Next Scientists
Journal of Management and Economics

TYPE Original Research
PAGE NO. 28-32

Check for updates

Blockchain-Enabled Risk Governance, Cybersecurity, and Sustainable Value Creation in Global Supply Chains: An Integrative Theoretical and Empirical Synthesis

Dr. Alejandro M. Ríos

Faculty of Economics and Management, University of Barcelona, Spain

OPEN ACCESS

SUBMITTED 01 December 2025
ACCEPTED 15 December 2025
PUBLISHED 31 December 2025
VOLUME Vol.05 Issue 12 2025

Abstract: The rapid digital transformation of global supply chains has intensified both opportunities for value creation and exposure to systemic risks, including operational disruptions, cybersecurity threats, regulatory non-compliance, and sustainability failures. Among emerging digital technologies, blockchain has attracted sustained scholarly and practitioner attention due to its distinctive properties of decentralization, immutability, transparency, and cryptographic security. This study develops a comprehensive, theory-driven and empirically grounded examination of blockchain technology as a foundational infrastructure for risk governance, resilience, cybersecurity, and sustainable value creation in contemporary supply chains. Drawing strictly and exclusively on the provided body of peer-reviewed literature, the article integrates perspectives from sustainable supply chain management, information systems, cybersecurity, operations management, strategic management, and organizational theory.

The research advances three primary objectives. First, it systematically elaborates the multifaceted mechanisms through which blockchain reshapes supply chain risk structures, extending beyond efficiency enhancement to include accountability, trust redistribution, and behavioral transformation among actors. Second, it situates blockchain-enabled supply chains within broader theoretical frameworks, including the resource-based view, dynamic capabilities, and institutional compliance regimes such as the General Data Protection Regulation, highlighting how blockchain can function simultaneously as a strategic resource, a governance mechanism, and a compliance-enabling architecture.

Third, it critically analyzes blockchain's role in mitigating systemic shocks, such as pandemics and cyberattacks, while acknowledging structural barriers, adoption risks, and unintended consequences.

Methodologically, the study employs a qualitative, integrative research design combining deep literature synthesis, conceptual modeling, and theory triangulation. Rather than aggregating empirical metrics, the analysis emphasizes causal reasoning, interpretive depth, and cross-disciplinary coherence. The findings demonstrate that blockchain's value in supply chains emerges not merely from technical deployment but from its alignment with organizational capabilities, regulatory environments, and socio-behavioral mechanisms. The discussion highlights key limitations, including governance complexity, scalability challenges, and cybersecurity paradoxes, and outlines future research directions focused on hybrid architectures, AI–blockchain convergence, and sector-specific regulatory harmonization. The article concludes that blockchain represents a transformative but contingent infrastructure whose long-term impact on supply chain resilience and sustainability depends on strategic orchestration rather than technological determinism.

Keywords: Blockchain, supply chain resilience, cybersecurity, sustainable supply chains, risk governance, digital transformation

Introduction

Global supply chains have undergone profound structural changes over the past two decades, driven by globalization, technological advancement, and increasing interdependence among geographically dispersed actors. While these developments have enabled unprecedented efficiency and market integration, they have also exposed supply chains to heightened levels of operational, financial, environmental, and cybersecurity risks. Disruptions such as geopolitical tensions, climate-related disasters, regulatory fragmentation, and global health crises have revealed the fragility of conventional supply chain governance mechanisms that rely heavily on centralized control, information asymmetry, and trust-based intermediaries (Min, 2019; Xiong et al., 2021).

Within this context, blockchain technology has emerged as a potentially transformative digital infrastructure capable of reconfiguring how information, value, and trust are generated and exchanged across supply networks. Unlike traditional databases, blockchain operates as a distributed ledger system in which transactions are recorded immutably and validated through cryptographic consensus mechanisms, thereby reducing reliance on centralized authorities (Saberi et al., 2019). Early discourse surrounding blockchain emphasized its association with cryptocurrencies, yet subsequent research has increasingly focused on its broader organizational and inter-organizational applications, particularly in supply chain management, risk mitigation, and cybersecurity (Chang et al., 2020; Hasanova et al., 2019).

Despite growing scholarly interest, the literature remains fragmented across disciplinary boundaries. Studies often examine isolated dimensions such as transparency, traceability, cybersecurity, or regulatory compliance, without sufficiently integrating these perspectives into a unified analytical framework. Moreover, while empirical evidence suggests that blockchain can enhance supply chain resilience and sustainability, adoption barriers, governance complexities, and unintended systemic risks remain underexplored (Etemadi et al., 2021; Körner et al., 2022). This fragmentation creates a critical literature gap: the absence of a holistic, theory-driven understanding of how blockchain reshapes risk governance and value creation in complex supply chain ecosystems.

This article addresses this gap by developing an integrative synthesis that connects blockchain technology with sustainable supply chain management, cybersecurity architectures, and strategic management theories. By grounding the analysis strictly in the provided references, the study avoids speculative extrapolation and instead builds cumulative knowledge through careful theoretical elaboration. The central research problem guiding this inquiry is how blockchain-enabled infrastructures alter the nature, distribution, and governance of risk in global supply chains, and under what conditions these alterations translate into sustainable competitive and societal value.

The significance of this research lies in its multi-level perspective. At the technological level, it examines blockchain's cryptographic and architectural properties. At the organizational level, it analyzes behavioral, strategic, and compliance-related implications. At the systemic level, it considers resilience against large-scale disruptions and cyber threats. By weaving these levels together, the article contributes to both academic theory and managerial practice, offering a nuanced understanding of blockchain as neither a panacea nor a passing trend, but as a contingent institutional technology embedded within broader socio-technical systems.

Methodology

The methodological approach adopted in this study is qualitative, integrative, and theory-centric, reflecting the conceptual nature of the research objectives. Rather than employing primary data collection or statistical modeling, the study relies on an in-depth synthesis of established peer-reviewed literature drawn exclusively from the provided references. This approach is particularly appropriate for examining emerging technologies such as blockchain, where theoretical consolidation and conceptual clarity are prerequisites for meaningful empirical generalization (Saberi et al., 2019).

The research design follows a structured interpretive process. First, the referenced studies were thematically clustered into core domains: sustainable supply chain management, supply chain risk and resilience, cybersecurity and data governance, regulatory compliance, and strategic value creation. Each cluster was analyzed to identify key constructs, causal mechanisms, and theoretical assumptions. Second, these constructs were examined across studies to uncover convergences, tensions, and gaps in the existing knowledge base. For instance, while some studies emphasize blockchain's transparency benefits, others highlight privacy and compliance challenges, necessitating a reconciliatory analytical lens (Rieger et al., 2019; Wylde et al., 2022).

Third, the study employs theory triangulation by interpreting blockchain-enabled supply chains through multiple theoretical frameworks, including the resource-based view, dynamic capabilities, and institutional theory. This triangulation enhances analytical rigor by preventing overreliance on a single explanatory paradigm and by situating technological effects within broader organizational and environmental contexts (Barney et al., 2021; Teece, 2020).

Importantly, the methodology emphasizes analytical depth over breadth. Each theoretical claim is elaborated through extensive reasoning, counter-argument consideration, and contextualization within the cited literature. The absence of quantitative metrics does not imply a lack of rigor; rather, rigor is achieved through logical coherence, comprehensive coverage of existing findings, and transparent linkage between evidence and interpretation.

Ethical considerations are implicitly addressed through strict adherence to citation integrity and avoidance of speculative claims beyond the empirical and theoretical boundaries established by the referenced works. The methodology thus aligns with best practices for conceptual research in operations management and information systems, providing a robust foundation for the subsequent analysis.

Results

The integrative analysis yields several interrelated findings concerning the role of blockchain in supply chain risk governance, cybersecurity, and sustainable value creation. These findings are presented descriptively, reflecting patterns and mechanisms identified across the literature rather than numerical outcomes.

A central finding is that blockchain fundamentally reconfigures information asymmetry in supply chains. By enabling shared, immutable ledgers accessible to authorized participants, blockchain reduces the opacity that traditionally characterizes multi-tier supply networks (Zelbst et al., 2020). This transparency facilitates traceability of products, transactions, and certifications, which in turn supports environmental and social sustainability objectives (Saberi et al., 2019). The literature consistently indicates that transparency alone is insufficient; its value emerges when combined with accountability mechanisms that align incentives and discourage opportunistic behavior.

Another significant finding conc erns supply chain resilience. Blockchain-enabled systems enhance resilience by improving visibility, coordination, and trust during disruptions. During the COVID-19 pandemic, blockchain-supported supply chains demonstrated greater adaptability by enabling real-time information sharing and reducing dependency on centralized intermediaries (Xiong et al., 2021). This resilience is not merely operational but systemic, as decentralized architectures mitigate single points of failure. However, the literature also cautions that resilience gains depend on network participation density and governance design, without which fragmentation may persist (Min, 2019).

Cybersecurity emerges as both a strength and a paradox within blockchain adoption. On one hand, cryptographic techniques and decentralized consensus mechanisms enhance data integrity and reduce certain attack vectors (Hasanova et al., 2019; Storublevtcev, 2019). On the other hand, smart contracts, interoperability layers, and user interfaces introduce new vulnerabilities that require complementary AI-driven security architectures (Muheidat & Tawalbeh, 2021; Sheth et al., 2022). The findings thus underscore that blockchain does not

eliminate cybersecurity risks but redistributes them across technological layers.

Regulatory compliance, particularly with data protection regimes such as the GDPR, represents another critical outcome domain. Blockchain's immutability conflicts with requirements for data erasure and modification, necessitating innovative design solutions such as off-chain storage and permissioned access (Rieger et al., 2019). Successful compliance is therefore contingent on architectural choices rather than inherent technological features.

Finally, from a strategic perspective, blockchain-enabled supply chains contribute to value creation when integrated with organizational capabilities. Firms that leverage blockchain as a strategic resource, rather than a standalone tool, achieve superior outcomes in transparency, trust, and stakeholder engagement (Barney et al., 2021; Teece, 2020). This finding highlights the contingent nature of blockchain's benefits.

Discussion

The findings invite a deeper interpretive discussion that situates blockchain-enabled supply chains within broader theoretical and practical debates. From a resource-based perspective, blockchain can be conceptualized as a valuable, rare, and imperfectly imitable resource when embedded within firm-specific routines and inter-organizational relationships (Barney et al., 2021). However, its value is not intrinsic; it arises from complementary assets such as governance structures, human expertise, and institutional legitimacy.

Dynamic capabilities theory further illuminates how firms adapt blockchain technologies to evolving environments. The ability to sense technological opportunities, seize them through investment and experimentation, and reconfigure organizational processes determines whether blockchain adoption yields sustained advantages (Teece, 2020). This perspective explains why similar blockchain implementations produce divergent outcomes across firms and sectors.

At the institutional level, blockchain challenges traditional regulatory and organizational arrangements by enabling decentralized autonomous coordination (Takagi, 2017). While this decentralization enhances efficiency and trust, it also raises questions about accountability, legal liability, and systemic risk (Körner et al., 2022). These tensions suggest that blockchain adoption must be accompanied by adaptive regulatory frameworks and hybrid governance models.

The discussion also acknowledges limitations within the existing literature. Many studies focus on conceptual benefits without longitudinal evidence of long-term performance impacts. Additionally, social and behavioral dimensions, such as resistance to transparency and power redistribution, remain underexplored despite their critical influence on adoption success (Chaudhuri et al., 2023). Future research should therefore adopt multi-method approaches that combine qualitative insights with empirical validation.

Conclusion

This article provides a comprehensive, theory-driven examination of blockchain technology as an enabler of risk governance, cybersecurity, resilience, and sustainable value creation in global supply chains. By synthesizing insights from diverse yet complementary strands of literature, the study demonstrates that blockchain's transformative potential lies not in technological novelty alone but in its capacity to reshape organizational relationships, governance mechanisms, and strategic capabilities.

The analysis underscores that blockchain adoption is inherently contingent, shaped by regulatory contexts, cybersecurity architectures, and dynamic capabilities. While the technology offers powerful tools for transparency, trust, and resilience, it also introduces new complexities that demand thoughtful design and institutional alignment.

Ultimately, blockchain should be understood as an evolving socio-technical infrastructure whose long-term impact on supply chains will depend on collective learning, cross-sector collaboration, and adaptive governance. This integrative perspective provides a robust foundation for future scholarly inquiry and informed managerial decision-making.

References

1. Barney, J. B., Ketchen, D. J., Jr., & Wright, M. (2021). Resource-based theory and the value creation framework. Journal of Management, 47, 1936–1955.

2. Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges

and opportunities. International Journal of Production Research, 58, 2082–2099.

3. Chaudhuri, A., Bhatia, M. S., Kayikci, Y., Fernandes, K. J., & Fosso-Wamba, S. (2023). Improving social sustainability and reducing supply chain risks through blockchain implementation. Annals of Operations Research, 327, 401–433.

4. Etemadi, N., Van Gelder, P., & Strozzi, F. (2021). An ISM modeling of barriers for blockchain adoption in supply chains towards cybersecurity. Sustainability, 13, 4672.

5. Hasanova, H., et al. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29, e2060.

6. Körner, M.-F., et al. (2022). Systemic risks in electricity systems: A perspective on the potential of digital technologies. Energy Policy, 164, 112901.

7. Min, H. (2019). Blockchain technology for enhancing supply chain resilience. Business Horizons, 62, 35–45.

8. Muheidat, F., & Tawalbeh, L. A. (2021). Artificial intelligence and blockchain for cybersecurity applications. Springer.

9. Rieger, A., et al. (2019). Building a blockchain application that complies with the EU general data protection regulation. MIS Quarterly Executive, 18, 263–279.

10. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57, 2117–2135.

11. Sheth, H. S. K., et al. (2022). Deep learning, blockchain based multi-layered authentication and security architectures. IEEE.

12. Storublevtcev, N. (2019). Cryptography in blockchain. Springer.

13. Takagi, S. (2017). Organizational impact of blockchain through decentralized autonomous organizations. International Journal of Economic Policy Studies, 12, 22–41.

14. Teece, D. J. (2020). Hand in glove: Open innovation and the dynamic capabilities framework. Strategic Management Review, 1, 233–253.

15. Wylde, V., et al. (2022). Cybersecurity, data privacy and blockchain: A review. SN Computer Science, 3, 127.

16. Xiong, Y., et al. (2021). The mitigating role of blockchain-enabled supply chains during the COVID-19 pandemic. International Journal of Operations & Production Management, 41, 1495–1521.

17. Zelbst, P. J., et al. (2020). The impact of RFID, IIoT, and blockchain technologies on supply chain transparency. Journal of Manufacturing Technology Management, 31, 441–457.