




Evaluating Risk Management Strategies in Fintech and Blockchain An Empirical Approach

Tri Hartono¹ , Fitra Putri Oganda² , Jack Williams^{3*} 

¹Faculty of Economics and Business, University of Raharja, Indonesia

²Department of Digital Business, University of Raharja, Indonesia

³Faculty of Management and Innovation, Pandawan Incorporation, New Zealand

¹tri.hartono@raharja.info, ²fitra.putri@raharja.info, ³jacky.liams@pandawan.ac.nz

*Corresponding Author

Article Info

Article history:

Received May 8, 2025

Revised May 30, 2025

Accepted May 30, 2025

Keywords:

Risk Management

Fintech

Blockchain

Cybersecurity

Regulatory Compliance



ABSTRACT

The rapid growth of fintech and blockchain technologies has revolutionized the financial sector, introducing innovative solutions but also posing unique risks. Managing these risks effectively is crucial for ensuring the stability and sustainability of these technologies. **This study aims** to evaluate the effectiveness of risk management strategies in fintech and blockchain sectors, focusing on identifying the most adopted strategies and assessing their impact on mitigating various risks. **A quantitative research design** was employed, using surveys to collect data from industry experts in fintech and blockchain companies. The data were analyzed using Structural Equation Modeling (SEM) with SmartPLS software to assess the relationships between risk management strategies and organizational outcomes. **The findings revealed** that cybersecurity protocols, regulatory compliance programs, and smart contract audits are the most commonly adopted risk management strategies. The study found that blockchain companies prioritize smart contract audits, while fintech companies focus more on cybersecurity and regulatory compliance. **Effective risk management** strategies are crucial for the growth and stability of fintech and blockchain sectors. The study recommends that companies integrate advanced technologies and prioritize regulatory compliance to mitigate risks and enhance trust.

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



DOI: <https://doi.org/10.33050/atm.v9i2.2473>

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

©Authors retain all copyrights

1. INTRODUCTION

The fintech and blockchain industries have witnessed unprecedented growth and innovation in recent years, fundamentally transforming the delivery and management of financial services [1]. Fintech, which encompasses the integration of advanced technologies into traditional financial services, has revolutionized banking, payments, and investment processes [2]. Similarly, blockchain technology enables decentralized, transparent, and immutable digital transactions, offering disruptive potential across multiple sectors, including finance, supply chain management, and healthcare [3].

As these technologies evolve, organizations face increasing complexity in managing risks inherent to their adoption and integration within mainstream financial systems [4, 5]. Notably, the decentralized architecture of blockchain introduces unique security vulnerabilities and regulatory compliance challenges [6]. Concurrently, fintech companies grapple with cybersecurity threats, data privacy concerns, and evolving regulatory landscapes due to the sensitive nature of financial data. Moreover, emerging technologies such as artificial

intelligence (AI) are beginning to influence risk management approaches, offering opportunities for real-time monitoring and predictive analytics [7].

In this context, aligning risk management strategies with global frameworks such as the Sustainable Development Goals (SDGs) particularly SDG 16, which promotes peace, justice, and strong institutions becomes crucial [8]. Effective regulatory compliance and robust cybersecurity measures directly contribute to fostering trustworthy, resilient financial ecosystems that support these global objectives [9].

As fintech and blockchain technologies become deeply integrated into the global financial ecosystem, the associated risks pose significant threats to their stability and sustainability [10, 11]. Critical risks include cybersecurity breaches, regulatory uncertainties, operational failures, and market volatility, all of which impede industry growth and stakeholder confidence. Despite growing awareness, empirical research remains limited on the effectiveness of organizational risk management strategies specifically tailored for fintech and blockchain contexts [12]. This study addresses this gap by systematically evaluating existing risk mitigation strategies to identify best practices and areas needing enhancement [13, 14].

The primary objective of this research is to empirically assess the risk management strategies implemented by fintech and blockchain companies. Specifically, the study aims to:

1. Identify the most widely adopted risk management strategies within fintech and blockchain sectors [15].
2. Evaluate the effectiveness of these strategies in addressing cybersecurity, regulatory compliance, operational disruptions, and market volatility risks [16].
3. Offer actionable recommendations to enhance risk management frameworks aligned with technological advancements and global sustainability goals [17].

This research contributes to the body of knowledge by providing empirical evidence on risk management effectiveness in fintech and blockchain domains [18, 19]. Insights from this study will assist organizations in strengthening their risk mitigation practices, thereby reducing vulnerabilities and improving operational resilience [20]. Additionally, the findings will inform policymakers and industry stakeholders seeking to foster secure, compliant, and sustainable financial technology ecosystems that advance the objectives of SDG 16 and harness innovations like AI for improved risk governance [21].

2. LITERATURE REVIEW

2.1. Risk Management in Fintech and Blockchain

Risk management within the fintech and blockchain sectors has garnered increasing scholarly attention due to the rapid adoption and inherent complexities of these technologies [22, 23]. Existing literature identifies several categories of risks faced by organizations, including cybersecurity threats, regulatory and compliance challenges, operational disruptions, and market volatility. Effective risk management practices are crucial to ensure the resilience and sustainability of fintech and blockchain innovations [24, 25]. These sectors operate within highly dynamic and technologically sophisticated environments, which amplify both opportunities and vulnerabilities. Thus, risk management frameworks must be adaptive, incorporating emerging technologies and evolving regulatory requirements to safeguard assets and maintain stakeholder trust.

2.2. Cybersecurity Risks

Cybersecurity remains a paramount concern across both fintech and blockchain platforms. The decentralized and transparent nature of blockchain exposes it to specific vulnerabilities such as 51% attacks, double-spending, and exploitation of smart contract bugs [26]. Such vulnerabilities can lead to substantial financial loss and undermine the trustworthiness of decentralized applications. Fintech firms, on the other hand, confront a broad spectrum of cyber threats, including hacking incidents, phishing attacks, data breaches, and identity theft, often exacerbated by the sensitive financial data they handle [27]. The proliferation of mobile banking, digital wallets, and online investment platforms has increased the attack surface for cybercriminals. Recent advances in AI-driven threat detection offer promising avenues to enhance cybersecurity defenses through real-time anomaly detection and predictive analytics [28, 29]. These AI-powered systems can identify sophisticated threats such as zero-day exploits and insider attacks, enabling proactive rather than reactive security postures.

2.3. Regulatory and Compliance Risks

Regulatory risk encompasses the complexities associated with adhering to diverse and evolving financial regulations globally [30]. The integration of blockchain technology into conventional financial systems introduces new challenges in complying with anti-money laundering (AML) laws, know-your-customer (KYC) mandates, and data privacy regulations such as the General Data Protection Regulation (GDPR) [31]. The rapid innovation pace often outstrips regulatory frameworks, resulting in uncertainty that can hinder adoption and scalability. Fintech companies must navigate a patchwork of jurisdictional regulations while maintaining compliance without sacrificing innovation [32]. Aligning regulatory strategies with Sustainable Development Goals (SDGs), especially SDG 16 which advocates for peace, justice, and strong institutions, underscores the importance of governance and ethical compliance as foundational elements for sustainable fintech and blockchain ecosystems.

2.4. Operational Risks

Operational risks in these sectors arise from technological failures, fraud, and complex system interdependencies. Blockchain systems, while offering transparency and immutability, carry risks associated with smart contract vulnerabilities such as coding errors, logical flaws, or insufficient testing, potentially leading to financial losses or service disruption [33]. Fintech companies face operational risks from software bugs, platform outages, and process inefficiencies that can compromise service delivery and customer satisfaction [34]. The increasing reliance on cloud services and third-party providers adds layers of complexity to operational risk management. The integration of AI and automation technologies presents opportunities to reduce operational risks by improving system reliability and enabling proactive issue detection through predictive maintenance and anomaly detection [35]. However, these technologies also introduce new risks related to algorithmic errors and model biases, necessitating rigorous oversight.

2.5. Market Risks

Market risks are predominantly associated with the inherent volatility of cryptocurrency markets and their broader impact on digital financial services [36]. The rapid price fluctuations in cryptocurrencies such as Bitcoin and Ethereum create liquidity risks and can adversely affect the financial stability of fintech firms with significant crypto exposure. These fluctuations also influence investor sentiment and user confidence, which are critical for platform adoption and retention [37]. Scholars emphasize that robust hedging strategies, including derivatives and options, alongside advanced risk analytics potentially leveraging AI for predictive modeling are essential to manage these uncertainties effectively [38]. Furthermore, market risks extend beyond price volatility to include systemic risks arising from macroeconomic factors, regulatory changes, and technological disruptions, all of which require sophisticated and adaptive risk management approaches.

3. RESEARCH METHOD

3.1. Research Design

This study employs a quantitative research design aimed at empirically evaluating the effectiveness of risk management strategies within fintech and blockchain companies [39]. By utilizing structured survey instruments alongside secondary data sources, the research seeks to capture comprehensive insights into current practices and their impact on mitigating various risk factors related to cybersecurity, regulatory compliance, smart contract audits, and market risk hedging [40].

3.2. Data Collection

Primary data will be collected through a structured questionnaire distributed to industry experts, risk managers, and compliance officers within fintech and blockchain organizations [41]. The questionnaire is designed to measure the adoption level and perceived effectiveness of different risk management strategies, as well as specific risk exposures faced by these companies [42]. Secondary data such as industry reports and company risk disclosures will be analyzed to complement and triangulate survey findings [43]. A purposive sampling technique will be employed to target respondents with relevant expertise and experience in the fintech and blockchain sectors [44, 45].

3.3. Hypotheses Development

Based on the literature review and empirical insights [46], the following hypotheses are proposed to evaluate the impact of key risk management strategies on organizational risk management effectiveness:

1. **H1:** Cybersecurity protocols have a positive effect on the overall risk management effectiveness in fintech and blockchain companies [47].
2. **H2:** Regulatory compliance programs positively influence risk management effectiveness in fintech and blockchain companies [48].
3. **H3:** Smart contract audits positively impact the risk management effectiveness, particularly in blockchain companies [49].
4. **H4:** Market risk hedging positively affects the risk management effectiveness in fintech and blockchain organizations [50].

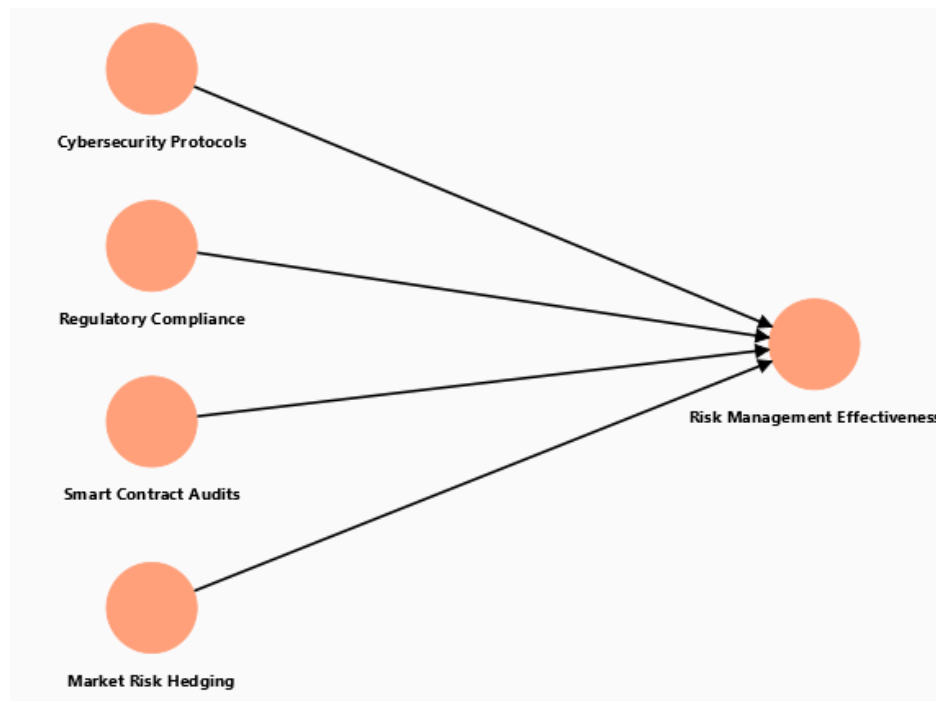


Figure 1. Hypothesis Model: The Impact of Risk Management Strategies on Risk Management Effectiveness

Figure 1 illustrates the proposed hypothesis model, where four key risk management strategies Cybersecurity Protocols (CP), Regulatory Compliance Programs (RC), Smart Contract Audits (SCA), and Market Risk Hedging (MRH) are hypothesized to have a positive influence on the overall Risk Management Effectiveness (RME) within fintech and blockchain companies. This model guides the empirical testing using Structural Equation Modeling (SEM) to assess the strength and significance of these relationships.

3.4. Data Analysis

Collected data will be analyzed using Structural Equation Modeling (SEM) via SmartPLS software. SEM is chosen due to its capability to model complex relationships among latent constructs and examine both direct and indirect effects of risk management strategies on organizational outcomes.

Prior to hypothesis testing, reliability and validity assessments including Cronbach's alpha, composite reliability (CR), and average variance extracted (AVE) will be conducted to ensure the adequacy of the measurement model. Once the measurement model is validated, the structural model will be evaluated to test the strength and significance of hypothesized paths. Bootstrapping procedures will be applied to assess the statistical significance of path coefficients, enabling robust inference on the effectiveness of the various risk management strategies.

4. RESULTS AND DISCUSSION

4.1. Risk Management Strategy Adoption

Table 1 presents the adoption rates of key risk management strategies across fintech and blockchain sectors. The data reveal that cybersecurity protocols and regulatory compliance programs are among the most widely implemented strategies in both industries, reflecting their critical importance in protecting sensitive financial information and ensuring adherence to legal frameworks. Notably, blockchain companies show a markedly higher adoption rate of smart contract audits compared to fintech firms. This difference underscores the operational reliance of blockchain platforms on smart contracts, which necessitates rigorous auditing to prevent vulnerabilities and potential financial losses. Meanwhile, market risk hedging appears moderately adopted, indicating that while market fluctuations are a concern, other risk types might receive higher prioritization.

Table 1. Adoption Rates of Risk Management Strategies in Fintech and Blockchain Sectors

Risk Management Strategy	Fintech Adoption (%)	Blockchain Adoption (%)
Cybersecurity Protocols	85	80
Regulatory Compliance Programs	75	70
Smart Contract Audits	50	90
Market Risk Hedging	60	50

Table 1 shows cybersecurity and regulatory compliance are widely adopted, with blockchain placing higher emphasis on smart contract audits. This reflects the inherent operational differences between the two sectors: blockchain platforms rely heavily on smart contracts to automate and enforce agreements without intermediaries, making the thorough auditing of these contracts essential to prevent vulnerabilities and financial losses. In contrast, fintech companies tend to prioritize cybersecurity measures and compliance programs to protect sensitive user data and adhere to stringent regulatory requirements in the highly regulated financial environment. The variation in adoption rates underscores the need for sector-specific risk management approaches that address the unique technological and regulatory challenges faced by fintech and blockchain organizations.

4.2. Measurement Model Reliability and Validity

Table 2 reports the reliability and validity statistics of the constructs measuring the effectiveness of risk management strategies. The Cronbach's Alpha values for all constructs exceed the commonly accepted threshold of 0.7, indicating strong internal consistency among survey items. Similarly, composite reliability (CR) values confirm the reliability of the latent constructs used in the analysis. The Average Variance Extracted (AVE) values surpass the 0.5 benchmark, providing evidence of convergent validity. These metrics collectively ensure that the measurement model is statistically sound, lending confidence to the interpretation of subsequent analyses involving these constructs. Such rigor in measurement validation is essential to accurately capture perceptions of effectiveness and support meaningful conclusions.

Table 2. Reliability and Validity Statistics of Risk Management Strategy Constructs

Construct	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
Cybersecurity Protocols	0.89	0.91	0.65
Regulatory Compliance Programs	0.87	0.89	0.62
Smart Contract Audits	0.91	0.93	0.68
Market Risk Hedging	0.85	0.88	0.60

Table 2 indicates strong internal consistency (Cronbach's Alpha > 0.8) and good convergent validity (AVE > 0.5) across all constructs. These metrics demonstrate that the survey items reliably measure their respective latent variables, ensuring that the data collected are both consistent and representative of the underlying theoretical concepts. The composite reliability (CR) values further confirm the robustness of the measurement model, indicating that the constructs possess high reliability beyond what Cronbach's Alpha alone can assess. Together, these statistics validate the appropriateness of the measurement instruments used in this study, supporting the accuracy of subsequent hypothesis testing and structural model evaluations.

4.3. Effectiveness Ratings of Risk Management Strategies

Table 3 shows the perceived effectiveness ratings on a scale from 1 to 5. The data reveal that smart contract audits receive the highest effectiveness rating, especially reflecting their critical role in the blockchain sector where automated contract execution demands rigorous oversight to prevent financial and operational risks. Cybersecurity protocols also score highly, underscoring their indispensable role in safeguarding fintech platforms against increasingly sophisticated cyber threats. Regulatory compliance programs maintain a strong effectiveness rating, indicating their importance in maintaining trust and legitimacy within highly regulated financial markets. Market risk hedging, while essential, scores slightly lower, which may reflect its situational application depending on the organization's exposure to market volatility.

Table 3. Perceived Effectiveness of Risk Management Strategies

Risk Management Strategy	Effectiveness Rating (1-5)
Cybersecurity Protocols	4.5
Regulatory Compliance Programs	4.2
Smart Contract Audits	4.7
Market Risk Hedging	4.0

The high effectiveness ratings in Table 3 complement the adoption data, with smart contract audits rated as most effective, especially in blockchain firms. This high rating underscores the critical role of smart contract audits in ensuring the security and reliability of blockchain operations, where automated contract execution without intermediaries can pose significant risks if vulnerabilities exist. The strong effectiveness attributed to cybersecurity protocols reflects the persistent threats fintech companies face from cyberattacks, necessitating continuous enhancement of protective measures. Regulatory compliance programs also receive favorable ratings, highlighting their importance in maintaining legal conformity and fostering trust among customers and regulators. Meanwhile, market risk hedging, although rated slightly lower, remains a vital tool in managing the financial uncertainties prevalent in both sectors, particularly given the volatility of cryptocurrency markets and fluctuating financial conditions. Collectively, these effectiveness ratings validate the prioritization of specific strategies tailored to the operational realities of fintech and blockchain environments.

4.4. Discussion

The results confirm the widespread adoption and perceived effectiveness of cybersecurity protocols and regulatory compliance programs across fintech and blockchain sectors. These strategies are essential for protecting sensitive data, ensuring adherence to complex regulatory requirements, and maintaining stakeholder confidence in highly digitized financial environments. Cybersecurity measures serve as a critical defense against increasingly sophisticated cyberattacks such as hacking, phishing, ransomware, and distributed denial-of-service (DDoS) attacks, which could lead to significant financial loss, data breaches, and irreparable reputational damage if left unaddressed. Given the evolving threat landscape, organizations continuously face the challenge of upgrading their security frameworks to detect and mitigate emerging vulnerabilities, including insider threats and supply chain attacks. Meanwhile, robust regulatory compliance programs help organizations navigate a complex and evolving legal landscape characterized by dynamic regulations such as the General Data Protection Regulation (GDPR), Anti-Money Laundering (AML) directives, and Know Your Customer (KYC) requirements. These programs foster transparency, accountability, and ethical business conduct, which are crucial for building and sustaining trust among customers, regulators, investors, and other stakeholders alike. The ability of fintech and blockchain firms to effectively comply with diverse jurisdictional requirements directly impacts their market legitimacy and operational continuity, particularly in cross-border financial services where regulatory discrepancies can pose significant risks.

Smart contract audits, although less prevalent in fintech, hold significant importance in blockchain due to their role in mitigating operational risks inherent to decentralized systems. Smart contracts automate the execution of agreements based on pre-defined coded rules without the need for intermediaries, enabling trustless transactions. However, this automation introduces unique vulnerabilities; coding errors, logical flaws, or security loopholes in smart contracts can lead to irreversible financial losses, unauthorized asset transfers, or exploitation by malicious actors. Prominent cases such as the DAO hack in 2016 exemplify the potential catastrophic impact of unchecked vulnerabilities in smart contracts. The high emphasis on comprehensive auditing practices among blockchain firms highlights their necessity in safeguarding these automated processes,

ensuring contract correctness, security, and compliance with intended business logic. This sector-specific focus illustrates the critical importance of developing tailored risk management frameworks that address the distinct technological intricacies and regulatory challenges faced by fintech and blockchain companies. Such frameworks must incorporate rigorous testing, formal verification techniques, and continuous monitoring to ensure that risk mitigation strategies align closely with their operational realities and evolving threat environments.

The strong reliability and validity metrics underpin the robustness of these findings, affirming that the survey instruments effectively capture the nuanced perceptions of risk management effectiveness within the industry. These results underscore the imperative for continual evolution and integration of emerging technologies such as artificial intelligence (AI) and machine learning (ML) to bolster real-time risk detection, predictive analytics, and adaptive response mechanisms. AI-driven solutions can enhance cybersecurity by automatically identifying anomalous network behavior, detecting zero-day vulnerabilities, and enabling faster incident response. Additionally, machine learning algorithms can optimize compliance monitoring by analyzing vast volumes of regulatory data and automating the identification of compliance gaps. By adopting agile, technology-driven risk management approaches, fintech and blockchain organizations can better navigate the increasingly complex and dynamic risk landscape, thereby enhancing operational resilience, maintaining regulatory compliance, and supporting sustainable growth in the face of rapid technological innovation and shifting regulatory expectations. Furthermore, fostering a culture of risk awareness and continuous learning within organizations will be vital to complement technological solutions, ensuring that personnel remain vigilant and prepared to address emerging risks effectively.

5. MANAGERIAL IMPLICATIONS

5.1. Strategic Technology Integration

One of the primary managerial implications of this study is the importance of proactively integrating advanced technologies particularly artificial intelligence (AI) and machine learning (ML) into risk management systems. Managers in both fintech and blockchain sectors must prioritize investments in intelligent technologies that support real-time monitoring, predictive analytics, and automated decision-making. These tools can significantly enhance an organization's ability to identify, assess, and respond to emerging threats swiftly. For example, AI-driven cybersecurity systems can detect anomalies in network traffic that may indicate a breach, while machine learning models can continuously adapt to new threat patterns. Therefore, leadership teams should foster a technology-forward mindset, ensuring that innovation in risk management remains aligned with operational goals and regulatory demands.

5.2. Tailored Risk Management Frameworks

The findings underscore the need for tailored risk management strategies that reflect the unique operational environments of fintech and blockchain firms. Managers should avoid one-size-fits-all frameworks and instead develop customized policies that address sector-specific risks such as the prominence of smart contract vulnerabilities in blockchain or the heavy regulatory oversight in fintech. For blockchain firms, emphasis should be placed on the regular auditing of smart contracts and the use of formal verification tools. In contrast, fintech managers must focus on enhancing data security protocols and strengthening compliance management systems to meet stringent legal obligations. Risk assessment procedures should be reviewed and updated regularly, taking into account changes in technology, regulation, and market behavior.

5.3. Enhancing Regulatory Readiness

Regulatory compliance emerged as a critical risk management strategy in both sectors. Managers must establish dedicated compliance units that can continuously track, interpret, and implement evolving legal frameworks across jurisdictions. This is especially important for firms operating internationally, where regulatory requirements may vary significantly. Proactive engagement with regulators, industry consortiums, and legal advisors will help managers anticipate changes and avoid penalties. In addition, embedding compliance into the company's culture through training and internal audits can reinforce its importance and ensure consistent application across departments.

5.4. Human Capital and Risk Culture Development

While technology plays a central role, the human element remains equally vital. Managers must cultivate a risk-aware organizational culture where employees understand the importance of their roles in minimizing risk. Regular training sessions, awareness programs, and scenario-based simulations can equip staff

with the necessary skills to identify and report potential issues promptly. Moreover, interdisciplinary collaboration between technical, legal, and business teams should be encouraged to ensure a holistic approach to risk management. Fostering such a culture not only improves operational resilience but also enhances employee accountability and responsiveness to threats.

5.5. Sustainable and Ethical Risk Governance

Lastly, managers should align risk management practices with broader sustainability and ethical governance goals. This includes supporting Sustainable Development Goal (SDG) 16 promoting peace, justice, and strong institutions by embedding transparency, accountability, and fairness into all risk-related decisions. Ethical considerations must guide the use of AI and data in risk mitigation, ensuring that technological interventions do not compromise privacy or widen inequalities. By adopting a sustainable risk governance model, managers can ensure long-term trust, regulatory harmony, and societal impact.

6. CONCLUSION

This study has comprehensively evaluated the adoption and perceived effectiveness of key risk management strategies within the fintech and blockchain sectors. The results indicate that cybersecurity protocols, regulatory compliance programs, and smart contract audits are the predominant strategies employed to mitigate risks related to data security, regulatory challenges, and operational vulnerabilities. These strategies are critical in addressing the unique complexities and technological nuances inherent to fintech and blockchain environments. Their widespread adoption underscores their importance in safeguarding sensitive financial information, maintaining operational continuity, and ensuring compliance with evolving legal frameworks, thereby sustaining stakeholder trust and confidence.


To enhance risk management effectiveness, fintech and blockchain organizations are encouraged to integrate cutting-edge technologies such as artificial intelligence and machine learning to enable real-time monitoring, advanced threat detection, and predictive analytics. Emphasizing regulatory compliance remains paramount in mitigating legal risks and aligning with global standards, which further strengthens market credibility. Looking ahead, future research should focus on exploring the automation potential of AI-driven risk management systems and examining the influence of organizational culture on the adoption and success of these strategies. Such insights will be essential in fostering resilient, adaptive, and sustainable financial technology ecosystems amid rapid innovation and increasing regulatory scrutiny.

7. DECLARATIONS

7.1. About Authors

Tri Hartono (TH)  <https://orcid.org/0009-0002-6233-8712>

Fitra Putri Oganda (FP)  <https://orcid.org/0000-0002-4590-0657>

Jack Williams (JW)  <https://orcid.org/0009-0004-0600-2418>

7.2. Author Contributions

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

7.3. Data Availability Statement

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

7.4. Funding

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

7.5. 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] S. Modilim, I. Bolarinwa, M. T. Omidiora, O. Tawo, and O. Sopitan, "Assessing the role of technology-driven ip management tools in safeguarding financial services innovation. 11," 2024.
- [2] U. N. Kayani, "Exploring prospects of blockchain and fintech: using slr approach," *Journal of Science and Technology Policy Management*, vol. 16, no. 1, pp. 5–41, 2025.
- [3] G. S. Putra, I. I. Maulana, A. D. Chayo, M. I. Haekal, R. Syaharani *et al.*, "Pengukuran efektivitas platform e-learning dalam pembelajaran teknik informatika di era digital," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 3, no. 1, pp. 19–29, 2024.
- [4] B. Rolando and H. Mulyono, "Managing risks in fintech: Applications and challenges of artificial intelligence-based risk management," *Economics and Business Journal (ECBIS)*, vol. 2, no. 3, pp. 249–268, 2024.
- [5] L. Kalai and M. Toukabri, "Risks, regulations, and impacts of fintech adoption on commercial banks in the united states and canada: a comparative analysis," *Thunderbird International Business Review*, vol. 66, no. 6, pp. 609–641, 2024.
- [6] N. Farazi, "Evaluating the impact of ai and blockchain on credit risk mitigation: A predictive analytic approach using machine learning," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 575–582, 2024.
- [7] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 21–34, 2021.
- [8] V. Basdekidou and H. Papapanagos, "Blockchain technology adoption for disrupting fintech functionalities: A systematic literature review for corporate management, supply chain, banking industry, and stock markets," *Digital*, vol. 4, no. 3, pp. 762–803, 2024.
- [9] H. Nobanee, N. O. D. Ellili, D. Chakraborty, and H. Z. Shanti, "Mapping the fintech revolution: how technology is transforming credit risk management," *Global Knowledge, Memory and Communication*, 2024.
- [10] D. Robert, F. P. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," *CORISINTA*, vol. 1, no. 1, pp. 61–69, 2024.
- [11] J. Yao and C. Yang, "Financial technology and climate risks in the financial market," *International Review of Financial Analysis*, vol. 99, p. 103920, 2025.
- [12] D. Alassaf, T. Daim, M. Dabic, and S. Alzahrani, "Fintech and entrepreneurship: An assessment model to evaluate policy instruments for fintech adoption by small and medium enterprises (smes)," *IEEE Transactions on Engineering Management*, 2024.
- [13] A. K. Yadav and V. P. Vishwakarma, "Blockchain role in enhancing financial risk management in banking sector using correlation analysis," *Computational Intelligence Applications in Cyber Security*, pp. 64–77, 2024.
- [14] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2021) Gebyar lomba inovasi digital mahasiswa lidm tahun 2021 resmi. Accessed: 2025-05-28. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/3481-gebyar-lomba-inovasi-digital-mahasiswa-lidm-tahun-2021-resmi>
- [15] T. Ayuninggati, E. P. Harahap, R. Junior *et al.*, "Supply chain management, certificate management at the transportation layer security in charge of security," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 1–12, 2021.
- [16] A. Areiza López, M. Bravo Sepúlveda, D. A. Bedoya Londoño, C. E. Zapata Molina, J. H. Guerrero Latorre, and P. A. Romero Díaz, "Taxonomy of operational risks infintech: A systematic literature review," 2023.
- [17] L. Singh, A. Chirputkar, and P. Ashok, "Risk management in the digital age: Fintech security strategies," in *2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI)*. IEEE, 2024, pp. 1–7.
- [18] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2023) Penguatan paud hi melalui kebijakan keterlibatan orang tua d. Accessed: 2025-05-28. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/11609-penguatan-paud-hi-melalui-kebijakan-keterlibatan-orang-tua-d>
- [19] S. Purnama, A. Sukmasari, and R. Bhandari, "The role of religiosity as a mediating variable in the rela-

- tionship between online transactions and customer satisfaction and loyalty in islamic banking,” *APTISI Transactions on Management*, vol. 5, no. 2, pp. 143–151, 2021.
- [20] P. Choudhary and M. Thenmozhi, “Fintech and financial sector: Ado analysis and future research agenda,” *International Review of Financial Analysis*, p. 103201, 2024.
- [21] M. F. Yani, C. Muhdiantini, and S. N. Aini, “Risk management in financial technology: A systematic literature review to support sustainability and security of digital financial services,” *SITEKNIK: Journal of Information Systems, Engineering and Applied Technology*, vol. 2, no. 1, pp. 149–158, 2025.
- [22] N. Lutfiani, A. Ivanov, N. P. L. Santoso, S. V. Sihotang, and S. Purnama, “E-commerce growth plan for msme’s sustainable development enhancement,” *CORISINTA*, vol. 1, no. 1, pp. 80–86, 2024.
- [23] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2024) Inovasi digital badan bahasa berkolaborasi dengan swasta cip. Accessed: 2025-05-28. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/12766-inovasi-digital-badan-bahasa-berkolaborasi-dengan-swasta-cip>
- [24] A. A. Karem and M. S. Azzahra, “Analyzing the impact of regulatory policies on financial stability and market dynamics in the banking industry,” *Inspirasi & Strategi (INSPIRAT): Jurnal Kebijakan Publik & Bisnis*, vol. 14, no. 2, pp. 83–91, 2024.
- [25] R. Wahyuni, B. Febriyanti, G. Laila, D. Sunaryo, and Y. Adiyanto, “Sustainability based financial risk management strategies for long term resilience: A systematic review,” *Indo-Fintech Intellectuals: Journal of Economics and Business*, vol. 4, no. 5, pp. 2625–2639, 2024.
- [26] S. A. Hasan, W. N. Al-Zahra, A. S. Auralia, D. A. Maharani, R. Hidayatullah *et al.*, “Implementasi teknologi blockchain dalam pengamanan sistem keuangan pada perguruan tinggi,” *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 3, no. 1, pp. 11–18, 2024.
- [27] J. Shi and Y. Wang, “Academic exploration of blockchain and ai in financial services,” *Journal of Electronic Business & Digital Economics*, 2025.
- [28] A. Ogunbajo, A. Q. Abidola, I. Taiwo, O. F. Adediran, and I. Agbo-Adediran, “How blockchain-enabled smart contracts and artificial intelligence are reshaping corporate governance frameworks in fintech and logistics industries,” 2025.
- [29] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi Republik Indonesia. (2024) Kemendikdasmen gelar karya kptk 2024 inovasi digital dalam d. Accessed: 2025-05-28. [Online]. Available: <https://www.kemendikdasmen.go.id/siaran-pers/11595-kemendikdasmen-gelar-karya-kptk-2024-inovasi-digital-dalam-d>
- [30] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, “Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness,” *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.
- [31] M. Paramesha, N. L. Rane, and J. Rane, “Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review,” *Partners Universal Multidisciplinary Research Journal*, vol. 1, no. 2, pp. 51–67, 2024.
- [32] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, “Modeling the consumers’ flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience,” *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
- [33] G. Garg, M. Shamshad, N. Gauhar, M. I. Tabash, B. Hamouri, and L. N. Daniel, “A bibliometric analysis of fintech trends: an empirical investigation,” *International Journal of Financial Studies*, vol. 11, no. 2, p. 79, 2023.
- [34] P. Radanliev, “The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the meta-verse,” *Financial Innovation*, vol. 10, no. 1, p. 1, 2024.
- [35] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, “Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station,” *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.
- [36] A. Alaassar, A.-L. Mention, and T. H. Aas, “Facilitating innovation in fintech: a review and research agenda,” *Review of Managerial Science*, vol. 17, no. 1, pp. 33–66, 2023.
- [37] V. Jain, R. Tiwari, R. Mehrotra, N. Bohra, A. Misra, and D. Pandey, “Role of technology for credit risk management: A bibliometric review,” in *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. IEEE, 2023, pp. 1–6.
- [38] B. E. Abikoye, T. Akinwunmi, A. O. Adelaja, S. Umeorah, and Y. Ogunsuji, “Real-time financial mon-

- itoring systems: Enhancing risk management through continuous oversight,” *GSC Advanced Research and Reviews*, vol. 20, no. 1, pp. 465–76, 2024.
- [39] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, “Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system.” *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.
- [40] G. Yoganandham, “Trends, challenges, and opportunities in india’s financial sector: Policy shifts, ai integration, and financial stability-an empirical assessment,” *GIS Science Journal*, vol. 12, no. 2, pp. 360–376, 2025.
- [41] D. Kumar, B. Phani, N. Chilamkurti, S. Saurabh, and V. Ratten, “Filling the sme credit gap: a systematic review of blockchain-based sme finance literature,” *Journal of trade science*, vol. 11, no. 2/3, pp. 45–72, 2023.
- [42] R. Jarvis and H. Han, “Fintech innovation: Review and future research directions,” *International journal of banking, finance and insurance technologies*, vol. 1, no. 1, pp. 79–102, 2021.
- [43] S. Pazouki, M. B. Jamshidi, M. Jalali, and A. Tafreshi, “Artificial intelligence and digital technologies in finance: a comprehensive review,” *Journal of Economics, Finance and Accounting Studies*, vol. 7, no. 2, pp. 54–69, 2025.
- [44] S. R. Addula, K. Meduri, G. S. Nadella, and H. Gonaygunta, “Ai and blockchain in finance: Opportunities and challenges for the banking sector,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 13, no. 2, pp. 184–190, 2024.
- [45] T. Pi, H. Hu, J. Lu, and X. Chen, “The analysis of fintech risks in china: Based on fuzzy models,” *Mathematics*, vol. 10, no. 9, p. 1395, 2022.
- [46] M. Bhandari, G. Tiwari, and M. Dhakal, “Enhancing transparency and accountability in sustainable finance through blockchain technology: A systematic review of the literature,” *Journal of Intelligent Management Decision*, vol. 4, no. 1, pp. 23–43, 2025.
- [47] M. Doumpos, C. Zopounidis, D. Gounopoulos, E. Platanakis, and W. Zhang, “Operational research and artificial intelligence methods in banking,” *European Journal of Operational Research*, vol. 306, no. 1, pp. 1–16, 2023.
- [48] P. A. Petare, R. Muthulakshmi, I. Bhattacharjee, S. Sharma, and S. M. Kumar, “The impact of financial innovation on corporate financial performance,” *Journal of Survey in Fisheries Sciences*, vol. 10, no. 1s, pp. 6245–6254, 2023.
- [49] P. Kamuangu, “Digital transformation in finance: A review of current research and future directions in fintech,” *World Journal of Advanced Research and Reviews*, vol. 21, no. 3, pp. 1667–1675, 2024.
- [50] S. Gupta, Y. Xie, and H. Zafar, “Fintech and digital payments: Developing a domain knowledge framework,” *Journal of Information Systems Education*, vol. 35, no. 2, pp. 189–202, 2024.