JURNAL MAGISTER HUKUM UDAYANA
(UDAYANA MASTER LAW JOURNAL)
Vol. 14 No. 1 May 2025
E-ISSN: 2502-3101 P-ISSN: 2302-528x
http: //ojs.unud.ac.id/index.php/jmhu

The Application of Blockchain Technology in Cross-Border Personal Data Transfer Activities in Indonesia: Opportunities and Challenges

I Made Marta Wijaya[1]

[1]Faculty of Law, Universitas Gadjah Mada, E-mail: imademartawijaaya1997@mail.ugm.ac.id

Article Information

Received: 13th November 2024
Accepted: 24th April 2025
Published: 25th April 2025

Keywords:
Opportunities and Challenges; Blockchain Technology; Transfer of Personal Data; Protection of Personal Data; Subjects Data

Corresponding Author:
I Made Marta Wijaya,
E-mail:
imademartawijaya1997@mail.ugm.ac.id

DOI:
10.24843/JMHU.2025.v14.i01.p11

Abstract

This research seeks to explain the opportunities and obstacles involved in utilizing blockchain technology for transferring personal data beyond Indonesia's legal boundaries, along with the advantages it offers to Personal Data Subjects. The research employs normative legal research with statute and conceptual approaches. Data was collected through document studies and interviews with experts and practitioners, and then analyzed descriptively qualitatively. The findings indicate that blockchain technology has the potential to improve the security, transparency, and efficiency of personal data transfers. Notable opportunities include decentralization features, traceable audit trails, and enhanced identity management solutions. However, challenges such as compliance with varying regulations, data localization, and privacy issues need to be addressed. The study concludes that the application of blockchain technology can provide significant benefits for Personal Data Subjects, offering better data protection and control, along with the fulfillment of rights under Law No. 27 of 2022. A holistic approach and supportive regulations are essential to maximize this technology's potential in cross-border data transfers.

I. Introduction

Challenges surrounding the security and safeguarding of personal data in Indonesia, especially regarding the use of advanced technology in personal data processing, continue to be pressing concerns that require immediate attention. A key aspect involves the transfer of personal data across international borders. Given the rapid development of the digital economy, which positions data as "the new oil and business resource"[1] and "*a new asset class*",[2] there is substantial international demand for the adoption of standardized personal data security and protection principles,[3] as practiced by the

[1] Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform: Jurnal Pembaharuan Hukum* 18, no. 2 (2022): 144–63, https://doi.org/10.14710/lr.v18i2.43307. h. 149

[2] Alex Pentland, "Trust in Digital Societies," in *Trusted Data*, 2020, 3–14, https://doi.org/10.7551/mitpress/12439.003.0002. h. 5.

[3] Rizaldy Anggriawan et al., "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?," *Hasanuddin Law Review* 8, no. 2 (2022): 95–110, https://doi.org/10.20956/halrev.v8i2.2844. h. 96.

European Union and the United States. Each country is encouraged to incorporate advanced technology into its personal data protection legal framework to equalize the level of data protection, especially concerning security,[4] ensuring that both data protection and the rights of Personal Data Subjects are maximally upheld.[5]

The Indonesia's Law Number 27 of 2022 on Personal Data Protection ("Law No. 27 of 2022") mandates that personal data processing, including data transfer, must observe data protection principles[6] to ensure the security of personal data and prevent data protection breaches.[7] Furthermore, the significant risks associated with data transfer activities, especially those extending beyond Indonesia's jurisdiction, highlight the necessity of upholding the key principles.[8]

The principle of equivalent personal data protection in cross-border data transfers requires that Personal Data Controllers aiming to transfer data outside Indonesia confirm that the receiving country's Personal Data Controller or Processor enforces a data protection level at least equal to that of Law No. 27 of 2022.[9] If this standard is not met, the Personal Data Controller ensures adequate and enforceable data protection.[10] Should this condition also not be fulfilled, requires obtaining consent from the Personal Data Subject before data transfer.[11] These rules reinforce the need for equivalent personal data protection, obligating Personal Data Controllers involved in cross-border transfers to adhere strictly to these standards.

The standards referenced by several countries, such as South Korea, Japan, Singapore, and Malaysia, for personal data protection levels are primarily derived from the European Union's General Data Protection Regulation 2016 (EU GDPR). This regulation has become the global benchmark for personal data protection. Indonesia has adopted these standards and incorporated them into Law No. 27 of 2022. As a result, all Personal Data Controllers are required to adjust their data protection regulations and systems to meet the provisions of Law No. 27 of 2022 by October 17, 2024. This includes fostering the development of personal data security systems with high-level encryption, immutability, and automatic consensus mechanisms in line with the law.

To date, personal data security and protection in Indonesia remain insufficient, as evidenced by numerous data breaches and hacking incidents. Since the enactment of Law No. 27 of 2022, Indonesia has seen 35 personal data breach cases by mid-2024, including major breaches affecting the *BPJS Kesehatan, Bank*

[4] Anggriawan et al. *Ibid*.

[5] Angga Hendiarto Susanto et al., "PERLINDUNGAN DATA PRIBADI KONSUMEN ATAS PEMBOBOLAN DATA RAHASIA NEGARA SEBAGAI PERWUJUDAN GOOD CORPORATE GOVERNANCE," *Jurnal Hukum Media Justitia Nusantara* 13, no. 1 (2023): 46–53, https://doi.org/https://doi.org/10.30999/mjn.v13i1.2634. h. 47.

[6] Article 16, paragraph (1) Law No. 27 of 2022.

[7] Article 16, paragraph (2) points (d) and (e) Law No. 27 of 2022.

[8] Article 56 of Law No. 27 of 2022.

[9] Article 56, paragraph (2) of Law No. 27 of 2022.

[10] Article 56, paragraph (3) of Law No. 27 of 2022.

[11] Article 56, paragraph (4) of Law No. 27 of 2022.

Syariah Indonesia (BSI),[12] the Population and Civil Registry,[13] and the Immigration Department's passport data. In 2024, a significant data breach at the National Data Center (PDN) disrupted almost all public services in Indonesia, impacting 239 central and regional government agencies due to a ransomware attack (LockBit 3.0) on the PDN Sementara 2 in Surabaya.[14] The data processed by PDN included personal data of all subjects in Indonesia.

These incidents highlight the vulnerability of Indonesia's personal data security systems compared to other countries such as the European Union. Furthermore, enforcement in these cases remains far below the penalty standards set by the EU GDPR, as proving the negligence of Personal Data Controllers, such as through data processing logs, is challenging. This underlines the urgency for Indonesia to develop strategic steps toward adopting and applying technology to enhance its personal data security and protection systems, especially in cross-border personal data transfer activities.

To bridge this gap and offer a technological solution that aligns innovation with personal data protection, the researcher suggests implementing blockchain technology as a system for managing cross-border personal data transfers beyond Indonesia's jurisdiction. Blockchain technology was initially proposed by Satoshi Nakamoto in 2008 and was implemented the next year as a foundational element of the digital currency Bitcoin.[15] Satoshi Nakamoto described blockchain as "a shared, immutable ledger for recording the history of transactions,"[16] further explaining that it functions as a distributed database whose structure ensures that any modifications or changes are interconnected and time-stamped across each block.[17]

Due to its secure, decentralized data creation and storage system, blockchain technology has since been applied in several other fields, including supply chains, healthcare databases, financial and banking records, and other business activities.[18] Given this

[12] CNN Indonesia, 2023, "4 Kasus Kebocoran Data di Semester I 2023, Mayoritas Dibantah, CNN Indonesia, URL: https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah, accessed on March 10, 2024.

[13] Novina Putri Bestari, 2023, "337 Data Dukcapil Bocor, Ahli: Saya Bingung Jika Disangkal", CNBC Indonesia, URL: https://www.cnbcindonesia.com/tech/20230717095112-37-454869/337-data-dukcapil-bocor-ahli-saya-bingung-jika-disangkal, accessed on March 10, 2024.

[14] Rahel Narda Chaterine and Krisiandi, 2024, "PDN Diretas, Kabareskrim: "Ransomware" Bukan Hal Mudah Ditangani," URL: https://nasional.kompas.com/read/2024/07/15/14414911/pdn-diretas-kabareskrim-ransomware-bukan-hal-mudah-ditangani, accessed on March 10, 2024.

[15] Nicola Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard," *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017* 2018-Janua (2018): 727–34, https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112. h. 730

[16] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://doi.org/10.1108/TG-06-2020-0114. h. 8.

[17] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." *Ibid*.

[18] Remo Manuel Frey et al., "The Effect of a Blockchain-Supported, Privacy-Preserving System on Disclosure of Personal Data," *2017 IEEE 16th International Symposium on Network Computing and*

versatility, blockchain technology is also a viable option for cross-border personal data transfer activities outside Indonesia's jurisdiction, as it is already recognized in many countries.

Applying blockchain technology is expected to enable Personal Data Controllers in Indonesia to meet the principles of equal security and personal data protection. Furthermore, it could enhance the effectiveness of monitoring and law enforcement in cases of data breaches, as it would be easier to trace records or logs during personal data transfers through a decentralized database, a characteristic inherent to blockchain technology. The adoption of blockchain technology as a measure for equalizing and enhancing Personal Data Protection to meet international standards in cross-border personal data transfer activities outside Indonesia's jurisdiction is implicitly feasible, as stipulated in Article 16, paragraph (2) points (d) and (e), in conjunction with Article 35 point (b) and Article 56, paragraph (2) of Law No. 27 of 2022.

The application of blockchain technology beyond cryptocurrency is not new. Numerous studies have revealed the potential uses of blockchain across nearly every field and aspect of life, which continues to evolve annually. Research on the evolution of blockchain technology from version 1.0 to version 3.0 (and moving toward 4.0), as well as its revolutionary applications in combination with technologies such as smart contracts and the Internet of Things (IoT) in and before the Industry 4.0 era, has been conducted by scholars like Damiano Di Francesco Maesa and Paolo Mori,[19] Suyel Namasudra et al.,[20] Mohd Javaid et al.,[21] and Yong Chen et al.[22] These studies demonstrate a wide range of potential blockchain applications, such as electronic voting, healthcare management, and supply chains, as well as the potential for building smart communities. However, they also highlight challenges such as security policies and high computational costs.

Other research also explores blockchain applications in information technology, automation, cybersecurity, and personal data, conducted by Konstantinos Christidis and Michael Devetsikiostis,[23] Shafaq Naheed Khan et al.,[24] Swarnendu Chatterjee and Shifa

Applications, NCA 2017 2017-Janua (2017): 1–5, https://doi.org/10.1109/NCA.2017.8171385. h. 3.

[19] Damiano Di Francesco Maesa and Paolo Mori, "Blockchain 3.0 Applications Survey," *Journal of Parallel and Distributed Computing* 138 (2020): 99–114, https://doi.org/10.1016/j.jpdc.2019.12.019.

[20] Suyel Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges," *Archives of Computational Methods in Engineering* 28, no. 3 (2021): 1497–1515, https://doi.org/10.1007/s11831-020-09426-0.

[21] Mohd Javaid et al., "Blockchain Technology Applications for Industry 4.0: A Literature-Based Review," *Blockchain: Research and Applications* 2, no. 4 (2021): 100027, https://doi.org/10.1016/j.bcra.2021.100027.

[22] Yong Chen et al., "Applications of Blockchain in Industry 4.0: A Review," *Information Systems Frontiers*, no. January (2022), https://doi.org/10.1007/s10796-022-10248-7.

[23] Konstantinos Christidis and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access* 4 (2016): 2292–2303, https://doi.org/10.1109/ACCESS.2016.2566339.

[24] Shafaq Naheed Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends," *Peer-to-Peer Networking and Applications* 14, no. 5 (2021): 2901–25, https://doi.org/10.1007/s12083-021-01127-0.

Qureshi,[25] Rajab Ssemwogerere and Balyejusa Gusite,[26] and Madhevendra Singh and Nitya Jain.[27] Findings from these studies show that combining blockchain with other technologies can automate workflows while also emphasizing its impact on cybersecurity by integrating block-generation algorithms and networks to protect sensitive data. Blockchain's use for security and data privacy has also been the focus of other studies, which highlight the importance of choosing appropriate data protection methods and policies for data deletion. Although challenges exist in data protection, blockchain technology can offer a solution for resolving data disputes through Online Dispute Resolution (ODR), providing an effective alternative to reduce the burden on traditional courts.

Furthermore, other studies reinforce the potential for blockchain application in cross-border personal data transfer activities outside Indonesia's jurisdiction. These applications have proven successful in various fields such as healthcare, banking and finance, agricultural supply chains, and even timber supply chains, as shown in research by Thomas McGhin et al.,[28] QingQiu Gan et al., [29] Rama Sharma and Anurag Singh,[30] and Lukas Stopfer et al.[31] These studies show blockchain's role in authentication, integrity, record sharing, IoT security, and patient empowerment in healthcare, while also critiquing its use in banking and finance due to privacy and accessibility issues. In agriculture, blockchain has been shown to enhance supply chain transparency and production, although there are challenges related to farmers' understanding and knowledge. Meanwhile, research in the timber supply chain highlights blockchain's potential to revolutionize the industry through secure, transparent tracking, raising hopes for sustainability and biodiversity conservation.

Referring to the findings of previous studies, this research differs and has its strengths by focusing on the Indonesian context, allowing for an in-depth understanding of the challenges and opportunities that may arise in applying blockchain technology within a specific legal framework. Additionally, establishing an appropriate legal framework for the implementation of this technology becomes a crucial aspect that can help balance technological innovation with data privacy protection. Using Lawrence M. Friedman's legal system theory as the basis for analysis provides a better understanding of how blockchain technology can be integrated into the existing legal system. This research also

[25] Nisha Dhanraj Dewani et al., *Handbook of Research on Cyber Law, Data Protection, and Privacy, Handbook of Research on Cyber Law, Data Protection, and Privacy*, 2022, https://doi.org/10.4018/978-1-7998-8641-9. h. 199

[26] Dewani et al. *Ibid*. h. 21.

[27] Dewani et al. *Ibid*. h. 226.

[28] Thomas McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities," *Journal of Network and Computer Applications* 135, no. January (2019): 62–75, https://doi.org/10.1016/j.jnca.2019.02.027.

[29] Qing Qiu Gan, Raymond Yiu Keung Lau, and Jin Hong, "A Critical Review of Blockchain Applications to Banking and Finance: A Qualitative Thematic Analysis Approach," *Technology Analysis and Strategic Management* 0, no. 0 (2021): 1–17, https://doi.org/10.1080/09537325.2021.1979509.

[30] Dewani et al., *Handbook of Research on Cyber Law, Data Protection, and Privacy*. *Ibid*. h. 103.

[31] Lukas Stopfer, Alexander Kaulen, and Thomas Purfürst, "Potential of Blockchain Technology in Wood Supply Chains," *Computers and Electronics in Agriculture* 216, no. November 2023 (2024): 108496, https://doi.org/10.1016/j.compag.2023.108496.

offers a comprehensive overview of the opportunities and challenges of blockchain technology implementation in Indonesia, particularly for cross-border personal data transfers outside Indonesia's jurisdiction. Considering the security and data protection aspects, this research may contribute ideas and insights to public policymakers and private sector entities involved in personal data processing.

Considering the benefits of blockchain technology for Data Subjects is crucial to ensuring efficiency, security, utility, and fairness. This research has the potential to contribute significantly to the development of blockchain technology and data protection, as well as serve as a guide for policies in Indonesia. Theoretically, this study proposes the application of blockchain technology for data transfers outside Indonesia's jurisdiction to meet data security equality principles. Practically, it provides an innovative solution for Personal Data Controllers to comply with Law No. 27 of 2022, supports the establishment of the Indonesian Data Protection Authority, and facilitates oversight using blockchain technology. This research aligns with SDG goals 9 (technological innovation) and 16 (strengthening legal structures).

The background, urgency, and importance of this research effectively highlight the study's direction, anticipated outcomes, and contributions to legal and technological fields, especially within Indonesia's data protection law framework. Consequently, this study aims to address the following critical questions: What opportunities and challenges does blockchain technology present for cross-border personal data transfers in terms of future data protection and security? Additionally, how does the use of blockchain in cross-border data transfers gives legal protection and benefit Personal Data Subjects in Indonesia?

This study aims to explore and outline the opportunities and challenges associated with applying blockchain technology in cross-border personal data transfers, focusing on future data protection and security. It also seeks to examine and explain whether the use of blockchain technology in these transfers offers benefits to Data Subjects in Indonesia.

2. Research Method

This research adopts a normative legal research methodology, based on Soerjono Soekanto's view that normative research focuses on document studies, examining legal materials from written regulations, and other legal sources[32] This study will focus on examining the legal norms in Indonesia regarding cross-border personal data transfer provisions, supported by relevant literature, and assess the research questions, from the perspective of Lawrence M. Friedman's legal system theory. Therefore, this legal research is descriptive, as its goal is to organize and classify phenomena to be depicted as clearly and thoroughly as possible.[33]

To support this normative legal research, various legal approaches are generally used, and this study focuses on two types of legal approaches: statute and conceptual

[32] Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat* (Jakarta: RajaGrafindo Persada, 2007). h. 14

[33] Maria SW Sumardjono, *Bahan Kuliah: Metodologi Penelitian Ilmu Hukum*, Revisi (Yogyakarta: Universitas Gadjah Mada, 2021). h. 7.

approaches.[34] The research relies on secondary data, including primary, secondary, and tertiary legal material sources relevant to this study,[35] along with supplementary data from interviews with experts and practitioners in data protection. Data collection is conducted through document/library studies [36] and interviews.[37] The gathered data will be processed, analyzed, and presented in a descriptive qualitative manner, using deductive reasoning.[38]

Aligned with the conceptual approach used in this study, the literature review offers insights for establishing the conceptual and theoretical frameworks employed as analytical tools to address the key research questions. The theoretical and conceptual frameworks used in this research include Lawrence M. Friedman's legal system theory (substance, structure, and legal culture),[39] Jeremy Bentham's theory of legal utility, [40] and the lex informatica concept introduced by Joel R. Reidenberg.[41] These theories and concepts are employed to achieve the research objectives. For instance, Lawrence M. Friedman's legal system theory will be applied to assess the opportunities and challenges of blockchain technology in cross-border personal data transfers, focusing on its substance, structure, and legal culture. Additionally, the concept of lex informatica will be used to examine how blockchain aligns with its core characteristics. Jeremy Bentham's theory of legal utility will also be employed to evaluate whether blockchain technology provides benefits to Data Subjects regarding the security and protection of personal data.

3. Result and Discussion

3.1. Blockchain Technology in the Concept of Lex Informatica

Blockchain is a distributed database technology that records and stores information across a network of computers, ensuring high security and reliability through

[34] Peter Mahmud Marzuki, *Penelitian Hukum*, IX (Jakarta: Prenadamedia Group, 2014). h. 133.

[35] Sumardjono, *Bahan Kuliah: Metodologi Penelitian Ilmu Hukum*. *Op.cit*, h. 22.

[36] Sumardjono. *Op.cit*, h. 30.

[37] Sumardjono. *Op.cit*, h. 32.

[38] Marzuki, *Penelitian Hukum*. *Op.cit*, h. 142.

[39] See Sulistiowati and Nurhasan Ismail, *Penormaan Asas-Asas Hukum Pancasila Dalam Kegiatan Usaha Koperasi Dan Perseroan Terbatas*, Cetakan I (Yogyakarta: Gadjah Mada University Press, 2018). h. 28.; Lawrence M. Friedman, *Sistem Hukum: Perspektif Ilmu Sosial, Terjemahan M. Khozim*, V (Bandung: Nusa Media, 2013). h. 16.; Sudikno Mertokusumo, *Teori Hukum (Edisi Revisi)* (Yogyakarta: Cahaya Atma Pustaka, 2014). *op.cit*, h. 17.

[40] See L.J. van Apeldoorn, *Pengantar Ilmu Hukum, Terjemahan Oleh Oetarid Sadino*, XXX (Jakarta: PT Pradnya Paramira, 2004). *op.cit*, h. 16.; Satjipto Rahardjo, *Ilmu Hukum* (Bandung: PT Citra Aditya Bakti, 2021). h. 243.; Zainal B. Septiansyah and Muhammad Ghalib, "Konsepsi Utilitarianisme Dalam Filsafat Hukum Dan Implementasinya Di Indonesia," *Ijtihad: Jurnal Hukum Islam Dan Pranata Sosial* 34, no. 1 (2018): 27–34, https://doi.org/10.15548/ijt.v34i1.3. h. 29.; Yogie Pranowo, "Prinsip Utilitarisme Sebagai Dasar Hidup Bermasyarakat," *Paradigma: Jurnal Filsafat, Sains, Teknologi, Dan Sosial Budaya* 26, no. 2 (2020): 172–79, https://doi.org/10.33503/paradigma.v26i2.789. h. 176.

[41] See Joel R Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology," *Texas Law Review* 76, no. 3 (1998): 553–93, http://ir.lawnet.fordham.edu/faculty_scholarshipat:http://ir.lawnet.fordham.edu/faculty_scholarship/42. h. 592-593.; Rahmat Dwi Putranto, *Teknologi Hukum Paradigma Baru Hukum Di Dunia Digital* (Jakarta: Kecana Prenada Media, 2023). h. 22.

cryptographic processes.[42] Introduced in 2009 with the emergence of Bitcoin,[43] blockchain operates on a peer-to-peer infrastructure where network users and blockchain miners facilitate transactions within a ledger known as Distributed Ledger Technology (DLT).[44] This is maintained through consensus mechanisms, digital signatures, and hash chains, providing advanced features such as traceability, integrity, security, and non-repudiation, while simultaneously preserving privacy in a decentralized manner.[45] The concept of a secure cryptographic chain of blocks was first proposed by Haber and Stornetta in 1991 and was enhanced by Finney with reusable proof of work.[46] The breakthrough of blockchain technology occurred in 2008 with the introduction of Bitcoin by Satoshi Nakamoto, marking the beginning of Blockchain 1.0, which focused on cryptocurrency,[47] followed by Blockchain 2.0 in 2014 with smart contracts and decentralized applications.[48] Currently, we are in the era of Blockchain 3.0 (moving towards 4.0), which aims to enhance transaction speed and scalability, and blockchain has evolved into various sectors, including IoT, demonstrating its potential beyond digital currencies.[49]

Blockchain technology has two main features: decentralized storage and authentication.[50] Decentralized storage is a fundamental feature of blockchain that enhances security and authentication by distributing records across multiple servers,[51] rather than relying on a single server. This also allows for faster data access, better system interoperability, higher data control, and improved data quality for research.[52] The decentralized infrastructure of blockchain ensures the authentication of records and personal information stored within its blocks, requiring a private key linked to a public key to create, modify, or view information. These keys are stored in software applications such as Bitcoin wallets, which can be adapted for other authentication processes, including identity verification and document validation.[53]

[42] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." h. 730-731.

[43] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 62.

[44] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things." h. 2293.

[45] Di Francesco Maesa and Mori. *Ibid.*, h. 101.

[46] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1499.

[47] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." h.1.

[48] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1500.

[49] Chen et al., "Applications of Blockchain in Industry 4.0: A Review." h.2.

[50] Muhammad Raffi Hasta Anggara, "The Presence of Commercial Banks in Metaverse'S Financial Ecosystem: Opportunities and Risks," *Journal of Central Banking Law and Institutions* 1, no. 3 (2022): 405–30, https://doi.org/10.21098/jcli.v1i3.28. h. 409

[51] Alexander Harryandi, Fira Natasha, and Muhammad Akbar, "Regulating Initial Coin Offering Amidst the Development of Crypto Assets in Indonesia," *Journal of Central Banking Law and Institutions* 1, no. 3 (2022): 537–70, https://doi.org/10.21098/jcli.v1i3.41. h. 543

[52] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1499-1500.

[53] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 66-67.

With these two main features, blockchain technology has several characteristics. First, once data is written on the blockchain, it cannot be altered, ensuring the integrity and reliability of the stored information.[54] Second, the blocks in the blockchain are interconnected through cryptographic hashes, making alterations difficult and ensuring that changing one block would invalidate all subsequent blocks.[55] Third, blockchain eliminates the need for a central authority, reducing costs and risks, while each participant maintains a copy of the blockchain, making it resistant to hacking attempts.[56]

Blockchain technology is generally recognized in three types and has two types of nodes. The types of blockchain technology include public networks (Public (Permissionless)) that are open to anyone,[57] private networks (Private (Permissioned)) that are limited to specific participants,[58] and consortium blockchains (Consortium or Federated) that combine features of both public and private networks.[59] Nodes in a blockchain network consist of mining nodes that authenticate and validate transactions and normal nodes that maintain a copy of the DLT and ensure network consistency.[60] The blockchain network operates through a peer-to-peer system where each node (client) maintains a copy of the blockchain.[61] Users interact with the network using a pair of private and public keys, where the private key signs transactions, and the public key identifies the user, ensuring the authenticity and integrity of the transactions.[62] Transactions are validated by neighboring nodes before being broadcast, mined, and packaged into candidate blocks, and valid blocks will be updated in the blockchain's DLT, while invalid blocks will be discarded.[63]

The consensus mechanism is used to maintain the consistency and authority of blockchain technology by agreeing on the order of transactions and preventing forks.[64] Key mechanisms include Proof-of-Work (PoW), used by Bitcoin, which requires nodes to solve complex puzzles to validate blocks;[65] Proof-of-Stake (PoS), which reduces computational costs by granting block validation rights based on node ownership;[66] and Practical Byzantine Fault Tolerance (PBFT) along with other Byzantine Fault Tolerance

[54] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things." h. 2293.

[55] Christidis and Devetsikiotis. *Ibid.*

[56] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1500.

[57] Di Francesco Maesa and Mori, "Blockchain 3.0 Applications Survey." h. 101.

[58] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things." h. 2298.

[59] Shubhani Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities," *Journal of Network and Computer Applications* 144, no. April (2019): 13–48, https://doi.org/10.1016/j.jnca.2019.06.018. h. 15.

[60] Aggarwal et al. h. 14.

[61] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things." h. 2293.

[62] Christidis and Devetsikiotis. h. 2294.

[63] Christidis and Devetsikiotis. h. 2295.

[64] Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities," 2019. h. 15.

[65] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." h. 3.

[66] Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities," 2019. *loc.cit.*

algorithms, used in private or permissioned networks involving leader selection and round processes to achieve consensus.[67]

Based on the above exposition, it is undeniable that blockchain technology possesses characteristics and a mode of operation that establishes a standard system of rules. This means that blockchain technology, as a network technology, independently sets its own rules with its inflexible nature. This indicates that blockchain technology fulfills the characteristics of the lex informatica concept. Lex informatica refers to a system of rules established by network technology, operating independently from traditional legal systems.[68] Unlike legal rules created through political processes and possessing territorial jurisdiction, lex informatica establishes rules for access and use of information through technological architecture, with rules that can be immutable policies or flexible policies.[69] These rules are governed by technology developers and social practices, and their enforcement is automatic and self-executing, contrasting with law enforcement in traditional legal systems.[70] Lex informatica offers flexible solutions to issues that traditional legal systems struggle to address, such as jurisdictional challenges and various national laws in a global network.[71] However, it is important to ensure that lex informatica pays attention to balancing between strong, immutable rules and more flexible rules that may be easier to overlook.[72]

Blockchain technology and lex informatica provide innovative solutions for digital rule management with their unique approaches. Blockchain technology emphasizes decentralization by distributing data across a network without the need for a central authority, enhancing security and resilience against cyber attacks. On the other hand, lex informatica addresses jurisdictional challenges by implementing rules directly within the network, ensuring global compliance without the constraints of national laws and facilitating cross-border information flows.

In terms of security and law enforcement, blockchain technology uses cryptographic hashes and the principle of immutability to maintain the integrity of data that cannot be altered once written. Lex informatica relies on automatic enforcement mechanisms, such as filters and translations, to ensure real-time compliance, providing a level of enforcement that is difficult for traditional legal systems to achieve. This creates a strong level of security with more efficient enforcement. Transparency and flexibility are also key distinctions. Blockchain technology, particularly public ones, offers high transparency and ease of auditing but often faces privacy challenges. Conversely, lex informatica offers greater flexibility in adapting rules to meet the specific needs of the network and user preferences, and it can be tailored to comply with various national rules. Lex informatica also implements redundancy and immutability in a more adaptive manner, and the consensus mechanisms and automatic enforcement in lex informatica

[67] Aggarwal et al. *Ibid*.

[68] Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology." h. 568-570.

[69] Reidenberg. *Ibid*., h. 571-573.

[70] Putranto, *Teknologi Hukum Paradigma Baru Hukum Di Dunia Digital*. h. 22.

[71] Putranto. *Ibid*.

[72] Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology." h. 584-586.

provide a quicker response to rule violations compared to the slower and more costly traditional legal methods.

Based on the above exposition, it can be concluded that the characteristics and operational model of blockchain technology closely align with the concept of lex informatica, particularly in terms of decentralization, security, and automatic enforcement. Blockchain's decentralized infrastructure, coupled with cryptographic mechanisms and consensus protocols, enables secure, transparent, and immutable data management without reliance on central authorities. This not only enhances system integrity but also strengthens individual control over personal data. The use of private and public key pairs ensures that data access and modifications are restricted to authorized users, while the system's self-executing nature enables real-time compliance and enforcement. Within the lex informatica framework, blockchain operates as a rule-setting and rule-enforcing technology that transcends national jurisdictions, facilitating cross-border data flows and global compliance with personal data protection standards. Thus, the integration of lex informatica principles into blockchain systems fosters a resilient, adaptive, and legally responsive information ecosystem capable of addressing contemporary challenges in digital governance and personal data security.

3.2. Provisions for Personal Data Transfer Outside Indonesia in Law No. 27 of 2022

Personal data transfer is a key aspect of Personal Data Processing under Article 16 of Law No. 27 of 2022, which covers activities such as presentation, transfer, and disclosure of data. Data transfer refers to the transmission of personal data from the Personal Data Controller to another party, whether electronically or non-electronically (Elucidation of Article 16 letter e). The data must be protected against unauthorized access, alteration, misuse, and other security risks during processing.

Processing must be based on the explicit, informed consent of the Data Subject for specific purposes (Article 20). Consent must be written, clear, and in simple language, and failure to meet these criteria renders it invalid (Article 22). Article 35 requires Personal Data Controllers to implement security measures to protect data from unlawful processing and to assess risks based on the nature of the data. Additionally, Article 39 mandates secure systems to prevent unauthorized access, especially for electronic data.

When transferring data outside Indonesia's jurisdiction, Article 56 of Law No. 27 of 2022 stipulates that such transfers are allowed only if the receiving country has equivalent or stronger data protection laws. If not, adequate protection must be ensured, and if these conditions are unmet, Data Subject consent is required.

A.A.B.N.A. Surya Putra (RAH's Data Protection Offficer) stated that, the provisions governing personal data transfer are further detailed in a Draft Government Regulation on the Implementing Regulations of the Personal Data Protection Law, with the most recent draft available as of August 31, 2023. Putra stated that, the regulation, specifically addressing personal data transfer outside Indonesia, is outlined in Chapter V, which spans Articles 181 to 196. This chapter is divided into four sections: the First Section covers general provisions for transferring personal data outside Indonesia's jurisdiction; the Second Section addresses the required level of personal data protection, ensuring it is equivalent to or greater than Indonesia's standards; the Third Section outlines the criteria for adequate and enforceable data protection; and the Fourth Section discusses the need for consent when transferring personal data outside the jurisdiction.[73]

Based on the description, an analysis can be made on the use of blockchain technology for transferring personal data outside Indonesia's jurisdiction in compliance with Law No. 27 of 2022. According to Articles 16, 20, 22, 35, and 56 of the law, the transfer of personal data is best carried out using a private blockchain or a consortium (federated) blockchain with tightly controlled nodes. This approach is supported by an analysis of the characteristics and benefits of these blockchain models, which provide enhanced security and control, aligning with the legal requirements for data protection and security.

First, a Private Blockchain (Permissioned) is characterized by access to this blockchain network being restricted only to verified and authorized participants.[74] A private blockchain offers strict control over who can read, write, and audit data within the network. This makes it ideal for highly regulated sectors that demand high throughput and stringent access control, such as personal data transfers. It ensures that only authorized entities can access and process the data, in compliance with the data security provisions outlined in Articles 35 and 39. Second, a Consortium Blockchain (Federated) is characterized by combining features of both public and private blockchains, with control distributed among several verified entities.[75] This network is faster and more efficient compared to public blockchains. Consequently, the advantages of a Consortium Blockchain (Federated) are particularly suited for collaboration among various organizations that must comply with strict regulations regarding personal data, and it can provide the necessary security and integrity in accordance with Articles 16 and 56.

For the transfer of personal data outside Indonesia's jurisdiction, the two types of blockchains mentioned would utilize miner nodes in a private blockchain and normal nodes in a consortium blockchain. In a private blockchain, miner nodes are responsible for authenticating, verifying, and validating transaction blocks.[76] These miner nodes are essential for maintaining the integrity and security of the blockchain network. With strict access controls in place, they ensure that only valid transactions are added to the blockchain, in alignment with Article 35 of Law No. 27 of 2022, which focuses on data security and preventing unauthorized access. This highlights the advantages of miner nodes in a private blockchain. In contrast, normal nodes in a consortium blockchain function to maintain copies of the blockchain ledger and coordinate with transactions that have been authenticated by miner nodes.[77] They ensure that the blockchain remains up-to-date and consistent across the network. This facilitates collaboration and trust among entities, in accordance with the provisions of Articles 16 and 56.

[73] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

[74] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1500.

[75] Namasudra et al. *Ibid*.

[76] Shubhani Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities," *Journal of Network and Computer Applications* 144, no. June (2019): 13–48, https://doi.org/10.1016/j.jnca.2019.06.018. h. 14.

[77] Aggarwal et al. *Ibid*.

The opinion above is based on several key considerations: Article 16 requires protection against unauthorized access, which can be achieved by private and consortium blockchains with strict access controls. Articles 20 and 22 mandate explicit, recorded consent, which can be securely documented via blockchain's cryptographic capabilities, ensuring transparency and reliability. Articles 35 and 39 emphasize the need for technical safeguards to prevent unauthorized access, which private and consortium blockchains can provide through their security systems. Finally, Article 56 ensures that personal data transfers outside Indonesia's jurisdiction meet adequate protection standards, which blockchain technology can ensure through cryptographic recording and verification of Data Subject consent.

Therefore, it can be concluded that private and consortium blockchains, utilizing tightly controlled miner nodes and normal nodes, are well-suited for transferring personal data outside Indonesia's jurisdiction, as stipulated by Law No. 27 of 2022. These blockchain types ensure secure data processing, strict access control, and proper management of Data Subject consent, while also offering a mechanism for the automatic and real-time enforcement of regulatory requirements.

3.3. Opportunities and Challenges in the Application of Blockchain Technology for Personal Data Transfer Activities Outside the Jurisdiction of Indonesia

Research conducted by Fabiano shows that blockchain technology faces significant challenges in protecting privacy and personal data due to its fundamental characteristics and regulatory requirements such as the EU GDPR.[78] Although technical solutions such as pseudonymization and data minimization can be applied, these solutions often conflict with the need for transparency and the complete storage of transaction histories. Additionally, the decentralized nature of blockchain complicates compliance with data protection provisions regulated under the EU GDPR, especially regarding data localization and jurisdictional issues.[79] Therefore, Fabiano recommends that blockchain technology must adjust its personal data protection strategies to balance transparency and decentralization with legal obligations, ensuring effective personal data protection that meets the standards set forth in the EU GDPR.[80]

Another study also indicates that there are still challenges in implementing blockchain technology in the realm of personal data processing. Research conducted by Remo Manuel Frey et al. in Switzerland and Germany revealed that while privacy-preserving systems like blockchain technology with monetization options may increase some individuals' interest in sharing personal data, this technology has not fully met expectations in terms of enhancing the desire to share data generally or addressing privacy concerns.[81] The findings emphasize that blockchain technology does not

[78] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." h. 731-733.

[79] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

[80] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." *Ibid*.

[81] The research conducted by Remo Manuel Frey and his colleagues in Switzerland and Germany between August and October 2016 involved sending email invitations to nearly 6,267 people, with 295 individuals accepting the invitation, as well as a Facebook advertisement that

significantly enhance users' willingness to disclose personal data compared to other privacy measures.[82] Factors such as technical knowledge and individual preferences have proven to play crucial roles, leading researchers to advocate for further studies to address these limitations and develop a better understanding of privacy preferences and user technology.[83]

Research by Aggarwal et al. explains that blockchain technology is increasingly integrated into Data Center Networks (DCNs) to enhance data security, integrity, and privacy. In DCNs, blockchain addresses data management and application hosting challenges with its decentralization and immutability features. While it provides benefits such as resistance to manipulation and secure access control, the complexity and resource requirements of blockchain pose challenges for real-time applications.[84]

Referring to previous research findings, it is important to analyze the challenges and opportunities for implementing blockchain technology in personal data transfer activities outside the jurisdiction of Indonesia. The analysis is conducted by referencing several previous studies related to the application of blockchain technology across various sectors, enabling the formulation of relevant challenges and opportunities that may arise if blockchain technology is effectively applied to personal data transfer activities outside the jurisdiction of Indonesia. The challenges of implementing blockchain technology in personal data transfer activities abroad or across borders include:

1. Regulatory Compliance: complying with various regulations in each country, such as the EU GDPR in the European Union, is highly complex due to the decentralized and globally distributed nature of blockchain systems.[85] The permanence of data storage in blockchain often conflicts with legal provisions, such as the ability to modify or delete personal data in accordance with EU GDPR requirements.[86]
2. Data Localization: many countries have strict rules about where personal data can be stored and processed. The distributed nature of blockchain makes it challenging to ensure that data remains within specific geographical boundaries.[87]
3. Data Control and Ownership: in a blockchain system, data is stored across multiple nodes in various locations, obscuring who owns and controls that data and complicating the management of access rights and personal data

generated 1,111 clicks on the questionnaire. Out of that number, 1,102 people started the survey, and 420 of them completed the survey and agreed to share their data for this research.

[82] Frey et al., "The Effect of a Blockchain-Supported, Privacy-Preserving System on Disclosure of Personal Data." h. 1-4.

[83] Frey et al. *Ibid.*, h. 5.

[84] Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities," 2019. h. 36-38.

[85] Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." h. 2918.

[86] Khan et al. *Ibid*.

[87] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 67.

ownership.[88] However, access rights and personal data ownership by Data Subjects are fundamental requirements that must be met in the context of personal data protection.[89]

4. Security and Privacy: while blockchain offers high security, its transparent characteristics may conflict with individuals' privacy needs.[90] Each transaction recorded on the blockchain is typically visible to all participants, even if the data has been pseudonymized.[91]
5. Interoperability: differences in blockchain standards and protocols across countries can hinder cross-jurisdictional data transfers.[92] A common agreement and international standards are needed to ensure seamless interoperability.[93]
6. Cost and Technical Complexity: the implementation and maintenance of blockchain technology require significant investments in infrastructure and human resources.[94] This poses a major challenge for many organizations, especially those operating across multiple jurisdictions.
7. Lack of Standardization: the absence of standardization in blockchain technology hampers widespread acceptance and integration across various sectors.[95] The lack of uniform standards complicates interoperability and the development of universally accepted solutions for personal data management.[96]
8. Privacy Rights Leakage: decentralized storage, while eliminating central service providers, raises concerns about the privacy rights of Data Subjects.[97] Accessing data from public DLT requires private keys that may be exposed, especially in sensitive data contexts, where privacy is paramount.[98]
9. Key Management Issues: effective key management is crucial for maintaining blockchain security. Current blockchain key management methods face challenges due to the impracticality of using one key per block and the risk of exposing all data if a single key is compromised.[99]

[88] Javaid et al., "Blockchain Technology Applications for Industry 4.0: A Literature-Based Review." h.7.

[89] Hasil wawancara dengan Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M. pada tanggal 18 Juli 2024.

[90] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 67.

[91] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1511.

[92] Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities." h. 43.

[93] Di Francesco Maesa and Mori, "Blockchain 3.0 Applications Survey." h. 104.

[94] Namasudra et al., "The Revolution of Blockchain: State-of-the-Art and Research Challenges." h. 1511-1512.

[95] Namasudra et al. h. 1511.

[96] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 67

[97] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." h. 731.

[98] Fabiano. Ibid. h. 732.

[99] McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities." h. 67.

10. Scalability and Performance: blockchain systems, particularly those using Proof-of-Work (PoW), face scalability issues.[100] High computational demands result in slow transaction speeds and rising costs, which can be problematic in environments with large data volumes or many participants.[101]

Despite the numerous challenges in applying blockchain technology to personal data transfer activities outside national jurisdictions or across borders, there are also opportunities that can be optimized in the future, including:

1. Enhanced Security: blockchain offers strong security features, such as immutable records and decentralized consensus mechanisms, which can enhance personal data protection against tampering and unauthorized access.[102]
2. Transparency and Trust: The transparent nature of blockchain provides a verifiable audit trail for every data transfer activity, increasing the trust of Data Subjects.[103] This transparency is particularly valuable in applications where data integrity and accountability are crucial.[104]
3. Decentralized Identity Management: blockchain can simplify electronic identification (eID) by creating a secure distributed system for identity verification.[105] This can reduce redundancy, improve efficiency, and ensure that personal data is handled securely and in accordance with privacy regulations.[106]
4. Interoperability and Integration: while interoperability between different blockchain models remains a challenge, blockchain has the potential to act as a common platform for integrating various systems to facilitate seamless data transfers across networks and applications.[107]
5. Smart Contract and Privacy Protection: advances in smart contract technology, such as the Hawk model, provide a framework for privacy-preserving contracts.[108] This enhances the secure execution of agreements while protecting sensitive information, making blockchain a viable option for managing personal data.[109]

[100] Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." h. 2919.

[101] Khan et al. *Ibid*.

[102] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." h. 2301.

[103] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

[104] Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." h. 2912.

[105] Fabiano, "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." h. 733.

[106] Fabiano. *Ibid*.

[107] Aggarwal et al., "Blockchain for Smart Communities: Applications, Challenges and Opportunities." h. 43.

[108] Ahmed Kosba et al., "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 2016, 839–58, https://eprint.iacr.org/2015/675.pdf. h. 16.

[109] Di Francesco Maesa and Mori, "Blockchain 3.0 Applications Survey." h. 111.

6. Two Layer Solutions: innovations such as Layer 2 protocols (e.g., Bitcoin Lightning Network and Ethereum Plasma) address scalability issues by offloading transactions from the main blockchain.[110] These solutions can improve transaction speeds and reduce costs, making blockchain more practical for high-volume data transfers.[111]

In summary, while blockchain technology offers significant opportunities for securing and managing personal data, addressing inherent challenges—such as standardization, privacy concerns, and scalability—remains crucial for effective implementation and broader adoption. Therefore, it is necessary to establish a relevant legal framework for the application of blockchain technology for cross-border personal data transfers in Indonesia, which can be analyzed based on Lawrence M. Friedman's legal system theory, encompassing three main aspects: legal substance, legal structure, and legal culture.[112]

In terms of legal substance, this includes regulations and provisions [113] that govern specific aspects of blockchain technology and personal data transfers. The legal framework needed in the future from the perspective of legal substance should provide a legal basis for personal data processing, including provisions for personal data transfers abroad.[114] Law No. 27 of 2022 needs to be supported by implementing regulations that specifically govern the use of blockchain in personal data transfers, to be issued by the PDP Agency, which will derive its authority from the Government Regulation that is currently being drafted. Such regulations should address issues such as equal data protection, data subject consent, and the protection of personal data privacy rights. Additionally, regulations governing the use of information and communication technology, such as cybersecurity and data storage regulations, must be adjusted to support the integration of blockchain technology. Furthermore, the application of blockchain in personal data transfer activities outside Indonesia's jurisdiction should also consider international standards, such as the EU GDPR in the European Union, to ensure compliance with the principle of equal personal data protection.

From the perspective of legal structure, this encompasses the institutions and mechanisms that support the enforcement of law [115] and the application of blockchain technology in personal data transfer activities outside Indonesia. In the implementation of blockchain technology for personal data transfer outside Indonesia's jurisdiction, the legal structure plays a crucial role. The Personal Data Protection Agency (PDP) must have a deep understanding of blockchain and information technology to formulate policies, oversee data processing, and ensure data security. The PDP agency needs to

[110] Khan et al., "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." h. 2919.

[111] Khan et al. *Ibid*. h. 2920.

[112] Friedman, *Sistem Hukum: Perspektif Ilmu Sosial, Terjemahan M. Khozim*. h. 16.

[113] Mertokusumo, *Teori Hukum (Edisi Revisi)*. h. 17.

[114] Article 56 Law No. 27 of 2022.

[115] Sudikno Mertokusumo, *Penemuan Hukum Sebuah Pengantar*, Cet. II (Yogyakarta: Liberty, 2007). h. 19. See also, Sulistiowati and Ismail, *Penormaan Asas-Asas Hukum Pancasila Dalam Kegiatan Usaha Koperasi Dan Perseroan Terbatas*. h. 28.

collaborate with the National Standardization Agency (BSN) to develop technical standards and blockchain interoperability, as well as to provide socialization and technical guidance to Personal Data Controllers. The application of blockchain is expected to enhance legal certainty, transparency, and effective supervision while reducing the potential for abuse of power in law enforcement. With the implementation of blockchain, it is hoped that incidents of personal data breaches can be reduced and law enforcement in cases of personal data violations can be improved, as evidenced by breach data cases in Indonesia. Should data breaches occur, the judiciary must also be prepared to handle disputes related to blockchain technology and personal data. Law enforcement authorities need to be trained to understand and enforce new regulations related to blockchain and personal data protection, both in Indonesia and in other countries such as the EU GDPR.

The third aspect, legal culture, includes attitudes, understanding, and acceptance among the public and legal professionals [116] towards new technologies like blockchain. In Indonesia, the relevant legal culture that needs to be developed to build a comprehensive legal framework involves raising awareness and understanding among the public regarding personal data protection and blockchain technology through education and training. These activities are crucial and should be enhanced among legal professionals, regulators, and the general public to improve understanding and acceptance of blockchain technology in personal data transfer activities. The public and business actors must understand the benefits and risks of blockchain technology. Acceptance of blockchain technology as a medium and system for personal data transfer must be cultivated through effective socialization and education. Additionally, legal practices should adapt to the realities of blockchain technology, including adjusting habits in personal data management and dispute.

Based on the above description, to support the application of blockchain technology in personal data transfer activities outside the jurisdiction of Indonesia, there needs to be a coordinated effort to update the legal substance with specific regulations, strengthen the legal structure with appropriate institutions and mechanisms, and build a legal culture that supports the adoption of this technology. A holistic approach that encompasses the three elements of Friedman's legal system theory will ensure that blockchain technology can be effectively implemented in accordance with high standards of personal data protection.

3.4. Benefits Analysis of the Blockchain Technology Application in Personal Data Transfer Activities for Data Subjects

Jeremy Bentham, as cited by Satjipto Rahardjo[117] explains that "humans will act in such a way that they maximize pleasure and minimize suffering, and the ethical standard used here is whether an action produces happiness." According to Jeremy Bentham, "good is happiness, and evil is suffering, and there is a close relationship between the two, so the task of law is to preserve good and prevent evil (to maintain the utility of

[116] Friedman, *Sistem Hukum: Perspektif Ilmu Sosial, Terjemahan M. Khozim*. h. 16. Lihat juga Mertokusumo, Teori Hukum (Edisi Revisi). h. 17. See also, Sulistiowati and Ismail, *Penormaan Asas-Asas Hukum Pancasila Dalam Kegiatan Usaha Koperasi Dan Perseroan Terbatas*. h. 29.

[117] Rahardjo, *Ilmu Hukum*. H. 243.

law)." [118] Bentham's perspective actually stems from his significant concern for individuals. He desires that the law primarily guarantees happiness for individuals, rather than for society as a whole. However, Bentham does not deny that, in addition to individual interests, the interests of society also need to be considered.

Bentham also attempted to calculate the pleasure value of various human activities in order to compare their quantities against each other. He identified seven dimensions to consider in this calculation: the intensity of pleasure, the duration of pleasure, the certainty of achieving pleasure, the proximity of achieving pleasure, the consistency of the pleasure produced, the absence of contrary sensations from the pleasure, and the number of people affected by that pleasure.[119] From these seven variables, they can be further simplified into three forms of pleasure preference to facilitate moral calculations:[120] **how intense or frequent the pleasure is obtained/given, how enduring the pleasure is enjoyed, and how quickly the pleasure occurs in the near future**. Bentham, as noted by Theo Hujibers, emphasizes that "the goal of the state and law is to achieve the greatest happiness for the greatest number."

Bentham's opinion regarding the seven variables that can be simplified into three main variables—intensity, durability, and speed of pleasure—can be used to analyze the benefits of implementing blockchain technology in personal data transfer outside the jurisdiction of Indonesia. Blockchain technology supports personal data protection by providing a reliable level of security for Data Controllers and also contributes to fulfilling the rights of Data Subjects in accordance with Articles 5 to 13 of Law No. 27 of 2022. This evaluation will demonstrate the extent to which blockchain technology aligns with the value of utility in Bentham's utilitarian theory.

The first indicator is **how intensive or frequent the pleasure is obtained/given**: blockchain technology provides mechanisms that enable better and more transparent personal data control. By using blockchain technology, every transaction involving personal data can be tracked in real-time, allowing Data Subjects to monitor and control the use of their data more frequently. This fulfills the Data Subject's right to access and obtain copies of their personal data as guaranteed by Article 6 of Law No. 27 of 2022. Blockchain technology enables Data Subjects to easily access and obtain copies of their data, enhancing the frequency and ease of fulfilling this right. Additionally, the right to object to the processing of personal data, as guaranteed by Article 8 of Law No. 27 of 2022, is also fulfilled, as blockchain technology facilitates continuous monitoring of data usage, allowing Data Subjects to object more frequently if their data is used without appropriate consent.[121]

The second indicator is **how enduring the pleasure is enjoyed**: blockchain technology provides data resilience guarantees through its immutability feature. Data stored in the

[118] Septiansyah and Ghalib, "Konsepsi Utilitarianisme Dalam Filsafat Hukum Dan Implementasinya Di Indonesia." h. 29.

[119] Pranowo, "Prinsip Utilitarisme Sebagai Dasar Hidup Bermasyarakat." h. 176.

[120] Endang Pratiwi, Theo Negoro, and Hassanain Haykal, "Teori Utilitarianisme Jeremy Bentham: Tujuan Hukum Atau Metode Pengujian Produk Hukum?," *Jurnal Konstitusi* 19, no. 2 (2022): 269–93, https://doi.org/10.31078/jk1922. h. 281.

[121] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

blockchain cannot be altered or deleted without a trace, thus providing long-term protection for the integrity of personal data. From this indicator, the implementation of blockchain technology also fulfills the Data Subject's right to complete and update personal data as guaranteed by Article 7 of Law No. 27 of 2022. With blockchain technology, any changes to personal data will be recorded and tracked, ensuring that data updates can be done securely and accurately. The implementation of blockchain technology also fulfills the Data Subject's right to seek and obtain compensation as guaranteed by Article 10 of Law No. 27 of 2022 in the event of personal data misuse. This is because blockchain technology provides strong and immutable evidence that Data Subjects can use to seek compensation from Data Controllers who process personal data not in accordance with the approved processing purposes.[122]

The third indicator is **how quickly the pleasure occurs in the near future**: blockchain technology enables fast and efficient data transfers without requiring intermediaries. With a rapid consensus mechanism, data transactions can be completed within seconds or minutes, reducing the waiting time for Data Subjects to see the results of their actions related to personal data. This indicates that the implementation of blockchain technology can fulfill the Data Subject's right to know the purpose and legal basis for processing personal data as guaranteed by Article 5 of Law No. 27 of 2022. Blockchain technology can quickly provide information about the purpose and legal basis for data processing, including in personal data transfer activities, helping Data Subjects make faster and more accurate decisions when giving their consent. Additionally, the implementation of blockchain technology also allows Data Subjects to withdraw their consent as guaranteed by Article 13 of Law No. 27 of 2022. If a Data Subject decides to withdraw their consent, blockchain technology allows for the rapid processing of that request, ensuring that their right to withdraw consent is promptly respected and executed.[123]

Based on the analysis that considers the three main variables of Jeremy Bentham's utilitarian theory, it can be said that the implementation of blockchain technology in personal data transfer activities outside the jurisdiction of Indonesia offers significant benefits for Data Subjects, particularly in fulfilling the rights guaranteed by Law No. 27 of 2022. According to Bentham's three utilitarian variables, blockchain technology enhances the intensity of data control, provides long-term protection for data integrity, and enables fast processing for fulfilling the rights of Data Subjects. This is in line with the principle of equal protection of personal data in Law No. 27 of 2022, as it meets the provisions in Articles 5 to 13 of Law No. 27 of 2022 that regulate various fundamental rights for Data Subjects in the context of personal data protection.

4. Conclusion

Blockchain technology holds significant potential to enhance security, transparency, and efficiency in the transfer of personal data outside Indonesia's jurisdiction. Its primary advantages include improved security through decentralization and data immutability, increased transparency with verifiable audit trails, and the potential for developing

[122] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

[123] Interview Results with Data Protection Officer RAH (the House of Legal Experts), A.A.B.N.A. Surya Putra, S.H., LL.M., on July 18, 2024.

more secure identity management solutions. Smart contracts can further protect privacy and facilitate more efficient legal processes in data transfers.

However, challenges remain, including compliance with varying regulations across jurisdictions, data localization issues, decentralized data ownership and control, and privacy risks arising from blockchain's transparency. Technical issues such as scalability, interoperability, and implementation complexity also pose obstacles. A holistic approach is essential to support the application of blockchain technology in personal data transfers, referencing Lawrence M. Friedman's legal system theory.

From a legal substance perspective, specific regulations supporting blockchain-based personal data processing and transfers must align with international standards, such as the EU GDPR. Structurally, the Personal Data Protection Agency (PDP) must possess adequate competencies and collaborate with domestic and international bodies to establish technical standards and oversight for data transfers that meet global privacy standards. Culturally, increasing awareness and understanding among the public, legal professionals, and businesses about blockchain's potential and risks is crucial, achieved through effective outreach and education.

According to Jeremy Bentham's utilitarian theory, implementing blockchain technology in personal data transfers significantly benefits Indonesian data subjects. It enhances individuals' control over their personal data, provides long-term protection through data immutability, and enables rapid processing of their rights. In the context of Law No. 27 of 2022, blockchain supports the fulfillment of guaranteed rights, including access, objection, data updating, awareness of processing purposes, and withdrawal of consent. An evaluation based on Bentham's three main variables—intensity, durability, and speed—demonstrates that blockchain technology upholds the legal utility principle by delivering greater happiness to data subjects through improved protection, increased control, and swift responses to their needs. Thus, the application of blockchain technology offers tangible benefits and supports the protection and fulfillment of personal data subjects' rights as outlined in Law No. 27 of 2022.

Acknowledgments

The author would like to express gratitude to the Research and Publication Unit of the Faculty of Law, Gadjah Mada University, for their support of this research. The author was accepted as a Grant Recipient under the 2024 Student Research Grant Program, which facilitated the smooth execution of this research with the provided funding. Special thanks are also extended to Mrs. Alfatika Aunuriella Dini, S.H., M.Kn., Ph.D., the mentor for this research, for her support throughout the research process and the writing of this research article Additionally, the author appreciates the constructive

feedback received from fellow grant recipients in the Technology Mentoring Group during the Peer Review Workshop stage.

Reference

Aggarwal, Shubhani, Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Kim Kwang Raymond Choo, and Albert Y. Zomaya. "Blockchain for Smart Communities: Applications, Challenges and Opportunities." *Journal of Network and Computer Applications* 144, no. April (2019): 13–48. https://doi.org/10.1016/j.jnca.2019.06.018.

———. "Blockchain for Smart Communities: Applications, Challenges and Opportunities." *Journal of Network and Computer Applications* 144, no. June (2019): 13–48. https://doi.org/10.1016/j.jnca.2019.06.018.

Anggriawan, Rizaldy, Andi Agus Salim, Yordan Gunawan, and Mohammad Hazyar Arumbinang. "Passenger Name Record Data Protection under European Union and United States Agreement: Security over Privacy?" *Hasanuddin Law Review* 8, no. 2 (2022): 95–110. https://doi.org/10.20956/halrev.v8i2.2844.

Ayunda, Rahmi. "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform: Jurnal Pembaharuan Hukum* 18, no. 2 (2022): 144–63. https://doi.org/10.14710/lr.v18i2.43307.

Apeldoorn, L.J. van. *Pengantar Ilmu Hukum, Terjemahan Oleh Oetarid Sadino*. XXX. Jakarta: PT Pradnya Paramira, 2004.

Chen, Yong, Yang Lu, Larisa Bulysheva, and Mikhail Yu Kataev. "Applications of Blockchain in Industry 4.0: A Review." *Information Systems Frontiers*, no. January (2022). https://doi.org/10.1007/s10796-022-10248-7.

Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access* 4 (2016): 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.

CNN Indonesia, 2023, "4 Kasus Kebocoran Data di Semester I 2023, Mayoritas Dibantah, CNN Indonesia, URL: https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah, diakses 10 Maret 2024.

Dewani, Nisha Dhanraj, Zubair Ahmed Khan, Aarushi Agarwal, Mamta Sharma, and Shaharyar Asaf Khan. *Handbook of Research on Cyber Law, Data Protection, and Privacy*. *Handbook of Research on Cyber Law, Data Protection, and Privacy*, 2022. https://doi.org/10.4018/978-1-7998-8641-9.

Fabiano, Nicola. "Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard." *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017* 2018-Janua (2018): 727–34. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112.

Francesco Maesa, Damiano Di, and Paolo Mori. "Blockchain 3.0 Applications Survey." *Journal of Parallel and Distributed Computing* 138 (2020): 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019.

Frey, Remo Manuel, Pascal Buhler, Alexander Gerdes, Thomas Hardjono, Klaus Ludwig Fuchs, and Alexander Ilic. "The Effect of a Blockchain-Supported, Privacy-Preserving System on Disclosure of Personal Data." *2017 IEEE 16th International Symposium on Network Computing and Applications, NCA 2017* 2017-Janua (2017): 1–

5. https://doi.org/10.1109/NCA.2017.8171385.

Friedman, Lawrence M. *Sistem Hukum: Perspektif Ilmu Sosial, Terjemahan M. Khozim*. V. Bandung: Nusa Media, 2013.

Gan, Qing Qiu, Raymond Yiu Keung Lau, and Jin Hong. "A Critical Review of Blockchain Applications to Banking and Finance: A Qualitative Thematic Analysis Approach." *Technology Analysis and Strategic Management* 0, no. 0 (2021): 1–17. https://doi.org/10.1080/09537325.2021.1979509.

Harryandi, Alexander, Fira Natasha, and Muhammad Akbar. "Regulating Initial Coin Offering Amidst the Development of Crypto Assets in Indonesia." *Journal of Central Banking Law and Institutions* 1, no. 3 (2022): 537–70. https://doi.org/10.21098/jcli.v1i3.41.

Huijbers, Theo. *Filsafat Hukum*. XXIV. Yogyakarta: PT Kanisius, 2021.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Shahbaz Khan, and Rajiv Suman. "Blockchain Technology Applications for Industry 4.0: A Literature-Based Review." *Blockchain: Research and Applications* 2, no. 4 (2021): 100027. https://doi.org/10.1016/j.bcra.2021.100027.

Khan, Shafaq Naheed, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, and Anoud Bani-Hani. "Blockchain Smart Contracts: Applications, Challenges, and Future Trends." *Peer-to-Peer Networking and Applications* 14, no. 5 (2021): 2901–25. https://doi.org/10.1007/s12083-021-01127-0.

Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts." In *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 839–58, 2016. https://eprint.iacr.org/2015/675.pdf.

Marzuki, Peter Mahmud. *Penelitian Hukum*. IX. Jakarta: Prenadamedia Group, 2014.

Mertokusumo, Sudikno. *Penemuan Hukum Sebuah Pengantar*. Cet. II. Yogyakarta: Liberty, 2007.

———. *Teori Hukum (Edisi Revisi)*. Yogyakarta: Cahaya Atma Pustaka, 2014.

McGhin, Thomas, Kim Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. "Blockchain in Healthcare Applications: Research Challenges and Opportunities." *Journal of Network and Computer Applications* 135, no. January (2019): 62–75. https://doi.org/10.1016/j.jnca.2019.02.027.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://doi.org/10.1108/TG-06-2020-0114.

Namasudra, Suyel, Ganesh Chandra Deka, Prashant Johri, Mohammad Hosseinpour, and Amir H. Gandomi. "The Revolution of Blockchain: State-of-the-Art and Research Challenges." *Archives of Computational Methods in Engineering* 28, no. 3 (2021): 1497–1515. https://doi.org/10.1007/s11831-020-09426-0.

Novina Putri Bestari, 2023, "337 Data Dukcapil Bocor, Ahli: Saya Bingung Jika Disangkal", CNBC Indonesia, URL: https://www.cnbcindonesia.com/tech/20230717095112-37-454869/337-data-dukcapil-bocor-ahli-saya-bingung-jika-disangkal, diakses 10 Maret 2024.

Pentland, Alex. "Trust in Digital Societies." In *Trusted Data*, 3–14, 2020. https://doi.org/10.7551/mitpress/12439.003.0002.

Pranowo, Yogie. "Prinsip Utilitarisme Sebagai Dasar Hidup Bermasyarakat." *Paradigma: Jurnal Filsafat, Sains, Teknologi, Dan Sosial Budaya* 26, no. 2 (2020): 172–79. https://doi.org/10.33503/paradigma.v26i2.789.

Pratiwi, Endang, Theo Negoro, and Hassanain Haykal. "Teori Utilitarianisme Jeremy Bentham: Tujuan Hukum Atau Metode Pengujian Produk Hukum?" *Jurnal*

Konstitusi 19, no. 2 (2022): 269–93. https://doi.org/10.31078/jk1922.

Putranto, Rahmat Dwi. *Teknologi Hukum Paradigma Baru Hukum Di Dunia Digital*. Jakarta: Kecana Prenada Media, 2023.

Raffi Hasta Anggara, Muhammad. "The Presence of Commercial Banks in Metaverse'S Financial Ecosystem: Opportunities and Risks." *Journal of Central Banking Law and Institutions* 1, no. 3 (2022): 405–30. https://doi.org/10.21098/jcli.v1i3.28.

Reidenberg, Joel R. "Lex Informatica: The Formulation of Information Policy Rules through Technology." *Texas Law Review* 76, no. 3 (1998): 553–93. http://ir.lawnet.fordham.edu/faculty_scholarshipat:http://ir.lawnet.fordham.edu/faculty_scholarship/42.

Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: PT Citra Aditya Bakti, 2021.

Rahel Narda Chaterine and Krisiandi, 2024, "PDN Diretas, Kabareskrim: "Ransomware" Bukan Hal Mudah Ditangani," URL: https://nasional.kompas.com/read/2024/07/15/14414911/pdn-diretas-kabareskrim-ransomware-bukan-hal-mudah-ditangani, diakses 31 Juli 2024.

Ridian Eka Saputra, 2023, "Dugaan Data 34 Juta Paspor WNI Bocor, Pengamat: Banyak yang Tidak Valid", Tempo.com, URL: https://video.tempo.co/read/34284/dugaan-data-34-juta-paspor-wni-bocor-pengamat-banyak-yang-tidak-valid, diakses 10 Maret 2024.

Silvana Febriari, 2023, "Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023", Metrotvnews.com, URL: https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023, diakses 10 Maret 2024.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada, 2007.

Sulistiowati, and Nurhasan Ismail. *Penormaan Asas-Asas Hukum Pancasila Dalam Kegiatan Usaha Koperasi Dan Perseroan Terbatas*. Cetakan I. Yogyakarta: Gadjah Mada University Press, 2018.

Sumardjono, Maria SW. *Bahan Kuliah: Metodologi Penelitian Ilmu Hukum*. Revisi. Yogyakarta: Universitas Gadjah Mada, 2021.

Safiranita, Tasya, Ahmad M. Ramli, Denidah Olivia, Ferry Gunawan C., and Ega Ramadayanti. "The Role of E-Commerce in Escalation of Digital Economy in The New Normal Era Based on Law Number 27 of 2022 Concerning Personal Data Protection." *Jurnal Penelitian Hukum De Jure* 22, no. 4 (2022): 437–50. https://doi.org/10.30641/dejure.2022.v22.437-450.

Septiansyah, Zainal B., and Muhammad Ghalib. "Konsepsi Utilitarianisme Dalam Filsafat Hukum Dan Implementasinya Di Indonesia." *Ijtihad: Jurnal Hukum Islam Dan Pranata Sosial* 34, no. 1 (2018): 27–34. https://doi.org/10.15548/ijt.v34i1.3.

Stopfer, Lukas, Alexander Kaulen, and Thomas Purfürst. "Potential of Blockchain Technology in Wood Supply Chains." *Computers and Electronics in Agriculture* 216, no. November 2023 (2024): 108496. https://doi.org/10.1016/j.compag.2023.108496.

Susanto, Angga Hendiarto, Dhanar Setya Wahyu, Rizal Faiz Mahtum, and Azizah Rettyaningrum. "Perlindungan Data Pribadi Konsumen Atas Pembobolan Data Rahasia Negara Sebagai Perwujudan Good Corporate Governance." *Jurnal Hukum Media Justitia Nusantara* 13, no. 1 (2023): 46–53. https://doi.org/https://doi.org/10.30999/mjn.v13i1.2634.

Laws and Regulations

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union L 119/1, May 4, 2016.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820).