Journal of Web Innovation and Technologies
E-ISSN (xxxx-xxxx) P-ISSN (xxxx-xxxx)

The Role of Blockchain in Enhancing Security and Privacy in Digital Transactions

Mar'atus Solikhah
STMIK LIKMI, Indonesia
Corresponding email: maratussholikhah615@gmail.com

Abstract

Security and privacy in digital transactions have become major concerns as the use of online platforms across various sectors increases. Blockchain presents a promising technology with its decentralization, transparency, and robust encryption capabilities to ensure data integrity and confidentiality. This research aims to explore blockchain's role in enhancing the security and privacy of digital transactions and identify implementation challenges.

The research method used a qualitative approach with case studies on five blockchain-based e-commerce platforms and involved 100 active users. Data were collected through interviews, questionnaires, and observations, then analyzed using thematic analysis techniques and descriptive statistics. The results showed that more than 80% of respondents felt blockchain provided a higher level of security than traditional systems, while 70% of users reported an increased sense of security in data privacy. Blockchain has been proven to reduce the risk of transaction fraud and information leakage by giving users full control over their personal data.

However, this research also revealed barriers, particularly related to scalability, cost, and transaction speed. Identified solutions include utilizing more efficient consensus mechanisms such as proof-of-stake and implementing layer-two technologies like the Lightning Network. The findings demonstrate blockchain's transformative potential in creating trustless digital transaction environments while highlighting the necessity for technological advancement in consensus algorithms and network infrastructure. This study contributes theoretical insights into blockchain's privacy-preserving mechanisms and provides practical frameworks for organizations considering blockchain adoption in their digital transaction systems. Thus, blockchain has significant potential to revolutionize digital witnessing by enhancing security and privacy, although further innovation is needed for its widespread and sustainable adoption.

Keywords : Blockchain, Digital Security, Data Privacy, Digital Transactions, Encryption

1. Introduction

Data security and privacy have become critical issues in the growing number of digital transactions, both in the financial, trade, and government sectors (Anderson et al., 2021; Kumar & Shukla, 2022). According to the 2024 Global Cybersecurity Report, cybercrime costs are projected to reach $10.5 trillion annually by 2025,

with data breaches affecting over 4.1 billion records globally in 2023 alone. Digital commerce and transactions requiring high trust on web-based platforms often face challenges related to data leaks, information manipulation, and cyberattacks that can harm both users and service providers (Nguyen et al., 2020). The European Union's General Data Protection Regulation (GDPR) and similar privacy regulations worldwide have intensified the need for robust data protection mechanisms, imposing fines of up to 4% of annual global turnover for non-compliance.

One technological innovation believed to improve security and privacy in digital transactions is blockchain technology. Blockchain, first introduced through cryptocurrencies like Bitcoin, is now being implemented in various sectors to secure digital transactions and user data (Smith et al., 2019; Zhao et al., 2021)**.** The global blockchain market, valued at $7.18 billion in 2022, is projected to grow at a CAGR of 87.7% from 2023 to 2030, indicating widespread recognition of its transformative potential**.**

With the increasing adoption of e-commerce and the digitalization of financial services, the need for technology that can guarantee the security and privacy of user data is increasingly pressing (Brown & Green, 2020). Recent high-profile data breaches, including the 2023 MOVEit vulnerability that affected over 2,100 organizations globally, underscore the urgency for more secure transaction systems. However, although blockchain has been implemented in various industries, technical challenges and mass adoption remain obstacles that need to be overcome. Therefore, it is important to explore more deeply how blockchain can be optimized to strengthen security systems and maintain data confidentiality in digital transactions (Choi et al., 2020). This research addresses the critical gap in understanding how blockchain technology can be strategically implemented to address contemporary digital privacy challenges while maintaining operational efficiency.

Blockchain is known for its decentralized, transparent, and secure nature through the use of strong encryption techniques. Data recorded in a blockchain cannot be altered without the consent of the entire network, making it ideal for enhancing the integrity and security of digital transactions (Kumar et al., 2020). A study by Zhang & Tan (2021) shows that the use of blockchain in digital payment systems can reduce the potential for fraud and data leakage, which are major problems in online transactions. In this regard, blockchain provides a more secure and reliable solution compared to traditional systems that still rely on intermediaries or centralized institutions.

Several previous studies have explored the application of blockchain in various contexts, such as financial transactions, medical data management, and digital identity security (Miller & Harrison, 2020; Lee & Kim, 2021). However, while many have discussed blockchain's potential to enhance the security of digital transactions, few have focused on how blockchain can enhance user data privacy specifically in broader transactions, such as e-commerce and non-financial transactions on digital platforms (Patel & Verma, 2020; Zhang et al., 2022). Existing literature primarily concentrates on cryptocurrency applications, leaving a significant research void in understanding blockchain's role in protecting personal data across diverse digital transaction ecosystems**.**

The research gap becomes more apparent when examining the intersection of blockchain technology with emerging privacy regulations and user expectations. While technical studies have extensively documented blockchain's cryptographic capabilities, there remains limited empirical evidence on user perceptions of blockchain-enhanced privacy in real-world digital transaction scenarios. Although numerous studies have addressed the fundamental theory of blockchain and its applications in specific sectors, the lack of research examining the direct impact of blockchain on user data privacy across various types of digital transactions constitutes a major gap in the existing literature (Miller et al., 2019; Wang & Tan, 2020). Furthermore, most studies focus on Western contexts, with limited research examining blockchain adoption challenges in emerging economies where digital transaction growth is most rapid.

Many studies focus solely on the technical aspects of blockchain without considering the practical implications of its real-world use, such as scalability, implementation costs, and integration with existing systems. The disconnect between theoretical blockchain capabilities and practical implementation challenges represents a critical knowledge gap that this study aims to address**.** Therefore, this study aims to fill this gap by analyzing the application of blockchain in the context of digital transaction privacy and security.

This study is unique in that it integrates blockchain technical analysis with case studies on various digital transaction platforms that prioritize user data security and privacy. While many studies emphasize blockchain's potential in the financial sector, this study develops a new perspective by exploring blockchain applications across a broader range of sectors, including e-commerce, online education, and public administration systems (Chang & Liu, 2021). By employing a mixed-methods approach that combines technical analysis with user perception studies, this research provides a comprehensive understanding of blockchain's practical impact on digital transaction security and privacy**.** Thus, this study contributes to a more holistic understanding of blockchain's potential to strengthen data privacy and security across various digital transactions.

The urgency of this research is further underscored by the accelerating digital transformation post-COVID-19, which has increased digital transaction volumes by over 300% globally. With remote work, digital payments, and online services becoming the norm, the need for robust, privacy-preserving transaction mechanisms has never been more critical. The primary objective of this research is to explore how blockchain technology can be applied to enhance security and privacy in digital transactions, as well as to identify potential challenges and opportunities arising from its use. Specifically, this study seeks to: (1) evaluate the effectiveness of blockchain in enhancing digital transaction security, (2) assess user perceptions of blockchain-based privacy protection, (3) identify implementation barriers and practical solutions, and (4) provide evidence-based recommendations for stakeholders considering blockchain adoption. **It** also aims to provide insights into how blockchain can address key issues in digital transactions, such as fraud, data theft, and personal information leakage. It also aims to provide practical recommendations for companies and policymakers on implementing blockchain to enhance user data privacy and security in the future.

2. Method

Type:

This research uses a qualitative approach with a case study method. This qualitative approach was chosen to explore the application of blockchain technology in improving the security and privacy of digital transactions. The case study method allows researchers to explore in depth how blockchain is used in real-world practice to address security and privacy issues on digital platforms.

Population and Sample (Population and Sampling)

The population in this study is digital platforms that implement blockchain for the security and privacy of digital transactions. The research sample consists of two main groups:

1. E-commerce Platforms and Digital Services: This sample includes five major e-commerce platforms that use blockchain technology to enhance the security and privacy of user data.
2. Platform Users: This sample consists of 100 active users who use these platforms for digital transactions and have experience in transacting through blockchain-based systems.

The sample was selected using a purposive sampling technique, where respondents were selected based on certain criteria, namely users involved in digital transactions on platforms that adopt blockchain and service providers that actively integrate this technology.

Research Instruments

The instruments used in this research include:

1. Semi-Structured Interviews: Interviews were conducted with blockchain technology managers or developers involved in implementation on digital platforms. The purpose of these interviews was to gain in-depth information about the challenges, benefits, and processes of blockchain implementation.
2. Questionnaire: A questionnaire was distributed to 100 users to collect data related to their perceptions of data security and privacy in digital transactions using blockchain.
3. Observation: Observations were made of user interactions with digital platforms to assess user experiences regarding the security and privacy offered by blockchain technology.

Data Collection Technique (Data Collection Technique)

Data is collected using the following three techniques:

1. Interviews: Semi-structured interviews were conducted with five managers and developers from e-commerce platforms using blockchain. The purpose of these interviews was to understand how blockchain is implemented, as well as the challenges and solutions encountered in its implementation.
2. Questionnaire: A questionnaire was distributed to 100 users to gather information about their perceptions of the security and privacy provided by blockchain. The questionnaire included questions related to users' levels of trust, satisfaction, and concerns regarding their data privacy.

3. Observations: Observations were conducted on five digital platforms that use blockchain for digital transactions. Researchers observed user interactions and how security and privacy features were implemented in everyday user experiences.

Research Procedure

The research procedure consists of the following stages:

1. Preparation: Develop research instruments, including questionnaires and interview guides. Additionally, select a digital platform that implements blockchain technology.
2. Data Collection: Data was collected through interviews with platform managers and developers, questionnaires distributed to users, and observations of user interactions with the platform. Interviews and observations were conducted over a four-week period.
3. Data Analysis: Data obtained from interviews, questionnaires, and observations will be analyzed to identify key themes related to security and privacy in digital transactions using blockchain.
4. Reporting: The results of the analysis will be compiled in the form of a research report that includes findings, discussions, and recommendations related to the use of blockchain in improving the security and privacy of digital transactions.

Ethical Considerations

All participants provided informed consent before data collection. Confidentiality was maintained by anonymizing all personal identifiers and storing data securely. The research protocol was approved by the institutional ethics committee, ensuring compliance with data protection regulations.

Data Analysis Technique:

Qualitative data obtained from interviews and observations will be analyzed using thematic analysis. This technique involves coding the data to identify key themes related to blockchain's application in improving security and privacy. To ensure coding reliability, two independent researchers performed initial coding, with inter-coder agreement of 85% achieved through iterative discussion and refinement. Furthermore, quantitative data from the questionnaire will be analyzed using descriptive statistics to illustrate user satisfaction with the security and privacy provided by blockchain. Data triangulation was employed by comparing findings across different data sources (interviews, questionnaires, observations) to enhance validity and reliability of the results. This analysis will provide an overview of how blockchain impacts the user experience in terms of security and privacy in digital transactions.

3. Results & Discussion

Implementation of Blockchain in Improving Digital Transaction Security

The use of blockchain to improve the security of digital transactions has shown very positive results. Data obtained from interviews with e-commerce platform managers and users shows that more than 80% of the 100 users surveyed

felt that blockchain systems provided a higher level of security compared to traditional systems, which are more vulnerable to hacking (Smith et al., 2019; Zhao et al., 2021). Users reported that the use of decentralized technology in blockchain reduces the risk of transaction fraud, and the reliability of encryption ensures that transaction data remains secure.

Blockchain uses a decentralized and encrypted data structure, making it nearly impossible for third parties to alter or manipulate it (Nguyen et al., 2020). According to Zhang & Tan (2021), the transparency and audibility offered by blockchain provide an additional layer of protection against cyber threats. This technology also reduces reliance on central authorities, which are vulnerable to attacks, a problem in traditional payment systems (Choi et al., 2020). The security offered by blockchain also allows companies to build trust with users, which is crucial in e-commerce and digital financial services.

International case studies demonstrate similar findings. The implementation of blockchain in Estonia's e-Residency program has processed over 1 million secure digital transactions without a single reported security breach since 2014. Similarly, Walmart's blockchain-based food traceability system has reduced the time required to trace contaminated products from weeks to seconds, demonstrating blockchain's practical security applications beyond financial transactions.

However, challenges remain, particularly regarding blockchain scalability, which can hinder the processing of very large transactions in a short time (Patel & Verma, 2020). While this technology offers very robust security solutions, transaction speed and network capacity remain major concerns for industries that rely on high transaction volumes. Comparative analysis with traditional systems reveals that while blockchain processes 7-15 transactions per second compared to Visa's 24,000, emerging solutions like sharding and layer-2 protocols are addressing these limitations.

Table 1: Improving Digital Transaction Security with Blockchain

Security Features	Impact on Transaction Security (%)
Decentralization	85%
Data Encryption	90%
Transparency	80%

Source: Research Data (2022)

Blockchain in Improving User Data Privacy

The use of blockchain in digital transactions also shows significant improvements in data privacy. Based on questionnaire results, approximately 70% of users who transact on blockchain-based platforms feel more secure in terms of their personal data privacy compared to platforms that do not use blockchain (Kumar et al., 2020; Lee & Kim, 2021). This is due to blockchain's ability to control access to personal data, allowing only authorized parties to access sensitive information.

Blockchain enables self-sovereign identity management, where users have full control over their personal data (Miller & Harrison, 2020). The use of smart contracts allows transactions to occur only if certain conditions are met, without the need for third parties who could misuse user information (Patel & Verma, 2020). According to Choi et al. (2020), this privacy is particularly important in the e-commerce and financial services sectors, where customer data is often the target of theft and misuse.

The implementation of zero-knowledge proofs in blockchain systems further enhances privacy by enabling transaction validation without revealing sensitive information. Projects like Zcash and Monero demonstrate how blockchain can provide complete transaction privacy while maintaining network security and integrity.

While blockchain promises increased privacy, issues related to decentralized data storage remain to be resolved. Given that every node in a blockchain network holds a copy of transactions, this can potentially create problems related to managing and accessing large amounts of personal data (Wang & Tan, 2021). However, emerging solutions like off-chain storage and encrypted data sharding are addressing these concerns by storing only hashed references on-chain while maintaining actual data in secure, encrypted off-chain repositories.

Regulatory frameworks are evolving to accommodate blockchain privacy features. The GDPR's "right to be forgotten" initially appeared incompatible with blockchain's immutability, but solutions using encrypted data with deletable keys are emerging as viable compromises between regulatory compliance and blockchain benefits.

Challenges and Solutions in Blockchain Implementation in Digital Transactions

Although blockchain offers robust security and privacy solutions, its implementation in digital transactions still faces several challenges. Data from interviews with platform managers revealed that 60% of them faced challenges in terms of blockchain scalability to handle high transaction volumes in a short time (Brown & Green, 2020). Furthermore, transaction fees associated with blockchain are also a barrier, as each transaction requires higher processing fees compared to traditionalsystems.

One of the biggest challenges in implementing blockchain is its ability to process transactions quickly and efficiently. According to Zhang et al. (2022), although blockchain is highly secure, the transaction verification process can take a long time, especially if the network has many nodes. This leads to transaction delays, which can be detrimental to users who value speed. One proposed solution is the use of blockchains with more efficient consensus systems, such as proof-of-stake (PoS), which can reduce the computational burden and increase transaction speed (Nguyen et al., 2020).

The energy consumption challenge is significant, with Bitcoin's network consuming approximately 110 TWh annually. However, proof-of-stake consensus mechanisms reduce energy consumption by over 99%, as demonstrated by

Ethereum's transition to Ethereum 2.0, which decreased its energy usage from 112 TWh to 0.01 TWh annually.

Additionally, to address transaction cost issues, companies can use second-layer solutions such as the Lightning Network, which enables faster transactions at lower costs, without compromising security (Patel & Verma, 2020). interoperability protocols like Polkadot and Cosmos are also emerging as solutions to blockchain fragmentation, enabling seamless asset and data transfer across different blockchain networks.

Policy and regulatory considerations vary significantly across jurisdictions. While countries like Switzerland and Singapore have developed comprehensive blockchain-friendly regulations, others maintain restrictive approaches that hinder adoption. The regulatory uncertainty creates additional implementation challenges for organizations considering blockchain integration.

For industries beyond e-commerce, blockchain applications show promising results. In healthcare, blockchain-based medical records ensure patient privacy while enabling secure data sharing among authorized providers. In education, blockchain credentials prevent diploma fraud while giving students control over their academic records. Government applications include secure voting systems and transparent public service delivery, demonstrating blockchain's versatility across sectors.

Table 2: Challenges of Blockchain Implementation in Digital Transactions

Challenge	Percentage of Managers Experiencing Problems (%)
Scalability	60%
Transaction Fees	55%
Transaction Speed	50%

Source: Research Data (2022)

4. Conclusion

This research shows that the application of blockchain technology in digital transactions has a significant impact on improving data security and privacy. Blockchain provides a more secure solution with its decentralization, encryption, and transparency, reducing the risk of data leaks and transaction fraud. Furthermore, blockchain also enhances user data privacy by giving users full control over their personal information, which is crucial in digital transactions.

However, challenges related to scalability, transaction costs, and speed remain obstacles to widespread blockchain implementation. Therefore, while blockchain offers many advantages in terms of security and privacy, further innovation is needed to increase efficiency and reduce costs, such as the use of layer-two technologies or more efficient consensus systems

5. References

Brown, A., & Green, T. (2020). *Blockchain: A new era in digital transactions*. Journal of Digital Innovation, 5(2), 45-60.

Choi, W., Lee, S., & Kim, Y. (2020). *The role of blockchain in securing digital transactions*. Journal of Information Security, 35(1), 102-115.

Kumar, S., & Shukla, A. (2020). *Blockchain technology: Implications for digital transaction security*. International Journal of Cyber Security, 8(3), 123-134.

Lee, J., & Kim, H. (2021). *Leveraging blockchain for enhanced privacy in e-commerce transactions*. Journal of Digital Privacy, 10(3), 234-245.

Miller, A., & Harrison, T. (2020). *Blockchain in e-commerce: Enhancing trust and security*. Journal of Business Research, 68(4), 78-85.

Nguyen, T., Tran, P., & Vu, H. (2020). *Blockchain for digital privacy: A review of applications and challenges*. Journal of Privacy and Security, 6(2), 59-74.

Patel, R., & Verma, A. (2020). *Blockchain: The future of privacy and security in digital transactions*. International Journal of Technology Management, 52(3), 67-79.

Wang, J., & Tan, C. (2021). *Data security and blockchain technology*. Journal of Information Technology and Security, 19(1), 91-105.

Zhang, L., Wu, Q., & Tan, J. (2022). *Blockchain for secure digital transactions: Trends and future perspectives*. Journal of Digital Transactions, 12(4), 202-215.