Volume 22, Number 2, (2025). Pages: 357-575.
Istinbath : Jurnal Hukum
ISSN : Print 1829-8117 – Online 2527-3973

Integration of Blockchain Technology in the Criminal Justice System: Challenges of Regulation, Data Security, and Legitimacy of Digital Evidence

Robby Malaheksa[1], Heni Siswanto[2], Agus Triono[3]
Universitas Lampung, Indonesia
Email: robby.malaheksa@gmail.com

Abstract

The development of digital technology has brought significant changes to the criminal justice system, particularly in the management of digital evidence. However, challenges such as data manipulation, evidence validity, and storage security remain significant issues. Blockchain, a technology that offers transparency, security, and data traceability, has great potential for application in the criminal justice system for more effective digital evidence management. This study aims to analyze the application of blockchain in the criminal justice system, particularly in relation to the validity of evidence, integrity, and digital evidence management. The methods used include a literature review and comparative analysis of conventional systems and blockchain-based models. The findings show that the implementation of blockchain can improve the security and protection of digital evidence through hashing and encryption mechanisms that are difficult to manipulate. In addition, this technology enables the decentralized recording of digital evidence transactions, thereby reducing the risk of abuse by certain parties. Therefore, the adoption of blockchain technology in the criminal justice system has the potential to strengthen the credibility and efficiency of the legal evidence process.

Keywords: *Blockchain, Criminal Justice System, Digital Evidence Management, Data Security*

Abstrak

Perkembangan teknologi digital telah membawa perubahan signifikan pada sistem peradilan pidana, terutama dalam pengelolaan bukti digital. Namun, tantangan seperti manipulasi data, validitas bukti, dan keamanan penyimpanan tetap menjadi masalah utama. Blockchain, sebagai teknologi yang menawarkan transparansi, keamanan, dan jejak data, memiliki potensi besar untuk diterapkan dalam sistem peradilan pidana guna pengelolaan bukti digital yang lebih efektif. Artikel ini bertujuan untuk menganalisis penerapan blockchain dalam sistem peradilan pidana, khususnya terkait validitas bukti, integritas, dan pengelolaan bukti digital. Metode yang digunakan meliputi tinjauan literatur dan analisis perbandingan antara sistem konvensional dan model berbasis blockchain. Temuan menunjukkan bahwa implementasi blockchain dapat meningkatkan keamanan dan perlindungan bukti digital

melalui mekanisme hashing dan enkripsi yang sulit dimanipulasi. Selain itu, teknologi ini memungkinkan pencatatan terdesentralisasi transaksi bukti digital, sehingga mengurangi risiko penyalahgunaan oleh pihak tertentu. Oleh karena itu, adopsi blockchain dalam sistem peradilan pidana berpotensi memperkuat kredibilitas dan efisiensi dalam proses bukti hukum.

Kata kunci: *Blockchain, Sistem Peradilan Pidana, Manajemen Bukti Digital, Keamanan Data*

Istinbath: Jurnal Hukum
Website : http://e-journal.metrouniv.ac.id/index.php/istinbath/index

Received : 2025-05-04 | Published : 2025-12-23.

Introduction

The Society 5.0 era not only impacts law enforcement but also emphasizes the need for a human-oriented approach that is not solely bound by legal norms. This initiative aims to build a principled, simple, fast, and cost-efficient judicial system that adapts to technological advances.[1] This principle is in line with Kusumaatmadja's ideas in his theory of Development Law, which emphasizes the need for a paradigm shift in Indonesian society towards a modern legal framework that functions not only as a set of rules but also as a primary tool for social reform.[2] Therefore, criminal law reform must be carried out through a policy-oriented approach that involves value considerations. Consequently, criminal law reform must also be value-oriented and aim to align criminal law with the socio-political, socio-philosophical, and socio-cultural values of Indonesian society.[3]

Indonesia's criminal justice system is based on positive law, as stipulated in Law No. 8 of 1981 concerning the Criminal Procedure Code (KUHAP), which regulates all procedures related to criminal proceedings. The process begins with an investigation and examination by the police, followed by prosecution by the Attorney General's Office and

[1] Gautami Tripathi, Mohd Abdul Ahad, and Gabriella Casalino, "A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges," *Decision Analytics Journal* 9 (December 2023): 100344, https://doi.org/10.1016/j.dajour.2023.100344.

[2] Budi Pramono, *Sosiologi Hukum* (Surabaya: Scopindo Media Pustaka, 2020).

[3] Barda Arief Nawawi, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Fajar Interpratama Mandiri, 2017).

then a trial.[4] The purpose of this criminal justice process is to ensure justice, legal certainty, the usefulness of the law, and the protection of human rights for individuals accused of committing criminal acts.[5]

Thus, the digitization of the criminal justice system must be implemented using digital technology to improve efficiency, transparency, and accuracy in the management of criminal justice processes. This includes the application of technologies such as electronic document management, electronic court systems, video conferencing, and artificial intelligence (AI)-based applications in the judicial system.[6] Likewise, the management of digital evidence is increasingly vital to support the success of criminal trials, especially in complex and sophisticated cases in both the physical and cyber worlds.[7] The goal is to modernize the criminal justice system and promote more effective and inclusive law enforcement.[8]

In practice, digital transformation has given rise to new forms of evidence such as photos, videos, recordings, and other digital documents or information. Digital evidence is inherently vulnerable and easily altered, meaning that it can be easily modified or manipulated. Therefore, regulations are required to ensure that such evidence can be legally used in the criminal justice system. However, based on Law Number 11 of 2008 concerning Electronic Information and Transactions, digital evidence is legally recognized and can be submitted to court. In addition, the Constitutional Court accepts digital media as admissible evidence. Therefore, establishing clear procedural rules for managing digital evidence in the criminal justice system is essential to ensure compliance with these legal standards.

---

[4] Silvina Helen Sondang Sihaloho, "Perbandingan Asas Legalitas Kitab Undang-Undang Hukum Pidana (KUHP) Dan Hukum Islam," *Jurnal Hukum Respublica* 21, no. 1 (2021), https://doi.org/10.31849/respublica.v21i2.8315.

[5] Alwi Padly Harahap et al., "KEMANUSIAAN DAN KEADILAN: MENGEKSPLORASI HAK ASASI MANUSIA DALAM KONTEKS HUKUM ISLAM," *HAKAM: Jurnal Kajian Hukum Islam Dan Hukum Ekonomi Islam* 8, no. 1 (July 2024), https://doi.org/10.33650/jhi.v8i1.8205.

[6] A. Haleem et al., "A Review of Blockchain Technology Applications for Financial Services," *Bench Council Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022), https://doi.org/10.1016/j.tbench.2022.100073.

[7] Tenriajeng Andi Papada, Muhamad Karim Said, and Wiwie Heryani, "Kedudukan Alat Bukti Yang Diperoleh Melalui Teknologi Informasi Dalam Pembuktian Tindak Pidana Informasi Dan Transaksi Elektronik," *Jurnal Al-Qadau* 7, no. 1 (2020), https://doi.org/10.24252/alqadau.v7i1.14892.

[8] O. Olukoya, "Assessing Frameworks for Eliciting Privacy and Security Requirements from Laws and Regulations," *Computers & Security*, ahead of print, 2022, https://doi.org/10.1016/j.cose.2022.102697.

Recent studies show that attention to blockchain in the context of data security is driven not only by its technological aspects but also by its capacity to respond to the fundamental weaknesses of conventional data management systems. The immutability and transparency of blockchain are understood as structural mechanisms that strengthen data integrity while limiting the scope of information manipulation.[9] In this framework, decentralization serves as an effective risk mitigation strategy because the systematic distribution of data across multiple nodes reduces the probability of system failure.[10] At a technical level, the use of advanced cryptography does not merely serve as a security tool but as an epistemic foundation that ensures data validity and authenticity.[11] Furthermore, the auditable nature of blockchain presents a new paradigm in data governance, in which permanent and verifiable transaction records enable more accountable oversight.[12]

However, the literature is relatively limited in systematically examining the implementation of blockchain technology in the criminal justice system, particularly in relation to the management of digital evidence. Therefore, this study aims to fill this gap through an analysis of the application of blockchain technology in the management of digital evidence in the criminal justice system. Thus, this study theoretically and practically expands the discourse on blockchain-based data security into the realm of the criminal justice system, which has been facing serious challenges in maintaining the integrity, authenticity, and sustainability of the chain of custody of digital evidence.

---

[9] V. Ahmad et al., "Blockchain Technology for Secure and Intelligent Industry Applications," in *Fostering Sustainable Businesses in Emerging Economies: The Impact of Technology* (2023), 147–65, https://doi.org/10.1108/978-1-80455-640-520231010; C.R. Mohan et al., "Blockchain-Based Solutions for Enhancing Data Integrity and Security," 2024, 1416–20, https://doi.org/10.1109/IC3I61595.2024.10828945.

[10] O. Oberoi and S. Raj, "Advanced Cryptographic Technologies in Blockchain," in *Blockchain Technology in Corporate Governance: Transforming Business and Industries* (2022), 327–51, https://doi.org/10.1002/9781119865247.ch15; W. Alzuabi, Y. Ismail, and W. Elmedany, "Privacy and Security Issues in Blockchain Based IoT Systems: Challenges and Opportunities," 2022, 258–65, https://doi.org/10.1109/3ICT56508.2022.9990679.

[11] M. Tratiya et al., "Pros and Cons of Consensus Method in the Context of Blockchain," in *Digital Transformation and Sustainability of Business* (2025), 408–11, https://doi.org/10.1201/9781003606185-94; A. Almomani et al., "Usage of Blockchain Technology for Improving Computer Security," paper presented at 2024 25th International Arab Conference on Information Technology, ACIT 2024, 2024, https://doi.org/10.1109/ACIT62805.2024.10877007.

[12] B. Aliya et al., "Ensuring Information Security of Web Resources Based on Blockchain Technologies," *International Journal of Advanced Computer Science and Applications* 14, no. 6 (2023): 834–43, https://doi.org/10.14569/IJACSA.2023.0140689; P.K. Chaurasia et al., "Anonymous Crime Reporting Using Blockchain and Smart Contract," 2024, 1059–64, https://doi.org/10.1109/ICPCSN62568.2024.00176.

Method

This study uses a case study approach to analyze the implementation of blockchain technology in the management of digital evidence in Indonesia. This approach allows for an in-depth exploration of how blockchain is applied across various sectors and the extent to which this technology aligns with existing regulations. This study employs a juridical-empirical method supported by a descriptive approach and literature review, which provides an in-depth analysis of normative regulations based on practical occurrences in society. This study focuses on the issue of digital evidence management, specifically the use of blockchain technology in the criminal justice system, based on secondary data collection. The data are contextual and aimed at understanding the concepts and knowledge related to blockchain.

This study aims to evaluate the use of blockchain as a mechanism for managing digital evidence in Indonesia from a legal perspective and to identify the challenges faced in integrating blockchain with existing regulations. It also seeks to provide recommendations for policymakers to support the implementation of blockchain technology in the management of digital evidence in Indonesia. By analyzing the juridical aspects of this technology, this study offers new insights for readers and provides a solid foundation for policymakers to prepare for technological developments by creating more responsive regulations. Furthermore, the findings of this study are expected to encourage the broader adoption of blockchain across various sectors. Data analysis was conducted using a descriptive qualitative method. Data were collected from various sources and analyzed to identify patterns, themes, and relationships relevant to the topic of the study. This analysis yields key findings that form the basis for recommendations to policymakers.

Results and Discussion

One important principle in the management of digital evidence is that the transfer and management of documents must be identifiable and arranged chronologically. This principle is intended to ensure that every action taken on digital evidence is fully documented and remains unchanged from the start to the end. Therefore, an instrument is required to ensure that the implementation of digital evidence management is conducted properly and accurately. Currently, blockchain technology is deemed capable of

providing a solution. The function of blockchain, which can adopt a ledger to record/store data/information in a place (block) within a network, logs and stores all data/information entered and managed using a decentralized system and cryptography. Decentralization ensures that all stored data/information are distributed across all blocks connected in a peer-to-peer network in real time with timestamps. Meanwhile, cryptography is a technique used to encrypt data/information within the blocks and transform it with a unique code composed of randomly arranged numbers/letters called a hash, allowing the blocks within the network to be interconnected through this hash code.

If a cyber-attack occurs with the intention of altering the data within a block, the other blocks connected in a decentralized manner will detect and validate it through hash matching using a consensus mechanism. Consequently, the data that will be used or validated are from all the connected blocks. Blockchain technology is a platform that allows any changes or data storage to be known by other parties connected within the blockchain. In contrast, the cryptographic system enhances data security, making it more resistant to manipulation, as the data recording/storage mechanism is transparent and immutable.[13] In Indonesia, there are no specific regulations regarding the management of digital evidence. Additionally, there is still debate about the validity of digital evidence and whether it can stand alone or requires corroboration from other evidence. However, considering its characteristics, digital evidence is classified as silent evidence (*stille getuigen*) that must be supported by other evidence, such as witnesses, experts, the defendant, or documents. Thus, digital evidence is increasingly recognized as physical evidence.[14]

Concept of Data Security in the Context of Digital Evidence Management

In the era of digitalization, data are the most valuable assets for both the government and society. Data are a crucial resource for making accurate decisions in all aspects, helping to solve problems and identify trends. However, the use of digital technology also carries potential data security risks, such as leaks, theft, manipulation, and unlawful use for the benefit of other parties. Therefore, the concept of data security

[13] Hukumonline, "Chain of Custody Berbasis Blockchain Dalam Penanganan Bukti Digital," 2024, https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam-penanganan-bukti-digital-lt64ce49bc3bf67/.

[14] Kemitraan and Lembaga Kajian dan Advokasi Independensi Peradilan, *Naskah Akademik Kerangka Hukum Perolehan, Pemeriksaan, Dan Pengelolaan Bukti Elektronik* (Jakarta, 2019).

is critical in the digital age.[15] There are three aspects of data security: confidentiality, integrity, and availability. These three aspects are related to maintaining the privacy of data from unauthorized parties and preventing unauthorized access to data or unlawful data use.[16]

Data authenticity ensures that data are not manipulated without the knowledge or consent of the authorized party. Data integrity guarantees that data are not corrupted or lost during storage or transmission. Data availability concerns the accessibility of data by authorized parties when required. This emphasizes the importance of supporting the use of the latest security technologies and strict safeguards. The implementation of appropriate and relevant security technologies will ensure that important data and information are protected from unauthorized access or manipulation. Additionally, the use of security technologies will help society comply with laws and regulations related to data security.[17]

The use of technology for data security alone is insufficient; strict security procedures are also necessary as an essential part of safeguarding data. This includes managing access rights and user controls, as well as policies for using regularly updated secure devices. Additionally, a disaster recovery plan must include procedures for data backup, restoration, and system recovery. This plan should be tested regularly to ensure preparedness for disasters and detrimental events. In the era of digital transformation, data security risks are becoming increasingly complex and escalating. Therefore, an effective data security strategy that continuously updates technology and implements stringent security practices to minimize risks should be applied.[18]

Definition of Blockchain Technology and Its Characteristics

[15] I.-C. Lin and T. Liao, "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security* 19 (2017), https://doi.org/10.6633/IJNS.201709.19(5).01.

[16] Centre for Innovation Policy and Governance, *Big Data, Kecerdasan Buatan, Blockchain, Dan Teknologi Finansial Di Indonesia: Usulan Desain, Prinsip Dan Rekomendasi Kebijakan* (Jakarta: Ditjen Aptika, 2018), https://aptika.kominfo.go.id/wp-content/uploads/2018/12/KajianKominfo-CIPG-compressed.pdf.

[17] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning," *IEEE Transactions on Industrial Informatics* 15, no. 6 (2019), https://doi.org/10.1109/TII.2018.2890203.

[18] J. Hoesada, "Disaster Recovery Planning: Manajemen Bencana Administrasi Dan Akuntansi," CRMS Indonesia, 2023, https://crmsindonesia.org/publications/disaster-recovery-planningmanajemen-bencana-administrasi-dan-akuntansi/.

The sophistication of blockchain technology has become widely known in recent years, especially as the underlying technology behind the emergence of cryptocurrencies such as Bitcoin. However, the potential of blockchain is far greater than that of cryptocurrency. Blockchain can be used in various sectors, such as banking, healthcare, and energy. In the context of digital evidence management, blockchain can be used to enhance data security, centralize data processing, and store digital data. One of the main advantages of blockchain technology is its ability to transmit and store data in a decentralized manner. This means that stored data are much safer because if one piece of data in the network encounters an issue or a cyberattack occurs, other data in different networks will still be available.[19]

Blockchain has a strong encryption system, where each piece of data stored in the blockchain can only be accessed by individuals who have the correct encryption key, ensuring that the stored data cannot be read by unauthorized parties. Blockchain also features a transparency system, which is crucial for digital transformation. This means that every transaction or block in the blockchain can be accessed and verified by all parties involved. Additionally, blockchain is difficult to manipulate because each network is sequentially linked to the previous and subsequent networks.[20] Each block in the network must approve and verify any new data added to a blockchain. If there is an attempt to manipulate data in one block, the entire blockchain will be affected and will not be approved by other blocks in the network. Therefore, blockchain is considered to be very secure against data manipulation attempts by unauthorized parties.

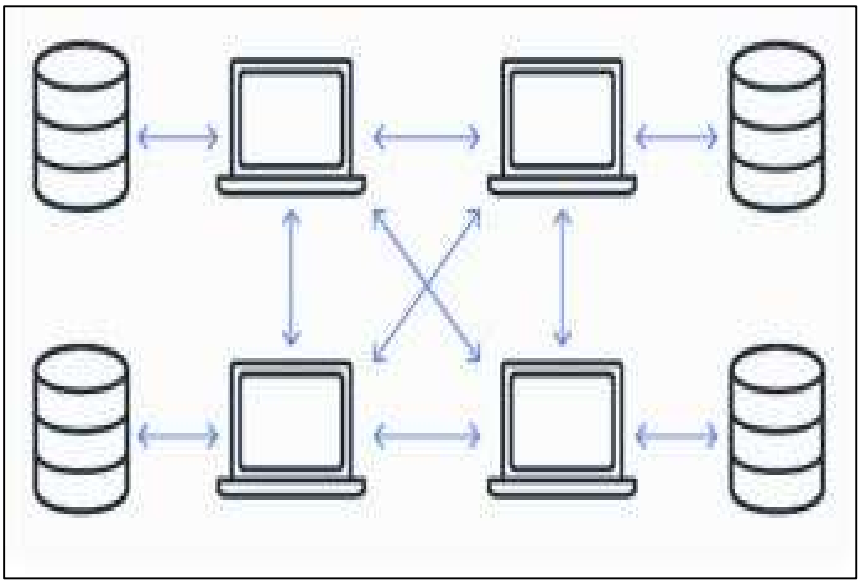
The process of verification and validation in blockchain is also very fast and efficient, as it does not require intermediaries or third parties, thus saving time and cost. Blockchain technology can enhance data security in the management of digital evidence. Evidence stored in the network can be locked with a strong encryption system, ensuring that only individuals with the encryption key can access and read the data stored in the network. Furthermore, it allows evidence to be stored and shared securely and in a

[19] A. Argani and W. Taraka, "Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertipikat Pada Perguruan Tinggi," *ABDI: Jurnal Pengabdian Dan Pemberdayaan Masyarakat* 1, no. 1 (2020), https://doi.org/10.34306/abdi.v1i1.121.

[20] Lin and Liao, "A Survey of Blockchain Security Issues and Challenges."

decentralized manner.[21] Blockchain does not store data at a centralized point but rather distributes it across the entire blockchain network. Every person connected to the network will have an identical copy of the stored data, and if one copy is compromised by a cyberattack or damage, other copies remain accessible.[22]

Figure 1. Illustration of the Blockchain Framework



Source: aws.amazon.com

Although Blockchain offers many benefits in the management of digital evidence, there are challenges that need to be addressed, one of which is the issue of scalability. This is because every piece of data entered by the network must be verified before being stored, which can increase costs when the network underperforms.[23] Despite these challenges, blockchain technology continues to evolve and improve significantly. Some innovations, such as new consensus algorithms and the use of auxiliary technologies, such as the Lightning Network, have accelerated the data verification and validation process within the blockchain network, thereby reducing costs and enhancing scalability.[24]

[21] Lady Liesdyana Pratiwi, "Implementasi Blockchain Pada Akuntansi Dan Audit Di Indonesia," *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan* 4, no. 6 (January 2022): 2185–203, https://doi.org/10.32670/fairvalue.v5i01.873.

[22] Amazon Web Services, "Apa Itu Teknologi Blockchain? Penjelasan Tentang Blockchain," Amazon Web Services, 2023, https://aws.amazon.com/id/what-is/blockchain/.

[23] B. E. Atmomintarso and Wirawan, "Sistem Pelaporan Pajak Pertambahan Nilai Pada Web Dengan Menggunakan Teknik Blockchain," *Jurnal Teknik ITS* 10, no. 2 (2021), https://media.neliti.com/media/publications/499988-none-094e50e4.pdf.

[24] Pluang, "Mengenal Konsep Algoritma Konsensus Dalam Blockchain," 2022, https://pluang.com/id/blog/resource/mengenal-konsep-algoritmakonsensus.

In Indonesia, blockchain technology still requires socialization and education regarding its usage. One of the main barriers is the lack of understanding and awareness of blockchain technology among the public and policymakers. In addition, unclear and inconsistent regulations pose challenges to the use of blockchain technology in Indonesia. Although Bank Indonesia has launched regulations related to the use of blockchain, many institutions have not fully understood or implemented them. Therefore, with innovation and a better understanding of blockchain, it is hoped that the use of this technology will expand in the future.[25]

Implementation of Blockchain in Criminal Justice System

One example of legal empowerment in the Society 5.0 era is the optimization of blockchain technology implementation in the legal field. Blockchain technology can be utilized to realize transparency, efficiency, and effectiveness in the criminal justice system. In the context of digital evidence, such as data from electronic devices, including smartphones, computers, and social media, it has become increasingly important in investigation and trial processes. This phenomenon not only has positive impacts, such as improved accuracy in evidence collection, but also creates new challenges related to validity and fairness. One significant impact of using digital evidence is the increased efficiency of law enforcement. Digital data enables law enforcement agencies to track criminal activities more quickly and effectively than before. However, on the other hand, the growing reliance on digital evidence also poses risks to the integrity of the justice system.[26]

Digital Evidence can be defined as information that is generated, stored, or transmitted in digital form and holds legal value in judicial processes. In today's digital era, digital evidence is becoming increasingly important because of the rapid advancement of technology and the growing use of electronic devices in various aspects of life. This definition encompasses various types of data that can be obtained from devices such as computers, smartphones, social media, and other sources.[27] According to

[25] H. S. Bashar, H. Purnamasari, and E. Priyanti, "Analisis Penerapan Blockchain Di Indonesia, Menuju Revolusi Pelayanan Publik Dan Kearsipan," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 9, no. 8 (2022): 3023–29, https://doi.org/10.31604/jips.v9i8.2022.3023-3029.

[26] Faisal Syukri, "Penggunaan Bukti Digital Dalam Persidangan Pidana: Antara Validitas Dan Keadilan," *CAUSA: Jurnal Hukum Dan Kewarganegaraan* 6, no. 6 (2024), https://doi.org/10.3783/causa.v2i9.2461.

[27] Peter Mahmud Marzuki, *Penelitian Hukum*, 15th ed. (Jakarta: Kencana, 2021).

According to Goodman, digital evidence refers to all electronic-based information that can be used to prove or disprove facts in court. He emphasizes that digital evidence includes data that is not only actively recorded by the user, such as text messages or electronic documents, but also includes passive data, such as metadata or digital footprints, which can help construct a timeline of events. For example, activity logs on a specific device can show when a file was modified or accessed, providing important clues for an investigation.[28]

Digital evidence includes files or documents stored in electronic formats and encompasses various other forms of information, such as emails, text messages, images, videos, and audio recordings. This information often plays a key role in uncovering the facts of a criminal case. The existence of digital evidence allows investigators to trace and analyze information that cannot be accessed using conventional methods. Data obtained from social media platforms can provide additional and highly valuable context for the investigative process. Digital evidence has several unique characteristics in the legal context. First, its intangible nature allows it to be easily copied and transferred, unlike physical evidence such as tangible objects. Moreover, digital evidence can be quickly deleted or manipulated, which increases the challenges regarding the validity and integrity of the evidence.

The presence of digital evidence has changed the way investigations are performed. In the past, investigators relied on witnesses and physical evidence to build cases. However, with digital evidence, investigators now have access to a wider and more diverse range of information than before. In many cases, digital evidence can provide clarity regarding the sequence of events, the perpetrator's intent, and the interactions between the individuals involved. However, the use of digital evidence also raises new challenges, one of the biggest being ensuring the authenticity and integrity of the evidence. Before digital evidence can be accepted in court, the party presenting the evidence must demonstrate that it was obtained legally. Therefore, the process of collecting digital evidence must adhere to strict and transparent procedures and must not violate the law, employing appropriate techniques to maintain the integrity of the data as a principle that must be upheld.

[28] Dimas Fauzi, "Keamanan Bukti Digital Dalam Proses Hukum Di Indonesia," *Jurnal Hukum Pidana*, no. 2 (2020).

In Indonesia, the existence of digital evidence is outlined in Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). This law serves as the legal basis for the use of digital evidence in the criminal justice system and states that digital evidence can be used as valid evidence in court. However, despite the recognition of digital evidence in the law, challenges and gaps remain that must be addressed to ensure that the use of evidence is effective and fair. Digital evidence has become increasingly relevant with the rise of cybercrime and information technology-related crimes. In an era where transactions and social interactions are increasingly conducted online, understanding and regulating digital evidence has become crucial. This requires law enforcement, lawyers, and judges to have a deeper understanding of digital evidence, including how to collect, analyze, and present it in legal proceedings. Therefore, digital evidence is not just information in an electronic format but also an important tool for upholding justice and the law in this digital age. Recognition and a solid understanding of digital evidence will help create a more effective and responsive legal system to the challenges of the future.[29]

The implementation of blockchain technology in Indonesia offers great potential for enhancing data security and efficiency across various sectors. The Indonesian government has introduced several initiatives to strengthen the use of digital technology, such as blockchain for the verification and validation of digital evidence.[30] However, its implementation still faces several challenges, such as unclear regulations, limited infrastructure, and a lack of understanding of blockchain technology.[31] Another challenge is the limited infrastructure, particularly in remote areas. Fast and stable infrastructure is crucial for adopting blockchain technology because it requires reliable Internet access. Therefore, the lack of adequate infrastructure is a barrier to the implementation of blockchain technology in Indonesia.[32]

The Indonesian government is currently working to improve Internet access across the country. One of these initiatives is the Palapa Ring program, which aims to build an

[29] Syukri, "Penggunaan Bukti Digital Dalam Persidangan Pidana: Antara Validitas Dan Keadilan."

[30] Centre for Innovation Policy and Governance, *Big Data, Kecerdasan Buatan, Blockchain, Dan Teknologi Finansial Di Indonesia: Usulan Desain, Prinsip Dan Rekomendasi Kebijakan*.

[31] D. Budhijanto, "Blockchain Law, Perlindungan Data Pribadi Dalam Ekonomi Digital," Hukumonline, 2023, https://www.hukumonline.com/berita/a/blockchain-law--pelindungan-data-pribadi-dalam-ekonomi-digital-lt63cf37949e450/.

[32] Atmomintarso and Wirawan, "Sistem Pelaporan Pajak Pertambahan Nilai Pada Web Dengan Menggunakan Teknik Blockchain."

Internet network infrastructure in Indonesia. Additionally, the government plans to establish a national data center to facilitate centralized and secure storage. Apart from infrastructure challenges, the lack of understanding of blockchain technology also poses a problem in its adoption in Indonesia. Some people still perceive blockchain as a complex technology that is difficult to comprehend. To address this issue, the government needs to increase educational campaigns and awareness programs about blockchain technology and its benefits to society. Training and courses can be provided to students, university students, and the general public to enhance their understanding and awareness of this technology.[33]

Overall, the implementation of blockchain technology in digital evidence management has the potential to enhance data security and operational efficiency. With the proper adoption of blockchain technology, Indonesia can play a significant role in the global blockchain ecosystem and strengthen its position as a country that is undergoing rapid digital transformation.[34] The implementation of blockchain technology in digital evidence management is an emerging global trend. Developed countries, such as the United States and China, have developed initiatives and projects using blockchain across various sectors. Indonesia needs to continue to develop and enhance its use, particularly in digital evidence management as part of the criminal justice system, to make law enforcement processes more transparent and accountable in their execution.[35]

Benefit and Risks of Using Blockchain for Digital Evidence Management

The use of blockchain technology in digital evidence management offers several significant benefits. First, it provides better data security than conventional technologies. With data stored in a decentralized and encrypted manner, security is enhanced, minimizing the risk of data loss or manipulation. The data stored in the blockchain also have high integrity, as any data entered cannot be altered or deleted without the consent of all involved parties. Conversely, blockchain technology also provides greater

[33] I. E. Maulani et al., "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi," *Jurnal Sosial Dan Teknologi* 3, no. 2 (2023), https://sostech.greenvest.co.id/index.php/sostech/article/view/634/1006.

[34] Pluang, "Mengenal Konsep Algoritma Konsensus Dalam Blockchain."

[35] Liu, Lin, and Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning."

transparency for each piece of data entered, as all data can be verified by all parties involved, significantly reducing the risk of fraud or manipulation.[36]

Blockchain technology also provides efficiency and speed in the process of data verification and validation without the need for intermediaries or third parties, thus reducing the costs and time required for these processes. However, the use of blockchain technology also comes with risks that need to be considered. One of these risks is dependency on the technology itself; therefore, if issues or failures occur, the data stored in the blockchain will also be affected. Additionally, security risks remain a serious concern in the use of blockchain technology.[37] No one can guarantee the possibility of a cyberattack successfully penetrating its security system, as this technology has limitations in terms of the scale and transaction capacity it can handle. Therefore, careful planning and management are required for the use of blockchain technology for digital evidence in Indonesia.[38]

Conclusion

Data security is a fundamental issue in the digital age, especially in the context of managing digital evidence in criminal justice systems. Blockchain offers a relevant and strategic approach through its characteristics of decentralization, immutability, and strong encryption, which can maintain the integrity, authenticity, and availability of data against the risks of leakage, theft, and manipulation. Efficient verification and validation mechanisms without intermediaries also increase the effectiveness of digital evidence management while strengthening the chain of custody in a transparent and auditable manner. However, the implementation of blockchain in law enforcement practices in Indonesia still faces structural challenges, particularly related to regulatory gaps or ambiguities, technological infrastructure limitations, and uneven understanding of blockchain-based systems among law enforcement officials. Therefore, comprehensive policy support is needed, ranging from updating the Criminal Procedure Code to accommodate digital evidence management mechanisms, strengthening human resource

[36] Angelita Nauli Panggabean, "MEMAHAMI DAN MENGELOLA TRANSFORMASI DIGITAL," preprint, Open Science Framework, October 22, 2021, https://doi.org/10.31219/osf.io/s36wq.

[37] Bashar, Purnamasari, and Priyanti, "Analisis Penerapan Blockchain Di Indonesia, Menuju Revolusi Pelayanan Publik Dan Kearsipan."

[38] Maulani et al., "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi."

capacity, and providing adequate facilities and infrastructure in all law enforcement institutions.

This study contributes to the enrichment of academic discourse and legal practice by offering a conceptual framework for the integration of blockchain technology in digital evidence management as part of technology-based criminal justice system reform. The main contribution of this study lies in its attempt to bridge the perspectives of information technology and the law of evidence, particularly in responding to the need for a more secure, transparent, and accountable evidence management system. However, this research has limitations because it focuses on conceptual and normative analysis; therefore, it does not fully capture the empirical dynamics of blockchain implementation in the field. Further research is needed to test the effectiveness of this technology through empirical case studies, institutional readiness analyses, and evaluations of its legal impact on criminal justice and law enforcement processes in Indonesia.

Bibliography

Ahmad, V., L. Goyal, T. Singh, and J. Kumar. "Blockchain Technology for Secure and Intelligent Industry Applications." In *Fostering Sustainable Businesses in Emerging Economies: The Impact of Technology*, 147–65. 2023. https://doi.org/10.1108/978-1-80455-640-520231010.

Aliya, B., U. Olga, B. Yenlik, and I. Sogukpinar. "Ensuring Information Security of Web Resources Based on Blockchain Technologies." *International Journal of Advanced Computer Science and Applications* 14, no. 6 (2023): 834–43. https://doi.org/10.14569/IJACSA.2023.0140689.

Almomani, A., N. Al Refai Mohammed, A. Aburomman, O.K.A. Alidmat, Q. Saber, F. Alshariedeh, and M. Khouj. "Usage of Blockchain Technology for Improving Computer Security." Paper presented at 2024 25th International Arab Conference on Information Technology, ACIT 2024. 2024. https://doi.org/10.1109/ACIT62805.2024.10877007.

Alzuabi, W., Y. Ismail, and W. Elmedany. "Privacy and Security Issues in Blockchain Based IoT Systems: Challenges and Opportunities." 2022, 258–65. https://doi.org/10.1109/3ICT56508.2022.9990679.

Amazon Web Services. "Apa Itu Teknologi Blockchain? Penjelasan Tentang Blockchain." Amazon Web Services, 2023. https://aws.amazon.com/id/what-is/blockchain/.

Argani, A., and W. Taraka. "Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertipikat Pada Perguruan Tinggi." *ABDI: Jurnal Pengabdian Dan Pemberdayaan Masyarakat* 1, no. 1 (2020). https://doi.org/10.34306/abdi.v1i1.121.

Atmomintarso, B. E. and Wirawan. "Sistem Pelaporan Pajak Pertambahan Nilai Pada Web Dengan Menggunakan Teknik Blockchain." *Jurnal Teknik ITS* 10, no. 2 (2021). https://media.neliti.com/media/publications/499988-none-094e50e4.pdf.

Bashar, H. S., H. Purnamasari, and E. Priyanti. "Analisis Penerapan Blockchain Di Indonesia, Menuju Revolusi Pelayanan Publik Dan Kearsipan." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 9, no. 8 (2022): 3023–29. https://doi.org/10.31604/jips.v9i8.2022.3023-3029.

Budhijanto, D. "Blockchain Law, Perlindungan Data Pribadi Dalam Ekonomi Digital." Hukumonline, 2023. https://www.hukumonline.com/berita/a/blockchain-law--pelindungan-data-pribadi-dalam-ekonomi-digital-lt63cf37949e450/.

Centre for Innovation Policy and Governance. *Big Data, Kecerdasan Buatan, Blockchain, Dan Teknologi Finansial Di Indonesia: Usulan Desain, Prinsip Dan Rekomendasi Kebijakan*. Jakarta: Ditjen Aptika, 2018. https://aptika.kominfo.go.id/wp-content/uploads/2018/12/KajianKominfo-CIPG-compressed.pdf.

Chaurasia, P.K., D. Rana, V. Rajaram, and S. Srividhya. "Anonymous Crime Reporting Using Blockchain and Smart Contract." 2024, 1059–64. https://doi.org/10.1109/ICPCSN62568.2024.00176.

Fauzi, Dimas. "Keamanan Bukti Digital Dalam Proses Hukum Di Indonesia." *Jurnal Hukum Pidana*, no. 2 (2020).

Haleem, A., M. Javaid, R. P. Singh, R. Suman, and S. Khan. "A Review of Blockchain Technology Applications for Financial Services." *Bench Council Transactions on*

Benchmarks, Standards and Evaluations 2, no. 3 (2022). https://doi.org/10.1016/j.tbench.2022.100073.

Harahap, Alwi Padly, Hakkul Yakin Siregar, Maulana Hasan Hasibuan, and M. Fajri Yusuf. "KEMANUSIAAN DAN KEADILAN: MENGEKSPLORASI HAK ASASI MANUSIA DALAM KONTEKS HUKUM ISLAM." *HAKAM: Jurnal Kajian Hukum Islam Dan Hukum Ekonomi Islam* 8, no. 1 (July 2024). https://doi.org/10.33650/jhi.v8i1.8205.

Hoesada, J. "Disaster Recovery Planning: Manajemen Bencana Administrasi Dan Akuntansi." CRMS Indonesia, 2023. https://crmsindonesia.org/publications/disaster-recovery-planningmanajemen-bencana-administrasi-dan-akuntansi/.

Hukumonline. "Chain of Custody Berbasis Blockchain Dalam Penanganan Bukti Digital." 2024. https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam-penanganan-bukti-digital-lt64ce49bc3bf67/.

Kemitraan and Lembaga Kajian dan Advokasi Independensi Peradilan. *Naskah Akademik Kerangka Hukum Perolehan, Pemeriksaan, Dan Pengelolaan Bukti Elektronik*. Jakarta, 2019.

Lin, I.-C., and T. Liao. "A Survey of Blockchain Security Issues and Challenges." *International Journal of Network Security* 19 (2017). https://doi.org/10.6633/IJNS.201709.19(5).01.

Liu, C. H., Q. Lin, and S. Wen. "Blockchain-Enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning." *IEEE Transactions on Industrial Informatics* 15, no. 6 (2019). https://doi.org/10.1109/TII.2018.2890203.

Marzuki, Peter Mahmud. *Penelitian Hukum*. 15th ed. Jakarta: Kencana, 2021.

Maulani, I. E., T. Herdianto, D. F. Syawaludin, and M. O. Laksana. "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi." *Jurnal Sosial Dan Teknologi* 3, no. 2 (2023). https://sostech.greenvest.co.id/index.php/sostech/article/view/634/1006.

Mohan, C.R., R. Saxena, K.T. Thilagham, P.K. Solleti, and S. Sivasubramanian. "Blockchain-Based Solutions for Enhancing Data Integrity and Security." 2024, 1416–20. https://doi.org/10.1109/IC3I61595.2024.10828945.

Nawawi, Barda Arief. *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Fajar Interpratama Mandiri, 2017.

Oberoi, O., and S. Raj. "Advanced Cryptographic Technologies in Blockchain." In *Blockchain Technology in Corporate Governance: Transforming Business and Industries*, 327–51. 2022. https://doi.org/10.1002/9781119865247.ch15.

Olukoya, O. "Assessing Frameworks for Eliciting Privacy and Security Requirements from Laws and Regulations." *Computers & Security*, ahead of print, 2022. https://doi.org/10.1016/j.cose.2022.102697.

Panggabean, Angelita Nauli. "MEMAHAMI DAN MENGELOLA TRANSFORMASI DIGITAL." Preprint, Open Science Framework, October 22, 2021. https://doi.org/10.31219/osf.io/s36wq.

Papada, Tenriajeng Andi, Muhamad Karim Said, and Wiwie Heryani. "Kedudukan Alat Bukti Yang Diperoleh Melalui Teknologi Informasi Dalam Pembuktian Tindak Pidana Informasi Dan Transaksi Elektronik." *Jurnal Al-Qadau* 7, no. 1 (2020). https://doi.org/10.24252/alqadau.v7i1.14892.

Pluang. "Mengenal Konsep Algoritma Konsensus Dalam Blockchain." 2022. https://pluang.com/id/blog/resource/mengenal-konsep-algoritmakonsensus.

Pramono, Budi. *Sosiologi Hukum*. Surabaya: Scopindo Media Pustaka, 2020.

Pratiwi, Lady Liesdyana. "Implementasi Blockchain Pada Akuntansi Dan Audit Di Indonesia." *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan* 4, no. 6 (January 2022): 2185–203. https://doi.org/10.32670/fairvalue.v5i01.873.

Sihaloho, Silvina Helen Sondang. "Perbandingan Asas Legalitas Kitab Undang-Undang Hukum Pidana (KUHP) Dan Hukum Islam." *Jurnal Hukum Respublica* 21, no. 1 (2021). https://doi.org/10.31849/respublica.v21i2.8315.

Syukri, Faisal. "Penggunaan Bukti Digital Dalam Persidangan Pidana: Antara Validitas Dan Keadilan." *CAUSA: Jurnal Hukum Dan Kewarganegaraan* 6, no. 6 (2024). https://doi.org/10.3783/causa.v2i9.2461.

Tratiya, M., R. Sangeetha, P.S. Danghi, and S.K. Rout. "Pros and Cons of Consensus Method in the Context of Blockchain." In *Digital Transformation and Sustainability of Business*, 408–11. 2025. https://doi.org/10.1201/9781003606185-94.

Tripathi, Gautami, Mohd Abdul Ahad, and Gabriella Casalino. “A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges.” *Decision Analytics Journal* 9 (December 2023): 100344. https://doi.org/10.1016/j.dajour.2023.100344.