legal need for an accountable authority.

1. Legal Certainty and Legal Challenges in Crypto Asset Transactions

In the Indonesian legal system, crypto asset transactions are partially regulated through several sectoral regulations, such as Bappebti Regulation Number 8 of 2021 concerning Guidelines for Organizing Physical Market Trading of Crypto Assets on Futures Exchanges, as well as Minister of Finance Regulation Number 119/PMK.010/2022 concerning Tax Provisions on Crypto Assets (Bappebti, 2024) . Both regulations recognize the legality of crypto assets as tradable commodities, but do not yet regulate them as legal tender. Thus, the legal status of crypto assets remains within the jurisdiction of *lex imperfecta* — are recognized to

a limited extent but have not yet been fully integrated into the national financial legal system. This normative uncertainty often gives rise to debate in civil and criminal cases involving crypto assets.

In judicial practice, a number of cases have emerged that touch on the issue of proof and ownership of blockchain-based digital assets. One of these is South Jakarta District Court Decision Number 605/Pdt.G/2022 And Jakarta High Court Decision No. 483/Pdt/2023 concerns a crypto asset ownership dispute between two parties claiming to be the rightful owners. In this case, the evidence consisted of: transaction hash, wallet address, and transaction history taken from block explorer used to prove the legal relationship between the plaintiff and the disputed digital assets. The judge, in his deliberations, stated that such evidence is admissible as long as it is verified by a digital forensics expert and meets the principles of data integrity. However, there is no established precedent regarding the evidentiary weight of blockchain data, so judges still have considerable discretion in assessing its validity based on personal beliefs.

In the context of legal theory, **Gustav Radbruch** teaches that legal certainty is one of the three basic values of law, along with justice and utility (Radbruch, 1973). Legal certainty provides stability, while justice and utility provide moral and social direction for the application of law. However, in the reality of digital law, the three often conflict. When technology develops faster than regulations, substantive justice can be achieved, but legal certainty is compromised because there are no definite norms. Thus, law must be responsive, not reactive, to technological innovation, as emphasized by **Philippe Nonet** And **Philip Selznick**, that modern legal systems must be able to adapt to social and technological changes in order to remain relevant (Nonet, P., & Selznick, 1978).

2. Inconsistency in Law Enforcement and Normative Voids

One of the direct implications of the use of blockchain in legal disputes is the occurrence of **inconsistency in law enforcement** among judicial institutions. In some cases, courts have recognized blockchain-based transactions as valid electronic evidence; however, in other cases, similar evidence has been rejected on the grounds that it does not meet the formal requirements for evidence (Fauzi, 2020). This discrepancy creates uncertainty for digital economy actors who need clarity regarding how blockchain data will be treated in court (Martinelli et al., 2024).

The vacuum of norms is also visible in terms of **Proof of ownership of crypto assets**. Blockchain does record transactions and ownership in the form of digital addresses (public keys), but there is no legal provision that explicitly links this public key to a person's legal identity (OJK Institute, 2024). Therefore, even if someone can show proof of transactions on a blockchain network, they cannot necessarily legally prove that they are the rightful owner of the asset without supporting documents such as a sales contract, custody agreement, or proof of account registration on a crypto asset exchange (Muhammad Syafiq, 2025). As a result, the concept of digital ownership becomes blurred, and legal certainty in crypto asset disputes is weakened.

This issue is further complicated because most crypto transactions are conducted across jurisdictions, using offshore exchanges or decentralized exchange (DEX) which does not have a legal entity in Indonesia (Musllim, 2025). When fraud or loss of assets occurs, law enforcement becomes difficult because no party can be held legally accountable. In this context, the principle of *lex loci contractus* And *lex site* becomes difficult to implement, because the location of the transaction and the legal subjects involved are not always within the same jurisdiction (JG Starke, 1989). This demonstrates the gap between the traditional, territorial-based concept of law and the global reality of digital law (Gozali et al., 2024).

3. Inconsistency in Law Enforcement and Normative Voids

Legal certainty is also closely related to the protection of the rights of legal subjects. In the blockchain context, legal protection includes ownership rights, the right to privacy, and the right to data integrity. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) strengthens individuals' rights to control their personal data, including the right to erase personal data (the right to erasure). However, this principle contradicts the nature of blockchain, which is immutable and cannot be changed or deleted. This inconsistency has the potential to create a conflict between the principle of privacy protection and the principle of data integrity. Therefore, a new legal mechanism is needed that can accommodate both principles, for example by implementing the concept of off-chain storage or zero-knowledge proof to protect personal data without compromising the integrity of the blockchain system (Putra & Prayudi, 2021). Furthermore, it is important to note that the national legal system must also provide certainty for third

parties acting in good faith. In many cases, digital asset transactions are conducted through smart contract , which automatically executes agreements without human intervention (Wright, 2018) . When an error or bug occurs in In smart contracts , the question is: who is legally responsible? In conventional legal systems, responsibility is determined based on intent (mens rea) and actions (actus reus); however, in automated systems, these two elements are blurred (Lessig, 2006) . Therefore, legal reforms are needed to regulate legal liability in the context of automated contracts to ensure legal certainty.

4. Jurisprudence and the Direction of Responsive Law Formation

In the context of jurisprudence, Indonesian courts are still in the early stages of assessing blockchain evidence. Although there is no leading Supreme Court ruling yet , several first-instance courts have affirmed that on-chain evidence is admissible as long as it meets the principles of authenticity, integrity, and relevance. However, to achieve stronger legal certainty, consistent precedent from the Supreme Court is needed for lower courts to use as a guide.

A strategic step that can be taken is to encourage the Supreme Court to issue a Circular Letter (SEMA) or Supreme Court Regulation (PERMA) regarding the admissibility of blockchain evidence. Such instruments can provide clear assessment standards for judges, thereby reducing disparities in decisions between courts. Furthermore, the Supreme Court can collaborate with the National Cyber and Crypto Agency (BSSN) to develop technical guidelines regarding the procedures for verifying digital evidence based on distributed ledger technology (DLT).

Within the framework of responsive legal theory proposed by Nonet and Selznick, legal regulations that adapt to technological developments demonstrate legal maturity in responding to social change (Nonet, P., & Selznick, 1978) . Thus, recognizing blockchain evidence and protecting digital asset ownership will increase public trust in the national legal system. This also strengthens the legitimacy of courts in resolving disputes in the digital age.

5. Normative Recommendations

Based on the above analysis, it can be concluded that the use of blockchain in crypto asset disputes has significant implications for legal certainty. To address this uncertainty, the following strategic steps are necessary:

- a) Drafting specific regulations regarding blockchain-based digital evidence, both through PERMA and amendments to the ITE Law.
- b) Establish a national digital verification agency, tasked with verifying the authenticity and integrity of blockchain data submitted as evidence in court.
- c) Establish international standards for digital asset verification, so that Indonesian court decisions can be recognized within the framework of cross-border cooperation.
- d) Improving the capacity of judges and law enforcement officers through technical training on blockchain technology and digital forensics.
- e) Developing national digital jurisprudence, which provides interpretive guidance for judges in assessing blockchain evidence.

These steps will not only strengthen legal certainty but also demonstrate Indonesia's readiness to face the era of digital transformation, which demands synergy between legal norms and technological innovation.

Blockchain-Based Digital Procedural Law Model for the Indonesian Justice System

1. Background and Urgency of Model Formation

Advances in digital technology over the past decade have challenged the classical legal procedures that have long been the foundation of justice in Indonesia. The most significant change has come from the emergence of technology. blockchain , which presents a digital transaction recording system that is **immutable** , **transparent** , and **distributed** (Tapscott et al., 1998) . Blockchain has changed the way people build trust without a central authority; in the context of procedural law, this raises fundamental questions about **how the state guarantees the validity of data that is not controlled by a particular institution**, but is actually more technically reliable.

In judicial practice, the emergence of blockchain-based evidence presents a new challenge. Many judges and advocates in Indonesia do not yet understand the concept. hash function , public key

infrastructure (PKI), or smart contracts, so digital evidence is often considered foreign or irrelevant (Fauzi, 2020). Yet, a growing number of disputes involve digital data, such as crypto assets, electronic transactions, or automated contracts. If the legal system does not adapt, it will result in **legal vacuum** where digital evidence is not recognized, even though it has the potential to contain significant material truth (Lilik Mulyadi, 2021).

The absence of a comprehensive digital procedural law model creates an imbalance between social development and legal structures. As stated by **Philippe Nonet** And **Philip Selznick**, non-adaptive laws would fall into the category repressive law, which merely maintains formalism without considering the needs of society (Nonet, P., & Selznick, 1978). Indonesia needs responsive law — law that actively adapts to social and technological changes without losing its moral character (Muhamad A., M. Rizan, 2025). Therefore, formation **blockchain-based digital procedural law model** not only a practical necessity, but also a constitutional imperative in order to guarantee **fair legal certainty** as mandated in Article 28D paragraph (1) of the 1945 Constitution. This model is expected to be able to bridge two worlds: **technical reliability of blockchain** and **state legal authority**.

2. Theoretical Foundations: From Positive Law to Responsive Law

The theoretical basis of this digital procedural law model rests on three major ideas.

- a) **integrative legal theory** as stated by **Romli Atmasasmita**, who combines legal certainty, justice, and utility (Atmasasmita, 2020). In the blockchain context, this theory means that the recognition of digital evidence should not solely follow technological logic but must also consider the principle of procedural fairness.
- b) **progressive legal theory** from **Satjipto Rahardjo**, who emphasized that law should be a tool for liberation, not a tool for limiting innovation (Rahardjo, 2019). Progressive law rejects narrow legalism that views technology as a threat, but instead sees it as a means to achieve more efficient and participatory justice. Blockchain as a system trustless is the embodiment of decentralized justice; progressive law must facilitate this potential to become part of the justice system.
- c) **responsive legal theory** from Nonet & Selznick, who positioned law as a moral system that must be able to interact with social complexity (Nonet, P., & Selznick, 1978). The blockchain-based procedural law model reflects this principle: law is no longer defensive against change, but rather actively integrates technology into its formal procedures.

These three theories form the epistemological framework for the digital procedural law model: law is not a static entity, but rather a system that continuously adapts to the dynamics of society and technology.

3. Normative Pillar: PERMA as a Judicial Instrument

To realize legal certainty in blockchain proof, **Supreme Court** must publish **Supreme Court Regulations (PERMA)** which specifically regulates the procedures for examining and assessing evidence based on distributed ledger technology (DLT). This PERMA becomes *lex specialis* for digital evidence and serves to fill gaps in criminal and civil procedural law. Important material in the PERMA includes at least:

- a) **Definition of blockchain proof** — that is, information or data stored in a distributed digital ledger, which can be verified through cryptographic mechanisms and network consensus.
- b) **Formal requirements for submitting evidence** — each party must include key metadata (hash value, timestamp, block number, merkle root, and public address) as well as an affidavit of authenticity explaining the origin of the data.
- c) **Technical verification** — the judge may order a digital forensic examination by an independent verification agency before deciding on the validity of the evidence.
- d) **Presumption of authenticity** — blockchain evidence verified by an official institution is considered valid until proven otherwise (rebuttable presumption).
- e) **Privacy protection** — personal data contained in blockchain transactions must be protected in accordance with the principles of Law Number 27 of 2022 concerning Personal Data Protection.

This PERMA not only provides technical guidance, but also creates consistency between court decisions, thus avoiding legal uncertainty which often occurs in digital cases.

4. Institutional Pillar: Digital Forensic Verification Center (DFVC)

The success of the digital procedural law model depends on the existence of an independent and trusted technical verification agency, namely the Digital Forensic Verification Center (DFVC). This agency could be established under the coordination of the Supreme Court in collaboration with the National Cyber and Crypto Agency (BSSN) and the National Research and Innovation Agency (BRIN). The DFVC's primary duties are:

- a) Verifying the authenticity of blockchain evidence through verification nodes owned or accessed by the institution.
- b) Issue a Digital Certificate of Authenticity, which is an official report explaining the verification method, hash value, and data integrity check results.
- c) Perform blockchain forensics on disputed evidence, including transaction tracing and wallet ownership validation.
- d) Develop national digital forensics standards recognized by the Supreme Court and other law enforcement agencies.

The DFVC will reduce judges' subjectivity in assessing technical evidence and standardize digital evidence practices across Indonesia. This institutional model is already in place in Estonia and Singapore, where national digital verification agencies collaborate directly with the courts.

5. Technical and Procedural Pillars

Procedurally, the submission and examination of blockchain evidence must follow the following stages:

- a) Submission Stage – the plaintiff or claimant submits evidence in digital form with metadata and an affidavit.
- b) Initial Verification Stage – the court checks the administrative completeness and determines whether technical verification is required.
- c) Technical Inspection Stage – DFVC or independent experts validate the hash and transaction data.
- d) Judicial Assessment Stage – the judge assesses the evidence based on authenticity, integrity, and relevance.
- e) Challenge Phase – the opposing party may submit comparative experts or counter-evidence.

This procedure ensures a balance between technological efficiency and procedural fairness. Furthermore, the Supreme Court can establish an e-Verification Portal System, integrated with e-Court and the DFVC, to facilitate judges' access to evidence verification reports.

6. Pillars of Data Protection and Digital Legal Ethics

In the blockchain context, the issues of privacy and data rights are crucial dimensions that cannot be ignored. Blockchain is immutable, while data protection laws provide the right to erase data. This conflict can be resolved with a technological-legal approach, namely the application of **off-chain data storage** for personal data, and **zero-knowledge proof (ZKP)** so that the verification process does not violate user privacy. In addition, it is necessary to form **National Digital Forensic Code of Ethics** which regulates the behavior of experts and verification bodies to ensure that examination results are reliable and not used unethically. This ethic also includes the expert's responsibility to explain technical findings in legal language that judges can understand.

7. Cross-Jurisdictional Pillars and International Cooperation

Because blockchain is global, a digital procedural law model cannot stand alone without the support of international cooperation. Indonesia needs to:

- a) Updating the Mutual Legal Assistance Treaty (MLAT) to cover cross-border exchange of digital evidence.
- b) Signing memorandums of understanding (MoUs) with countries such as Singapore, Estonia, and European Union members that already have blockchain proof standards.
- c) Adopting the principles in Regulation (EU) No. 910/2014 (eIDAS) that recognize digital signatures and evidence across jurisdictions.

This step will strengthen Indonesia's position in international litigation involving digital assets, while also enhancing the credibility of its judicial system in the eyes of the world.

8. Cross-Jurisdictional Pillars and International Cooperation

The digital procedural law model needs to be implemented in stages through three national implementation phases:

- a) Phase I (1–2 Years): Preparation of PERMA and establishment of DFVC pilot projects in Jakarta, Surabaya, and Medan.
- b) Phase II (3–4 Years): National training for judges, prosecutors, and advocates; integration of e-Court with the DFVC system; and development of national blockchain forensic standards.
- c) Phase III (5 Years and Above): Harmonization with international law, regulatory updates, and expansion of global cooperation.

Each phase must be followed by an evaluation based on performance indicators such as evidence verification time, judges' level of trust in the DFVC, and consistency of decisions between courts.

9. Implications for Legal Certainty and Justice

With the existence of a blockchain-based digital procedural law model, the Indonesian justice system will experience **epistemological transformation**: from a human-based belief system to a technology-based verification system. This increases **legal certainty** because every data can be tested and verified; while strengthening **procedural fairness**, because both parties have an equal opportunity to submit or challenge digital evidence. In addition, this model will strengthen **institutional accountability**: judges no longer have to evaluate technical evidence without basis, because there are verification institutions and standards that can be referred to (Muhamad A., M. Rizan, 2025). In the long term, Indonesian courts will be pioneers in the ASEAN region in implementing **digital procedural law that is adaptive and responsive to blockchain**.

10. Conclusion: The Future Direction of Indonesia's Digital Justice

Blockchain-based digital procedural law is not only a procedural reform measure, but also a revolution in the legal paradigm. With this model, the Indonesian justice system will move into the era of **Digital transparency, efficiency, and accountability**, where electronic evidence has equal status with conventional evidence. If implemented gradually with adequate human and institutional support, this model will become a new foundation for a fairer, more modern, and more trusted justice system in the era of digital transformation.

Conclusion

This study concludes that blockchain technology technically meets the requirements of authenticity, integrity, and reliability, which are key prerequisites for an electronic evidence system. Its immutability, cryptography-based verification system, and network consensus mechanism ensure high levels of security and traceability for data recorded in the blockchain. Within Indonesia's positive legal framework, the recognition of electronic information and documents as valid evidence, as stipulated in the Electronic Information and Transactions Law, provides a normative basis for the admissibility of blockchain-based evidence in judicial proceedings.

However, there are no specific regulations explicitly governing verification mechanisms, evidentiary standards, or procedures for submitting blockchain evidence in court. This normative gap means that the evidentiary power of blockchain in practice remains dependent on judicial interpretation and the testimony of digital forensic experts. Consequently, despite the recognition of crypto transactions and assets as subjects of civil disputes, the acceptance of blockchain evidence has not yet fully provided consistent and standardized legal certainty. From the perspective of the principle of legal certainty, this situation has the potential to create uncertainty for those involved in crypto asset transactions, particularly regarding the protection of rights and the enforcement of legal claims. Therefore, procedural law reforms are needed that can systematically and comprehensively integrate blockchain-based evidence. Strengthening technical regulations and harmonizing them with the personal data protection regime are crucial steps in realizing a digital justice system that is adaptive, responsive, and guarantees legal certainty in the digital economy era.

Suggestion

Based on the research findings, concrete steps are needed to strengthen legal certainty in blockchain-based evidence in Indonesia. First, the Supreme Court needs to draft technical regulations in the form of a

Supreme Court Regulation (PERMA) specifically governing the procedures for submitting, examining, and evaluating blockchain-based electronic evidence. This regulation must establish clear authentication standards, data integrity parameters, and digital forensic verification mechanisms to ensure uniformity of practice across the judiciary. Second, the government, along with relevant institutions, needs to develop accredited national digital forensics standards that can be consistently applied in the evidence process. These standards are crucial to ensure that the validity of blockchain evidence relies not solely on individual expert opinion but is based on objective and proven scientific methodology. Furthermore, capacity building for judges and law enforcement officials through specialized training on blockchain technology and crypto assets is an urgent need to bridge the gap in technical understanding. Third, regulatory harmonization between evidence law, crypto asset regulations, and personal data protection must be systematically implemented. This synchronization is crucial to prevent regulatory conflicts, particularly regarding the principle of blockchain data immutability and the right to delete personal data. With these steps, the Indonesian legal system is expected to progressively adapt to developments in digital technology and provide stronger legal certainty for those involved in crypto asset transactions.

References

- Akgiray, V. (2019). The Potential for Blockchain Technology in Corporate Governance. *OECD Corporate Governance Working Papers*, 21, 1–30.
- Arinanto, S. (2021). *Hukum dan Teknologi Digital*. Rajawali Pers.
- Atmasasmita, R. (2020). *Hukum Progresif dan Dinamika Keadilan Sosial*. Prenadamedia Group.
- Bappebti. (2024). *Laporan Tahunan Perdagangan Aset Kripto Indonesia Tahun 2024*.
- Bhattacharjee, T., Mahapatra, A. S., De, D., & Chowdhury, A. (2025). JudicBlock: Judicial Evidence Preservation Scheme Based on Blockchain Technology. *Blockchains*, 3(4), 11. <https://doi.org/10.3390/blockchains3040011>
- Fadilah, Deny Susanto, S. A. (2025). Traditional Decriminalization in a Digital World : Reconstructing Criminal Policy towards Bitcoin-Based Money Laundering in the Era of Decentralized Finance. *Journal Evidence Of Law*, 4(2), 753–762. <https://doi.org/10.59066/jel.v4i2.1523>
- Fauzi, A. M. (2020). *Forensik Digital dan Pembuktian Elektronik di Pengadilan*. UII Press.
- Gozali, L., Kristina, H. J., Yosua, A., Zagloel, T. Y. M., Masrom, M., Susanto, S., Tanujaya, H., Irawan, A. P., Gunadi, A., Kumar, V., Garza-Reyes, J. A., Jap, T. B., & Daywin, F. J. (2024). The improvement of block chain technology simulation in supply chain management (case study: pesticide company). *Scientific Reports*, 14(1), 1–18. <https://doi.org/10.1038/s41598-024-53694-w>
- Harahap, M. Y. (2020). *Hukum Acara Pidana Indonesia*. Sinar Grafika.
- Institute, O. (2024). *Kajian Sengketa Kripto dan Digital Finance di Indonesia*.
- J.G. Starke. (1989). *An Introduction to International Law*. Butterworths.
- Kobis, F. (2017). Kobis, F. (2017). Kekuatan Pembuktian Surat Menurut Hukum Acara Perdata. *Lex Crimen*, 106. *Lex Crimen*, VI(5), 105–113.
- Kumar, D., Kumar, S., & Joshi, A. (2023). Assessing the viability of blockchain technology for enhancing court operations. *International Journal of Law and Management*, 65(5), 425–439. <https://doi.org/10.1108/IJLMA-03-2023-0046>
- Lessig, L. (2006). *Code and Other Laws of Cyberspace*. Basic Books.
- Lilik Mulyadi. (2021). *Hukum Pembuktian dalam Sistem Peradilan Indonesia*. Mandar Maju.
- Mahkamah Agung Republik Indonesia. (2023). Putusan No. 605/Pdt.G/2022/PN Jkt.Sel dan Putusan No. 483/Pdt/2023/PT DKI . (Issue 605).
- Malaheksa, R., Siswanto, H., & Triono, A. (2025). Integration of Blockchain Technology in the Criminal Justice System: Challenges of Regulation, Data Security, and Legitimacy of Digital Evidence. *Istinbath: Jurnal Hukum*, 22(2), 357–375.
- Martinelli, I., Mahva Tsabita, N., Fitriani, A., Putri, E., & Novela, D. (2024). Legalitas dan Efektivitas Penggunaan Teknologi Blockchain Terhadap Smart Contract Pada Perjanjian Bisnis di Masa Depan. *Unes Law Review*, 6(4), 6–7.
- Marzuki, P. M. (2017). *Penelitian Hukum*. Kencana.
- Mertokusumo, S. (2002). *Hukum Acara Perdata Indonesia*. Liberty Yogyakarta.
- Muhamad A., M. Rizan, I. F. (2025). *Journal of S ocial and Economics Research*. *Jurnal Sosial Dan Ekonomi*, 3(2)(1), 123–138.

- Muhammad, S., Lase, N., Adinda, A., & Yuliantika, R. D. (2021). Padjadjaran Law Review KERANGKA HUKUM TEKNOLOGI BLOCKCHAIN BERDASARKAN HUKUM SIBER DI INDONESIA. Padjadjaran Law Research & Debate Society, 9(1), 1–20.
- Muhammad Syafiq, S. N. S. (2025). ANALISIS PENGGUNAAN BLOCKCHAINUNTUK MENINGKATKAN TRANSPARANSI DAN KEAMANAN DATA PADA PEMBUKTIAN PERCERAIAN DI PENGADILAN AGAMA. Journal of Innovative and Creativity, 5(2), 9662–9672.
- Mulyadi, L. (2022). Hukum Pembuktian dalam Perkara Pidana dan Perdata. Mandar Maju.
- Musllim, E. A. (2025). MODUS BARU TINDAK PIDANA PENCUCIAN UANG DENGAN MEMANFAATKAN TEKNOLOGI BLOK CHANGE DAN MATA UANG CRYPTO NEW. UIN Law Review, 1(2), 132–155.
- Nakamoto, S. (2017). Bitcoin: A Peer-to-Peer Electronic Cash System (Vol. 23, Issue 4, pp. 552–557). https://doi.org/10.1162/ARTL_a_00247
- Nonet, P., & Selznick, P. (1978). Law and society in transition: Toward responsive law. Harper & Row.
- Putra, A. S., & Prayudi, Y. (2021). Implementasi Multi Smart Contract pada Bukti Digital dan Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital. JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia), 6(2), 98–108. <https://doi.org/10.32528/justindo.v6i2.3945>
- Radbruch, G. (1973). Rechtsphilosophie. C.F. Müller.
- Rahardjo, S. (2019). Hukum Progresif: Sebuah Sintesa Hukum dan Keadilan. Kompas.
- Rosadi, S. D. (2020). Hukum Perlindungan Data Pribadi di Indonesia. Refika Aditama.
- Siregar, U., Siregar, S., S, A. R., & Batubara, I. (2025). Interoperabilitas Hukum dalam Penyelesaian Sengketa Bisnis Internasional Berbasis Blockchain : Kajian atas Tantangan Yurisdiksi dan Hukum yang Berlaku. Journal Evidence Of Law, 4(3), 1279–1288. <https://doi.org/https://doi.org/10.59066/jel.v4i3.1803>
- Subekti, R. (2009). Hukum Pembuktian (P. Paramita (ed.)).
- Tapscott, D., Ticoll, D., & Lowy, A. (1998). How technology behind bitcoin is changing money and the world. In Age of Networked Intelligence. An imprint of Penguin Random House LLC.
- Wahyudi Djafar, D. (2023). Perlindungan Data Pribadi di Indonesia. ELSAM.
- Widiana Purnawan, K. (2025). Perlindungan Hukum Terhadap Aset Digital Dalam Perspektif Hukum Perdata Internasional: Problem Kolisi Hukum, Pengakuan Putusan Asing, Dan Transformasi Menuju Era Lex Digitalis. Jurnal Kertha Wicara, 15(11).
- Wright, P. D. F. & A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.
- Zakiri, H. (2025). Pemanfaatan Blockchain sebagai Instrumen Transparansi Pemilu dalam Hukum Tata Negara Indonesia. Journal Evidence Of Law, 4(2), 737–752. <https://doi.org/https://doi.org/10.59066/jel.v4i2.1514>