

Indonesian Journal of Agrarian Law

ISSN: 3110-6633 (Online)

Vol. 4 Issue 1 (2027) 367-424

DOI: <https://doi.org/10.15294/jal.v4i1.54475>

Available online since: August 7, 2026



Reconstruction of National Agrarian Data Security through Blockchain Technology: An Urgency Following the PDNS 2 Ransomware Incident

Daffa Al-Fidaus Widhianto

Faculty of Law, Universitas Negeri Semarang, Semarang,
Indonesia

Corresponding email:

daffawidhianto100604@students.unnes.ac.id

Abstract

The digital transformation of land administration in Indonesia, characterized by the implementation of electronic land certificates under Minister of ATR/BPN Regulation

Number 1 of 2021, faces serious challenges in cyber security. The use of a centralized database system has proven to have a fatal single point of failure, as evidenced by the Ransomware attack on the Temporary National Data Center (PDNS) 2 in 2024 which paralyzed 282 government institutions, as well as the leakage of 1.3 billion data by the hacker Bjorka in 2022. This research aims to analyze the vulnerability of the current land data infrastructure and examine the urgency of adopting Blockchain technology as a land data protection solution. Using a normative legal research method with a statutory, conceptual, and case approach, the results indicate that the centralized system is no longer adequate to guarantee the integrity of national agrarian data amidst destructive cyber threats. Blockchain technology offers decentralization and immutability that can prevent data manipulation by "digital land mafias" through a transparent network consensus mechanism. The successful implementation of Blockchain in land registration in Georgia since 2016 provides empirical evidence that this technology can ensure the permanent integrity of land ownership history. Regulatory reconstruction accommodating distributed ledger technology in national agrarian law is a necessity to achieve absolute legal certainty for landholders in the digital age. This research recommends the establishment of Government Regulation-level regulations governing Blockchain technical standards, synchronization between regulations, and a pilot project in several land offices before national implementation.

Keywords

Blockchain; Data Security; Electronic Land Certificate; Land Registration; Ransomware.

Introduction

Land is a strategic asset for the Indonesian nation that possesses highly fundamental social, economic, and political dimensions for national sovereignty. As a limited agrarian resource, the possession and ownership of land are strictly regulated through a constitutional mandate in Law Number 5 of 1960 concerning Basic Regulations on Agrarian Principles (UUPA). Article 19 of the UUPA obligates the government to conduct land registration throughout the territory of the Republic of Indonesia to guarantee legal certainty for the public. Land registration is not merely an ordinary bureaucratic procedure, but rather the primary instrument for realizing agrarian legal order so that every inch of land has a lawful and indefeasible ownership status before the law.¹ In the current era of technological disruption, this mandate has undergone a radical transformation toward a digital system through the Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency (Permen ATR/BPN) Number 1 of 2021 concerning Electronic Certificates. This digitalization is projected to be capable of cutting long bureaucratic chains, increasing service transparency, while simultaneously serving

¹ Enan Sugiarto, "Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata," no. June (2016): 182–99.

as a strategic instrument to close the loopholes for land mafia practices that have long undermined the rights of the people.²

Land mafia practices in Indonesia have transformed into a systemic "legal pathology" that distorts market prices and hinders Foreign Direct Investment due to the high risk of agrarian litigation. This uncertainty of legal status triggers the phenomenon of dead capital, wherein land loses its function as an economic leverage instrument as well as bank collateral, particularly for the middle class and MSME actors. Consequently, structural economic stagnation occurs alongside state financial losses from potential land transaction taxes and BPHTB lost due to data manipulation. These losses are multiplicative, also encompassing the social burden of handling protracted land disputes within the national judicial system without any concrete resolution for the rightful owners.³

However, digital transformation that is not accompanied by the strengthening of security architecture precisely gives rise to new, more fundamental vulnerabilities. The use of a centralized database system in the land digital infrastructure possesses a structural flaw in the form of a single point of failure, where a failure or attack at a single central point can paralyze the entire system nationwide. This vulnerability is no longer a theoretical threat but has become an empirical fact

² Felishella Earlene et al., "Implikasi Kebijakan Reforma Agraria Terhadap Ketidaksetaraan Kepemilikan Tanah Melalui Lensa Hak Asasi Manusia Implications of Agrarian Reform Policies on Land Ownership Inequality through the Lens of Human Rights" 6, no. 2 (2023): 152–70.

³ Dian Aries Mujiburohman Maulana Rafi Danendra, "Pembentukan Bank Tanah: Merencanakan Ketersediaan Tanah Untuk Percepatan Pembangunan Di Indonesia," *Jurnal UNDIP Masalah-Masalah Hukum* 36, no. 4 (2022): 1–20.

following the Ransomware attack incident named Brain Cipher that paralyzed the Temporary National Data Center (PDNS) 2 in Surabaya in June 2024, resulting in 282 government agencies losing access to strategic data simultaneously.⁴ Previously, the breach of 1.3 billion SIM card registration data by the hacker Bjorka in September 2022 further proved the fragility of the centralized security system in Indonesia.⁵

The vulnerability of this data infrastructure has direct implications for the existence of the land mafia, which has now transformed from physical crime into cybercrime. The practice of land grabbing through the manipulation of digital land records (*warkah*) can be executed instantly without leaving physical traces, merely by exploiting security loopholes in the centralized database.⁶ The impact not only harms the public, who suddenly lose their rights to land, but also creates dead capital assets that cannot function as bank collateral, as well as hindering foreign investment due to the uncertainty of agrarian law. Thus, the state's failure to protect the integrity of land data is equivalent to the failure to protect the constitutional rights of citizens to land.

⁴ Indonesia CNN, "CNN Indonesia. (2024, Juni 24). BSSN: Gangguan Pusat Data Nasional Ulah Serangan Siber Ransomware. CNN Indonesia.,” 2024, <https://www.cnnindonesia.com/teknologi/20240624133250-192-1113404/bssn-gangguan-pusat-data-nasional-ulah-serangan-siber-Ransomware>.

⁵ Indonesia CNN, "CNN Indonesia. (2022, September 2). 1,3 Miliar Data Registrasi SIM Card Diduga Bocor. CNN Indonesia,” 2022, <https://www.google.com/amp/s/www.cnnindonesia.com/teknologi/20220902062206-192-842221/lagi-lagi-bocor-data-kali-ini-13-miliar-info-registrasi-kartu-si-m/amp>.

⁶ Dian Aries Mujiburohman, "Transformasi Dari Kertas Ke Elektronik: Telaah Yuridis Dan Teknis Sertipikat Tanah Elektronik," no. 5 (2021): 5, <https://doi.org/10.31292/bhumi.v7i1.472>.

Departing from these problems, this study proposes the main thesis that Blockchain technology is the most relevant solution for reconstructing the security architecture of agrarian data. As an antithesis to centralized systems, Blockchain offers decentralization through an immutable distributed ledger, where every data modification must be validated through a network consensus mechanism rather than by a single authority vulnerable to abuse.⁷ The successful implementation of Blockchain in land registration in Georgia since 2016 serves as empirical evidence that this technology is capable of guaranteeing the integrity of land ownership history permanently and transparently.⁸

Several previous studies have discussed the opportunities and obstacles of digital transformation in land administration. Challenges to data sovereignty remain very real despite the continuous development of land digital service infrastructure by the government.⁹ Aspects of land possession conflicts and the establishment of a land bank within an administrative framework have also become major

⁷ Maria Kaczorowska, "Blockchain-Based Land Registration: Possibilities and Challenges," *Masaryk University Journal of Law and Technology* 13, no. 2 (2019): 339–60, <https://doi.org/10.5817/MUJLT2019-2-8>; Zibin Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, 557–64, <https://doi.org/10.1109/BigDataCongress.2017.85>.

⁸ Nino Lazuashvili, Alex Norta, and Dirk Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia, Lecture Notes in Business Information Processing*, vol. 361 (Springer International Publishing, 2019), https://doi.org/10.1007/978-3-030-30429-4_15.

⁹ Kusmiarto Kusmiarto et al., "Digital Transformation of Land Services in Indonesia: A Readiness Assessment," *Land* 10, no. 2 (2021): 1–16, <https://doi.org/10.3390/land10020120>.

focuses in various contemporary agrarian law studies .¹⁰ However, current land law literature is still minimal in specifically analyzing the reconstruction of data security architecture following a nationwide destructive Ransomware attack. The position of this study (state of the art) intends to fill this gap by evaluating the failure of centralized systems and offering Blockchain technology as a more absolute data protection solution.¹¹

This study aims to: first, analyze the vulnerability of centralized database systems in the implementation of electronic land registration following the PDNS 2 incident; second, examine the relevance of Blockchain technology as a more absolute agrarian data protection solution; and third, formulate the urgency of regulating Blockchain technology within the national agrarian law framework. By employing a normative juridical research method through statutory, conceptual, and case approaches, this study is expected to provide academic contributions as well as policy recommendations for the transformation of land data security in Indonesia.

¹⁰ Rosi Pramula Anggriawan, Sutaryono Sutaryono, and M. Nazir Salim, "Penyelesaian Konflik Penguasaan Tanah HGU Dengan Masyarakat Di Bengkulu Utara," *Marcapada: Jurnal Kebijakan Pertanahan* 1, no. 1 (2021): 29–41, <https://doi.org/10.31292/jm.v1i1.2>; Maulana Rafi Danendra, "Pembentukan Bank Tanah: Merencanakan Ketersediaan Tanah Untuk Percepatan Pembangunan Di Indonesia."

¹¹ Johannes P Paavo and Rafael Rodríguez-puentes, "A Systematic Literature Review on Blockchain-Based Titles Registries for Transparent Land Administration 1 Introduction," no. 2008 (2025): 67–86.

A. Vulnerability of Centralized Database Systems in the Implementation of Electronic Land Registration

The implementation of electronic land registration, which refers to the Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency (Permen ATR/BPN) Number 3 of 2023, integrates spatial data in the form of land parcel maps and textual data regarding ownership details into a single repository. This policy integrates all spatial data in the form of land parcel maps along with textual data regarding ownership details into a single storage container. Although this repository integration is designed to facilitate bureaucratic control and nationwide policy synchronization, the concentration of data under a single control gives rise to fundamental cybersecurity problems. To comprehensively understand how the fragility of such architecture impacts the land law system, the analysis in this chapter will be detailed into several operational sub-chapters dissecting the structural weaknesses of centralized storage, empirical evidence of its collapse on a national scale, and its juridical impact on the guarantee of citizens' property rights.

1. Anatomy of the Single Point of Failure (SPoF) Structural Weakness in Land Servers

The implementation of electronic land registration based on contemporary technological structures places all national

land information assets into a single centralized database. This centralized storage architecture technically creates a fundamental structural weakness known as a Single Point of Failure (SPoF). In information security studies that rely on the protection of confidentiality, integrity, and availability known as the CIA Triad this centralized storage model places all vital state data in a vulnerable position.¹² The primary characteristic of a single server implies fragility in the element of data availability, where the security level of the entire digital ecosystem depends entirely on the resilience of a single primary infrastructure point. Consequently, if the ministry's main server experiences a technical failure, physical damage, or destructive cyber penetration, the level of data availability will drop sharply, triggering a systemic paralysis of public services across all regional land offices.¹³ This single repository serves as the sole operational entry point; thus, if this centralized control collapses, there is no alternative security pathway to maintain the continuity of nationwide agrarian data validation.

The fragility of this centralized architecture is essentially rooted in the misalignment between technological modernization and the legal characteristics of the land

¹² Subarkah Abdullah, "Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi," *Go Infotech: Jurnal Ilmiah STMIK AUB* 31, no. 1 (2025): 149–60, <https://doi.org/10.36309/goi.v31i1.371>; Jan Gościński and Artur D. Kubacki, *Land Registration Concepts in Translation, International Journal for the Semiotics of Law*, vol. 34 (Springer Netherlands, 2021), <https://doi.org/10.1007/s11196-020-09800-y>.

¹³ Tito Wira Eka Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia," *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–67.

registration system in Indonesia. Pursuant to the mandate of Article 19 of the Basic Agrarian Law (UUPA) and Government Regulation Number 24 of 1997, Indonesia adopts a negative system of registration with positive tendencies, a legal policy choice confirming that the state does not provide an absolute guarantee regarding the validity of the data contained within a certificate of title.¹⁴ The tendentially passive function of the National Land Agency (BPN) in land administration creates a new legal loophole when the conventional paper-based administrative system is simply transformed into a centralized digital platform without being accompanied by a distributed security architecture. Outlines that structural weaknesses such as a lack of clear procedures, cases of overlapping land titles, and unintegrated regulations have become unresolved pathologies since the era of analog documents. When a database that still harbors residual disputes is placed into the ministry's single repository, single-gate access control precisely provides an opportunity for the escalation of massive-scale data breach risks.¹⁵

The evolution of attack methods against public databases has now transformed from physical-analog crimes into highly organized, high-level cybercrimes. The centralized data storage model has become the primary target for cyber penetration aimed at locking access (ransomware) or instantly manipulating land histories. Weak perimeter security at the

¹⁴ A E Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia," no. 2337 (2025): 1466–77.

¹⁵ Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

ministry's single gateway triggers the evolution of "digital land mafia" practices capable of structurally exploiting public civil rights from a distance.¹⁶ Through illegal modifications to the centralized database, cybercriminals can alter ownership history, delete records of mortgage encumbrances, or issue overlapping land titles without leaving the physical traces of analog documents, which are usually easily detected via visual examination.¹⁷ The instantaneous nature of digital data modification makes the detection of land disputes more difficult to identify, thereby leaving the dignity of electronic certificates as robust legal evidence in court vulnerable to degradation.¹⁸

Furthermore, the latent danger of this centralized storage model lies in its high vulnerability to insider threats that exploit system administrator access rights. When a system relies solely on a single national repository, a user with high-level access rights (superuser access) possesses unrestricted authority to unilaterally alter spatial and textual data elements without requiring validation consensus from external verification nodes.¹⁹ This absence of multi-party control is exacerbated by weaknesses in cyber disaster recovery management, where data restoration becomes impossible if

¹⁶ Mujiburohman, "Transformasi Dari Kertas Ke Elektronik: Telaah Yuridis Dan Teknis Sertipikat Tanah Elektronik."

¹⁷ Rosiyati MH Thamrin et al., "Blockchain-Based Land Certificate Management in Indonesia," *ADI Journal on Recent Innovation (AJRI)* 2, no. 2 (2021): 232–52, <https://doi.org/10.34306/ajri.v2i2.339>.

¹⁸ Sugiarto, "Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata."

¹⁹ Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia" 2, no. 1 (2024): 8–16, <https://doi.org/https://doi.org/10.32520/albahts.v2i1.3044>.

the backup data ecosystem is still managed within the scope of the same centralized server.²⁰ This failure to segregate administrative oversight demonstrates that the systemic failure risk of the SPoF architecture is no longer just a theoretical prediction, but a real threat poised to collapse the legal validity of national land registration whenever the centralized server suffers destructive cyber penetration.

2. Empirical Manifestation of Public Sector Cyberattacks: A Case Study Analysis of the Brain Cipher Ransomware on PDNS 2 and the Hacker Bjorka

The structural vulnerability inherent in centralized database architecture is no longer a hypothetical risk, but has instead transformed into a tangible threat that paralyzes various public service sectors in Indonesia. The most destructive empirical manifestation of this centralized system weakness was clearly recorded in a cyberattack involving the Brain Cipher ransomware strain, which infected the Temporary National Data Center 2 (PDNS 2) infrastructure in Surabaya on June 20, 2024. According to an official report released by the National Cyber and Crypto Agency (BSSN), the cyberattack successfully exploited the public network defense perimeter and encrypted all data belonging to 282

²⁰ KOMDIGI, “Siaran Pers No. 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah,” 2024, <https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-412-hm-kominfo-06-2024-tentang-indikasi-serangan-siber-wamenkominfo-fokus-tangani-dampak-layanan-pemerintah>.

government agencies at both central and regional levels.²¹ The impact of this single point of main infrastructure failure triggered a massive paralysis of public digital service systems on a national scale. This widespread scale of damage was exacerbated by technical findings from the BSSN, which revealed that the encrypted data could not be recovered due to the backup data system being managed within the exact same centralized ecosystem.²² Placing primary data and backup data under a single centralized management regime constitutes a fundamental failure in cyber disaster recovery management, as such configuration caused all backup data to be encrypted simultaneously once hackers gained control of the primary server.

To provide a comprehensive overview of the distribution of impacts resulting from the collapse of the centralized architecture during the PDNS 2 incident, the details regarding the affected public service sectors are presented in the following table:

Table 1. Impact of the PDNS 2 Ransomware Attack on Public Services

No.	Sector	Affected Agency	Impact on Services	Disruption Duration
1	Immigration	Directorate General of Immigration	Disruption of passport issuance services and digital	3–5 days

²¹ CNN, “CNN Indonesia. (2024, Juni 24). BSSN: Gangguan Pusat Data Nasional Ulah Serangan Siber Ransomware. CNN Indonesia.”

²² KOMDIGI, “Siaran Pers No. 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah.”

			immigration services throughout Indonesia	
2	Investment	Investment Coordinating Board (BKPM)	Disruption to the investment licensing service system and the OSS (Online Single Submission) system	Not mentioned
3	Education	Ministry of Education, Culture, Research, and Technology (Kemendikbudristek)	Disruption of access to the national Education Core Data (Dapodik)	Not mentioned
4	Land Administration	National Land Agency (BPN) – several regions	Temporary disruption of access to electronic certificate data and digital land services	Not mentioned

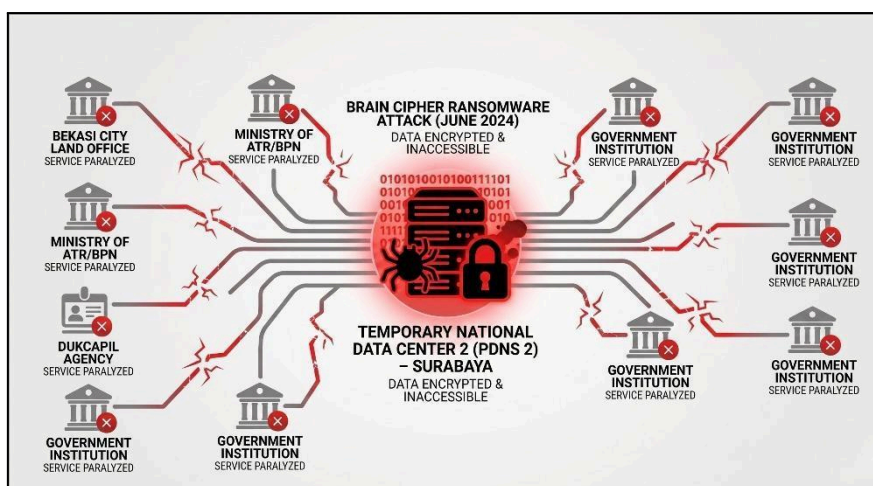
5	Other Public Services	278 central and regional government agencies	Various disruptions, from administrative services and public information systems to regional licensing services	2–14 days
---	-----------------------	--	---	-----------

Source: Compiled from BSSN reports (2024) and national news coverage

The data in Table 1 indicates that the duration of service disruptions varied depending on the complexity of system recovery for each respective agency, where certain specific duration data was not officially published and is thus marked as unavailable. The scope of impact encompasses 278 agencies integrated with the Temporary National Data Center (PDNS 2), spanning from central to regional services; hence, cross-verification with official BSSN reports or relevant ministerial circulars is highly recommended to ensure data accuracy for academic citation purposes. In the land sector itself, cyber interrogation of the centralized PDNS 2 server resulted in regional land office officials being locked out of digital access to the public electronic certificate of title database, which automatically halted the process of issuing, verifying, and registering transfers of citizens' land rights for several days.

Visually, the propagation pattern of damage resulting from the collapse of a single primary control point within this centralized architecture can be mapped through the infrastructure dependency flow as illustrated below:

Figure 1. Illustration of Centralized Architecture Vulnerabilities in the PDNS 2 Incident



Source: Processed based on the chronology of national cyber incidents (CNN Indonesia, 2024).

Beyond the threat of data access denial through ransomware encryption mechanisms, a centralized database architecture also harbors significant vulnerability to illegal data exfiltration. The weak perimeter security and fragile access control at the single storage gateway were vividly illustrated in the mass data breach executed by a hacker named Bjorka in September 2022. In that security incident, as many as 1.3 billion SIM card registration records were successfully accessed, extracted, and freely traded on cyber forums stemming from just a single point of weakness in a

central ministry server.²³ Subsequent investigations confirmed by the BSSN indicated that the breached data included sensitive citizen information variables, ranging from National Identification Numbers (NIK), full names, and domiciliary addresses to active telephone numbers.²⁴

This massive hacking of population data carries a multiplier effect that directly undermines the validity of the national electronic land registration system. Within the digital administrative ecosystem of the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (Kementerian ATR/BPN), the NIK and population identity variables serve as the primary parameters utilized by the system to verify the identity and legal capacity of the legal subjects holding land rights. Once billions of these identity data records fall into the hands of unauthorized third parties, the validity of the verification process in electronic land registration loses its degree of accuracy. The availability of compromised population data in cyberspace provides ample opportunity for malicious actors to commit digital identity theft in land transactions. That weak access controls on a single public server constitute the primary entry point for both insider and external threats that are difficult to detect via conventional security systems, as attackers manipulate access rights that appear legitimate to the centralized system.²⁵

²³ CNN, "CNN Indonesia. (2022, September 2). 1,3 Miliar Data Registrasi SIM Card Diduga Bocor. CNN Indonesia."

²⁴ MetroTV, "Kebocoran Data Kembali Terjadi, Kerja Kominfo Dan BSSN Dipertanyakan," 2024, <https://www.metrotvnews.com/read/bzGCzVPy-kebocoran-data-kembali-terjadi-kerja-kominfo-dan-bssn-dipertanyakan>.

²⁵ Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

3. Juridical Implications on the Guarantee of Legal Certainty of Land Rights and the State's Due Diligence Obligation

The implementation of land digitalization through electronic land certificates which is accommodated through the Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency (Permen ATR/BPN) Number 1 of 2021 carries immense legal consequences for national agrarian governance. Constitutionally, land registration is a mandate under Article 19 of the Basic Agrarian Law (UUPA), which aims to provide a guarantee of legal certainty and protection to land rights holders throughout the territory of the Republic of Indonesia. However, when this database is migrated into a centralized database system that possesses inherent technical vulnerabilities, the essence of "legal certainty" undergoes a significant degradation. Under the negative system of land registration with positive tendencies adopted by Indonesia pursuant to Government Regulation Number 24 of 1997, a certificate of title constitutes strong but rebuttable evidence (*prima facie* evidence), so that the physical data and legal data contained therein remain subject to challenge by another party in court at any time. This vulnerability multiplies within a centralized digital ecosystem; if the ministry's server suffers data corruption due to a cyberattack, or if unauthorized modifications occur without a physical audit trail, the civil rights of legitimate landowners are placed in a position of absolute uncertainty due to the absence of a

guarantee of the authenticity of information from the public authority.²⁶

Weak verification controls within the centralized land administration system have proven to trigger the emergence of new *modi operandi* of agrarian crimes that exploit digital bureaucratic loopholes. A clear manifestation of this systemic weakness is vividly recorded in a criminal case at the Purwodadi District Court through Decision Number 11/Pid.B/2024/PN Pwd. The case, involving the defendant, demonstrates how administrative verification flaws can be exploited to control a Right to Build (Hak Guna Bangunan / HGB) title Number 1 in Sugihmanik Village, Grobogan Regency, spanning an area of 826,491 m². The defendant was conclusively proven guilty of using a forged authentic deed executed before Notary Edy Riyanto to unilaterally manipulate the corporate board composition and transfer corporate assets of PT Azam Laksana Intan Buana (PT ALIB) without the approval of the legitimate corporate organs.²⁷

In the context of digital land registration law, this case establishes a valuable precedent regarding how fragile land rights protection is if the ministry's database is not integrated in real-time with external legal entity databases (such as the Directorate General of General Legal Administration of the Ministry of Law and Human Rights and the notary reporting system). The conventional centralized land registration system, which is passive and fragmented, has proven incapable

²⁶ Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia."

²⁷ Machfud.

of automatically cross-checking corporate documents that serve as the basis for large-scale land title transfers.²⁸ Consequently, the land mafia can easily exploit forged documents to register transfers of certificate titles or execute asset diversions digitally, creating a situation where legitimate landowners lose their civil rights without any early warning from the ministry's oversight system.

The cascading impact of this fragile centralized information infrastructure touches upon the law of evidence in judicial institutions. Under the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law), electronic information and/or electronic documents and their printouts constitute admissible legal evidence and hold an equal standing with conventional evidence in court trials.²⁹ However, the primary prerequisites for electronic documents to possess robust evidentiary value are the fulfillment of the principles of system reliability, data integrity, and non-repudiation.

When a national data center such as PDNS 2 is successfully breached by a ransomware attack that encrypts vital data,³⁰ or when sensitive population data leaks into the hands of the hacker Bjorka,³¹ the guarantee regarding the integrity and authenticity of such digital land documents is

²⁸ Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

²⁹ Sugiarto, "Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata."

³⁰ KOMDIGI, "Siaran Pers No. 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah."

³¹ MetroTV, "Kebocoran Data Kembali Terjadi, Kerja Kominfo Dan BSSN Dipertanyakan."

juridically vitiated. In civil procedural law, electronic land certificates originating from a database that has been infected or leaked will lose their credibility as reliable authentic evidence. Cyberattackers or internal actors (insider threats) can introduce minor alterations to land boundary coordinates or ownership details undetected by judges, thereby potentially resulting in erroneous court judgments that prejudice the actual rights holders.³²

From the perspective of administrative law, the failure to secure nationwide electronic land registration infrastructure constitutes serious administrative negligence. Pursuant to Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law), the Ministry of ATR/BPN acts as the Personal Data Controller, bearing the legal obligation to implement technical and organizational measures to protect public personal data against unauthorized processing, leaks, or destruction. This due diligence obligation demands that the ministry construct a resilient information security architecture capable of withstanding cyber disaster scenarios, including the provision of isolated and independent backup systems (disaster recovery).³³

When the ministry places primary data and backup systems within the same centralized ecosystem causing both to become simultaneously paralyzed due to a malware attack,³⁴ the state has legally failed to meet the due diligence

³² Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

³³ Abdullah, "Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi."

³⁴ KOMDIGI, "Siaran Pers No. 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah."

standards required for public data protection.³⁵ This negligence provides a solid juridical basis for affected citizens to file a civil lawsuit against the government on the grounds of an Unlawful Act by the Government (Onrechtmatige Overheidsdaad / OOD) to claim damages for the loss of legal guarantees protecting their agrarian data.

Macroeconomically, the legal uncertainty bred by this fragile centralized land database system revitalizes theoretical anxieties surrounding the creation of "dead capital." According to the theory of property rights formalization, robust legal guarantees over land serve as the primary key to transforming land from a mere physical object into active capital that can be used to leverage the economy.³⁶

When electronic land certificates are no longer backed by a resilient and trustworthy database system, the economic value of these certificates as credit security instruments in financial institutions will sharply decline. National banking institutions will enforce highly stringent prudential banking principles and potentially refuse electronic registrations of mortgages (Hak Tanggungan Elektronik / HT-el) if the reliability and validity of certificate data on the ministry's servers are doubted. This banking disincentive not only restricts access to capital for micro, small, and medium enterprises (MSMEs) that heavily rely on collateral certainty, but also triggers stagnation in the housing finance credit market. In the long run, global skepticism toward the integrity of national agrarian data will lower the interest of

³⁵ Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

³⁶ Maulana Rafi Danendra, "Pembentukan Bank Tanah: Merencanakan Ketersediaan Tanah Untuk Percepatan Pembangunan Di Indonesia."

foreign investors (Foreign Direct Investment) to invest their capital in land-based industrial sectors in Indonesia, given that legal certainty over land remains an absolute, non-negotiable prerequisite in international business risk calculations.

B. Relevance of Blockchain Technology as a More Absolute Agrarian Data Protection Solution

The paradigm shift from a centralized database system that harbors systemic failure risks toward decentralized technology gives rise to a revolutionary agrarian data security model. Fundamentally, the integration of digital land technology is no longer merely about organizing paper-based administrative procedures, but must redefine the essence of legal trust (trust protocol) in cyberspace as analyzed in the comparative study of decentralized architecture.³⁷ In the analog era, the authenticity of agrarian documents rested upon officials' signatures and wet institutional stamps, which proved to be highly passive and easily manipulated by land

³⁷ Filipe Pinto et al., "Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices' Digital Twins and Data," *Blockchain: Research and Applications* 7, no. 3 (2025): 100342, <https://doi.org/10.1016/j.bcra.2025.100342>; Victoria Lemieux, "Blockchain Technology for Recordkeeping Help or Hype? Blockchain Technology for Recordkeeping," *Blockchain Technology* ... 1, no. October (2016): 1–30, <https://www.idees-ideas.ca/sites/default/files/sites/default/uploads/general/2016/2016-sshrc-ksg-lemieux.pdf>.

cybercrime syndicates.³⁸ Through the adoption of a decentralized architecture, the guarantee of legal certainty transforms from subjective trust based on the personal authority of state apparatuses (centralized trust) into objective trust guarded by the integrity of transparent cryptographic algorithms (algorithmic trust).³⁹ To examine the effectiveness and reliability level of this technology in protecting citizens' property rights, this section will deeply dissect the resilience of distributed ledger architecture, cryptographic protection in mitigating insider threats, and a comparative analysis of the international land hybrid model in the Republic of Georgia.

1. Resilience of Distributed Ledgers Against Total Paralysis Risks

The contemporary electronic land registration model that relies on a single cloud computing infrastructure under the control of the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (Kementerian ATR/BPN) has proven highly vulnerable to crippling attacks such as DDoS (Distributed Denial of Service) and ransomware infiltration.⁴⁰ As an antithesis to this vulnerable model, Distributed Ledger Technology (DLT) offers absolute resilience by distributing identical copies of the land database to thousands of authorized network nodes across the

³⁸ Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia."

³⁹ Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

⁴⁰ Mujiburohman, "Transformasi Dari Kertas Ke Elektronik: Telaah Yuridis Dan Teknis Sertipikat Tanah Elektronik."

jurisdiction of Indonesia.⁴¹ With a laterally distributed architecture, data sovereignty is no longer dependent on a single main ministerial server. Should one of the primary nodes or the national data center experience total paralysis due to a cyber disaster or physical destruction, thousands of other nodes at the Regency/City Land Office level as well as partner state institutions (such as the BSSN and relevant ministries) will remain active in serving public transactions synchronously with zero downtime.⁴²

The resilience of this decentralized system rests upon a network consensus mechanism that automatically validates every change in the status of land rights.⁴³ In conventional centralized database systems, data modifications can be executed instantly merely by manipulating the access controls of a single administrator.⁴⁴ In a blockchain ecosystem, however, every transaction involving data additions, certificates, or registration of rights must undergo a rigorous distributed verification process, each node in the peer-to-peer network acts as an independent witness holding a complete copy of the entire transaction history (state database).⁴⁵ Changes to the status of land rights will only be considered legally valid if approved by a majority of the network nodes

⁴¹ Pinto et al., "Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices' Digital Twins and Data."

⁴² Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."

⁴³ Abdullah, "Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi."

⁴⁴ Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

⁴⁵ Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."

based on an agreed consensus algorithm, such as Proof of Authority (PoA), which is highly suited for a public service consortium with a high level of institutional trust.⁴⁶

To provide a more detailed overview of the operational resilience comparison between the current centralized database infrastructure and a blockchain-based decentralized architecture, an evaluation of various cyberattack scenarios is presented in Table 2 below:

Table 2. Resilience Comparison of Centralized Systems vs. Blockchain Against Attack Scenarios

No.	Attack Scenario	Centralized Database	Blockchain (Permissioned)
1	DDoS attack on the central server	Total paralysis (all services halted)	Resilient (other nodes remain active to provide services)
2	Ransomware encrypts data	Permanent data loss (if backups are also affected)	Data remains secure (other nodes maintain a complete copy)
3	Insider threat	Very high risk (unrestricted super-user access)	Low risk (requires multi-party consensus)
4	Physical server damage (Physical Corruption)	Total data loss	Data remains intact (stored in a distributed manner)

⁴⁶ Abdullah, “Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi.”

5	Recovery time (Recovery Time)	Days to weeks	Minutes to hours (node synchronization)
---	----------------------------------	---------------	---

Source: Compiled from Zheng et al. (2017) and Paavo & Rodríguez-Puentes (2024)

Based on the comparative analysis in Table 2 located prior to this paragraph, a permissioned blockchain architecture that restricts validation access rights solely to trusted nodes within the state consortium offers highly superior resilience advantages compared to conventional centralized databases. In terms of DDoS attacks, the absence of a single point of failure on the blockchain guarantees continuous availability of public services, as the attack traffic load will be distributed and absorbed by other active network nodes.⁴⁷ When confronted with a destructive ransomware attack scenario like the Brain Cipher PDNS 2 case, a centralized database faces a high risk of permanent data loss if its backup system also becomes infected due to being within the same centralized ecosystem.⁴⁸ Conversely, in a blockchain network, forced encryption on a single node will not damage the integrity of the overall system, because thousands of other distributed nodes still retain an intact and authentic copy of the ledger to instantly restore the affected node.

From the perspective of operational efficiency and accountability, this technical resilience is directly proportional to the reduction of land bureaucracy burdens, which have

⁴⁷ Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."

⁴⁸ KOMDIGI, "Siaran Pers No. 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah."

historically served as fertile breeding grounds for agrarian disputes. The National Land Agency (BPN), which historically held a passive administrative role, can transform into a proactive and preventive regulatory body through the utilization of a distributed ledger that presents land histories transparently, in real-time, and immutably. Automated data synchronization running across related institutions (such as ATR/BPN, BSSN, and Ditjen Dukcapil) via a peer-to-peer network will truncate exhausting non-litigation dispute mediation and facilitation processes. With recovery times shifting from weeks to minutes through a node consensus-based recovery mechanism, the guarantee of legal certainty provided by the state transforms from mere formal-administrative certainty into technical-material certainty that is absolutely protected.⁴⁹

2. SHA-256 Cryptographic Protection and Immutability Characteristics in Countering Insider Threats

The problem of insider threats (internal threats) is a land bureaucracy pathology that is most difficult to curb via conventional centralized database systems (Machfud & Suparjo, 2025). In conventional centralized server architectures, a database administrator (DBA) holds unrestricted access controls (superuser access) enabling them to directly manipulate data. Corrupt internal actors can manipulate SQL databases to alter landowners' names, spatial

⁴⁹ Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia"; Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends."

boundary coordinates, or even delete land registry source documents (warkah) without going through official procedures. These manipulative actions often leave no audit trail because such actors also possess the administrative authority to delete or doctor system logs to conceal traces of their illegal activities. Herein lies the fundamental difference from blockchain technology, which replaces the personal trust of state apparatuses (personal trust) with objective trust based on mathematical systems (algorithmic trust).⁵⁰

The primary strength of blockchain in fortifying land data against internal manipulation threats stems from the implementation of cryptographic hash functions, specifically the 256-bit Secure Hash Algorithm (SHA-256). In simple terms, the SHA-256 hash function operates like a "digital fingerprint" generator. Regardless of the size of the entered land registration document from electronic certificates of title to entire digital land registry source documents this algorithm will process it into a series of unique random hexadecimal codes 64 characters in length. This function is a one-way function, meaning that the system can easily generate a digital fingerprint from the original land document, yet it remains computationally impossible for anyone to reconstruct the contents of the land document solely by looking at its digital fingerprint code. The output of this function possesses an immense probability space reaching 2^{256} unique

⁵⁰ Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia"; Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia"; Pinto et al., "Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices' Digital Twins and Data."

combinations, a mathematical figure guaranteeing that no two different land documents will ever share the same digital fingerprint (collision resistance).⁵¹

It is this "digital fingerprint" characteristic that gives rise to absolute immutability through the concept of a chronological chain. Within a blockchain network, each page of the land registry (data block) is sequenced consecutively by embedding the digital fingerprint of the previous block into the new block. This chained linkage creates a powerful cyber domino effect in the event of data manipulation. If an internal actor attempts to illegally alter historical land registration transaction data for instance, changing a land area from the actual 1,000 m² to 1,001 m² the digital fingerprint of that block will immediately change radically and randomly. This single minor character change will instantly sever the connection with the subsequent block (broken chain), as the new block still references the old digital fingerprint code.⁵²

Technically and legally, a broken chain resulting from data engineering will be instantly detected and automatically rejected by the network consensus mechanism guarded by

⁵¹ Yusuf Anshori, A. Y. Erwin Dodu, and Dewa Made P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) Pada Tanda Tangan Digital," *Techno.Com* 18, no. 2 (2019): 110–21, <https://doi.org/10.33633/tc.v18i2.2166>; Suryawijaya, "Meneksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia."

⁵² Abdullah, "Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi"; Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends"; Mohammad Abdullah Mansoor et al., "Blockchain Technology for Land Registry Management in Developing Countries," *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering, ETECTE 2023 - Proceedings*, 2023, <https://doi.org/10.1109/ETECTE59617.2023.10396736>.

thousands of independent nodes. The validation of digital fingerprints and electronic signatures demonstrated absolute 100% accuracy in detecting and thwarting every data alteration attempt without requiring manual verification from external administrators. This protection is reinforced by the use of asymmetric key cryptography, where every issuance of a digital land document must be electronically signed using a private key exclusively held by the legitimate authorized official. Through this mechanism, internal ministerial actors lack the technical capability to forge the digital signatures of regional land officials due to mathematical constraints in reconstructing private keys from publicly recorded public keys.⁵³

Through this restructuring of cryptography-based security architecture, the existence of a "digital land mafia" collaborating with corrupt internal BPN actors can be permanently eliminated. Land digitalization must no longer be positioned merely as migrating physical documents into a fragile, centralized PDF format, but must instead be a fundamental reconstruction of the integrity of national agrarian data. Building a robust information security system demands compliance with fully distributed encryption standards. To ensure that the reliability of the program code executing this land logic is free from inherent vulnerabilities, regular code audits are absolutely imperative. Rigorous security testing is crucial to ensure that this blockchain-based land registration system is entirely sterile of cyber logic flaws

⁵³ Abdul Gani Pura Suratma and Abdul Azis, "Digital Signature Using QR Code By Advanced Encryption Standard Method," *Techno* 18, no. 1 (2017): 59–68; Mansoor et al., "Blockchain Technology for Land Registry Management in Developing Countries."

that could be exploited by internal actors to pass legally defective land registry source documents.⁵⁴

3. Comparative Analysis of Hybrid Architecture in the Land Administration System of the Republic of Georgia

To test the reliability of distributed ledger technology on a national scale, academic evaluations of land law must rely upon globally proven empirical evidence. In the international land administration landscape, the Republic of Georgia stands as a pioneer country that successfully reformed its land rights recording system from a post-Soviet era bureaucratic model vulnerable to internal manipulation into a transparent land ecosystem with high integrity. The success of agrarian reform in Georgia was achieved through a strategic partnership between the public sector, represented by the National Agency of Public Registry (NAPR), and The Bitfury Group as the technology infrastructure provider.⁵⁵

In formulating an adaptive national land policy model, comparative data regarding the operational details, document volume, and cost efficiency of Georgia's land hybrid architecture becomes an essential instrument. The detailed data concerning the technical-operational parameters of the

⁵⁴ Marwa Mnasri, Afef Jmal Maâlej, and Mohamed Jmaiel, "A Systematic Literature Review on Security Testing of Ethereum Smart Contracts," *Blockchain: Research and Applications* 7, no. 2 (2025): 100314, <https://doi.org/10.1016/j.bcr.2025.100314>; Rakhmat Kurniawan R, Rina Filia Sari, and Noor Azizah, "Sistem Validasi Keaslian Dokumen Digital Berbasis QR-Code," *Jurnal Teknologi Informasi* 4, no. 2 (2020): 321–27, <https://doi.org/10.36294/jurti.v4i2.1722>.

⁵⁵ Lazuashvili, Norta, and Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia*.

Republic of Georgia's hybrid system is presented in Table 3 below:

Table 3. Impact of the PDNS 2 Ransomware Attack on Public Services

No.	Parameter	Implementation Details
1	Year of Implementation	2016
2	Technology Development Partner	The Bitfury Group
3	Blockchain Architecture	Public Blockchain (Bitcoin) for timestamping; Private Blockchain for document storage
4	Accumulated Registered Documents	More than 1.5 million properties (up to 2024)
5	Security & Integrity Mechanism	Merkle Tree + Root Hash sent to the Bitcoin network
6	Estimated Cost per Transaction	USD 0.05–0.10 (hash fee to the Bitcoin network)
7	Impact on Public Trust	Increased significantly post-implementation

Source: Compiled from Lazushvili et al. (2019) and Shang & Price (2019)

Based on the empirical data in Table 3 located prior to this paragraph, the primary characteristic serving as the key to success for the Georgian land model is the utilization of a hybrid architecture. This hybrid concept explicitly segregates the storage of physical documents containing sensitive personal data from the anchoring of their integrity in the

public domain. In practical implementation, Georgia's NAPR never uploads citizens' land documents or digital certificates of title openly to the public Bitcoin blockchain network, which is accessible to anyone. This separation approach is highly crucial to avoid infringing upon landowners' privacy rights and to align freedom of information with the state's obligation to protect personal data privacy.⁵⁶

This security method works using cryptographic compression, analogized as a "Sealed File Index List". Complete digital land documents remain stored privately within secure government internal servers (private storage). Every day, thousands of digital fingerprints (hashes) from issued land certificates are grouped and summarized hierarchically to form a data pyramid called a Merkle Tree. At the apex of this pyramid, the system generates a single digital fingerprint in the form of a root hash that represents the entire contents of that file index list.⁵⁷

This root hash value or single seal is then periodically transmitted to be locked within the global Bitcoin blockchain network. From the perspective of cyber evidence law, recording the seal on a public blockchain provides an absolute guarantee of timestamping and non-repudiation, as the timestamp is automatically witnessed by thousands of independent computers worldwide. Should a title dispute arise in court in the future, the judge only needs to match the

⁵⁶ Lazushvili, Norta, and Draheim; Pinto et al., "Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices' Digital Twins and Data."

⁵⁷ Lazushvili, Norta, and Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia*.

digital fingerprint value of the electronic certificate held by the parties with the historical seal value that has been permanently locked on the global blockchain since the transaction was registered.⁵⁸

The administrative implication of this hybrid model is the creation of highly significant state budget efficiency in providing the guarantee of legal certainty. With transaction costs ranging between USD 0.05 and USD 0.10 per seal embedding, the state does not need to bear the burden of expensive public computing costs to secure agrarian data. This pattern demonstrates that a land hybrid architecture is capable of suppressing the operational failure risk of a Single Point of Failure while simultaneously fulfilling the principle of due care in processing public data. Through this efficient encrypted anchoring system, the land ministry can transform from a passive recording agency into the frontline in providing robust material legal protection for the public's civil rights over their land.⁵⁹

C. The Urgency of Regulating Blockchain Technology within the National Agrarian Law Framework

⁵⁸ Suratma and Azis, "Digital Signature Using QR Code By Advanced Encryption Standard Method."

⁵⁹ Lazushvili, Norta, and Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia*; Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia."

Theoretical empirical studies regarding the advantages of distributed ledger architecture and one way encryption protection will not possess practical leverage unless supported by progressive regulatory reconstruction. The digital transformation of land administration in Indonesia is currently still positioned merely as a migration from physical-analog document formats into a rigid and centralized database format. Fundamentally, this transition demands a restructuring of the national regulatory framework to provide robust legal recognition for decentralized storage systems. Without an adaptive recodification of agrarian law toward cyber developments, the utilization of this cutting-edge security technology will collide with conventional legal principles that have not accommodated the paperless nature of cyberspace. To formulate the direction of national agrarian policy in this era of disruption, this section will systematically dissect the legal gaps in existing regulations, design a secure governance transition model, and provide legal validity for cryptography-based encryption evidence in court proceedings.

1. Identification of Legal Gaps in Existing Digital Land Regulations

The implementation of electronic land registration in Indonesia currently rests upon two primary regulations, namely the Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency (Permen ATR/BPN) Number 1 of 2021 concerning Electronic Certificates and Permen ATR/BPN Number 3 of 2023 concerning the Implementation Provisions of

Government Regulation Number 24 of 1997 concerning Land Registration. Although both ministerial regulations have initiated the digitalization of national land documents, from a juridical-normative standpoint, these rules still harbor highly significant legal gaps. The primary limitation of these existing regulations lies in the preservation of a rigid centralized database paradigm. Both Permen ATR/BPN Number 1 of 2021 and Number 3 of 2023 mandate that all spatial and legal data management rely on the ministry's single cloud infrastructure, without providing any room for the adoption of distributed ledger technology.⁶⁰

The absence of a legal framework accommodating this decentralized architecture implies operational uncertainty in the field. Land registration officers lack a legal basis to distribute certificate data to external verification nodes because it is prohibited by the monopolistic principle of single oversight within the national agrarian administration. To map out in detail the various points of legal gaps⁶¹ between existing digital land regulations and the technical requirements of blockchain-based cybersecurity, the gap analysis is presented in Table 4 below:

Table 4. Identification of Legal Gaps in Digital Land Regulations

⁶⁰ Mujiburohman, "Transformasi Dari Kertas Ke Elektronik: Telaah Yuridis Dan Teknis Sertipikat Tanah Elektronik"; Yusuf Daeng et al., "Analisis Penerapan Sistem Keamanan Siber Terhadap Siber Di Indonesia," *Journal Of Social Science Research* 3, no. 6 (2023): 1135–45.

⁶¹ Kusmiarto et al., "Digital Transformation of Land Services in Indonesia: A Readiness Assessment"; Mansoor et al., "Blockchain Technology for Land Registry Management in Developing Countries."

No.	Aspect	Existing Regulation	Requirement for Blockchain	Legal Gap
1	Data Infrastructure	Regulation of the Minister of ATR/BPN No. 3/2023: Centralized database	Distributed Ledger Technology (DLT)	Not yet explicitly regulated
2	Validation Mechanism	Single authority (Ministry/BPN)	Multi-party consensus (network nodes)	Does not yet have a legal basis
3	Legal Status of Hash	Not explicitly recognized	Instrument of proof equivalent to a deed	Probative force is not yet clear
4	Audit Trail	Relies on internal system logs	Permanent, transparent, and immutable audit trail	Audit standards are not yet defined
5	Cyber Security	No specific minimum standard	Resilience against a Single Point of Failure	Security regulations are not yet adequate

Source: Researcher's analysis, 2026

Based on the legal gap analysis data in Table 4 located prior to this paragraph, the most crucial legal gap lies in the absence of juridical recognition for cryptographic hash values as admissible legal evidence within national land procedural law. In the traditional civil law system of evidence, the authenticity of a document depends on the presence of an authorized official's wet signature and an official institutional stamp. When documents are migrated to digital forms, Permen ATR/BPN Number 1 of 2021 has indeed accommodated the use of certified electronic signatures. However, if such data is encrypted to form a digital fingerprint code (cryptographic hash) and recorded within a blockchain network, the evidentiary legal status of that code remains in limbo. There is no specific rule confirming that an immutable land hash value within a distributed ledger possesses material probative force equivalent to an authentic deed executed by a land official in court.⁶²

The subsequent juridical gap touches upon the validation mechanisms and audit trail aspects of digital land information systems (Pusat Inovasi Kota dan Komunitas Cerdas, 2021). Permen ATR/BPN Number 3 of 2023 positions the BPN as the sole authority controlling the database, rendering the transaction log recording mechanism entirely dependent on the internal logs of the ministry's server. This type of internal log system is legally very weak, as it lacks external integrity guarantees and can be manipulated at any time by corrupt internal administrators with superuser access to erase traces of

⁶² Sugiarto, "Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata"; Daeng et al., "Analisis Penerapan Sistem Keamanan Siber Terhadap Siber Di Indonesia."

land bureaucracy crimes. Conversely, robust information security standardization demands a permanent, transparent, and fully distributed audit trail that can only be achieved if there is a strong legal basis for the operation of multi-party consensus mechanisms. Regulatory adjustments must be made immediately so that the national land registration system possesses reliable minimum security criteria against the risk of destructive cyberattacks.⁶³

2. Regulatory Strategy Based on a Controlled Polycentricity Governance Transition Phase

The adoption of a paperless, decentralized infrastructure within an agrarian public service system that has historically been centralized and monopolistic cannot be executed instantaneously overnight. Enforcing cyber technology policies hastily without balancing bureaucratic readiness, digital literacy disparities, and computing infrastructure limitations across various regions risks triggering a dysfunction in national land administration. Therefore, a regulatory strategy design is required to divide the system migration process into stages, thereby providing a secure space for juridical and operational adaptation for state apparatuses and the public as service users. The theory of Controlled Polycentricity governance developed by Lakadawala offers an ideal theoretical transition bridge, wherein the ministry can laterally decentralize data nodes

⁶³ Mnasri, Maâlej, and Jmaiel, "A Systematic Literature Review on Security Testing of Ethereum Smart Contracts"; Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

while maintaining its primary oversight function under the legal framework of state sovereignty⁶⁴.

To provide juridical guidelines for the government in establishing the phased migration of land certificate data from conventional centralized databases toward a secure distributed ledger network, the division of governance transition phases is presented in Table 5 below:

Table 5. Transition Phases of Blockchain Implementation in

No.	Transition Phase	Blockchain Design Type	Main Characteristics	Implementation in Land Administration
1	Phase 1 (Initial Coordination)	Controlled Polycentricity	Selective decentralization with centralized oversight; limited distribution of authority; inter-organizational coordination; layered accountability	Regional land offices begin to connect within a limited network under central supervision
2	Phase 2 (Cross-Agency Integration)	Hybrid Blockchain	Combining public and private elements; transaction verification through a	Coordination among BPN, BSSN, Kominfo, and Kemendagri within a single

⁶⁴ Kusmiarto et al., “Digital Transformation of Land Services in Indonesia: A Readiness Assessment”; Yu Chen Hozefa Lakadawala, Komla Dzigbede, “Blockchain Technology for Public Services: A Polycentric Governance Synthesis” 2 (2024): 306–12.

			limited consensus mechanism; inter-agency interoperability	land data ecosystem
3	Phase 3 (Full Implementation)	Permissioned Blockchain	Restricted access to authorized nodes; consensus rules established by the central authority; maintaining centralized oversight	All national land offices as authorized nodes within a permissioned network

Source: Compiled from Lakadawala, H., et al. (2026).

Based on the tactical grouping parameters in Table 5 placed prior to this paragraph, the implementation of Phase 1 focuses on establishing initial coordination through a Controlled Polycentricity design. This initial phase design provides legality for land offices at the regency and city levels to act as local verification network nodes within their administrative boundaries under strict supervision from the central ministry. This restriction is legally strategic to ensure the construction of layered accountability, where any data entry errors or cyber anomalies at the regional level can be instantly isolated before spreading to the national system. Regional land registration officers obtain validation to digitally process local spatial and legal data, while the central

ministry continues to act as the sole supervisory institution holding full control over the system's validity protocols.⁶⁵

The subsequent transition shifts to Phase 2, which demands the integration of cyber systems across state institutions using a Hybrid Blockchain architecture. Under this hybrid framework, the security aspects of national land data are connected in real-time with partner ministries and cyber defense agencies, such as the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Informatics (Kominfo), and the Directorate General of Population and Civil Registration (Kemendagri). This multi-agency collaboration produces reliable data protection guarantees, since the validation of land legal subjects is cross-locked using the national population database, while system resilience is strictly monitored by the state crypto authority. This lateral integration also aligns the legal standing of the agrarian ministry as the Personal Data Controller with the mandate of the Personal Data Protection Law (the PDP Law), which requires secure and accountable data interoperability among public sector management institutions.⁶⁶

The apex of this transitional governance is achieved in Phase 3, which realizes absolute national land digitalization through a Permissioned Blockchain model. In this final stage, all national land offices throughout the territory of the Republic of Indonesia are activated as legitimate independent validator nodes, interconnected within a massive closed-loop

⁶⁵ Hozefa Lakadawala, Komla Dzigbede, "Blockchain Technology for Public Services: A Polycentric Governance Synthesis."

⁶⁶ Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia."

network. This controlled decentralization model provides a robust governance rationale against cyber threats, because access rights to validate and modify certificate data are absolutely restricted to state apparatuses holding official legal mandates. Regulations regarding these phased regulatory transitions serve as vital administrative law instruments to guide national land bureaucratic reform safely, measurably, and free from procedural law shake-ups concerning evidence due to technological failures in the midst of the system modification process.⁶⁷

3. Codification of the Legal Standing of Cryptographic Hashes and Digital Signatures as Authentic Evidence

The reconstruction of agrarian evidence law demands the codification of the legal standing of cryptographic hashes as legal evidence possessing strong material probative force in court. Thus far, the admissibility of electronic evidence in national civil procedural law still depends on the visual integrity of digital documents, which within a centralized system has proven highly vulnerable to untraceable manipulation. When land certificate data is encrypted into a unique code via the SHA-256 algorithm and recorded within a blockchain network, the hash value acts as an absolute and unforgeable "digital fingerprint". The codification of new norms in land procedural law must affirm that matching a hash value registered in a distributed ledger possesses a strong degree of proof to conclusively verify the authenticity of land

⁶⁷ Hozefa Lakadawala, Komla Dzigbede, "Blockchain Technology for Public Services: A Polycentric Governance Synthesis."

registration source documents. Formal recognition of this technical characteristic serves as a crucial legal instrument to transform the paradigm of civil evidence from subjective trust based on physical documents toward objective trust based on transparent cryptographic integrity.⁶⁸

The step of strengthening digital agrarian evidence is perfected through the consistent integration of electronic signatures utilizing asymmetric key cryptographic methods. In agrarian law enforcement, the forgery of wet signatures and official institutional stamps has proven to be the conventional bureaucratic loophole most frequently exploited by land crime syndicates, as recorded in the Purwodadi District Court Decision Number 11/Pid.B/2024/PN Pwd. To eliminate this criminal loophole, new regulations must grant absolute legality for the use of public key and private key pairs issued by an official Electronic Certification Provider (PSrE) in every land transaction. Through this mechanism, proving the authenticity of the parties' consent in digital land rights transfer transactions can be validated with an accuracy level reaching 100%, owing to the uniqueness of the private key, which is impossible for the land mafia to illegally reconstruct. Robust juridical recognition of cryptography-based digital signatures will break the chain of ownership disputes resulting from forged signatures, which historically account for the highest number of land cases in civil judicial institutions.⁶⁹

⁶⁸ Sugiarto, "Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata."

⁶⁹ Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia"; Suratma and Azis,

At the level of regulatory synchronization, the codification of this cyber evidence must successfully align the principles within the UUPA, the Electronic Information and Transactions Law (the ITE Law), and the Personal Data Protection Law (the PDP Law). The historical lack of harmonization among sectoral regulations has triggered uncertainty for judges in trials when assessing the probative force of electronic documents originating from databases that have previously suffered data breaches. In accordance with the principles of data protection due diligence, electronic land documents whose hash values are securely anchored to a hybrid blockchain network provide an assurance that the data remains sterile from unauthorized modifications. Therefore, amendments to electronic land registration regulations must explicitly define the technical eligibility standards of distributed storage systems so that every digital record therein is widely recognized by judicial authorities as valid authentic evidence binding upon the parties. This robust regulatory synchronization will not only strengthen the standing of cyber civil evidence but also guarantee compliance with the personal data protection law to safeguard the asset data sovereignty of all Indonesian citizens.⁷⁰

4. Regulatory Framework for Public-Private Partnerships and the Protection of Data

“Digital Signature Using QR Code By Advanced Encryption Standard Method”; Anshori, Erwin Dodu, and Wedananta, “Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) Pada Tanda Tangan Digital.”

⁷⁰ Suryawijaya, “Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia”; Kaczorowska, “Blockchain-Based Land Registration: Possibilities and Challenges.”

Sovereignty

The regulatory framework overshadowing public-private partnerships (Public-Private Partnership / PPP) serves as a vital administrative law instrument to sustain national land blockchain infrastructure. In practice, providing massive computing power and maintaining distributed network nodes across Indonesia demand funding and technological expertise that are difficult to satisfy independently through the ministry's budget. To minimize state capital expenditure, new regulations must facilitate the involvement of private technology providers as system development partners, mirroring the successful collaboration between Georgia's National Agency of Public Registry (NAPR) and The Bitfury Group since 2016. The configuration of these partnership models must be meticulously designed so as not to degrade state sovereignty over land data, which constitutes a vital national object, ensuring that control over determining the permissioned blockchain architecture remains under the absolute power of the ministry as the holder of data sovereignty. Regulating the boundaries of private involvement serves as the initial fortress to align operational efficiency with compliance regarding constitutional law principles.⁷¹

The restriction of authority and strict separation of roles between state institutions and private parties must be codified in implementing regulations to prevent the risk of illegal

⁷¹ Lazushvili, Norta, and Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Case study of Georgia*; Qiuyun Shang and Allison Price, "A Blockchain Based Land Titling Project In The Republic Of Georgia. Innovations / Blockchain for Global Development," *Innovations* 12, no. August (2019): 72–78; Hozefa Lakadawala, Komla Dzighede, "Blockchain Technology for Public Services: A Polycentric Governance Synthesis."

public data acquisition by private actors. Under the framework of the Personal Data Protection Law (the PDP Law), the Ministry of ATR/BPN acts as the Personal Data Controller holding juridical control over citizens' certificate data, whereas private partners can only be positioned as Personal Data Processors tasked with maintaining the functional smoothness of the network nodes' physical infrastructure. Implementing rules must explicitly prohibit private partners from decrypting sensitive data, unilaterally altering records, or transferring data outside the jurisdiction of the Republic of Indonesia in accordance with national data sovereignty principles. Through this juridical separation, control over the primary private key and authorization of the consensus mechanism remains in the hands of civil servants holding legal mandates, maximizing the suppression of potential third-party commercial interest interventions against the validity of digital land registration source documents.⁷²

Another dimension of this partnership regulation must be capable of mandating massive citizen awareness programs to construct solid public trust toward the new land registration system. The reliability of sophisticated cryptographic encryption technology will not provide effective legal protection if the public does not comprehend how to secure their private keys or remains vulnerable to cyber social engineering crimes. Therefore, regulations at the Government Regulation level must obligate the ministry

⁷² Suryawijaya, "Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia"; Pinto et al., "Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices' Digital Twins and Data."

alongside private partners to periodically conduct agrarian digital literacy campaigns and provide clear administrative indemnity guarantees if systemic cyber failures occur. This focused collaboration will drive the transformation of the ministry's role from a passive document recorder into a reliable preventive supervisory body in compressing the operational space of agrarian crime syndicates in the digital era. This robust regulatory synchronization generates absolute material legal certainty while simultaneously ensuring that the agrarian data sovereignty of the Indonesian people stands tall amidst the heavy currents of global cyber technology disruption.⁷³

Conclusion

This study reinforces that the reliance of national land administration on a centralized database architecture creates a structural vulnerability in the form of a Single Point of Failure that is no longer adequate to stem modern destructive cyber threats. The empirical evidence of the paralysis of 282 government agencies due to the Brain Cipher ransomware attack on PDNS 2, as well as the mass population identity breach by the hacker Bjorka, demonstrates that the single-gate storage model has degraded the guarantee of legal certainty mandated by Article 19 of the Basic Agrarian Law (UUPA). As a comprehensive antithesis, the adoption of distributed

⁷³ Lazuashvili, Norta, and Draheim, *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Case study of Georgia*; Machfud, "Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia."

ledger technology offers a model of absolute resilience through authorized network consensus mechanisms and an immutability characteristic based on SHA-256 cryptography that automatically rejects any unilateral data modification attempt. The successful integration of a hybrid model by the National Agency of Public Registry (NAPR) of the Republic of Georgia serves as a strong empirical foundation showing that securing a "digital fingerprint" without publishing sensitive data files to cyberspace can align the principle of freedom of information with the absolute obligation to protect public personal data.

The implementation of this decentralized land system demands a progressive regulatory reconstruction to bridge the legal gaps within Permen ATR/BPN Number 1 of 2021 and Number 3 of 2023, which remain dominated by the centralized server paradigm. The government needs to initiate the formulation of a regulation at the level of a Government Regulation that explicitly provides a robust legal standing for cyber cryptographic hash values so they are widely recognized by judicial authorities as valid authentic evidence that is binding upon the parties in court proceedings in accordance with the principles of the ITE Law. This new regulatory framework must also formulate a strict separation of roles between the Ministry of ATR/BPN as the Personal Data Controller and private technology providers as the Personal Data Processor under the corridor of the PDP Law to protect agrarian data sovereignty as a vital national object. A regulatory strategy executed in stages through three phases of Controlled Polycentricity governance starting from limited coordination of regional land offices to national permissioned

blockchain integration constitutes a safe, measurable approach free from procedural law shake-ups concerning evidence amidst the era of global cyber technology disruption.

References

- Abdullah, Subarkah. "Implementasi Blockchain Untuk Keamanan Data Akademik Dalam Sistem Informasi Perguruan Tinggi." *Go Infotech: Jurnal Ilmiah STMIK AUB* 31, no. 1 (2025): 149–60. <https://doi.org/10.36309/goi.v31i1.371>.
- Anggriawan, Rosi Pramula, Sutaryono Sutaryono, and M. Nazir Salim. "Penyelesaian Konflik Penguasaan Tanah HGU Dengan Masyarakat Di Bengkulu Utara." *Marcapada: Jurnal Kebijakan Pertanahan* 1, no. 1 (2021): 29–41. <https://doi.org/10.31292/jm.v1i1.2>.
- Anshori, Yusuf, A. Y. Erwin Dodu, and Dewa Made P. Wedananta. "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) Pada Tanda Tangan Digital." *Techno.Com* 18, no. 2 (2019): 110–21. <https://doi.org/10.33633/tc.v18i2.2166>.
- CNN, Indonesia. "CNN Indonesia. (2022, September 2). 1,3 Miliar Data Registrasi SIM Card Diduga Bocor. CNN Indonesia," 2022. <https://www.google.com/amp/s/www.cnnindonesia.com/teknologi/20220902062206-192-842221/lagi-lagi-bocor-data-kali-ini-13-miliar-info-registrasi-kartu-sim/amp>.
- . "CNN Indonesia. (2024, Juni 24). BSSN: Gangguan Pusat Data Nasional Ulah Serangan Siber Ransomware.

- CNN Indonesia.,” 2024.
<https://www.cnnindonesia.com/teknologi/20240624133250-192-1113404/bssn-gangguan-pusat-data-nasional-ulah-serangan-siber-Ransomware>.
- Daeng, Yusuf, Jimmy Levin, Muhammad Razzaq Prayudha, Nindy Putri Ramadhani, Susanto Imanuel, and Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng. “Analisis Penerapan Sistem Keamanan Siber Terhadap Siber Di Indonesia.” *Journal Of Social Science Research* 3, no. 6 (2023): 1135–45.
- Earlene, Felishella, Benny Djaja, Fakultas Hukum, Universitas Tarumanagara, and Jakarta Barat. “Implikasi Kebijakan Reforma Agraria Terhadap Ketidaksetaraan Kepemilikan Tanah Melalui Lensa Hak Asasi Manusia Implications of Agrarian Reform Policies on Land Ownership Inequality through the Lens of Human Rights” 6, no. 2 (2023): 152–70.
- Gościński, Jan, and Artur D. Kubacki. *Land Registration Concepts in Translation. International Journal for the Semiotics of Law*. Vol. 34. Springer Netherlands, 2021.
<https://doi.org/10.1007/s11196-020-09800-y>.
- Hozefa Lakadawala, Komla Dzigbede, Yu Chen. “Blockchain Technology for Public Services: A Polycentric Governance Synthesis” 2 (2024): 306–12.
- Kaczorowska, Maria. “Blockchain-Based Land Registration: Possibilities and Challenges.” *Masaryk University Journal of Law and Technology* 13, no. 2 (2019): 339–60.
<https://doi.org/10.5817/MUJLT2019-2-8>.
- KOMDIGI. “Siaran Pers No.

- 412/HM/KOMINFO/06/2024 Tentang Indikasi Serangan Siber, Wamenkominfo: Fokus Tangani Dampak Layanan Pemerintah,” 2024. <https://www.komdigi.go.id/berita/siaran-pers/detail/siaran-pers-no-412-hm-kominfo-06-2024-tentang-indikasi-serangan-siber-wamenkominfo-fokus-tangani-dampak-layanan-pemerintah>.
- Kusmiarto, Kusmiarto, Trias Aditya, Djurdjani Djurdjani, and Subaryono Subaryono. “Digital Transformation of Land Services in Indonesia: A Readiness Assessment.” *Land* 10, no. 2 (2021): 1–16. <https://doi.org/10.3390/land10020120>.
- Lazuashvili, Nino, Alex Norta, and Dirk Draheim. *Integration of Blockchain Technology into a Land Registration System for Immutable Traceability: A Casestudy of Georgia. Lecture Notes in Business Information Processing*. Vol. 361. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-30429-4_15.
- Lemieux, Victoria. “Blockchain Technology for Recordkeeping Help or Hype? Blockchain Technology for Recordkeeping.” *Blockchain Technology ...* 1, no. October (2016): 1–30. <https://www.idees-ideas.ca/sites/default/files/sites/default/uploads/general/2016/2016-sshr-ksg-lemieux.pdf>.
- Machfud, A E. “Digitalisasi Pertanahan Dan Pendaftaran Tanah Elektronik: Evaluasi Efektivitasnya Dalam Menekan Mafia Tanah Di Indonesia,” no. 2337 (2025): 1466–77.
- Mansoor, Mohammad Abdullah, Mohsin Ali, Abdul Mateen,

- Mohammad Kaleem, and Sajid Nazir. "Blockchain Technology for Land Registry Management in Developing Countries." *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering, ETECTE 2023 - Proceedings*, 2023.
<https://doi.org/10.1109/ETECTE59617.2023.10396736>.
- Maulana Rafi Danendra, Dian Aries Mujiburohman. "Pembentukan Bank Tanah: Merencanakan Ketersediaan Tanah Untuk Percepatan Pembangunan Di Indonesia." *Jurnal UNDIP Masalah-Masalah Hukum* 36, no. 4 (2022): 1–20.
- MetroTV. "Kebocoran Data Kembali Terjadi, Kerja Kominfo Dan BSSN Dipertanyakan," 2024.
<https://www.metrotvnews.com/read/bzGCzVPy-kebocoran-data-kembali-terjadi-kerja-kominfo-dan-bssn-dipertanyakan>.
- Mnasri, Marwa, Afef Jmal Maâlej, and Mohamed Jmaiel. "A Systematic Literature Review on Security Testing of Ethereum Smart Contracts." *Blockchain: Research and Applications* 7, no. 2 (2025): 100314.
<https://doi.org/10.1016/j.bcra.2025.100314>.
- Mujiburohman, Dian Aries. "Transformasi Dari Kertas Ke Elektronik: Telaah Yuridis Dan Teknis Sertipikat Tanah Elektronik," no. 5 (2021): 5.
<https://doi.org/10.31292/bhumi.v7i1.472>.
- Najwa, Fadhila Rahman. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia" 2, no. 1 (2024): 8–16.

- <https://doi.org/https://doi.org/10.32520/albahts.v2i1.3044>.
- Paavo, Johannes P, and Rafael Rodríguez-puentes. “A Systematic Literature Review on Blockchain-Based Titles Registries for Transparent Land Administration 1 Introduction,” no. 2008 (2025): 67–86.
- Pinto, Filipe, Catarina Ferreira da Silva, Sergio Moro, and Pedro Aquino. “Consumer-Controlled Digital Twin Architecture: How Blockchain Technology Gives Consumers Control over Their Smart Devices’ Digital Twins and Data.” *Blockchain: Research and Applications* 7, no. 3 (2025): 100342. <https://doi.org/10.1016/j.bcra.2025.100342>.
- R, Rakhmat Kurniawan, Rina Filia Sari, and Noor Azizah. “Sistem Validasi Keaslian Dokumen Digital Berbasis QR-Code.” *Jurnal Teknologi Informasi* 4, no. 2 (2020): 321–27. <https://doi.org/10.36294/jurti.v4i2.1722>.
- Shang, Qiuyun, and Allison Price. “A Blockchain Based Land Titling Project In The Republic Of Georgia. Innovations / Blockchain for Global Development.” *Inninations* 12, no. August (2019): 72–78.
- Sugiarto, Enan. “Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata,” no. June (2016): 182–99.
- Suratma, Abdul Gani Pura, and Abdul Azis. “Digital Signature Using QR Code By Advanced Encryption Standard Method.” *Techno* 18, no. 1 (2017): 59–68.
- Suryawijaya, Tito Wira Eka. “Mengeksplorasi Implementasi

Sukses Dalam Transformasi Digital Di Indonesia.” *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–67.

Thamrin, Rosiyati MH, Eka Purnama Harahap, Alfiah Khoirunisa, Adam Faturahman, and Kenita Zelina. “Blockchain-Based Land Certificate Management in Indonesia.” *ADI Journal on Recent Innovation (AJRI)* 2, no. 2 (2021): 232–52. <https://doi.org/10.34306/ajri.v2i2.339>.

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.” *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, 557–64.

Acknowledgments

None.

Funding Information

None.

Statement of Conflict of Interest

The authors state that there is no conflict of interest regarding the publication of this article.

Statement on Publication Ethics and Originality

All authors declare that this work is original and has never been published in any form or in any media, nor is it under consideration for

publication in any journal, and all sources cited in this work adhere to the basic standards of scientific citation.

Generative AI Statement

AI was utilized in the preparation of this manuscript exclusively for copy-editing and language polishing purposes, with no application in content generation, data interpretation, or conceptual development.

*This Page
Intentionally Left
Blank*