Financial Risk and Management:
An International Journal
Volume 2, Number 2, 2023

Blockchain Risk Management Practices in Financial Institutions: A Literature Review

Salsabiela Amanda Putri[1*]

[1] Universitas Diponegoro, Semarang, Indonesia

Article history:
Received: August 24, 2023
Revised: September 8, 2023
Accepted: October 13, 2023
Published: December 30, 2023

Keywords:
Blockchain,
Financial Institutions,
Governance,
Regulation,
Risk Management.

Identifier:
Zera Open
Page: 86-97
https://zeraopen.com/journal/frmij

Abstract

This article examines how financial institutions manage the risks associated with blockchain adoption at a time when distributed ledger technology is moving from experimental pilots into core banking, insurance and capital markets processes. The main question is how blockchain specific operational, cyber, legal and governance risks are identified, assessed and controlled within established risk management frameworks. The study uses a systematic literature review of peer reviewed research to consolidate dispersed evidence from information systems, finance and regulation. The results show that institutions tend to rely on permissioned architectures, consortia governance and layered controls to contain security, compliance and reputational risks, while many implementations remain at pilot or limited scale. The article discusses these patterns through thematic analysis of risk categories and control mechanisms. The main findings highlight that effective blockchain risk management is central to realizing promised efficiency and transparency benefits, and that robust empirical evaluations of specific practices are still relatively scarce.

1. Introduction

Blockchain applications have moved rapidly from pilot projects to production systems in payments, trade finance, insurance and capital markets, positioning distributed ledger technology as a core infrastructure in financial services. This transition raises complex risk management questions related to technology reliability, cyber security, legal enforceability, data governance and systemic stability, especially where permissioned blockchains are tightly coupled with existing legacy systems. While early narratives often celebrated blockchain as an inherently secure and transparent technology, recent experience in financial institutions shows that poor design choices, weak governance and misaligned incentives can generate new vulnerabilities rather than reduce risk (Casino et al., 2019; Hughes et al., 2019). Understanding how financial institutions identify, assess and mitigate these emerging risks has therefore become an important agenda for both practitioners and regulators.

Scholars have started to map this landscape from different angles. Governance oriented work highlights the challenges of decision rights, control mechanisms and accountability in distributed ledger platforms used for payments and settlement infrastructures (Zachariadis et al., 2019). Sector specific reviews in insurance and related financial services emphasize regulatory compliance, contract certainty and claims handling risks when smart contracts automate complex products and multi-party arrangements (Brophy, 2020; Ante, 2021). Empirical evidence suggests that migration of core information systems to blockchain architectures can influence systemic risk exposures of financial institutions, but the

direction and magnitude of this effect depend on implementation choices and network design (Mselmi, 2020). Taken together, this literature shows a growing concern with risk, yet it remains fragmented across technologies, sectors and risk types, with limited synthesis of concrete risk management practices at the institutional level.

This article responds by offering a systematic literature review of peer reviewed studies published between 2018 and 2022 that examine blockchain related risk management within financial institutions, including banks, insurers and other regulated intermediaries. The study asks how these institutions conceptualize blockchain specific risks, which governance and control mechanisms they employ, and how these practices affect financial, operational and compliance outcomes. Using a structured search and screening protocol, the review consolidates dispersed evidence into an integrated framework of risk categories, control tools and organizational capabilities. The results aim to clarify the problem of how financial institutions can adopt blockchain while maintaining prudential soundness and regulatory compliance, highlight misalignments between technological promises and actual risk outcomes, and identify research gaps that require further empirical investigation. By articulating these insights, the article is expected to inform risk managers, regulators and technology providers who seek to design blockchain solutions that are not only innovative but also robust, auditable and aligned with the core mandate of financial stability.

2. Literature Review

The emerging literature on blockchain in financial services has evolved from a focus on technological potential to a more nuanced discussion of risks and governance. Early reviews highlight how distributed ledgers promise enhanced transparency, automation, and efficiency in payments, clearing, trade finance, and asset servicing, while also stressing that these benefits are contingent on robust risk controls within financial institutions (Casino et al., 2019; Hughes et al., 2019). Recent sector-specific reviews reinforce that blockchain is increasingly embedded across e-finance and banking, but that adoption is shaped by trust, regulatory uncertainty, and operational constraints rather than purely by efficiency gains (Pal et al., 2021; Trivedi et al., 2021). In parallel, bibliometric work on smart contracts documents rapid growth in research on security, verification, and vulnerabilities, underscoring that automation itself introduces new forms of risk that financial firms must manage (Ante, 2021).

Within this broader stream, several recent contributions explicitly link blockchain to risk management and control systems. Javaid et al. (2022) show that financial service providers view blockchain as a tool for improving authenticity, security, and fraud prevention, yet also note gaps in managing cyber risk, smart contract flaws, and governance conflicts across consortia. Adoption studies in the banking sector indicate that perceived security, regulatory support, and organizational readiness are critical determinants of willingness to deploy blockchain solutions in core processes (Khatri & Kaushik, 2021; Pal et al., 2021). These insights suggest that risk is not merely an externality of blockchain adoption, but a central

lens through which financial institutions evaluate and configure blockchain-based infrastructures.

At the same time, existing reviews seldom provide a structured synthesis of how financial institutions operationalize blockchain risk management across different risk categories such as operational, cyber, legal, compliance, and reputational risk. Much of the current work either surveys applications at a high level, or focuses on technical or market aspects without systematically mapping the internal controls, governance mechanisms, and risk frameworks used by banks, insurers, and other financial intermediaries (Casino et al., 2019; Trivedi et al., 2021; Javaid et al., 2022). This leaves an important gap regarding how blockchain-specific risks are identified, monitored, and mitigated within established risk management architectures. By conducting a systematic literature review that concentrates on the risk management practices of financial institutions in blockchain projects, the present article seeks to consolidate fragmented evidence, highlight best practices and recurring weaknesses, and outline priorities for regulators and practitioners who aim to integrate blockchain safely into financial systems.

3. Methods

The article uses a systematic literature review to synthesize existing research on blockchain risk management practices in financial institutions. The review focuses on peer reviewed journal articles published between 2018 and 2022 to capture the period when blockchain applications in banking, insurance and capital markets began moving from pilots to implementation. Searches were conducted in

major academic databases such as Scopus, Web of Science and Google Scholar, complemented by targeted searches on publisher platforms relevant to information systems, finance and management. Keyword combinations included terms related to blockchain, financial institutions, banks, insurance, risk management, cyber risk and compliance. Only English language articles that explicitly discussed blockchain applications in financial institutions and addressed at least one aspect of risk or risk management were considered. Conference papers, non-academic reports and studies outside the time window or outside the financial sector were excluded.

After the initial search, duplicates were removed and titles and abstracts were screened to identify potentially relevant studies. Full texts of the remaining articles were then reviewed against predefined inclusion criteria to ensure that they examined blockchain use in financial institutions and provided substantive discussion of risk categories, controls, governance mechanisms or risk frameworks. For each included article, data were extracted on context, type of financial institution, blockchain application, risk types considered, risk management practices and key findings. The analysis followed a qualitative, thematic approach, grouping studies according to major risk categories and types of control or governance mechanisms. This approach allowed the review to identify common patterns, gaps and tensions in how financial institutions conceptualize and manage blockchain related risks.

4. Results and Discussion

The review shows that research on blockchain risk management in financial institutions is still at an early but rapidly evolving stage. Most studies are conceptual

or review based, mapping benefits, challenges and emerging functionality rather than offering empirical insights from within banks and insurers. Ali et al. (2020) classify the literature around blockchain enabled financial benefits and challenges, noting that operational, regulatory and cybersecurity risks represent major barriers to large scale adoption. Similar concerns appear in the work of Pal et al. (2021), who observe that financial institutions often rely on pilots or consortia to limit exposure to these risks while experimenting with new business models. Khatri and Kaushik (2021) further show that perceptions of security, privacy and compliance risks strongly shape how banks incorporate blockchain into their risk management frameworks.

Across the evidence base, a consistent set of risk categories emerges. Operational and technological risks are prominent, especially those related to smart contract vulnerabilities, key management, consensus mechanisms and interoperability with legacy systems. Javaid et al. (2022) emphasize that while blockchain improves traceability and reduces fraud, it also introduces new single points of failure associated with cryptographic keys and software bugs, which must be addressed within banks' operational risk taxonomies. Cyber risk is another central theme. Feng et al. (2018) demonstrate that insufficient investment in network security by blockchain participants can destabilize the entire system, indicating that cybersecurity cannot be viewed as an external or isolated technical issue.

A second cluster of research focuses on governance, regulatory and legal risks. Ali et al. (2020) and Pal et al. (2021) stress that uncertainty surrounding data protection rules, consumer rights, securities regulation and cross border supervision complicates the design of effective control systems. Khatri and Kaushik (2021) find

that many banks turn to permissioned networks and consortium-based governance structures to preserve accountability and auditability. Empirical work by Grima et al. (2021) shows that insurance sector experts recognize blockchain's potential for improving digital operational resilience, but remain cautious about integration challenges and the alignment of blockchain systems with evolving regulatory frameworks such as the EU Digital Operational Resilience Act.

The literature also illustrates how blockchain is being embedded into broader risk management and strategy functions. Daluwathumullagamage and Sims (2021) identify behavioural, regulatory and managerial considerations that financial institutions must address in order to integrate blockchain safely within existing frameworks. Javaid et al. (2022) highlight a range of use cases including fraud detection, real time auditing and secure credit reporting, but note that many implementations remain experimental and lack rigorous evaluation. Taken together, these studies suggest that institutions are gradually shifting from exploratory pilots toward more structured adoption aligned with the three lines of defense model. Yet evidence on the effectiveness of specific controls, governance arrangements and metrics remains limited.

Overall, the reviewed studies converge on several implications. Blockchain related risk management cannot be treated as a purely technical matter; operational, cyber, legal and strategic dimensions must be integrated into a coordinated framework. Permissioned networks, consortium governance and clearly defined roles appear to be the predominant mitigation strategies in regulated sectors such as payments, trade finance and insurance. At the same time, significant research gaps

remain, particularly regarding quantitative assessments of how blockchain adoption affects risk profiles, capital requirements and loss events over time. More empirical, longitudinal and cross jurisdictional studies are needed to evaluate which risk management practices actually enhance safety, reliability and compliance in financial institutions.

5. Conclusion

This review concludes that blockchain adoption in financial institutions is shaped as much by risk considerations as by technological potential. Across banking, insurance and capital markets, blockchain is framed not only as an enabler of efficiency, transparency and automation, but also as a source of new operational, cyber, legal and governance risks. The synthesis of recent literature shows that financial institutions rarely adopt blockchain in a straightforward manner. Instead, they experiment through pilots, consortia and permissioned networks that allow them to test functionality while containing exposure to security, compliance and reputation risks. In this sense, blockchain risk management has become central to whether and how the technology advances from experimentation to critical financial infrastructure.

The findings also highlight that traditional risk categories remain relevant but require reinterpretation in a distributed ledger context. Operational risk now includes smart contract vulnerabilities, key management failures and complex interoperability issues with legacy systems. Cyber risk extends beyond perimeter security to strategic behavior of nodes within blockchain networks. Legal and regulatory risks arise from

uncertainty over data protection, consumer rights, supervisory oversight and cross border rules. At the same time, the literature suggests that when these risks are addressed through careful architecture design, consortium governance and clear allocation of responsibilities, blockchain can support fraud reduction, real time auditing and stronger digital operational resilience. This aligns with prior work that treats governance and institutional trust as prerequisites for realizing the promised benefits of financial innovation.

Despite growing interest, the evidence base remains fragmented and skewed toward conceptual work, early stage use cases and short term perspectives. There is limited systematic analysis of how specific controls, governance models and regulatory arrangements actually affect risk profiles, capital requirements or loss events over time in different types of financial institutions. Future research needs to deepen and broaden the empirical foundation by examining live implementations, collecting longitudinal data and including more diverse institutional and jurisdictional contexts. By bringing together insights from information systems, finance, regulation and risk management, this article underlines the need for integrated frameworks in which blockchain design, governance choices and risk control practices are evaluated jointly. Such an approach can help financial institutions and regulators move from cautious experimentation toward more confident, evidence-based decisions about the safe and effective use of blockchain in financial services.

References

Ali, O., Ally, M., Clutterbuck, P., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management, 54*, 102199.

Ante, L. (2021). Smart contracts on the blockchain–A bibliometric analysis and review. *Telematics and Informatics, 57*, 101519.

Brophy, R. (2020). Blockchain and insurance: a review for operations and regulation. *Journal of financial regulation and compliance, 28*(2), 215-234.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics, 36*, 55-81.

Daluwathumullagamage, D. J., & Sims, A. (2021). Fantastic beasts: blockchain based banking. *Journal of Risk and Financial Management, 14*(4), 170.

Feng, S., Wang, W., Xiong, Z., Niyato, D., Wang, P., & Wang, S. S. (2018). On cyber risk management of blockchain networks: A game theoretic approach. *IEEE Transactions on Services Computing, 14*(5), 1492-1504.

Grima, S., Kizilkaya, M., Sood, K., & ErdemDelice, M. (2021). The perceived effectiveness of blockchain for digital operational risk resilience in the European Union insurance market sector. *Journal of Risk and Financial Management, 14*(8), 363.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits,

limitations, emerging research themes and research agenda. *International journal of information management, 49*, 114-129.

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil transactions on benchmarks, standards and evaluations, 2*(3), 100073.

Khatri, A., & Kaushik, A. (2021). Systematic literature review on blockchain adoption in banking. *Journal of Economics Finance and Accounting, 8*(3), 126-146.

Mselmi, A. (2020). Blockchain technology and systemic risk. *International journal of economics and financial Issues, 10*(2), 53-60.

Pal, A., Tiwari, C. K., & Behl, A. (2021). Blockchain technology in financial services: a comprehensive review of the literature. *Journal of Global Operations and Strategic Sourcing, 14*(1), 61-80.

Trivedi, S., Mehta, K., & Sharma, R. (2021). Systematic literature review on application of blockchain technology in E-finance and financial services. *Journal of technology management & innovation, 16*(3), 89-102.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and organization, 29*(2), 105-117.