West Science Information System and Technology
Vol. 3, No. 03, December 2025, pp. 176~184

Blockchain Implementation for Digital Financial Transaction Data Security

Sayed Achmady
Universitas Jabal Ghafur

Article Info

Article history:

Received December, 2025
Revised December, 2025
Accepted December, 2025

Keywords:

Blockchain; Digital Financial Transactions; Data Security; Financial Technology; Indonesia

ABSTRACT

The rapid expansion of digital financial services in Indonesia has increased the importance of ensuring secure, transparent, and reliable transaction data management. Traditional centralized financial systems face challenges related to data breaches, fraud, and system vulnerability, prompting the need for more advanced security technologies. This study examines the implementation of blockchain technology in enhancing the security of digital financial transaction data in Indonesia. A quantitative research approach was employed using a sample of 65 respondents who are users and practitioners of digital financial services. Data were collected through a structured questionnaire measured on a five-point Likert scale and analyzed using SPSS version 25. The results of simple linear regression analysis indicate that blockchain implementation has a positive and significant effect on digital financial transaction data security. Blockchain implementation explains 54.9% of the variance in data security, highlighting its substantial role in improving confidentiality, data integrity, transparency, and fraud prevention. The findings provide empirical support for the adoption of blockchain technology as a strategic solution to strengthen digital financial system security in Indonesia.

Corresponding Author:

Name: Sayed Achmady
Institution: Universitas Jabal Ghafur
Email: sayedachmady@unigha.ac.id

1. INTRODUCTION

The rapid digitalization of the financial sector in Indonesia has fundamentally transformed the way financial transactions are conducted [1]. The widespread adoption of digital payment systems, mobile banking, and financial technology (fintech) platforms has increased transaction efficiency, accessibility, and financial inclusion [2]. However, alongside these benefits, the growing volume of digital financial transactions has also heightened concerns related to data security, privacy protection, fraud, and system vulnerability. Cyberattacks, data breaches, and unauthorized access to financial data have become critical challenges that threaten public trust in digital financial services [3].

In Indonesia, the expansion of digital finance is strongly supported by government initiatives aimed at accelerating the digital economy and strengthening the national financial system [4]. Nevertheless, the existing

centralized data management systems used by many financial institutions remain vulnerable to manipulation, single points of failure, and cyber threats [5]. These weaknesses highlight the urgent need for more robust and resilient technological solutions that can ensure the security, integrity, and transparency of digital financial transaction data.

Blockchain technology has emerged as a disruptive innovation with significant potential to address these challenges [6]. Blockchain operates on a decentralized ledger system that records transactions across multiple nodes, making data difficult to alter without collective consensus. Its core characteristics—immutability, transparency, cryptographic security, and decentralization—offer a new paradigm for securing digital financial data. By eliminating reliance on a single central authority, blockchain reduces the risk of data tampering and enhances trust among transaction participants [7].

Despite the growing global interest in the application of blockchain technology within the financial sector, empirical studies that specifically examine its implementation and effectiveness in securing digital financial data in the Indonesian context remain scarce, as most existing research emphasizes conceptual frameworks, regulatory analyses, or case studies from developed economies, leaving a notable gap in quantitative evidence regarding how blockchain adoption influences perceptions of transaction security among users and financial stakeholders in Indonesia; therefore, this study aims to empirically investigate the role of blockchain technology in enhancing the security of digital financial transaction data in Indonesia through a quantitative approach by collecting data from 65 respondents using a Likert-scale questionnaire and analyzing it with SPSS version 25 to measure the impact of blockchain implementation on key security dimensions, including confidentiality, data integrity, transparency, and fraud prevention, with the findings expected to contribute to the academic literature by offering empirical insights into blockchain-based financial security while also providing practical implications for policymakers, financial institutions, and fintech providers in developing secure and trustworthy digital financial systems in Indonesia.

2. LITERATURE REVIEW

2.1 Digital Financial Transactions and Data Security

The rapid growth of digital financial transactions has transformed the delivery of financial services by enabling faster, more efficient, and more inclusive access to financial products—encompassing activities such as mobile payments, online banking, electronic wallets, and fintech-based services—yet despite these advantages, digital financial systems remain heavily dependent on information technology infrastructure, rendering them vulnerable to cyber threats, data breaches, identity theft, and financial fraud, which has made data security a critical concern for both service providers and users [8]; in this context, digital financial data security refers to the protection of transaction data from unauthorized access, alteration, misuse, and destruction, with key dimensions including confidentiality, integrity, availability, transparency, and authentication, while traditional centralized systems that rely on single databases managed by trusted intermediaries tend to create single points of failure that heighten the risk of cyberattacks, vulnerabilities that become increasingly pronounced as transaction volumes grow and underscore the urgent need for more secure technological solutions [9].

2.2 *Blockchain Technology Concept*

Blockchain is a distributed ledger technology that records transactions in a decentralized and chronological manner across a network of computers, or nodes, where each transaction is grouped into a block and linked to the previous block through cryptographic hash functions to form an immutable chain of records, ensuring that once transactions are validated and recorded, the data cannot be altered without network consensus, thereby maintaining data integrity and reliability [10]; the core characteristics of blockchain—decentralization, immutability, transparency, and cryptographic security—eliminate reliance on a central authority and reduce the risk of data manipulation, ensure transaction records are permanent and tamper-resistant, enable authorized participants to verify transactions in real time, and protect sensitive information through robust authentication mechanisms, making blockchain particularly well suited for applications that demand high levels of trust and security, especially in the context of financial transactions [11].

2.3 *Blockchain in Financial Systems*

Blockchain technology has gained considerable attention in the financial sector for its potential to enhance transaction security, reduce operational costs, and improve system efficiency, as it can be applied to various financial functions such as payment systems, clearing and settlement processes, digital identity management, and fraud detection [12]; by enabling peer-to-peer transactions without intermediaries, blockchain shortens transaction processing time and minimizes the risks of human error and intentional manipulation, while prior studies indicate that it strengthens financial system security through improved data integrity and transparency and a reduced likelihood of fraud, further reinforced by the use of smart contracts—self-executing agreements embedded within blockchain networks—that automate processes and enforce predefined rules to enhance transaction reliability, although challenges related to scalability, regulatory uncertainty, and technological complexity continue to hinder widespread adoption, particularly in developing economies [13].

2.4 *Blockchain and Digital Financial Data Security*

From a data security perspective, blockchain offers distinct advantages over conventional systems, as its cryptographic structure ensures that transaction data are encrypted and accessible only to authorized parties, thereby enhancing confidentiality, while the immutable nature of its records prevents unauthorized data modification and safeguards data integrity, and the transparency of blockchain networks enables real-time transaction monitoring and auditing that support fraud prevention and accountability [14]; empirical studies further indicate that users generally perceive blockchain-based systems as more secure and trustworthy than traditional digital transaction platforms because decentralized verification reduces dependence on third-party trust and increases confidence in transaction validity, although the overall effectiveness of

blockchain implementation remains contingent on factors such as user awareness, system design, and successful integration with existing financial infrastructure [15].

2.5 *Research Gap and Hypothesis Development*

Although the potential of blockchain technology in securing digital financial transactions has been widely discussed, empirical quantitative studies that examine its impact in the Indonesian context remain limited, as most existing research emphasizes conceptual frameworks or case studies from developed countries, leaving a gap in understanding how blockchain implementation influences users' perceptions of data security in emerging economies such as Indonesia; accordingly, this study seeks to address this gap by empirically analyzing the effect of blockchain implementation on the security of digital financial transaction data in Indonesia, and based on theoretical considerations and empirical insights from prior studies, a research hypothesis is subsequently proposed.

H1: The implementation of blockchain technology has a positive and significant effect on the security of digital financial transaction data in Indonesia.

3. RESEARCH METHODS

3.1 Research Design and Approach

This study employs a quantitative research approach to examine the effect of blockchain implementation on the security of digital financial transaction data in Indonesia. The quantitative design is selected to allow for objective measurement and statistical analysis of relationships between variables. The research adopts a cross-sectional survey method, where data are collected at a single point in time to capture respondents' perceptions and experiences related to blockchain-based digital financial transactions.

3.2 Population and Sample

The population of this study comprises individuals in Indonesia who use and practice digital financial services, including mobile banking, digital payment platforms, and fintech applications, and due to limited access to the entire population, a sample of 65 respondents was selected using a non-probability purposive sampling technique to ensure that participants possessed sufficient knowledge or experience with digital financial transactions as well as awareness of blockchain technology [16]; this sample size is considered adequate for exploratory quantitative analysis and is consistent with previous studies that have employed similar methodological approaches in research on technology adoption and financial data security.

3.3 Research Variables and Operational Definitions

This study involves two main variables, namely the independent variable and the dependent variable, where the independent variable is blockchain implementation (X), defined as the extent to which blockchain technology is applied in digital financial transaction systems and measured through indicators such as decentralization, data immutability, transaction transparency, cryptographic security, and system reliability, while the dependent variable is digital financial transaction data security (Y), which refers to the protection of digital financial transaction data from unauthorized access, alteration, and misuse and is measured using indicators including confidentiality, data integrity, transparency, fraud prevention, and user trust, with each indicator assessed through statement items measured on a Likert scale [17].

3.4 Data Collection Method

Primary data in this study were collected using a structured questionnaire developed based on relevant literature and consisting of closed-ended statements measured on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), allowing respondents to express the intensity of their perceptions regarding blockchain implementation and digital financial data security; the questionnaire was distributed electronically to facilitate broader reach and ease of response, and prior to full distribution, a preliminary review was conducted to ensure the clarity and relevance of all measurement items.

3.5 Data Analysis Technique

The collected data were analyzed using SPSS version 25 through several stages, beginning with descriptive statistics to summarize respondent characteristics and describe the distribution of responses for each variable, followed by validity testing of questionnaire items using Pearson's product-moment correlation, where items were considered valid if the correlation coefficient exceeded the critical value at a 0.05 significance level, and reliability testing using Cronbach's Alpha to assess internal consistency, with values above 0.70 indicating acceptable reliability; subsequently, inferential statistical analysis was conducted using simple linear regression to test the research hypothesis by examining the effect of blockchain implementation on digital financial transaction data security, with the significance of the relationship evaluated through t-tests and the coefficient of determination (R^2) to assess the explanatory power of the independent variable.

4. RESULTS AND DISCUSSION

4.1 Respondent Characteristics

A total of 65 valid questionnaires were collected and analyzed in this study. Respondents consisted of users and practitioners of digital financial services in Indonesia. Based on descriptive analysis, the majority of respondents actively use digital payment platforms and mobile banking services, indicating adequate exposure to digital financial transactions.

Table 1. Respondent Profile

Characteristics	Category	Frequency	Percentage (%)
Gender	Male	36	55.4
	Female	29	44.6
Age	20–29 years	24	36.9
	30–39 years	27	41.5
	≥ 40 years	14	21.6
Digital Finance Usage	< 1 year	12	18.5
	1–3 years	29	44.6
	> 3 years	24	36.9

Table 1 presents the demographic profile of the respondents involved in this study and provides an overview of their basic characteristics. In terms of gender, the sample is relatively balanced, with male respondents accounting for 55.4 percent and female respondents comprising 44.6 percent of the total sample, indicating that perceptions of digital financial transaction security and blockchain implementation were captured from both male and female users without extreme dominance from one group. Regarding age distribution, most respondents are in the productive age range, with the largest proportion aged 30–39 years (41.5 percent), followed by those aged 20–29 years (36.9 percent), while respondents aged 40 years and above constitute 21.6 percent. This age composition suggests that the majority of

participants are digitally active individuals who are likely familiar with digital financial services and emerging technologies. In terms of digital finance usage experience, nearly half of the respondents (44.6 percent) have used digital financial services for one to three years, while 36.9 percent have more than three years of experience, and only 18.5 percent have used such services for less than one year. This indicates that most respondents possess sufficient experience with digital financial transactions, strengthening the credibility of their perceptions regarding data security and the implementation of blockchain technology.

4.2 Descriptive Statistics of Research Variables

Descriptive statistics were used to evaluate respondents' perceptions of blockchain implementation and digital financial transaction data security.

Table 2. Descriptive Statistics

Variable	N	Minimum	Maximum	Mean	Std. Deviation
Blockchain Implementation (X)	65	3.10	4.80	4.12	0.43
Data Security (Y)	65	3.00	4.90	4.25	0.46

Table 2 presents the descriptive statistics of the main variables examined in this study, namely blockchain implementation (X) and digital financial transaction data security (Y), where the blockchain implementation variable records a mean score of 4.12 on a five-point Likert scale, indicating that respondents generally perceive the application of blockchain technology in digital financial transactions as relatively high, with minimum and maximum values of 3.10 and 4.80 suggesting some variation in perceptions but an overall tendency toward the upper end of the scale, and a standard deviation of 0.43 reflecting relatively low response dispersion and consistent views among respondents; similarly, the data security variable shows a slightly higher mean score of 4.25, indicating a high perceived level of security in digital financial transaction data, with minimum and maximum values of 3.00 and 4.90 demonstrating moderate variability in responses, as also reflected by a standard deviation of 0.46, and taken together, these descriptive results suggest that respondents not only acknowledge the presence of blockchain-related features in digital financial systems but also associate them with a high level of transaction data security, providing an initial indication of a positive relationship between blockchain implementation and data security perceptions.

4.3 Validity and Reliability Test Results

The results of the instrument testing indicate that all questionnaire items have correlation coefficients exceeding the critical r-table value of 0.244, confirming their validity, while reliability analysis further shows strong internal consistency, as reflected by Cronbach's Alpha values of 0.872 for the blockchain implementation variable with eight items and 0.891 for the data security variable with nine items; since both values are well above the accepted threshold of 0.70, these findings confirm that all measurement instruments used in this study are reliable and suitable for further statistical analysis.

4.4 Regression Analysis Results

Simple linear regression was conducted to test the effect of blockchain implementation on digital financial transaction data security.

Table 3. Simple Linear Regression Results

Model	Unstandardized B	Std. Error	t-value	Sig.
Constant	1.214	0.512	2.37	0.021
Blockchain Implementation (X)	0.738	0.089	8.29	0.000

Table 3 presents the results of the simple linear regression analysis examining the effect of blockchain implementation on digital financial transaction data security, which reveal that blockchain implementation has a positive and statistically significant influence on data security, as reflected by an unstandardized coefficient (B) of 0.738 with a t-value of 8.29 and a significance level of 0.000, well below the 0.05 threshold, indicating that higher levels of blockchain implementation are associated with substantial improvements in perceived digital financial transaction data security, likely due to blockchain features such as decentralization, immutability, and cryptographic protection; additionally, the constant value of 1.214 is also statistically significant (Sig. = 0.021), representing the baseline level of data security in the absence of blockchain implementation, and overall, these findings provide strong empirical support for the proposed research hypothesis by confirming that blockchain implementation plays a significant role in strengthening digital financial transaction data security in Indonesia.

The coefficient of determination results show an R value of 0.741 with an R Square of 0.549 and an Adjusted R Square of 0.542, indicating that blockchain implementation explains 54.9 percent of the variance in digital financial transaction data security, while the remaining 45.1 percent is attributable to other factors not examined in this study, suggesting that although blockchain implementation plays a substantial role in enhancing data security, additional technological, organizational, and behavioral variables may also influence security outcomes in digital financial transactions.

4.5 Discussion

The results of this study empirically demonstrate that blockchain implementation significantly enhances the security of digital financial transaction data in Indonesia, as reflected by the high regression coefficient, which indicates that improvements in key blockchain characteristics—such as decentralization, immutability, and cryptographic security—are strongly associated with increased perceptions of data confidentiality, integrity, transparency, and fraud prevention [18]. These findings support the theoretical argument that blockchain's decentralized ledger structure minimizes single points of failure and reduces opportunities for data manipulation, leading respondents to perceive blockchain-based systems as more trustworthy than conventional centralized financial systems, a perception that is consistent with prior studies emphasizing the role of blockchain in strengthening transaction transparency and auditability as critical mechanisms for fraud mitigation in digital finance [19], [20].

Furthermore, the relatively high R^2 value suggests that blockchain implementation plays a substantial role in shaping data security perceptions among digital finance users in Indonesia, although the remaining unexplained variance indicates that other factors—such as regulatory frameworks, user literacy, and institutional trust—may also influence digital financial security and warrant further investigation in future research. Overall, this study provides robust quantitative evidence of blockchain technology's potential as a strategic solution for enhancing the security of digital financial transaction data, offering important practical implications for financial institutions and policymakers to consider blockchain adoption as part of the development of a secure and trustworthy digital financial ecosystem in Indonesia.

5. Conclusion

This study concludes that the implementation of blockchain technology has a positive and significant impact on the security of digital financial transaction data in Indonesia. The empirical findings demonstrate that blockchain's core characteristics—such as decentralization, immutability, transparency, and cryptographic protection—effectively enhance data confidentiality, integrity, and resistance to fraud. The results also indicate that blockchain implementation contributes substantially to users' perceptions of trust and security in digital financial services. Despite these promising outcomes, a portion of data security is influenced by other factors beyond blockchain, suggesting the need for further research incorporating regulatory, institutional, and behavioral dimensions. Overall, this study provides valuable empirical evidence for financial institutions and policymakers to consider blockchain adoption as a key component in developing a secure and sustainable digital financial ecosystem in Indonesia.

Reference

[1] M.-S. Jameaba, "Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Industry and Beyond," *DOI https//doi. org/10.32388/CSTTYQ*, vol. 2, 2022.

[2] M. C. El Amri, M. O. Mohammed, and A. M. Bakr, "Enhancing financial inclusion using FinTech-Based payment system," in *Islamic FinTech: Insights and Solutions*, Springer, 2021, pp. 191–207.

[3] A. Oladinni and O. O. Odumuwagun, "Enhancing cybersecurity in fintech: safeguarding financial data against evolving threats and vulnerabilities," *Int. J. Comput. Appl. Technol. Res.*, vol. 14, no. 1, pp. 62–78, 2025.

[4] D. Sudiantini, P. P. Rizky, and A. Hazarika, "Digital economy and financial inclusion in reviving the national economy: A Management Strategy," *Revenue J. Manag. Entrep.*, vol. 1, no. 1, pp. 64–75, 2023.

[5] E. Paul *et al.*, "Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors," *Int. J. Soft Comput.*, vol. 14, no. 3, pp. 1–16, 2023.

[6] A. Gawanmeh and J. N. Al-Karaki, "Disruptive technologies for disruptive innovations: Challenges and opportunities," in *ITNG 2021 18th International Conference on Information Technology-New Generations*, Springer, 2021, pp. 427–434.

[7] C. Komalavalli, D. Saxena, and C. Laroiya, "Overview of blockchain technology concepts," in *Handbook of research on blockchain technology*, Elsevier, 2020, pp. 349–371.

[8] A. Adejumo and C. Ogburie, "Strengthening finance with cybersecurity: Ensuring safer digital transactions," *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 1527–1541, 2025.

[9] M. A. Adegbite, "DATA PRIVACY AND DATA SECURITY CHALLENGES IN DIGITAL FINANCE," *J. Digit. Secur. Forensics*, vol. 2, no. 1, pp. 6–19, 2025.

[10] S. S. Sarmah, "Understanding blockchain technology," *Comput. Sci. Eng.*, vol. 8, no. 2, pp. 23–29, 2018.

[11] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Comput. Sci.*, vol. 9, p. e1705, 2023.

[12] D. Yermack and A. Fingerhut, "Blockchain technology's potential in the financial system," in *Proceedings of the 2019 financial market's conference*, sn, 2019.

[13] T. Kukman and S. Gričar, "Blockchain for quality: Advancing security, efficiency, and transparency in financial systems," *FinTech*, vol. 4, no. 1, p. 7, 2025.

[14] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *2016 2nd international conference on contemporary computing and informatics (IC3I)*, IEEE, 2016, pp. 463–467.

[15] T. M. Tan and S. Saraniemi, "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," *J. Acad. Mark. Sci.*, vol. 51, no. 4, pp. 914–939, 2023.

[16] D. Sugiyono, *Metode penelitian kuantitatif kualitatif dan R&D*. 2017.

[17] Sugiyono, *Metode Penelitian Kuantitatif Kualitatif dan R&D*. Bandung: Alfabeta, 2010.

[18] T. W. E. Suryawijaya and M. E. S. Wibowo, "Enhancing data security by blockchain technology: Investigating the effective execution of digital transformation initiatives in Indonesia," *Glob. Policy J. Int. Relations*, vol. 11, no. 02, 2023.

[19] D. Roeck, H. Sternberg, and E. Hofmann, "Distributed ledger technology in supply chains: a transaction cost perspective," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2124–2141, 2020.

[20] D. P. Mishra, R. K. Kukreja, and A. S. Mishra, "Blockchain as a governance mechanism for tackling dark side effects in interorganizational relationships," *Int. J. Organ. Anal.*, vol. 30, no. 2, pp. 340–364, 2022.