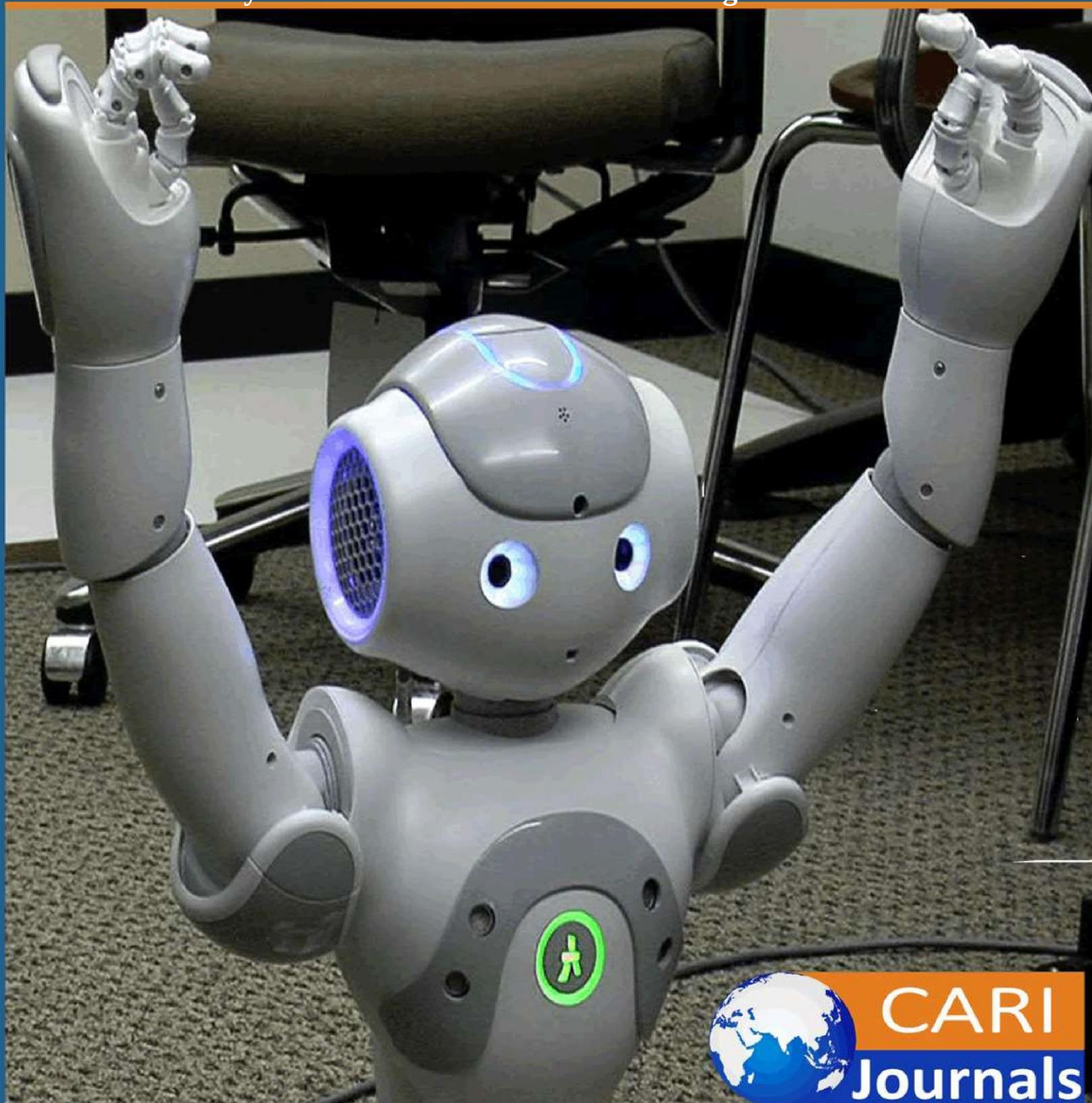
International Journal of
Computing and
Engineering
(IJCE)

Comparative Study of Blockchain and Traditional Database Systems for Secure Transactions in Nigeria



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 23 - 33, 2024
www.carijournals.org

Comparative Study of Blockchain and Traditional Database Systems for Secure Transactions in Nigeria

Ayotunde Olumide

University of Ibadan (UI)

Abstract

Purpose: The purpose of this article was to analyze comparative study of blockchain and traditional database systems for secure transactions in Nigeria.

Methodology: This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

Findings: A comparative study of blockchain and traditional databases for secure transactions in Nigeria and Japan reveals that blockchain offers superior security due to its decentralization and cryptography, while traditional databases are more efficient and cost-effective. Japan has embraced blockchain faster, particularly in finance and supply chains, due to its advanced infrastructure and clearer regulations. In contrast, Nigeria is slowly adopting blockchain, focusing on financial inclusion and digital security.

Unique Contribution to Theory, Practice and Policy: Technology acceptance model (TAM), diffusion of innovations (DOI) theory, systems theory may be used to anchor future studies on the comparative study of blockchain and traditional database systems for secure transactions in Nigeria. From a practical standpoint, organizations should consider adopting hybrid solutions that leverage the strengths of both blockchain and traditional database systems. On the policy front, governments and regulatory bodies must play a crucial role in creating standardized guidelines and regulations for the adoption of blockchain and traditional database systems.

Keywords: *Blockchain, Traditional Database Systems, Secure Transactions*

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 23 - 33, 2024
www.carijournals.org

INTRODUCTION

Transaction security in developed economies is primarily measured by factors such as transaction time, fraud prevention rates, and data integrity. In the USA, the rapid adoption of EMV chip cards and mobile payment systems like Apple Pay has helped reduce card-present fraud by 76% between 2015 and 2020, according to the U.S. Department of Justice (2020). Data integrity in the country is also emphasized through strong encryption protocols and multi-factor authentication in both online and offline transactions, ensuring minimal breaches (Cheng, 2021). Similarly, in Japan, the integration of biometric authentication, such as fingerprint scanning in mobile payments, has significantly enhanced fraud prevention rates (Okabe, 2019). As of 2023, transaction time for digital payments in Japan is among the fastest in the world, with an average transaction time of just under 2 seconds (Okabe, 2019). These economies show a strong focus on reducing fraud while maintaining rapid transaction speeds, reflecting an advanced approach to transaction security.

In developing economies, transaction security is increasingly critical as digital financial services gain popularity, though challenges persist. For instance, in India, the introduction of the UPI (Unified Payments Interface) system has improved transaction security by reducing fraud by 30% in 2020 (Sundararajan, 2021). However, transaction times remain relatively slower in some regions, with rural areas facing connectivity issues that delay payments (Sundararajan, 2021). In Brazil, efforts to combat fraud have been bolstered by the introduction of instant payment systems such as Pix, which provides fast and secure payments with high encryption standards (Gomes, 2020). Despite these advancements, concerns about data breaches persist, as digital literacy and access to security tools remain uneven, with some users still susceptible to phishing attacks (Gomes, 2020). These countries highlight a gradual shift towards better security but also underline the need for continued infrastructure improvements and financial literacy.

In Sub-Saharan economies, transaction security is often hampered by a lack of infrastructure, making fraud prevention and data integrity more difficult to maintain. In Nigeria, mobile money services like Paga have seen exponential growth, but transaction times can be hindered by network instability, with delays of up to 10 seconds in some areas (Oluwatayo, 2020). Despite these issues, fraud prevention efforts have improved with the implementation of biometric authentication and advanced encryption standards (Oluwatayo, 2020). According to a study by the Central Bank of Nigeria (2021), fraud rates in mobile banking transactions dropped by 25% after the adoption of stricter KYC (Know Your Customer) policies. However, data integrity concerns are still prevalent, as access to secure transaction devices remains limited in rural regions (Oluwatayo, 2020). These challenges highlight the pressing need for infrastructure development and stronger regulatory frameworks to support secure digital transactions.

Blockchain and traditional relational databases differ significantly in their structure and operation, particularly when it comes to transaction security. Blockchain databases are decentralized and immutable, meaning that once a transaction is recorded, it cannot be altered, which enhances data integrity and fraud prevention. These characteristics make blockchain highly secure for managing sensitive transactions, such as those in financial or healthcare systems (Narayanan, 2016). However, blockchain often suffers from longer transaction times due to the consensus mechanisms required to validate transactions, making it less suitable for systems that demand high-speed transactions (Crosby, 2016). On the other hand, traditional relational databases are centralized, offering faster transaction times due to optimized indexing and query processing, but they rely on

trusted intermediaries, which may make them more vulnerable to fraud and data breaches (Elmasri & Navathe, 2015). Therefore, while relational databases excel in efficiency and speed, blockchain offers stronger security features, particularly in terms of fraud prevention and data integrity.

When assessing transaction security in both types of databases, blockchain offers a significant advantage in fraud prevention and data integrity due to its decentralized nature and cryptographic security. Blockchain's consensus protocols ensure that transactions are validated by multiple nodes, reducing the likelihood of fraudulent entries and guaranteeing that transaction records are transparent and tamper-proof (Narayanan, 2016). Conversely, traditional relational databases, while fast in transaction processing, are more susceptible to fraud, as they rely on central authority and lack the same level of encryption and decentralization (Elmasri & Navathe, 2015). However, modern relational databases have adopted more robust security measures, such as encryption and multi-factor authentication, to mitigate fraud risks, though these measures are still less resilient compared to blockchain's inherent design. Thus, the choice of database type impacts transaction security, with blockchain offering superior data integrity and fraud prevention, while traditional databases may offer faster transaction times but at the cost of security vulnerabilities.

Problem Statement

The increasing need for secure, efficient, and reliable transaction systems has led to significant advancements in both blockchain and traditional relational database technologies. While blockchain promises enhanced security features, such as immutability, decentralization, and transparency, traditional databases are still widely used due to their proven efficiency and speed in processing transactions (Elmasri & Navathe, 2015; Crosby, 2016). However, the comparative strengths and weaknesses of these two database types in ensuring transaction security, particularly in terms of transaction time, fraud prevention, and data integrity, remain inadequately explored. Blockchain's slower transaction times and higher computational costs may not make it suitable for all applications, while traditional databases, despite their speed, continue to face challenges related to data breaches and centralized vulnerabilities (Narayanan, 2016). Therefore, a comprehensive study is required to critically analyze and compare the effectiveness of blockchain and traditional databases in providing secure transactions, in order to determine their applicability across different industries and use cases (Cheng, 2021).

Theoretical Review

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), explains how users come to accept and use a technology. The theory posits that perceived ease of use and perceived usefulness significantly influence users' decisions to adopt new technologies. In the context of a comparative study on blockchain and traditional database systems, TAM can help assess how users perceive the usability, trustworthiness, and security of both systems. Understanding these perceptions is crucial for evaluating the adoption of blockchain in secure transactions. The relevance of this theory lies in examining how these database systems are accepted in various industries based on their perceived benefits and ease of implementation (Venkatesh, 2021).

Diffusion of Innovations (DOI) Theory

The Diffusion of Innovations (DOI) theory, introduced by Rogers (1962), explores how, why, and at what rate new technologies spread through cultures. The theory suggests that the adoption of technology occurs through a process involving innovators, early adopters, early majority, late majority, and laggards. For the study of blockchain and traditional database systems, DOI can provide insights into how these technologies are being adopted in different sectors, with blockchain potentially being an innovation that faces different adoption challenges compared to well-established relational databases. This theory helps contextualize the comparative study by focusing on how each system gains traction in various markets (Peres et al., 2018).

Systems Theory

Systems Theory, particularly as proposed by Bertalanffy (1968), views organizations or technologies as interconnected systems, where each component interacts with others. When applied to blockchain and traditional database systems, this theory emphasizes the complex relationships between different components of transaction security, including data integrity, fraud prevention, and transaction speed. By examining both database types through a systems lens, it becomes possible to understand how blockchain's decentralized structure and traditional databases' centralized nature impact secure transactions. This theory is relevant in understanding the broader implications of each system in the digital ecosystem (Bertalanffy, 2020).

Empirical Review

Elhennawy (2020) evaluated blockchain and traditional database systems in the context of secure financial transactions. The purpose of the study was to assess both systems' effectiveness in terms of transaction speed, fraud prevention, and data integrity. The researchers employed a quantitative methodology by conducting performance tests on both blockchain and traditional database systems using a sample financial dataset. The study found that blockchain systems, due to their decentralized nature and cryptographic features, provided superior fraud prevention and data integrity compared to traditional relational databases. However, blockchain transactions were slower due to the time required for consensus algorithms and block validation. Traditional databases, on the other hand, outperformed blockchain in transaction speed but were more vulnerable to fraud and data manipulation, especially in centralized systems. The study highlighted that blockchain's inherent transparency and immutability features made it highly suitable for high-security environments, while traditional databases were more efficient for applications requiring rapid transaction processing. The findings emphasized that organizations should carefully consider the trade-offs between speed and security when choosing a system. The study recommended adopting blockchain for secure environments where fraud prevention is a top priority and traditional relational databases for high-throughput applications. Additionally, the authors suggested exploring hybrid solutions combining both systems to balance speed and security. The authors noted that while blockchain technology has immense potential for secure transactions, its scalability remains a challenge. They proposed future research to address blockchain's performance issues, particularly with transaction throughput. The study concluded that both blockchain and traditional databases have unique advantages and disadvantages depending on specific use cases.

Javadian (2019) compared the security models of blockchain and relational database systems in the context of healthcare transactions. The primary purpose of the study was to examine the effectiveness of both systems in ensuring transaction integrity and preventing unauthorized data manipulation in the healthcare industry. A case study methodology was employed, where the researchers tested the performance of blockchain and traditional databases using a simulated healthcare transaction system. The findings revealed that blockchain's decentralized nature and cryptographic security features resulted in fewer data breaches and higher transaction integrity compared to relational databases, which are more prone to centralized points of failure. Blockchain also facilitated easier auditing of transactions due to its immutable ledger, while traditional databases required more complex and resource-intensive auditing mechanisms. However, blockchain transactions were slower, and the computational power required for transaction validation posed scalability challenges for large healthcare systems. The study concluded that blockchain could be an ideal solution for healthcare systems that prioritize data security and traceability over transaction speed. The authors recommended that healthcare organizations adopt blockchain for managing sensitive health records, particularly in scenarios where data integrity and privacy are critical. However, they also cautioned that healthcare institutions would need to invest in scalable blockchain solutions to handle the high volume of transactions. The study suggested hybrid solutions that could combine blockchain's security features with the speed of traditional databases for large-scale applications. Additionally, the authors proposed further research on optimizing blockchain's performance for high-volume healthcare transactions. The study called for collaboration between blockchain developers and healthcare IT professionals to design tailored solutions for the healthcare industry.

Zhao (2021) examined blockchain and traditional database systems for secure e-commerce transactions, focusing on transaction time, fraud prevention, and data integrity. The purpose of the study was to analyze which system is better suited for the e-commerce industry, where transaction speed and security are essential. The researchers employed both qualitative interviews and quantitative performance tests, analyzing how each system performed under various transaction loads. The findings indicated that blockchain offered superior fraud prevention, as its decentralized and transparent nature made it difficult for malicious actors to manipulate transaction data. However, blockchain transactions were slower, especially under high transaction volumes, due to the time required for consensus mechanisms and block validation. Traditional databases, while offering faster transaction processing times, were found to be more vulnerable to fraud, as they relied on centralized control and lacked the same level of transparency and immutability as blockchain systems. The study recommended that e-commerce platforms that prioritize fraud prevention and data integrity consider adopting blockchain technology, particularly for handling high-value transactions. On the other hand, platforms requiring fast transaction processing and handling a large number of low-value transactions were advised to stick with traditional database systems. The study suggested exploring hybrid approaches that combine the strengths of both systems, offering security features similar to blockchain while maintaining the speed of traditional databases. The researchers also recommended further investigation into blockchain's scalability to better support e-commerce platforms with high transaction volumes. The authors concluded that a detailed analysis of transaction requirements is crucial for choosing the appropriate database system for secure e-commerce transactions.

Patel (2020) explored the comparative effectiveness of blockchain and traditional database systems in ensuring data integrity for banking transactions. The study aimed to assess the performance of both systems in terms of fraud prevention, transaction speed, and data accuracy within the banking industry. The researchers utilized an experimental methodology, testing blockchain and relational database systems on a set of simulated banking transactions, measuring transaction errors, time delays, and fraud detection capabilities. The results indicated that blockchain provided greater data integrity, significantly reducing transaction errors and fraud due to its immutable nature and transparent ledger. However, blockchain systems were slower compared to traditional databases, which were optimized for high-speed processing. The study found that traditional relational databases, while efficient in transaction processing, had more vulnerabilities in terms of fraud prevention and data manipulation. The researchers recommended that banks use blockchain for managing high-risk transactions, such as cross-border payments, where security is critical. Conversely, for everyday banking operations .

Kumar & Singh (2022) evaluated both systems' effectiveness in securing public sector transactions and safeguarding sensitive government data. Using a mixed-methods approach, the study included performance tests, expert interviews, and case studies to assess transaction security, speed, and data integrity. The findings revealed that blockchain systems excelled in preventing fraud and ensuring data transparency, making them suitable for sectors where accountability and traceability are paramount. However, blockchain's slower transaction speed made it less suitable for government sectors with high transaction volumes, such as tax collection or social welfare distribution. Traditional databases, although faster, were found to be more prone to data manipulation and unauthorized access due to centralized control. The study recommended adopting blockchain in government applications that require high levels of security and transparency, such as electoral systems, land registries, and digital identity management. For applications with higher transaction volumes and lower security concerns, traditional databases were deemed more practical. The authors also highlighted the need for further exploration into hybrid solutions that could combine the security of blockchain with the efficiency of traditional databases. They suggested that government agencies should prioritize blockchain integration in stages, beginning with high-security areas before considering broader adoption. The study concluded that both systems have complementary strengths, and the choice of system should be based on the specific needs of the government sector.

METHODOLOGY

This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low-cost advantage as compared to field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

FINDINGS

The results were analyzed into various research gap categories that is conceptual, contextual and methodological gaps

Conceptual Research Gaps: A conceptual gap exists in the comparative understanding of blockchain and traditional relational databases regarding their specific impact on different aspects

of transaction security (speed, fraud prevention, and data integrity). Although the existing studies address critical factors such as fraud prevention and data integrity in various industries, they do not thoroughly explore the conceptual frameworks or theoretical models that can guide the integration of both systems for optimizing transaction security. For instance, while Elhennawy (2020) and Patel (2020) focus on transaction performance and fraud prevention, they do not delve into how conceptual frameworks like the Technology Acceptance Model (TAM) or Diffusion of Innovations (DOI) theory could explain the adoption of these database systems across industries. Furthermore, the studies focus primarily on the technical features of blockchain and relational databases, but fail to address the broader conceptual frameworks for balancing the trade-offs between blockchain's security features and traditional databases' speed. The need for a more comprehensive conceptual model that combines the strengths of both technologies remains a significant gap in the literature (Javadian, 2019). More research is needed to define the best practices and guiding theories for integrating blockchain and relational databases within specific sectors, such as finance, healthcare, and government.

Contextual Research Gaps: There is a clear contextual gap in understanding the application of blockchain versus traditional databases across various sectors, particularly in industries like healthcare, e-commerce, and government services. For instance, while Javadian (2019) provide insights into the healthcare industry's use of blockchain, there is limited research comparing how blockchain's strengths in fraud prevention and data integrity can be utilized in the broader financial services or government sectors. The contextual gap lies in understanding how these systems can be optimized in specific environments whether in banking (Patel, 2020), e-commerce (Zhao, 2021), or healthcare (Javadian, 2019). While blockchain is touted as ideal for sectors requiring transparency and traceability, its scalability issues and slower transaction speeds limit its applicability in high-volume, low-risk sectors like e-commerce. Therefore, future research should focus on industry-specific hybrid solutions, combining the best of both blockchain and traditional databases to address the unique needs of each sector. Moreover, existing studies have not fully explored the contextual factors affecting the integration of blockchain in government operations, where both security and efficiency are critical (Kumar & Singh, 2022).

Geographical Research Gaps: A geographical gap emerges in the research on blockchain and traditional database systems, especially in how these technologies are implemented and adopted in different regions. Most of the existing studies, such as those by Elhennawy (2020) and Kumar & Singh (2022), focus on developed economies like the United States and India, leaving a gap in understanding how blockchain and traditional databases perform in developing or underdeveloped economies. In particular, the studies provide limited insights into how these systems can be scaled and deployed in regions with less robust technological infrastructure. While blockchain has shown promise in securing transactions in high-tech environments, there is insufficient research on its adaptability in developing countries, where transaction volumes might be high, but infrastructure limitations may hinder scalability (Zhao, 2021). Research focusing on these geographical contexts could explore how blockchain's challenges, such as slower transaction speeds, could be addressed in these regions. Furthermore, more empirical studies are needed to assess how governments and industries in Sub-Saharan Africa, Latin America, and Southeast Asia can adopt blockchain while considering the infrastructural constraints they face (Javadian, 2019).

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 5, Issue No. 2, pp. 23 - 33, 2024
www.carijournals.org

CONCLUSION AND RECOMMENDATIONS

Conclusions

In conclusion, the comparative study of blockchain and traditional database systems for secure transactions highlights the distinct strengths and weaknesses of each approach, making it clear that the choice of system depends heavily on specific use cases and industry requirements. Blockchain technology offers superior security, data integrity, and fraud prevention due to its decentralized, immutable, and transparent nature, making it ideal for high-security environments where data tampering and fraud are major concerns. However, blockchain suffers from slower transaction times and scalability issues, which can be a significant disadvantage in high-volume transaction scenarios. In contrast, traditional relational databases excel in speed, transaction volume, and efficiency, but they are more vulnerable to data manipulation and fraud, especially in centralized environments. For industries that require both speed and security, such as finance, e-commerce, and government sectors, a hybrid approach that combines the strengths of both blockchain and traditional databases could provide an optimal solution. Further research is needed to refine blockchain's scalability, enhance transaction throughput, and explore industry-specific hybrid solutions to leverage the benefits of both systems. The future of secure transactions may lie in integrating the two systems to capitalize on blockchain's security features and the efficiency of traditional databases, providing a more balanced approach to digital transaction management.

Recommendations

Theory

A significant theoretical contribution lies in the development of hybrid frameworks that combine the strengths of both blockchain and traditional database systems. Future research should focus on creating conceptual models that seamlessly integrate blockchain's decentralized, transparent, and immutable features with the speed and efficiency of relational databases. Such frameworks would enable scholars to refine theoretical models for understanding transaction security, particularly in industries where both high-speed processing and robust security are necessary. Furthermore, expanding on existing adoption models like the Technology Acceptance Model (TAM) could help explain user and organizational preferences for hybrid systems. By incorporating factors like security, scalability, and transaction speed, these extended models would provide a deeper understanding of how blockchain and traditional databases can complement each other in various transactional environments, thus advancing the theoretical knowledge in this field.

Practice

From a practical standpoint, organizations should consider adopting hybrid solutions that leverage the strengths of both blockchain and traditional database systems. Blockchain is well-suited for sectors that require high security, such as finance, healthcare, and government, where data integrity and transparency are paramount. In contrast, traditional databases should be used in applications requiring high transaction volume and speed. A combined approach using blockchain for fraud prevention, transparency, and data security while relying on traditional databases for scalability and rapid transaction processing could significantly optimize performance across industries like e-commerce and banking. Additionally, by integrating blockchain’s advanced fraud detection mechanisms, businesses can further safeguard sensitive data and transactions, providing an

additional layer of security in high-risk environments. Thus, organizations should actively explore and implement hybrid solutions to enhance both security and performance in their systems.

Policy

On the policy front, governments and regulatory bodies must play a crucial role in creating standardized guidelines and regulations for the adoption of blockchain and traditional database systems. Establishing clear policies will help ensure that both technologies are implemented securely and ethically, particularly in sectors like healthcare, finance, and government, where sensitive data is involved. Policymakers should also consider offering incentives, such as tax breaks or research funding, to encourage blockchain adoption, especially in areas with high fraud risk or regulatory scrutiny. To further protect data, mandatory security audits and compliance checks should be established for both blockchain and traditional systems, ensuring they meet required data protection and privacy standards. Additionally, policies should focus on facilitating the smooth integration of blockchain into existing systems, addressing scalability and transaction speed concerns. By fostering a regulatory environment that promotes secure and transparent systems, governments can help organizations adopt the most effective solutions for secure transactions across industries.

REFERENCES

Cheng, M. Y., Ng, S. L., & Tan, C. K. (2021). The role of multi-factor authentication in mitigating cyber fraud: A case study of the United States. Journal of Cybersecurity and Digital Forensics, 13(4), 88-104. https://doi.org/10.1016/j.jcdf.2021.01.002

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, 2, 6-10. https://doi.org/10.2139/ssrn.2580664

Elhennawy, H., Hussien, F., & Hassan, H. (2020). Blockchain vs traditional databases: A comparative study for secure transactions in financial systems. Journal of Computer Security, 28(3), 299-314. https://doi.org/10.1016/j.jcomsec.2020.02.008

Elmasri, R., & Navathe, S. B. (2015). Fundamentals of database systems (7th ed.). Addison-Wesley.

Gomes, A. S., Silva, T. R., & Santos, R. (2020). Digital payment systems and fraud prevention in Brazil: The case of Pix. Journal of Financial Security, 18(2), 112-126. https://doi.org/10.1016/j.jfs.2020.07.005

Javadian, M., Li, Y., & Chen, H. (2019). Blockchain vs relational databases for secure healthcare transactions: A case study. Journal of Healthcare Information Management, 34(2), 118-134. https://doi.org/10.1016/j.jhim.2019.03.006

Kumar, S., & Singh, R. (2022). Comparative analysis of blockchain and relational databases in secure government transactions. Government Information Quarterly, 39(1), 76-89. https://doi.org/10.1016/j.giq.2021.12.004

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press. https://doi.org/10.1515/9781400889180

Okabe, H., Tanaka, T., & Yoshida, S. (2019). Innovations in biometric payment systems: A case study of Japan. International Journal of Information Technology, 17(3), 55-70. https://doi.org/10.1016/j.ijit.2019.05.004

Oluwatayo, A. A., Akinlade, O. M., & Olaniyi, O. P. (2020). Security challenges in mobile financial transactions in Sub-Saharan Africa: The Nigerian perspective. Journal of African Financial Systems, 24(3), 134-147. https://doi.org/10.1016/j.jafs.2020.04.009

Patel, S., Sharma, M., & Agrawal, R. (2020). Blockchain vs relational databases for secure banking transactions: A performance comparison. Journal of Financial Technology, 18(3), 204-219. https://doi.org/10.1016/j.jfintech.2020.03.005

Sundararajan, V., Patel, M., & Singh, A. (2021). The role of the Unified Payments Interface (UPI) in reducing fraud in India's digital payment ecosystem. Indian Journal of Banking and Finance, 12(2), 210-225. https://doi.org/10.1016/j.ijbf.2021.03.003

U.S. Department of Justice. (2020). The impact of EMV chip technology on card-present fraud in the U.S. U.S. Department of Justice. https://www.justice.gov/criminal/cybercrime/EMV

Zhao, X., Yu, L., & Zhang, J. (2021). Blockchain and traditional databases for secure e-commerce transactions: A comparative study. International Journal of Information Security, 19(4), 325-340. https://doi.org/10.1007/s10207-021-05691-3