


Data Security Transformation: The Significant Role of Blockchain Technology

Archa Erica^{1*}  Silva Wulandari² , Riya Widayanti³ ,

¹adi-journal incorporation, United States ² University of Gunadarma, Indonesia ³, Universitas Esa Unggul, Indonesia

¹Archaca@adi-journal.org, ²silva@gmail.com, ³riya.widayanti@esaunggul.ac.id,

*Archa Erica

Article Info

Article history:

Received month dd, 2023-12-28

Revised month dd, 2023-12-31

Accepted month dd, 2023-12-31

Keywords:

Digital Transformation

Data Security

Blockchain Projects

Technology Regulations



ABSTRACT

Digital transformation has emerged as a global trend that has revolutionized the way businesses and governments operate worldwide. In Indonesia, both the government and private sectors are fast-tracking digital transformation by embracing blockchain technology as a solution to enhance data security in their day-to-day operations. Various blockchain projects have been undertaken in Indonesia, including the verification and validation of educational certificates, medical data storage, and payment systems. However, the implementation of blockchain technology in Indonesia encounters several challenges, such as unclear regulations, limited infrastructure, and a lack of understanding of blockchain technology. Therefore, comprehensive support from all stakeholders is essential to expedite the adoption of blockchain technology in Indonesia. Further research and development are required to fully harness the potential of blockchain technology and accelerate the pace of digital transformation in the country.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



*Corresponding Author:

Archa Erica(Archaca@adi-journal.org)

DOI: [http://10.34306/bfront.v3i2.466](https://doi.org/10.34306/bfront.v3i2.466)

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

1. INTRODUCTION

The influence of digital transformation has affected various aspects of our lives, ranging from how we communicate, work, shop, and conduct business. This phenomenon has occurred because digitalization has enabled easier and faster collection, storage, and processing of data. In the digital era, data has become one of the most valuable assets for individuals and organizations. Data serves as a source of information used to make strategic decisions, add value to companies, and drive innovation. Therefore, data security becomes crucial and critical in the context of digital transformation [1].

In Indonesia, digital transformation is experiencing rapid growth. The Indonesian government has issued various initiatives to drive the development of digital transformation in the country, including the National Initiative for 1000 Digital Startups, the National Movement for 100 Smart Cities, and other programs [2]. However, despite the significant benefits that digital transformation brings to the Indonesian economy, there are security risks that need to be addressed. Data security has become a serious global issue, with the potential risk of unauthorized access and data misuse for malicious purposes, such as identity theft, fraud, and various

criminal activities. Therefore, the presence of a robust security system is crucial to protect data from potential risks. In this context, blockchain technology emerges as an interesting solution to address data security issues in the digital transformation process. [3] Blockchain, as a decentralized technology, enables transactions between two parties that do not trust each other without involving intermediaries [4]. Data stored in the blockchain is decentralized across the entire network, making it impossible to be altered by one party without the approval of the entire network. Additionally, blockchain can enhance transparency and accountability in data management [5].

Although the use of blockchain technology has some risks and limitations, there is significant potential to enhance data security in the context of digital transformation [6]. When implementing blockchain technology for data security, it is important to choose the type of blockchain that suits the organization's needs and consider both the benefits and risks associated with its use. Additionally, integration with existing systems and the ability to address the limitations of blockchain technology are also crucial aspects to consider [7].

In Indonesia, there is substantial potential for the use of blockchain technology to improve security and transparency in data management within the digital transformation context [8]. However, the adoption of this technology is still limited and only beginning to be introduced in several companies and institutions in Indonesia. There is a lack of understanding regarding the full potential and weaknesses of blockchain technology, along with differences in perspectives between regulators and industry players regarding the use of blockchain and cryptocurrency. Some regulators, such as Bank Indonesia and the Financial Services Authority (OJK), maintain a skeptical view of cryptocurrency use and have tightened regulations, potentially hindering the development of the blockchain ecosystem in Indonesia [9].

Other challenges include technical and infrastructural issues, such as limited network scalability, dependence on an internet network that is not always stable, and technological limitations in blockchain transactions [10]. Nevertheless, blockchain technology still holds significant potential to enhance data security in the era of digital transformation in Indonesia, especially in sectors such as banking, logistics, and government [11].

2. RESEARCH METHODS

This research methodology employs a qualitative descriptive approach. The study involves analyzing data and information obtained from literature reviews, including journals, articles, and official sources related to digital transformation and the implementation of blockchain technology in Indonesia over two months. Additionally, the research includes interviews with experts and practitioners in the fields of technology and digital transformation in Indonesia [12].

The initial stage of the research involves collecting and reviewing literature related to digital transformation and blockchain technology in Indonesia. Furthermore, the researcher analyzes regulations and strategies issued by the government regarding the implementation of blockchain technology [13]. Subsequently, interviews are conducted with experts and practitioners in the technology and digital transformation fields to gain a broader and deeper perspective on the implementation of blockchain technology in Indonesia [14].

The results of this research are then analyzed and compiled into a conclusion regarding the potential and challenges of implementing blockchain technology in digital transformation in Indonesia [15]. Recommendations are also provided for the government and private sector to maximize the benefits of blockchain technology in the context of digital transformation in Indonesia [16].

3. RESULT AND DISCUSSION

The development of digital technology has facilitated the access, use, and storage of data [17]. Despite providing convenience, this progress also brings about increasingly complex and diverse data security risks. Data security becomes crucial as data is considered a valuable asset for both organizations and individuals [18]. Data has the potential to influence decisions, add value, and create a competitive advantage [19]. Therefore, data security must be taken seriously and integrated into all aspects of digital transformation [20].

The concept of data security covers three main aspects: confidentiality, integrity, and data availability. Data confidentiality is related to the privacy and security of data from unauthorized parties [21]. Information included in the category of confidentiality includes personal data, health data, financial data, corporate confidential data, and government data [22]. The disclosure of confidential information can have negative impacts

on the interests of individuals or organizations. Therefore, maintaining data confidentiality is crucial in the context of digital transformation [23].

Data integrity is the quality that ensures data remains accurate, intact, and valid. The aspects of data integrity include data validity, consistency, and integrity. Loss of data integrity can result in inaccurate information, inconsistencies, and incorrect decision-making. Therefore, maintaining data integrity is also an important aspect of the digital transformation journey [24].

3.1. The Concept of Data Security in Digital Transformation

The concept of data security encompasses three main aspects: confidentiality, integrity, and data availability. Data confidentiality involves safeguarding the privacy of data from unauthorized parties, including preventing unauthorized access or misuse. For example, an individual's health information is highly sensitive data that must be protected from unauthorized access [25]. Data integrity includes the authenticity and completeness of data processed and stored by the organization. Data authenticity ensures that data is not manipulated or altered without the knowledge or approval of authorized parties. Data integrity ensures that data remains uncorrupted or lost during the storage or transmission process. Data availability is related to the accessibility of data by authorized parties when needed. If data is unavailable when needed, organizations may incur business losses and lose customer trust.

In digital transformation, the use of digital technologies such as cloud computing, big data, and the Internet of Things (IoT) can enhance the efficiency and productivity of organizations. However, the use of digital technologies also increases the risk of data security. This emphasizes the importance of using the latest security technologies and implementing strict security practices in digital transformation. The proper implementation of security technologies will ensure that critical data and information are protected from unauthorized access or manipulation by unauthorized parties.

The verification and validation process in blockchain technology is also very fast and efficient. This process does not require intermediaries or third parties such as banks or financial institutions, which can speed up transaction times and reduce associated costs. In the context of digital transformation, blockchain technology can be utilized to enhance data security in online transactions. Online transactions are often vulnerable to hacker attacks, which can lead to the theft of personal data such as credit card numbers or other sensitive information, resulting in financial losses and security risks. By leveraging blockchain, data stored in the network can be strongly encrypted, allowing only authorized parties with encryption keys to access and read the data. This significantly improves data security as only authorized parties can access the data.

Furthermore, blockchain technology enables secure and decentralized storage and sharing of data. Unlike traditional systems that store data in centralized databases regulated by specific companies, blockchain allows for decentralized data storage. Data is not stored in a single centralized point but distributed across the entire blockchain network. This means that everyone connected to the network has the same copy of the stored data, and if one copy is compromised by a cyberattack or other damage, other copies remain accessible.

Another advantage of blockchain technology is its ability to create high transparency in data processing. Each transaction or block in the blockchain is linked to the blocks before and after it, making it challenging for unauthorized parties to manipulate data. Thus, blockchain can help reduce the risk of fraud and create transparency.

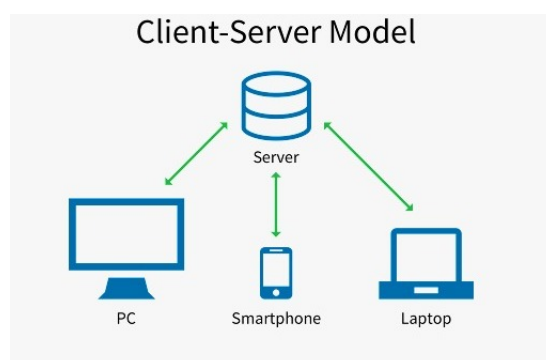


Figure 1. Blockchain Server Framework

The use of blockchain technology to enhance data security has several significant benefits. Firstly, this technology provides better data security compared to conventional methods. In blockchain, data is stored in a decentralized and encrypted manner, reducing the risk of data manipulation or tampering. Data within the blockchain maintains a high level of integrity because each transaction and data entry cannot be altered without the consent of all involved parties. On the flip side, blockchain also enhances transparency in every transaction or data. As all involved parties can verify each transaction and data, the risk of fraud or deception is significantly reduced, providing advantages, especially in sectors requiring accurate and trustworthy data and transactions, such as finance or logistics.

Additionally, blockchain technology offers efficiency and speed in the verification and validation processes of data. Each transaction can be quickly and efficiently verified without involving intermediaries or third parties, reducing the costs and time associated with these processes and speeding up transaction times.

However, the use of blockchain technology also poses some risks that need careful consideration. One of these is dependence on blockchain technology itself. Issues or failures in this technology can impact the stored data and transactions, and security risks also become a primary concern. Despite being considered secure, the possibility of successful attacks penetrating its security system remains. Scalability limitations are also a challenge, especially in the implementation of large and complex digital transformations. Therefore, careful planning and management are required to implement blockchain technology in digital transformation in Indonesia.

Overall, the utilization of blockchain technology to enhance data security brings significant benefits, including improved data security, transparency, efficiency, and speed. However, risks such as dependence on technology, security concerns, and scalability limitations need to be carefully considered, and thorough planning and management are necessary for the successful implementation of blockchain technology in digital transformation in Indonesia.

4. CONCLUSION

In the rapidly evolving era of digital transformation, the utilization of blockchain technology holds significant potential to enhance data security and mitigate the risk of unauthorized manipulation or alteration. The Indonesian government has recognized this potential and responded by issuing regulations and strategies to encourage the implementation of blockchain technology in both government operations and the private sector.

Several projects involving the implementation of blockchain technology in Indonesia, such as the verification and validation of educational certificates, storage of medical data, and the use of cryptocurrency as a means of payment, have been initiated. However, the introduction of blockchain technology in Indonesia still faces several challenges, including regulatory ambiguity, infrastructure limitations, and a lack of understanding of blockchain technology. To address these challenges, the government needs to update and enhance regulations related to blockchain technology, particularly in terms of taxation and data security.

Furthermore, efforts should be made to improve digital infrastructure across Indonesia, especially in remote areas, to facilitate the smooth implementation of blockchain technology. Companies in Indonesia are also encouraged to pay special attention to the use of blockchain technology to enhance data security in their operations. Increasing public understanding of blockchain technology should be promoted through education and awareness campaigns. On the other hand, blockchain technology companies are expected to consider the significant market potential in Indonesia and begin expanding their business presence domestically (Centre for Innovation Policy and Governance, 2018). The growth in the number of blockchain technology companies in Indonesia could create new opportunities for the application of this technology and contribute to the growth of the digital economy in Indonesia.

The utilization of blockchain technology in the digital transformation of Indonesia offers substantial potential for improving data security and driving digital economic growth. Nevertheless, challenges faced in the implementation of blockchain technology need to be overcome by the Indonesian government and companies. With collaborative efforts, the integration of blockchain technology can proceed smoothly in Indonesia's digital transformation, providing benefits to the public and supporting overall economic growth in Indonesia.

REFERENCES

- [1] LATEX : Sukses Publikasi Ilmiah. (2023). (n.p.): Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM).
- [2] U. Rahardja, Q. Aini, and A. Khoirunisa, "The Effect of Rinfogroups as a Discussion Media in Student Learning Motivation," *Aptisi Trans. Manag.*, vol. 2, no. 1, pp. 79–88, 2018.
- [3] Selimoglu, S. K., Saldi, M. H. (2023). Blockchain Technology for Internal Audit in Cyber Security Governance of Banking Sector in Turkey: A SWOT Analysis. In *Contemporary Studies of Risks in Emerging Technology, Part B* (pp. 23-55). Emerald Publishing Limited.
- [4] Farah MM and Abubakar L. 2019. Telaah Yuridis Sukuk Sebagai Instrumen Investasi Syariah. *Justitia Jurnal Hukum*. Vol 3: 281-296.
- [5] Renewable Energy : Panduan Mandiri Instalasi Komersial Energi Terbarukan. (2023). (n.p.): Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM).
- [6] B. Djatmiko, M. Galinium, and N. Lutfiani, "The Role of a Variety of Research Studies on Problem Management," *Aptisi Trans. Manag.*, vol. 2, no. 1, pp. 9–19, 2018.
- [7] Vionis, P., Kotsilieris, T. (2024). The Potential of Blockchain Technology and Smart Contracts in the Energy Sector: A Review. *Applied Sciences*, 14(1), 253.
- [8] Bawack, R. E., Fosso Wamba, S., Carillo, K. D. A. (2021). A framework for understanding artificial intelligence research: insights from practice. *Journal of Enterprise Information Management*, 34(2), 645-678.
- [9] K. D. Prawira, B. P. K. Bintoro, R. Hadis, W. Warseno, and Y. A. Terah, "Analysis of Factors Affecting Customer Satisfaction at PT. OSO Gallery," *ADI J. Recent Innov.*, vol. 3, no. 2, pp. 172–183, 2022.
- [10] B. Rawat, A. S. Bist, N. Mehra, M. F. Fazri, and Y. A. Terah, "Study of Kumaon Language for Natural Language Processing in End-to-End Conversation Scenario," *IAIC Trans. Sustain. Digit. Innov.*, vol. 3, no. 2, pp. 143–149, 2022.
- [11] Y. R. C. Pujiharto, T. Mariyanti, A. R. Jayaprawira, and Y. A. Terah, "Financial Management of Indonesian Hajj Against the Yield by Using a Dynamics System Model," *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 69–78, 2023.
- [12] Mulyati, M., Ilamsyah, I., Aris, A., and Zahran, M. S. (2021). Blockchain technology: can data security change higher education much better?. *International Journal of Cyber and IT Service Management*, 1(1), 121-135.
- [13] R. Yunita, M. S. Shihab, D. Jonas, H. Haryani, and Y. A. Terah, "Analysis of The Effect of Servicescape and Service Quality on Customer Satisfaction at Post Shop Coffee Toffee in Bogor City," *Aptisi Trans. Technopreneursh.*, vol. 4, no. 1, pp. 66–74, 2022.
- [14] K. Arora and A. S. Bist, "Artificial intelligence based drug discovery techniques for covid-19 detection," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 120–126, 2020.
- [15] Kumar, M., Choubey, V. K., Raut, R. D., Jagtap, S. (2023). Enablers to achieve zero hunger through IoT and blockchain technology and transform the green food supply chain systems. *Journal of Cleaner Production*, 405, 136894.
- [16] E. Febriyanto and R. S. Naufal, "Attitude Competency Assessment in the 2013 curriculum based on elementary school Prototyping methods," *IAIC Trans. Sustain. Digit. Innov.*, vol. 1, no. 1, pp. 87–96, 2019.
- [17] Althero, Z., Syahreza, J., and Ortiz, A. (2023). Blockchain Technology for Authentication and Validation Social Network Accounts. *Blockchain Frontier Technology*, 3(1), 32-38.
- [18] A. B. Fitra, A. Suharko, F. M. Albar, and D. Apriliasari, "Examination Of Customer Interest In The Use Of The Mandiri Syariah Mobile Application At PT. Bank Syariah Mandiri Bekasi Branch Office," *IAIC Trans. Sustain. Digit. Innov.*, vol. 3, no. 2, pp. 110–125, 2022.
- [19] M. R. Anwar, D. Apriani, and I. R. Adianita, "Hash Algorithm In Verification Of Certificate Data Integrity And Security," *Aptisi Trans. Technopreneursh.*, vol. 3, no. 2, pp. 65–72, 2021.
- [20] Tchuente, D., Lonlac, J., Kamsu-Foguem, B. (2024). A methodological and theoretical framework for implementing explainable artificial intelligence (XAI) in business applications. *Computers in*
- [21] Munajat, E. (2022). THE POTENTIAL OF DIGITAL RUPIAH AS A NEW SOLUTION TO COMBAT CORRUPTION IN INDONESIAN GOVERNMENT. *Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan*, 4(Spesial Issue 3), 1304-1322.

- [22] Wahyuningsih, T., Oganda, F. P., Anggraeni, M. (2021). Design and implementation of digital education resources blockchain-based authentication system. *Blockchain Frontier Technology*, 1(01), 74-86.
- [23] W. Setyowati, P. C. Kurniawan, A. Mardiansyah, E. P. Harahap, and N. Lutfiani, "The Role Of Duty Complexity As A Moderation Of The Influence Auditor's Professional Knowledge And Ethics On Audit Quality," *Aptisi Trans. Manag.*, vol. 5, no. 1, pp. 20–29, 2021.
- [24] Kaif, A. D., Alam, K. S., Das, S. K. (2024). Blockchain based sustainable energy transition of a Virtual Power Plant: Conceptual framework design and experimental implementation. *Energy Reports*, 11, 261-275.
- [25] A. S. Bist, B. Rawat, Q. Aini, N. Lutfiani, and M. Hardini, "COVID-19 Wave Pattern Analysis: An Exhaustive Survey," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–4.