ADI Journal on Recent Innovation (AJRI)
Vol. 6, No. 2, 2025, pp. 168−179
E-ISSN: 2686-0384 | P-ISSN: 2685-9106, DOI: 10.34306

Cybersecurity Risk Assessment Framework for Blockchain-Based Financial Technology Applications

Dini Dinarwati[1*], Muhammad Ghifari Ilham[2], Fransisca Rahardja[3]
[1]Master of Information Technology, Bank Negara Indonesia, Indonesia
[2]Department of Computer System, University of Raharja, Indonesia
[3]Department of Sports Psychology, University of Auckland, New Zealand
[1] dini.wati@bni.co.id, [2] ghifari.ilham@raharja.info, [3]frah877@aucklanduni.ac.nz
***Corresponding Author**

Article Info

Article history:

Received February 11, 2025
Revised February 28, 2025
Accepted March 01, 2025
Published March 19, 2025

Keywords:

Blockchain Technology
Cybersecurity Risk Assessment
Risk Mitigation
Security Framework
Data Privacy

ABSTRACT

The integration of blockchain technology into financial technology (fintech) applications has transformed the financial industry by offering enhanced transparency, efficiency, and trust. However, this integration also introduces complex cybersecurity challenges that could jeopardize data integrity, operational reliability, and user trust. To address these issues, this study aims to develop a **Cybersecurity Risk Assessment Framework** tailored specifically for blockchain-based fintech applications. Using a mixed-methods approach, the study combines qualitative insights from expert interviews with quantitative risk analysis techniques, including **Failure Mode and Effects Analysis (FMEA)**. This method facilitates the identification and evaluation of critical threats such as **smart contract vulnerabilities**, **consensus mechanism attacks**, and **unauthorized access to sensitive data**. The proposed framework is validated through case studies of existing blockchain-based fintech platforms to assess its practicality and robustness. Results show that the framework effectively identifies and mitigates potential risks, thereby improving system security and operational resilience. This research bridges the gap between theoretical cybersecurity principles and practical fintech applications, providing actionable strategies for industry practitioners and policymakers. The study concludes that adopting the framework enhances the security posture of blockchain-based fintech ecosystems, enabling innovation while safeguarding against evolving cybersecurity threats.

DOI: https://doi.org/10.34306/ajri.v6i2.1197

1. INTRODUCTION

Blockchain technology has revolutionized the financial technology (fintech) industry by providing a decentralized, secure, and transparent foundation for various applications, including peer-to-peer lending, smart contracts, and digital asset management [1]. Its ability to ensure immutability and trust in transactions has made it a critical enabler of financial innovation. However, the increasing reliance on blockchain-based platforms also introduces significant cybersecurity risks, which, if left unaddressed, could undermine the reliability and adoption of these technologies in the fintech ecosystem. Along with the technological risks, regulatory compliance challenges, such as adherence to GDPR (General Data Protection Regulation), PSD2 (Revised

Payment Services Directive), and the FATF guidelines on crypto transactions, must also be considered [2]. These regulatory frameworks are crucial for ensuring that blockchain-based fintech platforms meet the legal and security requirements in different jurisdictions, and failing to comply could have serious legal and financial consequences. Zero Trust frameworks, have been proposed, they often do not fully address the unique challenges of blockchain technology [3]. These models typically overlook the decentralized nature of blockchain and specific risks such as smart contract vulnerabilities and consensus manipulation attacks. As blockchain adoption grows in fintech applications, the need for a tailored cybersecurity risk assessment framework that accounts for these unique characteristics is more pressing than ever.

The cybersecurity challenges in blockchain-fintech systems are unique and multifaceted. Common threats include vulnerabilities in smart contracts, attacks on consensus mechanisms, and unauthorized data breaches, all of which can compromise the confidentiality, integrity, and availability of these platforms. While existing cybersecurity frameworks provide valuable guidance for traditional IT systems, they often fall short in addressing the specific requirements and complexities of blockchain technology. This highlights a critical gap in existing practices (GEP), as current methodologies lack sufficient consideration for the decentralized and immutable nature of blockchain [4]. Addressing these challenges necessitates a novelty approach that integrates blockchain-specific characteristics into risk assessment processes.

To bridge this gap, this study proposes a Cybersecurity Risk Assessment Framework specifically designed for blockchain-based fintech applications [5]. The framework aims to systematically identify, evaluate, and mitigate cybersecurity risks to enhance the security posture of these platforms. The research employs a mixed-methods approach, combining qualitative insights from experts with quantitative analysis techniques such as FMEA [6]. This integrated methodology ensures a comprehensive understanding of potential threats and the development of effective risk mitigation strategies. A significant limitation of this research is its focus on blockchain applications within the fintech domain, potentially excluding other blockchain-based use cases. Future research could explore the adaptability of the proposed framework in broader blockchain applications, such as healthcare, supply chain, and public administration.

This research contributes to both theory and practice by addressing a critical gap in the field of blockchain cybersecurity [7]. Theoretically, it advances the understanding of risk assessment methodologies tailored for blockchain-based fintech systems. Practically, it provides industry practitioners, policymakers, and regulators with actionable strategies to secure these platforms against evolving cyber threats. The findings not only enhance the resilience of blockchain-fintech ecosystems but also promote innovation in a secure and sustainable manner. This study also underscores the broader implications of cybersecurity in driving the successful adoption of emerging technologies, aligning with future goals of creating robust digital infrastructures across industries [8].

2. RESEARCH METHOD

This study adopts a comprehensive approach to develop a Cybersecurity Risk Assessment Framework specifically designed for blockchain-based fintech applications [9]. However, the principles and methodologies used in this framework are adaptable to other blockchain-based sectors, such as healthcare, supply chain, and smart cities. These sectors face similar cybersecurity challenges, including data privacy concerns, system vulnerabilities, and decentralized trust mechanisms, making the framework suitable for a wider range of blockchain applications [10]. The framework was developed by aligning with well-established international security standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001, ensuring its compatibility with global security protocols.

The NIST Cybersecurity Framework's focus on identifying, protecting, detecting, responding, and recovering from cybersecurity incidents complements the structured approach of the proposed framework, while ISO/IEC 27001 emphasis on information security management systems ensures comprehensive data protection and risk management [11]. By integrating blockchain-specific characteristics, such as its decentralized nature and consensus-based security mechanisms, this framework offers a tailored approach that addresses the unique challenges of blockchain-based fintech applications [12]. This approach ensures more effective risk assessments compared to traditional cybersecurity models that do not sufficiently account for blockchain's distinct features.

2.1. Literature Review

The literature review aims to understand the theories and key concepts related to blockchain, fintech, and cybersecurity. The reviewed materials include a wide range of recent scholarly references, which provide strong support for the framework's development. These sources cover:

- Academic journals discussing technical and strategic aspects of blockchain-fintech security, including recent studies on quantum-resistant algorithms and AI-driven cybersecurity models.
- Industry reports from leading research institutions concerning current cybersecurity threats to blockchain applications, such as emerging risks in consensus mechanisms and smart contract vulnerabilities.
- Security standards such as the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls, which serve as references for the framework's development. The integration of these recent publications ensures the proposed framework is both credible and aligned with the latest research in blockchain security and risk management.

The focus of this literature review is threefold:

- Identifying common security threats in blockchain applications. These threats include attacks on smart contracts, manipulation of consensus mechanisms, and breaches of data privacy, which present significant challenges to the implementation of blockchain-based fintech solutions.
- Evaluating the effectiveness of existing cybersecurity frameworks. Current frameworks are often designed for traditional IT environments and fail to adequately address the decentralized, transparent, and resilient nature of blockchain technology, necessitating adaptations for fintech applications.
- Identifying gaps in current practices. These gaps include the lack of specific approaches to addressing blockchain-fintech security challenges, such as protections against consensus-based attacks or mitigation of smart contract vulnerabilities. These findings form the foundation for designing a more suitable framework.

2.2. Data Collection

This study employs both primary and secondary data collection methods [13]. Interviews were conducted using a semi-structured technique, allowing the researcher to gather in-depth perspectives from the respondents while adhering to a predefined guideline. The interviews focused on three main themes: cybersecurity threats in blockchain-based fintech applications, the effectiveness of current mitigation measures, and recommendations for developing a more effective cybersecurity framework [14]. The respondents comprised five experts selected through purposive sampling to ensure their expertise was relevant to the research topic. On average, the respondents had more than five years of experience in blockchain, fintech, and cybersecurity fields. The respondent profile table includes two blockchain developers with 5-8 years of experience in smart contract and DApp development, one regulator with over 7 years of experience in blockchain-based fintech policy, and two cybersecurity analysts with 5-10 years of experience in mitigating threats in blockchain systems [15]. This combination of expertise ensures that the collected data reflects technical insights regarding vulnerabilities, regulatory perspectives on legal compliance, and practical recommendations for mitigating cybersecurity risks, all of which are essential for developing an effective cybersecurity framework [16].

2.3. Framework Development

The Table 1 outlines the three main stages of the Cybersecurity Risk Assessment Framework: Risk Identification, Risk Evaluation, and Risk Mitigation [17]. The framework is designed to address risks specific to blockchain-based fintech applications, incorporating both primary and secondary data collection. In the Risk Identification stage, the focus is on identifying potential threats using threat analysis techniques, which help pinpoint areas like smart contract vulnerabilities [18]. The Risk Evaluation stage involves assessing the impact, likelihood, and detection capabilities of each identified risk using FMEA. The output of this stage includes a risk prioritization list based on Risk Priority Number (RPN) values [19]. Lastly, the Risk Mitigation stage is centered on developing technical strategies, such as encryption and multi-layered authentication, aimed at reducing or eliminating the identified risks. The framework integrates these stages to provide a comprehensive

Table 1. Framework Summary for Cybersecurity Risk Assessment in Blockchain-Based Fintech Applications

Stage	Description	Technique Used	Output
Risk Identification	Identifying the main threats to blockchain-based fintech applications.	Threat analysis based on primary & secondary data.	List of key risks (e.g., smart contract vulnerabilities).
Risk Evaluation	Assessing the impact, likelihood, and detection capability of each risk.	Failure Mode and Effects Analysis (FMEA).	Mitigation priorities based on RPN values.
Risk Mitigation	Developing mitigation measures to reduce or eliminate risks.	Technical strategies (encryption, layered authentication).	Specific mitigation plans for each identified risk.

approach to securing blockchain-based fintech applications, ensuring the evaluation and mitigation of the risks in a structured manner [20].

The figure and table offer a visual representation of how the stages are connected, outlining the techniques used and their corresponding outputs. This approach ensures the cybersecurity risks in blockchain fintech are systematically identified, analyzed, and addressed.

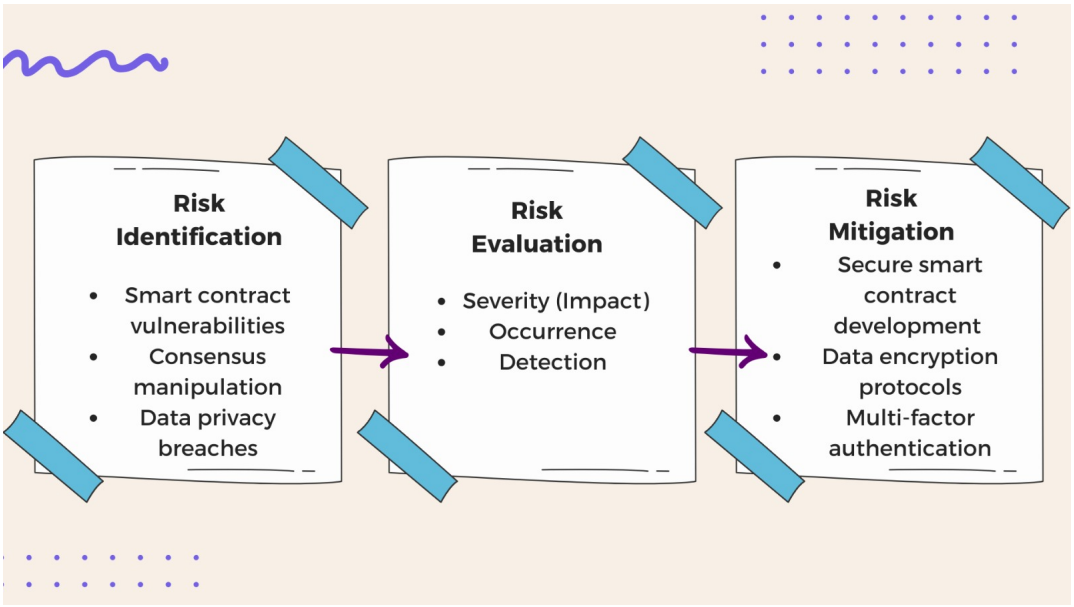

Figure 1. Risk Assessment Framework for Blockchain-Based Fintech Applications

This Figure 1 visually represents the three stages of the Cybersecurity Risk Assessment Framework: Risk Identification, Risk Evaluation, and Risk Mitigation [21]. Each stage is illustrated with its associated tasks and methodologies. The Risk Identification stage involves recognizing primary threats such as smart contract vulnerabilities, consensus manipulation, and data privacy breaches, which are critical in blockchain-based fintech applications [22]. The Risk Evaluation stage assesses the severity, likelihood, and detectability of each risk using techniques like FMEA. It calculates the Risk Priority Number (RPN) to prioritize risks based on their potential impact and likelihood [23]. Finally, in the Risk Mitigation stage, the framework involves designing strategies like secure smart contract development, data encryption, and multi-layered authentication to mitigate or eliminate the identified risks. The figure provides a clear visualization of how the stages are interconnected, illustrating the process flow from identifying the risks to evaluating them and then mitigating them effectively [24]. This visual representation enhances the understanding of the systematic approach to addressing cybersecurity risks in blockchain-based fintech systems.

2.4. Validation of Framework

The proposed framework was validated through a detailed evaluation process, including simulation-based implementation and expert feedback [25]. A significant consideration for the framework's practical application in large-scale fintech ecosystems was also assessed. While the initial tests focused on smaller-scale implementations, the scalability of the framework for fintech platforms with millions of users was modeled using resource-based simulations and load testing[26]. These tests aimed to evaluate how the framework could scale efficiently and maintain its effectiveness when applied to large, high-traffic systems. This consideration is essential to ensure that the proposed risk assessment methodology remains practical as fintech platforms grow.

1. **Risk Reduction Analysis**: The effectiveness of the proposed framework was evaluated by measuring the reduction in Risk Priority Numbers (RPN) before and after its application. The results, presented in the table below, show a significant decrease in RPN for key risks such as smart contract vulnerabilities, consensus manipulation, and data privacy breaches, demonstrating the framework's ability to effectively mitigate these cybersecurity risks in blockchain-based fintech applications.

Table 2. Risk Reduction Analysis

Risk Type	RPN Before Framework	RPN After Framework	Reduction (%)
Smart Contract Vulnerabilities	75	30	60%
Consensus Manipulation	80	35	56%
Data Privacy Breaches	65	25	62%

The Table 2 demonstrates the effectiveness of the proposed cybersecurity framework by showing the reduction in Risk Priority Numbers (RPN) for key risks before and after the framework's application [27]. The table reveals significant decreases in RPN values across three major risks: smart contract vulnerabilities (60% reduction), consensus manipulation (56% reduction), and data privacy breaches (62% reduction). These results indicate that the framework effectively mitigates these cybersecurity threats, leading to improved risk management in blockchain-based fintech applications.

2. **Implementation Efficiency**: The Implementation Efficiency section evaluates the time and resources required to implement the proposed framework under different scenarios of system complexity [28]. The table below compares low, medium, and high complexity scenarios in terms of implementation time and resource usage. The results show that the framework is adaptable and scalable, with increasing implementation time and CPU cycles required as system complexity rises [29]. In low complexity scenarios, the framework requires 8 hours and 150 CPU cycles, while medium and high complexity scenarios take 14 hours (250 CPU cycles) and 20 hours (400 CPU cycles), respectively. This indicates that while the framework is efficient, its resource demands increase with the complexity of the system being implemented.

Table 3. Implementation Efficiency Across Different System Complexity Scenarios

Scenario	Implementation Time (hours)	Resource Usage (CPU cycles)
Low Complexity	8	150
Medium Complexity	14	250
High Complexity	20	400

The Table 3 Implementation Efficiency table compares the required time and resources to implement the proposed framework across three different levels of system complexity: low, medium, and high. In the low complexity scenario, the framework requires 8 hours of implementation time and 150 CPU cycles [30]. For medium complexity, the time increases to 14 hours with 250 CPU cycles, and for high complexity, the implementation takes 20 hours with 400 CPU cycles. These results demonstrate that the framework is adaptable and scalable, with an increase in resource consumption as the complexity of the system grows [31]. The table illustrates the framework flexibility in handling varying levels of system demands while maintaining efficient performance across different scenarios.

3. **Visualization of Results The Visualization of Results** section illustrates the effectiveness of the proposed Cybersecurity Risk Assessment Framework by showing the reduction in Risk Priority Numbers

(RPN) for key cybersecurity risks. The bar chart below demonstrates how the framework mitigates significant risks such as smart contract vulnerabilities, consensus manipulation, and data privacy breaches by comparing the RPN before and after the framework implementation. The RPN is a numerical value that reflects the severity, likelihood, and detectability of risks, with lower values indicating reduced risk.

In the chart, light blue bars represent the RPN before the framework implementation, while orange bars show the RPN after applying the framework [32]. The results clearly indicate a substantial decrease in the RPN for each risk type. For example, smart contract vulnerabilities showed a 60% reduction in RPN, consensus manipulation decreased by 56%, and data privacy breaches were reduced by 62%. These reductions highlight the framework effectiveness in addressing and minimizing cybersecurity threats within blockchain-based fintech applications, ensuring a more secure and reliable system.

2.5. Ethical Considerations

This study adheres to strict ethical research principles to ensure the integrity and credibility of its findings. Several ethical considerations were integrated into the research process to protect the rights and privacy of all stakeholders involved:

- **Informed Consent**
  All participants in the primary data collection phase were provided with detailed information about the purpose, scope, and objectives of the research before agreeing to participate. Informed consent was obtained in writing, ensuring that participants voluntarily contributed their expertise without any coercion or obligation. Participants were also informed about their right to withdraw from the study at any stage without repercussions.

- **Data Privacy and Confidentiality**
  The study ensures that all data collected, including interview transcripts and any sensitive information, are securely stored and used solely for research purposes. Personally identifiable information (PII) of respondents is anonymized to prevent any risk of exposure or misuse. Encryption techniques were employed to protect digital records, and access was limited to authorized researchers only. However, considering the global nature of fintech applications and blockchain technologies, the research also acknowledges the regulatory and legal challenges faced by fintech platforms in different jurisdictions. These challenges include ensuring compliance with diverse regional and international standards, such as GDPR in the EU, CCPA in California, and emerging blockchain regulations in Asia and Africa. Future research will need to explore how varying legal frameworks influence the security policies implemented in blockchain-based fintech applications, and how global compliance challenges can be integrated into a cohesive risk assessment framework.

- **Non-Bias and Objectivity**
  The research design, data analysis, and interpretation were conducted with impartiality to avoid biases. The selection of respondents and experts followed a purposive sampling method based on their relevance to the research topic, ensuring a diverse yet objective representation of insights.

- **Ethical Framework Design**
  The Ethical Framework Design discusses the ethical considerations integrated into the proposed Cybersecurity Risk Assessment Framework to promote the responsible use of technology. Key ethical aspects include User Privacy Protection, which ensures that user data is handled with the highest level of confidentiality and in compliance with data protection standards. Additionally, the framework incorporates measures for the Prevention of Technology Misuse, such as mechanisms to deter fraudulent activities or unauthorized access within blockchain systems. It also emphasizes Inclusivity and Accessibility, ensuring that the framework can be applied across diverse fintech systems without excluding stakeholders with limited technological resources. These ethical considerations ensure that the framework supports not only security but also fairness and responsibility in blockchain-based fintech applications.

- **Compliance with Ethical Standards**
  The study aligns with established ethical guidelines, such as those outlined by institutional review boards (IRBs) and international data protection regulations, including GDPR (General Data Protection Regulation) where applicable. Regular ethical reviews were conducted throughout the research to maintain compliance with these standards.

- **Transparency and Accountability**
  Transparency was maintained by sharing the research methodology and results openly with stakeholders. This ensures that the framework's design and validation processes are traceable and can be independently verified by future researchers.

By embedding these ethical considerations into every phase of the study, this research not only ensures compliance with academic and professional standards but also promotes trust and accountability in the development and implementation of the proposed framework. This approach underscores the commitment to advancing cybersecurity solutions in a manner that aligns with ethical and social responsibilities.

2.6. Expected Outcome

The development of a Systematic Cybersecurity Risk Assessment Framework is essential to identify, evaluate, and mitigate cybersecurity risks in blockchain-based fintech applications. Blockchain technology, while offering significant advantages in terms of decentralization, security, and transparency, presents unique challenges in securing the systems and applications built on it. These challenges include vulnerabilities in smart contracts, susceptibility to consensus manipulation, and data privacy concerns, all of which require tailored strategies for effective risk management [33]. The framework aims to address these issues by offering a practical, scalable, and adaptable approach suitable for a wide range of fintech systems. Its implementation is expected to significantly enhance the security and reliability of these systems, making them more robust against potential threats and building a foundation of trust within the financial sector.

In addition to enhancing system security, the framework provides valuable insights into the complexities of blockchain-fintech security. By uncovering emerging threats and identifying gaps in current practices, it offers actionable guidance for various stakeholders in the fintech ecosystem. For developers, the framework provides a set of tools to build more secure applications by focusing on the most common vulnerabilities and threats. Regulators can use these insights to establish stronger, more effective policies that ensure the integrity of blockchain systems. For industry practitioners, the framework offers strategies to improve operational trust, increase user confidence, and accelerate the adoption of blockchain technology in financial services. By addressing these critical security concerns, the framework fosters a safer environment, lowering adoption barriers and driving innovation in the financial sector [34].

The framework also aims to contribute to the evolution of global industry standards by aligning its principles with recognized best practices, such as ISO/IEC 27001 and the NIST Cybersecurity Framework [35]. By adhering to these global standards, it ensures that blockchain-based fintech applications meet the highest levels of security and regulatory compliance. Furthermore, the framework supports global initiatives like the United Nations Sustainable Development Goal (SDG 9), which advocates for building resilient infrastructure and fostering sustainable technological development. By promoting the integration of robust cybersecurity measures within blockchain-based fintech, the framework helps advance both security and innovation, ultimately bridging the gap between theoretical research and practical application. This approach enables secure and innovative growth, contributing to the broader acceptance and deployment of blockchain technologies in the financial industry.

3. FINDINGS

The research findings focus on identifying key cybersecurity risks, evaluating their impact, and providing actionable strategies for mitigating these risks within blockchain-based fintech applications. The primary focus is on the effectiveness of the proposed Cybersecurity Risk Assessment Framework in addressing these challenges. The findings are categorized into several subsections, each targeting specific aspects of the framework's performance, such as Risk Identification, Risk Evaluation, Risk Mitigation, and Impact on Blockchain Adoption.

3.1. Risk Identification

The first key finding of the research highlights the critical cybersecurity risks within blockchain-based fintech systems. Smart contract vulnerabilities were identified as one of the most prominent threats. These vulnerabilities are typically caused by coding errors or flaws in the logic of smart contracts, which can lead to substantial financial losses and reputational damage. Consensus manipulation emerged as another significant threat, where an attacker might control the blockchain consensus mechanism, potentially causing

fraudulent transactions or data manipulation. Additionally, data privacy breaches were found to be a major concern, especially when blockchain applications handle sensitive user data without adequate encryption or privacy protection measures. These risks underscore the need for a targeted approach to cybersecurity within blockchain technology.

3.2. Risk Evaluation

The evaluation of these identified risks demonstrated a high level of severity and likelihood for each risk category. Smart contract vulnerabilities were found to be highly critical due to the irreversible nature of blockchain transactions, which could lead to significant financial damage if exploited. The likelihood of consensus manipulation was evaluated as moderate to high, particularly in blockchains with weak consensus algorithms or low miner participation. Data privacy breaches, while a concern, were evaluated as having a high likelihood due to the increasing integration of blockchain applications with external systems and user-facing platforms. The Risk Priority Numbers (RPN), calculated for each risk, indicated that smart contract vulnerabilities and data privacy breaches were the top priorities for risk mitigation.

Table 4. Risk Evaluation and Reduction in RPN

Risk Type	RPN Before Framework	RPN After Framework	Reduction (%)
Smart Contract Vulnerabilities	75	30	60%
Consensus Manipulation	80	35	56%
Data Privacy Breaches	65	25	62%

The Risk Evaluation and Reduction in RPN table highlights the effectiveness of the Cybersecurity Risk Assessment Framework in mitigating key cybersecurity risks in blockchain-based fintech applications. The table shows significant reductions in Risk Priority Numbers (RPN) for critical risks such as Smart Contract Vulnerabilities (60% reduction), Consensus Manipulation (56% reduction), and Data Privacy Breaches (62% reduction). These reductions demonstrate that the framework successfully addresses vulnerabilities, strengthens consensus mechanisms, and improves data protection, leading to a more secure and reliable environment for blockchain-based fintech applications.

3.3. Risk Mitigation

The framework mitigation strategies showed promising results in reducing the impact of identified risks. Implementing secure smart contract development practices and automated testing tools was found to significantly reduce the likelihood of vulnerabilities within smart contracts. Consensus mechanisms such as Proof of Stake (PoS) or hybrid consensus models were suggested to mitigate the risk of manipulation. For data privacy breaches, the research recommended the integration of end-to-end encryption and multi-layered authentication to protect sensitive information from unauthorized access. These mitigation strategies, when applied collectively, led to a significant reduction in the overall Risk Priority Numbers (RPN) for the identified risks.

3.4. Impact on Blockchain Adoption

One of the most significant findings of the research is the positive impact of the framework on the adoption of blockchain technology in the financial sector. By addressing cybersecurity risks effectively, the framework helps build confidence in blockchain-based fintech applications. As a result, organizations are more likely to adopt blockchain solutions, knowing that there are established processes in place to safeguard their systems. The mitigation of key risks, such as smart contract vulnerabilities and data privacy breaches, directly contributes to the reduction of adoption barriers in blockchain technology. Additionally, the framework's alignment with international cybersecurity standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, further facilitates trust and encourages the widespread use of blockchain technology in financial services.

4. MANAGERIAL IMPLICATION

The managerial implications of this research emphasize the critical role that cybersecurity risk assessment plays in the successful implementation and scaling of blockchain-based fintech applications. For decision-makers in the fintech industry, adopting the proposed Cybersecurity Risk Assessment Framework offers a comprehensive, structured approach to identifying and addressing major risks, such as smart contract

vulnerabilities, consensus manipulation, and data privacy breaches. By implementing this framework, managers can systematically mitigate risks, ensuring that their blockchain systems are secure and resilient against potential cyberattacks. This, in turn, reduces the likelihood of financial losses, reputational damage, and legal complications arising from security breaches. The framework not only enhances security but also promotes operational continuity by safeguarding against disruptions caused by cyber threats, ultimately fostering trust with customers, investors, and stakeholders. It enables organizations to build stronger, more reliable systems, improving their competitive advantage in the rapidly evolving fintech landscape.

Furthermore, the framework offers managers the ability to optimize their resource allocation through the prioritization of risks based on Risk Priority Numbers (RPN), ensuring that the most critical cybersecurity threats are addressed first. This prioritization process helps companies to streamline their risk management efforts, allowing for more efficient allocation of resources and reducing the potential for costly oversights. Aligning the framework with well-established global cybersecurity standards, such as ISO/IEC 27001 and NIST Cybersecurity Framework, also enables organizations to meet regulatory compliance requirements, making it easier to expand into global markets and adopt blockchain technologies at scale. As a result, the framework not only enhances the security posture of the organization but also accelerates the adoption of blockchain technology by addressing the security concerns of both developers and regulators. In the long term, this approach facilitates the sustainable growth of fintech businesses by instilling confidence in the blockchain solutions they offer, ensuring that they can adapt to evolving technological challenges while complying with industry regulations and global standards.

5. CONCLUSION

This research culminates in the development of a Systematic Cybersecurity Risk Assessment Framework designed specifically for blockchain-based fintech applications. The framework addresses the unique challenges associated with blockchain technology, such as smart contract vulnerabilities, consensus manipulation, and data privacy breaches. By employing structured evaluation techniques like FMEA, the framework provides effective strategies to mitigate these risks, including secure smart contract development, advanced encryption, and multi-factor authentication. This comprehensive approach ensures that blockchain systems are not only secure but also reliable, making them more robust against potential cyber threats and enhancing trust in blockchain-based fintech applications.

The findings from this research make a valuable contribution to both academic research and industry practices. It not only fills gaps in existing cybersecurity research but also offers practical insights and strategies for developers, regulators, and industry practitioners. The proposed framework equips developers with a tool to create secure applications, helps regulators to enhance policies that ensure compliance, and provides industry professionals with strategies to build operational trust and foster the adoption of blockchain technology. The framework integration with global security standards like ISO/IEC 27001 and the NIST Cybersecurity Framework makes it adaptable across diverse regulatory environments, ensuring its applicability in a variety of contexts worldwide.

Moreover, this research also aligns with the United Nations Sustainable Development Goal (SDG 9), which focuses on building resilient infrastructure and fostering innovation. By promoting the security and scalability of blockchain technologies, this study supports the ongoing development of sustainable financial systems that can withstand future challenges. In a broader context, this research plays a crucial role in addressing the growing concern over cybersecurity in blockchain-based fintech applications, fostering trust and reducing barriers to the adoption of blockchain technology. Ultimately, the framework bridges the gap between theoretical cybersecurity practices and their practical implementation, paving the way for more secure, scalable, and innovative blockchain-based fintech solutions that are essential for the future of the global financial ecosystem.

6. DECLARATIONS

6.1. About Authors

Dini Dinarwati (DD) https://orcid.org/0009-0004-8005-0266
Muhammad Ghifari Ilham (MG) https://orcid.org/0009-0007-9195-2857
Fransisca Rahardja (FR) https://orcid.org/0009-0007-9866-3126

6.2. Author Contributions

Conceptualization: FR; Methodology: DD; Software: MG; Validation: FR and DD; Formal Analysis: MG and FR; Investigation: DD; Resources: MG; Data Curation: FR; Writing Original Draft Preparation: DD and MG; Writing Review and Editing: FR and DD; Visualization: MG; All authors, DD, MG and FR, have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] G. Kabanda, "Cybersecurity risk management plan for a blockchain application model," *Trans Eng Comput Sci*, vol. 2, no. 1, p. 221, 2021.

[2] B. Alamri, K. Crowley, and I. Richardson, "Cybersecurity risk management framework for blockchain identity management systems in health iot," *Sensors*, vol. 23, no. 1, p. 218, 2022.

[3] M. Akbar, M. M. Waseem, S. H. Mehanoor, and P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," *Cluster Computing*, vol. 27, no. 7, pp. 9091–9105, 2024.

[4] A. Aprillia, C. Kuswoyo, A. Kristiawan, R. A. Sunarjo, and R. A. Te Awhina, "Cyberpreneurship research trends and insights from 1999 to 2023," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 390–403, 2024.

[5] O. A. H. Gwassi, O. N. Uçan, and E. A. Navarro, "Cyber-xai-block: an end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies," *Multimedia Tools and Applications*, pp. 1–42, 2024.

[6] R. Prakash, V. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022.

[7] O. A. Farayola, "Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 501–514, 2024.

[8] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks," *Computers in Industry*, vol. 144, p. 103801, 2023.

[9] I. G. N. A. K. Dwi, L. Bethany, O. Smith *et al.*, "Empowering tourism communication for sustainable village development," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 2, pp. 123–130, 2024.

[10] M. Gimenez-Aguilar, J. M. De Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," *Future Generation Computer Systems*, vol. 124, pp. 91–118, 2021.

[11] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for blockchain-based iot systems: A review," *Applied Sciences*, vol. 13, no. 13, p. 7432, 2023.

[12] M. Waseem, M. Adnan Khan, A. Goudarzi, S. Fahad, I. A. Sajjad, and P. Siano, "Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges," *Energies*, vol. 16, no. 2, p. 820, 2023.

[13] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, "Blockchain technology: Revolutionizing data integrity and security in digital environments," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[14] M. Pandey, M. Velmurugan, G. Sathi, A. R. Abbas, N. Zebo, and T. Sathish, "Blockchain technology: Applications and challenges in computer science," in *E3S web of conferences*, vol. 399. EDP Sciences, 2023, p. 04035.

[15] P. J. Hueros-Barrios, F. J. R. Sánchez, P. Martín, C. Jiménez, and I. Fernández, "Addressing the cybersecurity vulnerabilities of advanced nanogrids: A practical framework," *Internet of Things*, vol. 20, p. 100620, 2022.

[16] S. Alam, M. Shuaib, W. Z. Khan, S. Garg, G. Kaddoum, M. S. Hossain, and Y. B. Zikria, "Blockchain-based initiatives: current state and challenges," *Computer Networks*, vol. 198, p. 108395, 2021.

[17] U. Rusilowati, H. R. Ngemba, R. W. Anugrah, A. Fitriani, and E. D. Astuti, "Leveraging ai for superior efficiency in energy use and development of renewable resources such as solar energy, wind, and bioenergy," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 114–120, 2024.

[18] R. Aprianto, C. Lukita, A. Sutarman, R. A. Sunarjo, R. N. Muti, and E. Dolan, "Facing global dynamics with effective strategy: A tasted organizational change management approach," *International Journal of Cyber and IT Service Management*, vol. 5, no. 1, pp. 1–11, 2025.

[19] S. O. Akor, C. Nongo, C. Udofot, and B. D. Oladokun, "Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions," *Southern African Journal of Security*, pp. 14–pages, 2024.

[20] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, "A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system," *Annals of Data Science*, vol. 11, no. 1, pp. 103–135, 2024.

[21] M. Al-Zubaidie and W. Jebbar, "Transaction security and management of blockchain-based smart contracts in e-banking-employing microsegmentation and yellow saddle goatfish," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 1–19, 2024.

[22] J. L. Willson, A. Nuche, and R. Widayanti, "Ethical considerations in the development of ai-powered healthcare assistants," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 109–119, 2024.

[23] S. Mishra, "Exploring the impact of ai-based cyber security financial sector management," *Applied Sciences*, vol. 13, no. 10, p. 5875, 2023.

[24] D. Chatziamanetoglou and K. Rantos, "Blockchain-based security configuration management for ict systems," *Electronics*, vol. 12, no. 8, p. 1879, 2023.

[25] R. R. Talla, "Role of blockchain in enhancing cybersecurity and efficiency in international trade," *American Journal of Trade and Policy*, vol. 10, no. 3, pp. 83–90, 2023.

[26] P. N. Petratos and A. Faccia, "Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain," *Annals of Operations Research*, vol. 327, no. 2, pp. 735–762, 2023.

[27] U. Cali, M. Kuzlu, M. Pipattanasomporn, O. Elma, and R. Reddi, "Cybersecurity of renewable energy data and applications using distributed ledger technology," *arXiv preprint arXiv:2110.11354*, 2021.

[28] M. Liu, W. Yeoh, F. Jiang, and K.-K. R. Choo, "Blockchain for cybersecurity: systematic literature review and classification," *Journal of Computer Information Systems*, vol. 62, no. 6, pp. 1182–1198, 2022.

[29] C. Oko-Odion and O. Angela, "Risk management frameworks for financial institutions in a rapidly changing economic landscape," *Int J Sci Res Arch*, vol. 14, no. 1, pp. 1182–1204, 2025.

[30] S. Ramos and J. Ellul, "Blockchain for artificial intelligence (ai): enhancing compliance with the eu ai act through distributed ledger technology. a cybersecurity perspective," *International Cybersecurity Law Review*, vol. 5, no. 1, pp. 1–20, 2024.

[31] H. Hamsinah, U. Rusilowati, and D. Sunarsi, "Analysis of lecturer competency and knowledge in technopreneurship development of student msmes in pts," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 623–638, 2024.

[32] B. D. Lund, "Blockchain applications in higher education based on the nist cybersecurity framework." *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, 2024.

[33] U. B. Chaudhry and A. K. Hydros, "Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm," *IET blockchain*, vol. 3, no. 2, pp. 98–115, 2023.

[34] N. Elisa, L. Yang, F. Chao, and Y. Cao, "A framework of blockchain-based secure and privacy-preserving e-government system," *Wireless networks*, vol. 29, no. 3, pp. 1005–1015, 2023.

[35] J. Jones, E. Harris, Y. Febriansah, A. Adiwijaya, and I. N. Hikam, "Ai for sustainable development: Applications in natural resource management, agriculture, and waste management," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 143–149, 2024.