Digital Trust Architectures in Global Supply Chains: Beyond Blockchain Hype

Viraj P. Tathavadekar, Nitin R. Mahankale

Symbiosis International University, Pune, India

Email: Virajtatu@gmail.com, nitin.mahankale@scmspune.ac.in

Abstract

The proliferation of digital technologies in global supply chains has generated considerable enthusiasm for blockchain-based solutions as panaceas for transparency and trust deficits. However, this viewpoint challenges the prevailing techno-solutionist narrative by examining digital trust through a socio-governance lens that transcends technological determinism. Drawing from systems theory, platform capitalism, and governance literature, this paper argues that digital trust in global supply chains is fundamentally a socio-governance construct shaped by platform design choices and inter-organizational norms rather than merely a technological function. While distributed ledger technologies offer valuable capabilities for traceability and transparency, their implementation within existing power structures often reproduces rather than transforms underlying trust asymmetries. This analysis reveals how the architecture of digital trust systems reflects and reinforces particular governance arrangements, calling for a more nuanced understanding of how technology intersects with social, economic, and political dynamics in shaping supply chain relationships. The paper advocates for moving beyond blockchain hype toward comprehensive trust architectures that acknowledge the inherently social nature of trust formation and maintenance in complex global networks.

Keywords

Digital Trust, Blockchain, Supply Chain Governance, Platform Capitalism, Technological Solutionism, Transparency Systems

1. Introduction

The discourse surrounding digital transformation in global supply chains has become increasingly dominated by technological narratives that position blockchain and related distributed ledger technologies as revolutionary solutions to longstanding challenges of trust, transparency, and traceability [1]. This technological enthusiasm, while understandable given the complexity of modern supply networks, reflects a broader pattern of techno-solutionism that obscures the fundamentally social and political dimensions of trust formation in inter-organizational relationships.

Figure 1: The Blockchain Hype vs Reality Paradigm This figure illustrates the disconnect between blockchain's promised benefits and the persistent need for governance mechanisms, highlighting how technological solutions cannot eliminate the fundamental social dimensions of trust.

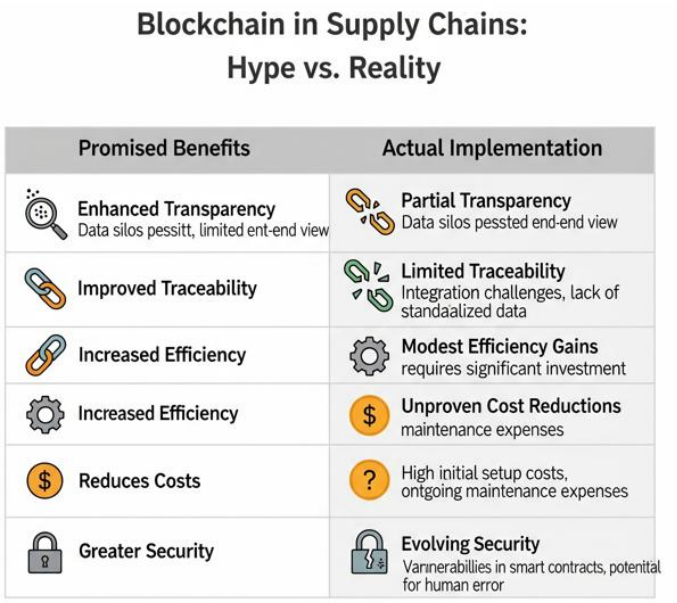

Figure 1. Blockchain Hype vs Reality in Supply Chains *Source: Authors Creation*

The COVID-19 pandemic exposed critical vulnerabilities in global supply chains, highlighting how interconnected networks of suppliers, manufacturers, and distributors could be disrupted by unforeseen events [1]. In response, many organizations and policymakers have turned to digital technologies as mechanisms for building more resilient and transparent supply systems. Blockchain, in particular, has been heralded as a transformative technology capable of creating immutable records, ensuring product authenticity, and enabling unprecedented levels of supply chain visibility [2,3].

However, this technological optimism often overlooks fundamental questions about how trust actually operates in complex social systems. Trust is not merely a technical problem to be solved through better information systems; it emerges from ongoing relationships, shared understandings, and institutional frameworks that govern behavior over time [4]. The architecture of digital trust systems inevitably reflects particular assumptions about governance, power, and legitimacy that shape how these technologies are implemented and experienced by different stakeholders.

This viewpoint paper argues that digital trust in global supply chains represents a socio-governance construct that cannot be reduced to technological capabilities alone. Instead of viewing blockchain and related technologies as neutral tools for enhancing transparency, we must examine how these systems embody particular governance arrangements and reproduce existing power asymmetries within supply networks [5,6]. The design of digital trust architectures involves fundamental choices about who controls information, how transparency is configured, and which forms of knowledge are privileged or marginalized.

By adopting a perspective informed by systems theory, platform capitalism, and governance literature, this analysis reveals how digital trust systems function as more than technical infrastructure. They operate as governance mechanisms that shape relationships between supply chain actors, influence the distribution of risks and rewards, and determine how different forms of value are created and captured [7,8]. Understanding these dynamics is essential for moving beyond simplistic narratives about technological solutions toward more nuanced approaches to building trust in global supply networks.

2. The Limits of Technological Solutionism

2.1 Deconstructing the Blockchain Panacea

The contemporary discourse around supply chain digitalization has been profoundly shaped by what can be characterized as blockchain evangelism a belief that distributed ledger technologies represent a fundamental solution to trust deficits in global trade networks [9,10]. This technological determinism assumes that by creating immutable, transparent records of transactions and product movements, blockchain systems can automatically generate trust between previously unknown or distrusting parties.

Figure 2: Technological Determinism vs Social Reality of Trust This diagram contrasts the linear logic of technological determinism with the complex social reality of trust formation, showing how power dynamics, cultural norms, and institutional frameworks shape trust relationships.

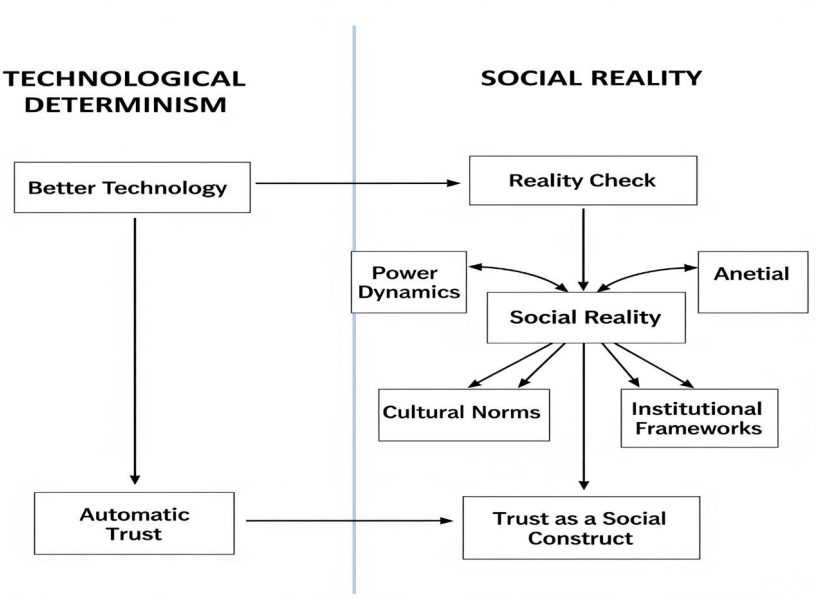

Figure 2. Technological Determinism vs Social Reality of Trust *Source: Authors Creation*

However, this perspective fundamentally misunderstands the nature of trust in complex social systems. Trust emerges from ongoing relationships, shared understandings, and institutional frameworks that govern behavior over time [4,11]. The assumption that better information systems automatically translate into higher levels of trust reflects a rationalist bias that overlooks the emotional, cultural, and political dimensions of inter-organizational relationships.

Moreover, the focus on blockchain as a trust-generating mechanism often obscures how these technologies may reinforce existing power asymmetries rather than challenging them. Large corporations with significant resources and technical capabilities are typically better positioned to shape blockchain implementations according to their interests, potentially creating new forms of digital dependency for smaller suppliers [8,12]. The governance structures embedded within blockchain systems including decisions about who can access information, how consensus is achieved, and what constitutes valid transactions—inevitably reflect the preferences and capabilities of dominant actors.

2.2 The Persistence of Governance Challenges

Despite claims about blockchain's potential to create "trustless" systems that eliminate the need for intermediaries, practical implementations in supply chains continue to require extensive governance mechanisms [5,13]. These include decisions about data standards, participation requirements, dispute resolution procedures, and mechanisms for handling non-compliance. Rather than eliminating governance challenges, blockchain systems often relocate these issues to new domains where they may be less visible but equally consequential.

The technical architecture of blockchain systems embeds assumptions about how trust should be constructed and maintained. For example, proof-of-work consensus mechanisms privilege computational power, while proof-of-stake systems favor those with existing token holdings [3,5]. These design choices have profound implications for who can participate meaningfully in blockchain-based supply chain systems and how different forms of value are recognized and rewarded.

Furthermore, the integration of blockchain systems with existing supply chain infrastructure reveals the persistence of traditional power relationships. Even when blockchain provides enhanced visibility into product movements, the interpretation of this information and decisions about how to respond remain subject to existing organizational hierarchies and market dynamics [6,14]. The technology may change how information is stored and accessed, but it does not automatically alter the fundamental relationships between buyers and suppliers or the broader institutional context within which these relationships operate.

3. Digital Trust as Socio-Governance Construct

3.1 Beyond Information Transparency

The prevailing approach to digital trust in supply chains must first be understood in the context of how trust actually operates in complex social systems. Trust is not simply a matter of information availability or verification capabilities; it emerges from ongoing relationships, shared understandings, and institutional frameworks that govern behavior over time [4,11]. This foundational understanding reveals the limitations of approaches that have been heavily influenced by transparency discourse that equates greater information availability with enhanced trust [15,16].

This information-centric perspective assumes that trust deficits stem primarily from information asymmetries that can be addressed through better data collection and sharing mechanisms. However, this view overlooks how transparency itself is a governance mechanism that shapes power relationships and creates new forms of vulnerability.

Figure 3: Transparency as Asymmetric Governance Mechanism This figure demonstrates how transparency requirements often flow asymmetrically from powerful to vulnerable actors, reproducing rather than challenging existing power imbalances in supply chain relationships.

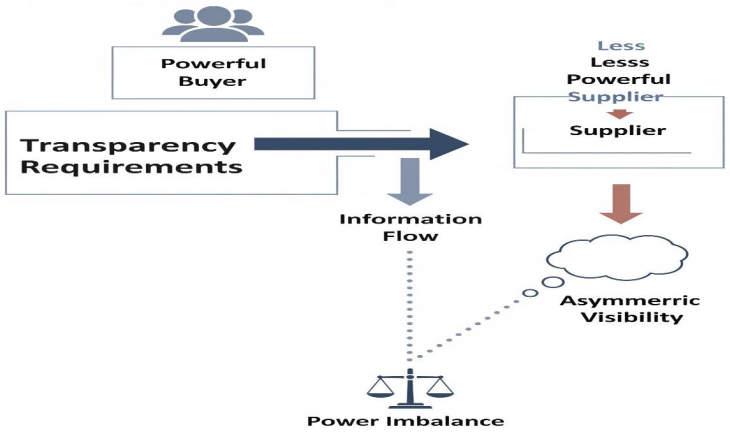

Figure 3. Transparency as Governance Mechanism *Source: Authors Creation*

Transparency is never neutral; it involves decisions about what information is made visible, to whom, and under what conditions [15,17]. In supply chain contexts, demands for transparency often flow from powerful buyers to less powerful suppliers, creating asymmetric visibility arrangements where upstream actors must expose their operations while downstream partners maintain greater privacy. Digital trust systems that prioritize transparency may therefore reproduce rather than challenge existing power imbalances.

Moreover, the focus on information transparency often neglects other dimensions of trust that may be equally important in supply chain relationships. These include competence trust (confidence in partners' capabilities), benevolence trust (belief in partners' goodwill), and integrity trust (assurance of honest behavior) [4,18]. While information systems can provide some evidence relevant to these dimensions, they cannot substitute for the relational processes through which trust is built and maintained over time.

3.2 Platform Capitalism and Digital Intermediation

The implementation of digital trust systems in global supply chains must be understood within the broader context of platform capitalism—an economic model where digital platforms serve as intermediaries that facilitate interactions between different groups of users while extracting value from these connections [7,19]. Many blockchain-based supply chain solutions operate according to platform logic, creating new forms of digital intermediation even as they claim to eliminate traditional intermediaries.

Figure 4: Platform Capitalism in Digital Trust Systems This diagram illustrates how digital trust platforms create new forms of intermediation and value extraction while claiming to eliminate traditional intermediaries, showing the persistence of platform-mediated power relationships.

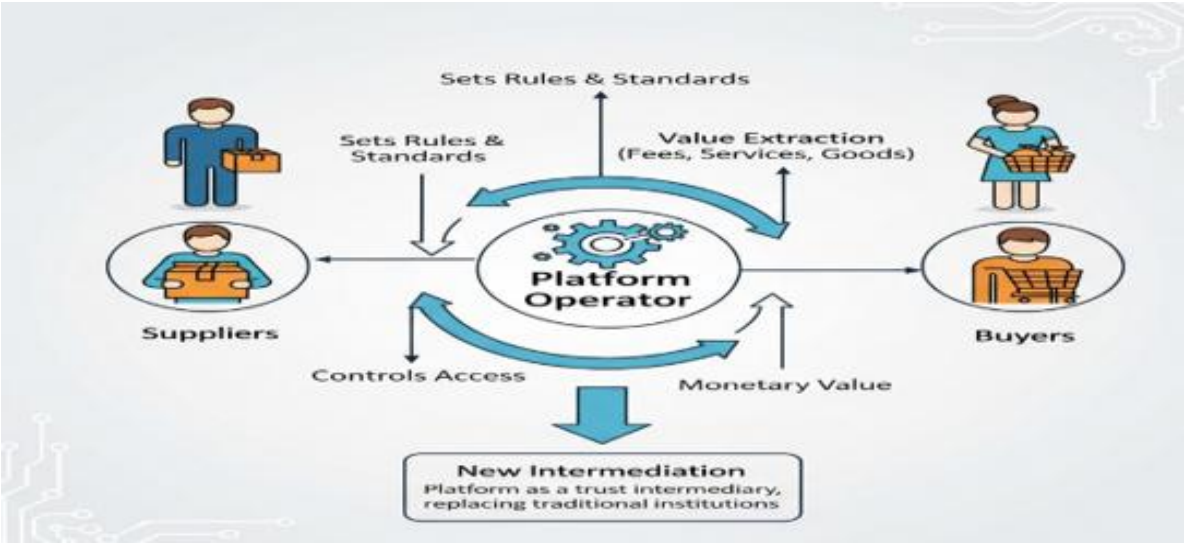

Figure 4. Platform Capitalism in Digital Trust Systems *Source: Authors Creation*

Platform-based trust systems typically involve the creation of digital ecosystems where multiple stakeholders interact according to rules and standards established by platform operators [8,20]. These platforms may provide valuable coordination functions, but they also create new dependencies and power asymmetries. Platform operators gain significant influence over how trust is constructed and maintained within their ecosystems, including the ability to modify rules, exclude participants, and extract value from user interactions.

The governance of platform-based trust systems involves complex negotiations between different stakeholder groups with varying interests and capabilities [6,19]. Large corporations may seek to use platforms to enhance their control over supply networks, while smaller suppliers may view participation as necessary for market access despite concerns about data sharing and dependency. These dynamics shape how digital trust architectures evolve and which forms of governance become embedded within technological systems.

3.3 Institutional Embeddedness and Path Dependencies

Digital trust systems do not emerge in institutional vacuums; they are developed and implemented within existing regulatory frameworks, industry standards, and organizational cultures that profoundly shape their design and operation [5,12]. The path dependencies created by existing institutional arrangements mean that new technologies are often adapted to fit established practices rather than transforming them fundamentally.

For example, regulatory requirements for supply chain due diligence or sustainability reporting influence how blockchain systems are designed and what information they prioritize [12,16]. Industry associations and standard-setting organizations play crucial roles in determining technical specifications and governance arrangements for digital trust platforms. Professional networks and organizational cultures shape how different actors interpret and respond to information provided by these systems.

These institutional influences mean that digital trust architectures inevitably reflect particular assumptions about legitimate authority, appropriate behavior, and valid knowledge [17,18]. Rather than creating neutral technical infrastructure, these systems embody specific governance arrangements that may privilege certain forms of expertise, favor particular organizational models, or reinforce existing power relationships. Understanding these dynamics is essential for evaluating the potential of different approaches to building digital trust in supply chains.

4. The Architecture of Digital Trust Systems

4.1 Design Choices and Governance Implications

The technical architecture of digital trust systems involves numerous design choices that have profound implications for how trust is constructed and maintained within supply networks [3,10]. These choices include decisions about data structures, consensus mechanisms, access controls, privacy protections, and integration protocols. While often presented as purely technical decisions, each of these choices embeds particular assumptions about governance and shapes the distribution of power within digital ecosystems.

Figure 5: Technical Design Choices and Their Governance Implications This framework shows how seemingly technical decisions about system architecture embed fundamental assumptions about governance, access, and power distribution within digital trust systems.

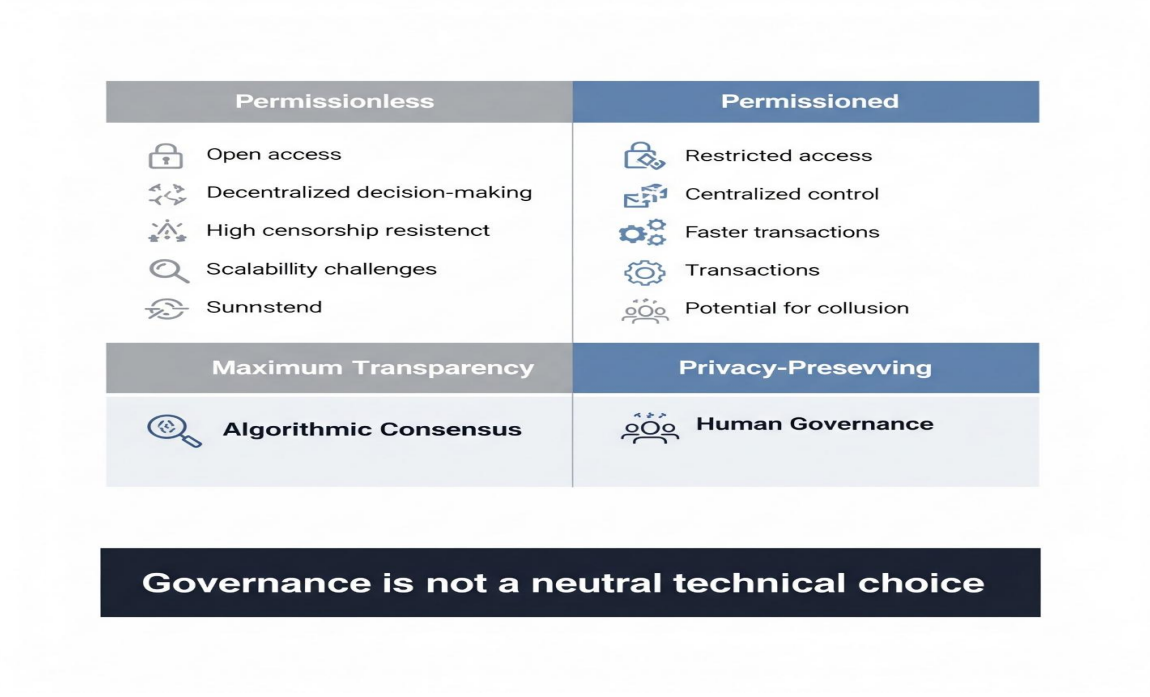

Figure 5. Technical Design Choices and Their Governance Implications Framework *Source: Authors Creation*

Consider, for example, the choice between permissioned and permissionless blockchain systems [5,11]. Permissionless systems allow anyone to participate in consensus processes, potentially democratizing access to trust infrastructure. However, they may be less suitable for supply chain applications where participants need to meet specific qualifications or comply with regulatory requirements. Permissioned systems provide greater control over participation but concentrate power in the hands of those who determine access criteria.

Similarly, decisions about data privacy and access controls reflect different philosophies about information sharing and transparency [18]. Some digital trust systems prioritize maximum transparency, making all transaction data visible to all participants. Others implement sophisticated privacy-preserving technologies that allow verification of claims without revealing underlying data. These choices have significant implications for competitive dynamics, regulatory compliance, and the distribution of information advantages within supply networks.

4.2 Identity and Verification Mechanisms

Digital trust systems must address fundamental questions about identity and verification that have no purely technical solutions [17,18]. How do we ensure that digital identities correspond to real-world entities? Who has the authority to verify claims about product origins, manufacturing processes, or sustainability practices? How do we handle disputes about the accuracy or completeness of recorded information?

The answers to these questions inevitably involve governance decisions about legitimate authority and acceptable evidence [10,14]. Traditional approaches often rely on certification bodies, industry associations, or regulatory agencies to provide verification services. Digital trust systems may create new roles for technical validators or community-based verification mechanisms, but they cannot eliminate the need for social processes that establish and maintain legitimacy.

Moreover, the integration of digital identity systems with existing institutional frameworks creates complex dependencies and potential points of failure [5,12]. If blockchain-based supply chain systems rely on government-issued business registrations or industry certifications for identity verification, they become vulnerable to weaknesses or corruption in these underlying systems. The challenge is not simply technical but involves building resilient governance arrangements that can adapt to changing circumstances while maintaining legitimacy.

4.3 Interoperability and Standards Governance

The development of digital trust systems in global supply chains raises important questions about interoperability and standards governance [3,13]. As different organizations and industries develop their own blockchain-based solutions, the risk of creating fragmented digital ecosystems that cannot communicate effectively becomes significant. Achieving interoperability requires coordination mechanisms that go beyond technical specifications to address governance arrangements and business models.

Standards governance involves negotiations between different stakeholder groups with varying interests in how digital trust systems should operate [6,19]. Technology vendors may prefer proprietary solutions that create competitive advantages, while users may favor open standards that prevent lock-in effects. Regulatory agencies may require certain features or capabilities, while industry associations may promote standards that reflect the preferences of their members.

The political economy of standards governance means that technical decisions about interoperability are never neutral [8,20]. They reflect particular assumptions about how digital ecosystems should be organized and who should control key infrastructure components. Understanding these dynamics is essential for evaluating different approaches to building digital trust architectures that can support the complexity and diversity of global supply networks.

5. Trust Formation in Complex Networks

5.1 Network Effects and Trust Dynamics

The formation of trust in global supply chains cannot be understood solely through bilateral relationships between buyers and suppliers; it must be analyzed as a network phenomenon where trust relationships emerge from complex interactions between multiple actors [1,7]. Digital trust systems operate within these network contexts and may either reinforce or disrupt existing trust patterns depending on their design and implementation.

Figure 6: Trust Formation in Centralized vs Distributed Networks This diagram compares how trust operates in centralized networks dominated by powerful buyers versus distributed networks with multiple trust pathways, illustrating how digital trust systems can either reinforce or transform existing network structures.

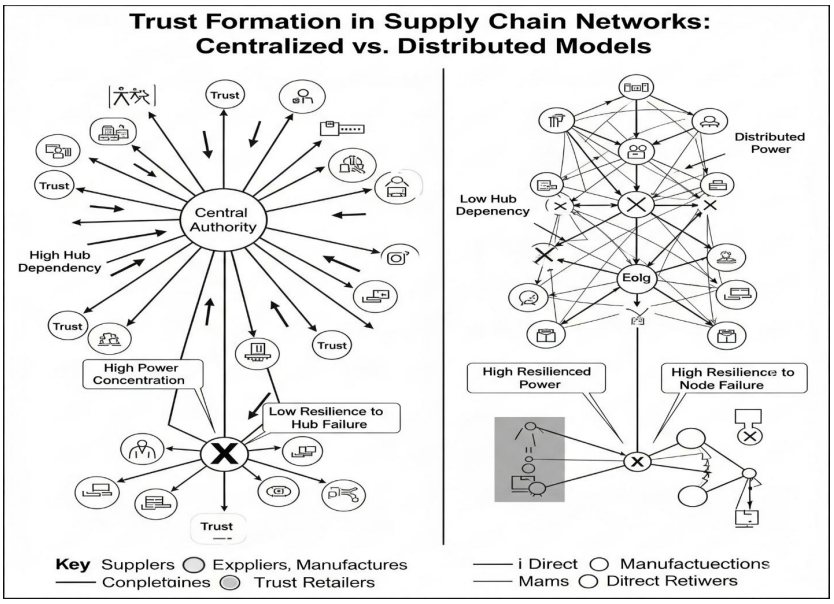

Figure 6. Trust formation in Supply Chain Network Centralized Vs Distributed Models *Source: Authors Creation*

Network effects play a crucial role in determining the success of digital trust platforms [8,19]. As more participants join a platform, it becomes more valuable for existing users, potentially creating positive feedback loops that drive adoption. However, these network effects can also create barriers to entry for competing platforms and concentrate power in the hands of early platform developers or dominant users.

The structure of supply networks influences how trust relationships develop and evolve over time [6,9]. Highly centralized networks with dominant buyers may experience different trust dynamics than more distributed networks with multiple centers of power. Digital trust systems may either preserve these existing structures or create opportunities for new forms of network organization, depending on how they are designed and governed.

5.2 Cultural and Institutional Variations

Global supply chains operate across diverse cultural and institutional contexts that shape how trust is understood and practiced [12,14]. What constitutes trustworthy behavior varies significantly between different business cultures, legal systems, and social contexts. Digital trust systems that assume universal definitions of trustworthiness may encounter resistance or unintended consequences when implemented across these diverse environments.

For example, some cultures emphasize relationship-based trust that develops through personal interactions and long-term commitments, while others favor institution-based trust that relies on formal rules and third-party enforcement mechanisms [4,18]. Digital trust systems that prioritize algorithmic verification and automated processes may conflict with relationship-based approaches to trust formation, potentially undermining rather than enhancing trust in certain contexts.

Similarly, different regulatory environments create varying requirements for data protection, cross-border information flows, and supply chain due diligence [5,16]. Digital trust systems must navigate these diverse requirements while maintaining coherent governance arrangements across multiple jurisdictions. This challenge cannot be solved purely through technical design but requires sophisticated governance mechanisms that can accommodate institutional diversity while preserving system integrity.

5.3 Resilience and Adaptation

Trust in global supply chains must be resilient enough to survive disruptions while remaining adaptable to changing circumstances [1,13]. The COVID-19 pandemic demonstrated how quickly supply network relationships can be strained or severed, requiring new approaches to risk management and contingency planning. Digital trust systems must be designed to support both stability and flexibility in these dynamic environments.

Figure 7: Balancing Stability and Adaptability in Trust Systems This framework illustrates the fundamental tension between the stability required for trust and the adaptability needed for resilience, highlighting key design challenges for digital trust architectures.

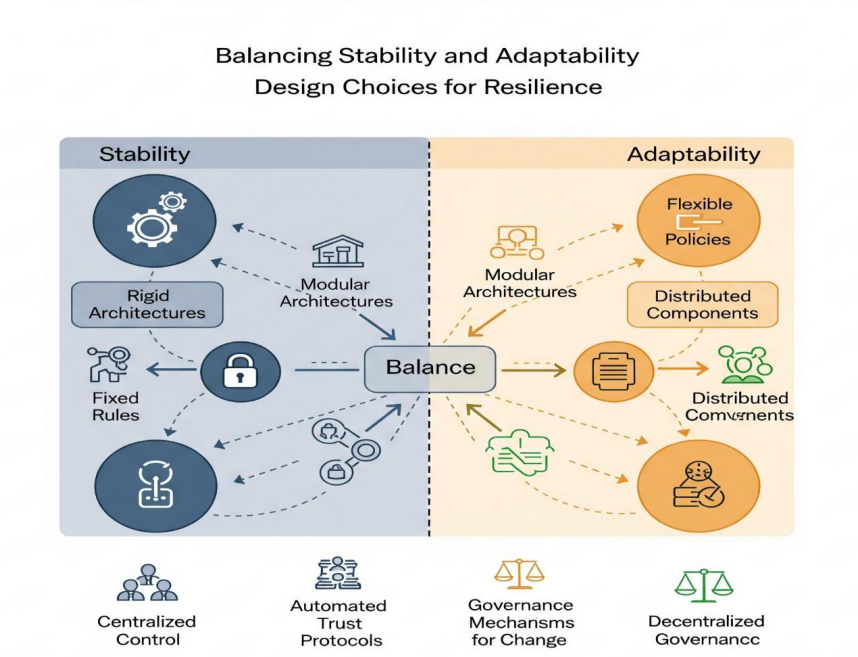

Figure 7. Balancing Stability and Adaptability Design Choices for resilience *Source: Authors Creation*

Resilient trust systems require redundancy and diversity that prevent single points of failure [6,10]. This may involve maintaining multiple verification mechanisms, preserving alternative communication channels, or developing backup governance arrangements that can function when primary systems are disrupted. However, redundancy and diversity create complexity that may undermine efficiency or create new vulnerabilities.

The challenge of building adaptive trust systems is particularly acute in the context of emerging technologies and evolving regulatory requirements [11,17]. Digital trust architectures must be able to incorporate new capabilities, respond to changing stakeholder expectations, and comply with evolving legal frameworks without compromising the stability that trust relationships require. This balance between stability and adaptability represents one of the most significant design challenges facing digital trust systems.

6. Platform Governance and Power Dynamics

6.1 The Political Economy of Trust Platforms

Digital trust platforms in supply chains operate within broader political economies that shape their development, governance, and effects [7,20]. These platforms are not neutral technical infrastructure but rather embody assumptions about market organization, value creation, and legitimate authority. Understanding their political dimensions is essential for evaluating their potential to enhance or undermine trust in supply chain relationships.

Figure 8: Political Economy of Digital Trust Platforms This diagram shows how different funding sources and ownership structures create varying incentives and governance arrangements in digital trust platforms, demonstrating the political nature of supposedly neutral technical infrastructure.

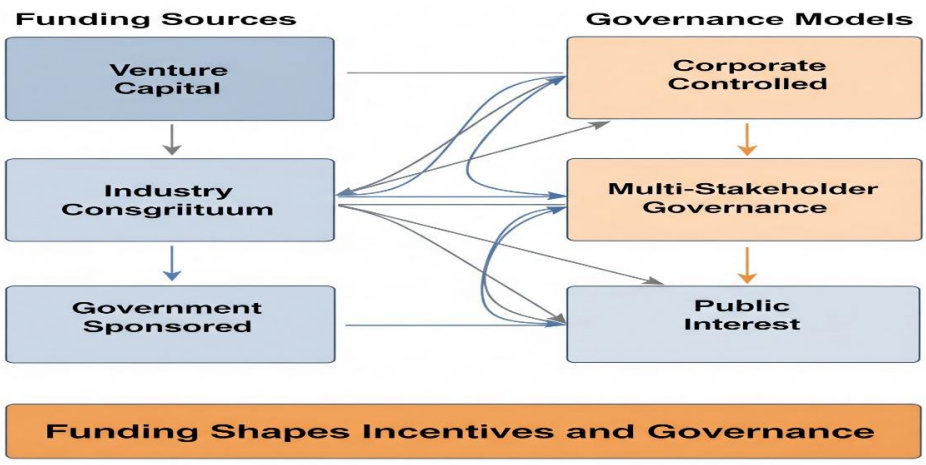

Figure 8. Political Economy of Digital Trust Platforms *Source: Authors Creation*

The financing and ownership structures of trust platforms significantly influence their governance arrangements and strategic priorities [8,19]. Platforms funded by venture capital may prioritize rapid growth and market capture over sustainability or stakeholder welfare. Those developed by industry consortiums may reflect the interests of dominant members rather than the broader ecosystem. Government-sponsored platforms may serve policy objectives that conflict with commercial interests.

Moreover, the business models adopted by trust platforms create incentives that shape how they operate and evolve [6,14]. Platforms that charge transaction fees may prioritize volume over quality, while those that monetize data may have incentives to collect more information than necessary for trust verification. Subscription-based models may favor larger users who can afford higher fees, potentially excluding smaller participants from trust ecosystems.

6.2 Algorithmic Authority and Governance

Digital trust systems increasingly rely on algorithmic processes for verification, scoring, and decision-making [18,17]. While these automated mechanisms may enhance efficiency and reduce human bias, they also create new forms of algorithmic authority that operate with limited transparency or accountability. The governance of algorithmic systems raises fundamental questions about legitimacy, fairness, and democratic participation.

Algorithmic trust systems embed particular assumptions about what constitutes evidence, how different factors should be weighted, and what outcomes are desirable [10,16]. These assumptions may not be visible to users or may be difficult to challenge through traditional governance mechanisms. The opacity of algorithmic decision-making can undermine trust rather than enhancing it, particularly when stakeholders cannot understand how determinations are made.

Furthermore, the data used to train and operate algorithmic trust systems may reflect historical biases or structural inequalities that get reproduced and amplified through automated processes [12]. If trust algorithms are trained on data that reflects past discrimination against certain suppliers or regions, they may perpetuate these patterns even when they are not explicitly programmed to do so. Addressing these challenges requires governance mechanisms that can ensure algorithmic accountability and fairness.

6.3 Resistance and Alternative Approaches

The implementation of digital trust systems in supply chains does not occur without resistance from stakeholders who may view these technologies as threatening their interests or autonomy [5,13]. Understanding patterns of resistance and the development of alternative approaches is crucial for assessing the likely evolution of digital trust architectures and their social implications.

Figure 9: Resistance Patterns and Alternative Development This framework illustrates different forms of resistance to dominant digital trust platforms and how they lead to the development of alternative approaches that embody different values and governance arrangements.

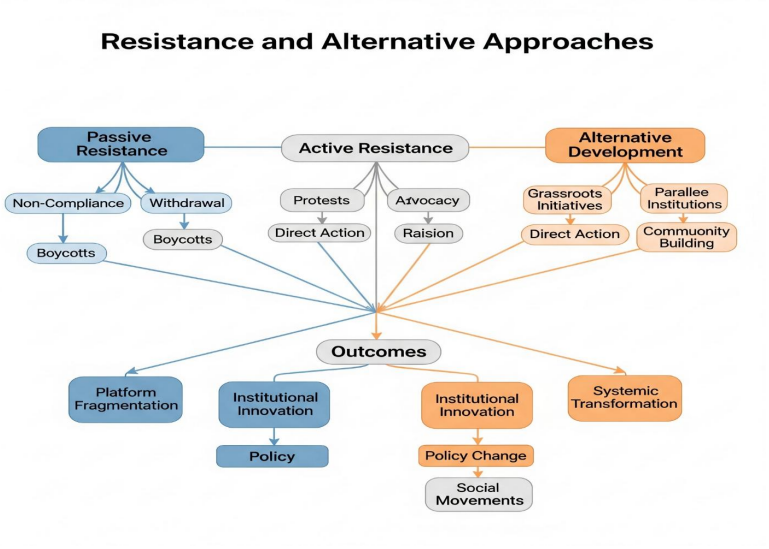

Figure 9. Resistance Patterns and Alternative Approaches *Source: Authors Creation*

Resistance to digital trust systems may take various forms, from passive non-compliance to active development of alternative platforms [6,9]. Suppliers may resist demands for greater transparency that expose their operations to competitive scrutiny or regulatory enforcement. Workers may oppose monitoring technologies that increase surveillance or performance pressure. Communities may reject systems that prioritize efficiency over local values or environmental protection.

These forms of resistance often lead to the development of alternative approaches to digital trust that embody different values and governance arrangements [7,14]. Community-based verification systems, cooperative platforms, and public digital infrastructure represent attempts to create trust architectures that serve broader stakeholder interests rather than just platform operators or dominant users. Understanding these alternatives is essential for imagining more democratic and equitable approaches to digital trust in supply chains.

7. Implications for Supply Chain Governance

7.1 Rethinking Transparency and Accountability

The analysis of digital trust as a socio-governance construct has significant implications for how we approach transparency and accountability in global supply chains [16]. Rather than viewing transparency as an unqualified good that automatically enhances trust, we must recognize that transparency systems embody particular power relationships and may create new forms of vulnerability or exploitation.

Figure 10: Rethinking Transparency and Accountability This comparison contrasts traditional information-centric transparency approaches with contextual transparency frameworks that consider power dynamics and relationship-building in designing accountability mechanisms.

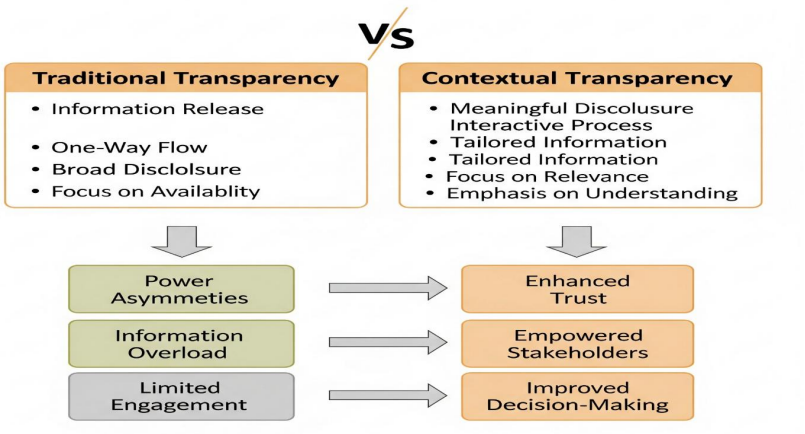

Figure 10. Rethinking Transparency and Accountability *Source: Authors Creation*

Effective transparency systems must be designed with careful attention to power dynamics and stakeholder interests [12,17]. This may involve creating asymmetric transparency arrangements that protect vulnerable actors while ensuring that powerful actors remain accountable for their impacts. It may also require developing privacy-preserving technologies that allow verification of claims without exposing sensitive commercial information.

Moreover, transparency alone is insufficient for accountability without corresponding mechanisms for enforcement and remediation [18,19]. Digital trust systems must be coupled with governance arrangements that can respond effectively to violations or disputes. This may involve developing new forms of multi-stakeholder governance that can coordinate action across diverse institutional contexts while respecting different legal and cultural frameworks.

7.2 Building Inclusive Digital Trust Ecosystems

Creating digital trust systems that serve the interests of all supply chain stakeholders requires explicit attention to inclusion and participation [8,20]. Many current approaches to blockchain-based supply chain solutions risk creating new forms of digital exclusion that marginalize smaller suppliers, developing country producers, or other vulnerable actors.

Inclusive digital trust ecosystems must address barriers to participation that go beyond technical access to include capacity building, governance representation, and value sharing [4,6]. This may involve developing simplified interfaces for less technically sophisticated users, providing training and support for platform adoption, or creating governance mechanisms that ensure meaningful participation by diverse stakeholders.

Furthermore, inclusive approaches to digital trust must recognize and accommodate different forms of knowledge and verification practices [9,14]. Rather than imposing uniform standards based on dominant technical or cultural frameworks, effective trust systems may need to support multiple verification mechanisms that reflect the diversity of global supply networks while maintaining overall system integrity.

7.3 Regulatory Implications and Policy Responses

The emergence of digital trust systems in global supply chains raises important questions for regulatory policy and international coordination [5,11]. Existing regulatory frameworks were generally developed for different technological and organizational contexts and may be inadequate for governing complex digital trust ecosystems that operate across multiple jurisdictions.

Figure 11: Regulatory Challenges and Policy Responses This framework maps the complex regulatory challenges posed by digital trust systems and outlines potential policy responses that balance innovation promotion with stakeholder protection and democratic governance.

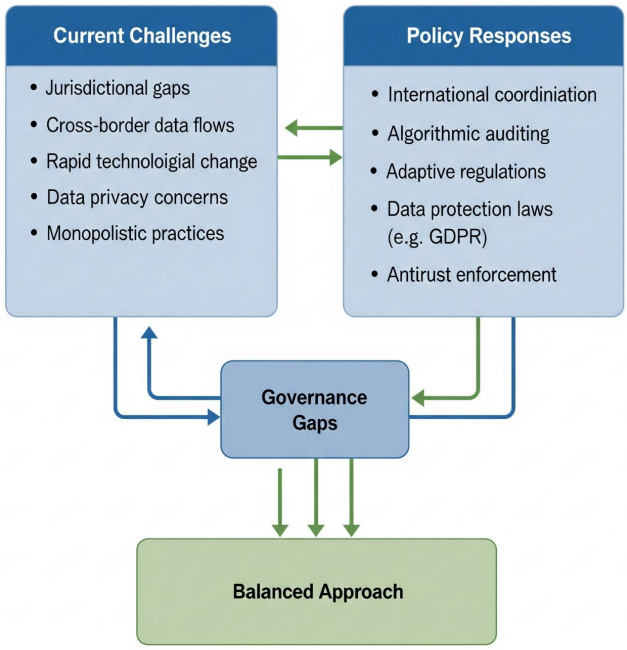

Figure 11. Regulatory Challenges and Policy Responses *Source: Authors Creation*

Regulatory responses to digital trust systems must balance the promotion of innovation with the protection of stakeholder interests and public values [13,16]. This may involve developing new forms of algorithmic auditing, ensuring data protection and privacy rights, or preventing the abuse of dominant positions in digital platforms. International coordination will be essential for addressing cross-border issues and preventing regulatory arbitrage.

Moreover, regulatory approaches must recognize the inherently political nature of digital trust systems and their governance implications [2,17]. Rather than treating these technologies as neutral technical infrastructure, policy makers must engage with questions about democratic participation, power distribution, and social justice that arise from their implementation. This may require new forms of multi-stakeholder governance that can coordinate across different institutional domains while maintaining legitimacy and effectiveness.

8. Future Directions and Research Implications

8.1 Methodological Considerations

The analysis of digital trust as a socio-governance construct requires methodological approaches that can capture both technical and social dimensions of these systems [1,10]. Traditional approaches that focus primarily on technical performance or economic efficiency may miss crucial aspects of how trust systems operate in practice and their broader social implications.

Future research on digital trust in supply chains should employ mixed-method approaches that combine technical analysis with ethnographic observation, stakeholder interviews, and institutional analysis [7,19]. This may involve studying how different actors interpret and respond to information provided by digital trust systems, how governance arrangements evolve over time, or how cultural and institutional contexts shape technology adoption and use.

Moreover, research on digital trust systems must be attentive to power dynamics and the political dimensions of technology development and implementation [3,12]. This may require critical approaches that examine whose interests are served by particular technical designs, how costs and benefits are distributed among different stakeholders, or how resistance and alternatives emerge in response to dominant approaches.

8.2 Theoretical Development

The conceptualization of digital trust as a socio-governance construct opens up numerous avenues for theoretical development that could enhance our understanding of technology-society relationships in global economic systems [4,14]. This may involve integrating insights from science and technology studies, political economy, and organization theory to develop more nuanced frameworks for analyzing digital trust systems.

Particularly promising areas for theoretical development include the governance of algorithmic systems, the political economy of platform ecosystems, and the dynamics of trust formation in networked organizations [18,20]. These theoretical advances could inform both academic research and practical efforts to design more effective and equitable digital trust architectures.

Furthermore, theoretical work on digital trust should engage with broader questions about democracy, justice, and sustainability in global economic systems [6,16]. This may involve examining how digital trust systems could support more democratic forms of supply chain governance, promote social and environmental sustainability, or reduce inequalities between different regions and communities.

8.3 Practical Applications

The insights from analyzing digital trust as a socio-governance construct have important implications for practitioners involved in designing, implementing, or governing digital trust systems [2,13]. These insights suggest the need for more participatory approaches to system design that involve diverse stakeholders in decisions about governance arrangements and technical specifications.

Figure 12: Practical Applications and Design Principles This framework provides concrete design principles and an implementation roadmap for practitioners seeking to develop digital trust systems that acknowledge their socio-governance nature.

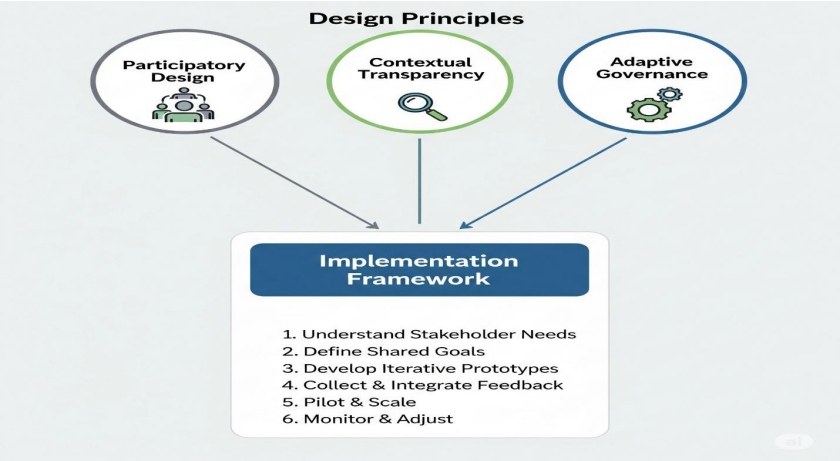

Figure 12. Practical Applications and Design Principles Framework *Source: Authors Creation*

Practical applications may involve developing new methodologies for stakeholder engagement, creating governance frameworks that can balance different interests and values, or designing technical architectures that support diverse forms of participation and representation [8,17]. This may also require new forms of professional education and capacity building that help practitioners understand the social and political dimensions of their technical work.

Moreover, practical efforts to build digital trust systems should be informed by ongoing research and evaluation that can identify unintended consequences, emerging challenges, or opportunities for improvement [9,11]. This may involve developing new metrics for assessing the social and political impacts of digital trust systems, creating feedback mechanisms that allow for continuous learning and adaptation, or establishing governance processes that can respond effectively to changing circumstances and stakeholder needs.

9. Conclusion

This viewpoint paper has argued that digital trust in global supply chains represents a fundamentally socio-governance construct rather than merely a technological function. While blockchain and related distributed ledger technologies offer valuable capabilities for enhancing transparency and traceability, their implementation within existing power structures often reproduces rather than transforms underlying trust asymmetries and governance arrangements.

The analysis reveals how the architecture of digital trust systems embeds particular assumptions about legitimate authority, appropriate transparency, and acceptable forms of verification. These design choices have profound implications for how power is distributed within supply networks, which stakeholders can participate meaningfully in trust ecosystems, and how different forms of value are created and captured. Rather than representing neutral technical infrastructure, digital trust systems operate as governance mechanisms that shape relationships between supply chain actors.

The perspective developed here challenges prevailing techno-solutionist narratives that position blockchain as a panacea for supply chain trust deficits. Instead, it calls for more nuanced approaches that recognize the inherently social and political dimensions of trust formation in complex organizational networks. This requires moving beyond narrow focuses on information transparency toward comprehensive trust architectures that acknowledge the diverse ways in which trust is constructed and maintained across different cultural and institutional contexts.

The implications of this analysis extend beyond academic understanding to encompass practical questions about how to design more effective and equitable digital trust systems. This may involve developing more participatory approaches to platform governance, creating inclusive mechanisms for stakeholder representation, or designing technical architectures that support diverse forms of verification and accountability. It also requires regulatory frameworks that can govern digital trust ecosystems while promoting innovation and protecting stakeholder interests.

Future research on digital trust in supply chains should employ methodological approaches that can capture both technical and social dimensions of these systems. This includes examining how different actors interpret and respond to digital trust technologies, how governance arrangements evolve over time, and how cultural and institutional contexts shape technology adoption and use. Theoretical development should integrate insights from multiple disciplines to develop more nuanced frameworks for analyzing the relationship between technology and governance in global economic systems.

The emergence of digital trust systems in global supply chains represents both an opportunity and a challenge for creating more transparent, accountable, and sustainable forms of economic organization. However, realizing this potential requires moving beyond blockchain hype toward more sophisticated understandings of how technology intersects with social, economic, and political dynamics in shaping supply chain relationships. Only by acknowledging the fundamentally socio-governance nature of digital trust can we hope to design systems that serve the interests of all stakeholders while supporting broader goals of sustainability, justice, and democratic participation in global economic governance.

The path forward requires sustained collaboration between technologists, social scientists, practitioners, and policymakers to develop digital trust architectures that can navigate the complexity of global supply networks while promoting values of transparency, accountability, and inclusion. This is not merely a technical challenge but a fundamental question about how we want to organize economic relationships in an increasingly digital and interconnected world.

References

[1] Bonadio, B., Huo, Z., Levchenko, A. A., & Pandalai-Nayar, N. (2021). Global supply chains in the pandemic. Journal of International Economics, 133, 103534. https://doi.org/10.1016/j.jinteco.2021.103534

[2] Chen, J., Cai, W., Luo, J., & Mao, H. (2024). How does digital trust boost open innovation? Evidence from a mixed approach. Technological Forecasting & Social Change, 212, 123953. https://doi.org/10.1016/j.techfore.2024.123953

[3] Chen, Q., & Duan, Y. (2023). Impact of information disclosure on global supply chain greenwashing: Is more information transparency always better? Transportation Research Part E, 178, 103288. https://doi.org/10.1016/j.tre.2023.103288

[4] Cromwell, J., Turkson, C., Dora, M., & Yamoah, F. A. (2025). Digital technologies for traceability and transparency in the global fish supply chains: A systematic review and future directions. Marine Policy, 178, 106700. https://doi.org/10.1016/j.marpol.2025.106700

[5] Farahani, B., Firouzi, F., & Luecking, M. (2020). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177, 102936. https://doi.org/10.1016/j.jnca.2020.102936

[6] Glassberg, I., Ilan, Y. B., & Zwilling, M. (2025). The key role of design and transparency in enhancing trust in AI-powered digital agents. Journal of Innovation & Knowledge, 10(5), 100770. https://doi.org/10.1016/j.jik.2025.100770

[7] Gourisetti, S. N. G., Cali, Ü., Choo, K. K. R., Escobar, E., Gorog, C., Lee, A., Lima, C., Mylrea, M., Pasetti, M., Rahimi, F., Reddi, R., & Sani, A. S. (2021). Standardization of the distributed ledger technology cybersecurity stack for power and energy applications. Sustainable Energy, Grids and Networks, 28, 100553. https://doi.org/10.1016/j.segan.2021.100553

[8] Gustafsson, M. T., Schilling-Vacaflor, A., & Pahl-Wostl, C. (2024). Governing transnational water and climate risks in global supply chains. Earth System Governance, 21, 100217. https://doi.org/10.1016/j.esg.2024.100217

[9] Gurbuz, M. C., Yurt, O., Ozdemir, S., Sena, V., & Yu, W. (2022). Global supply chains risks and COVID-19: Supply chain structure as a mitigating strategy for small and medium-sized enterprises. Journal of Business Research, 155, 113407. https://doi.org/10.1016/j.jbusres.2022.113407

[10] Hashimy, L., Treiblmaier, H., & Jain, G. (2021). Distributed ledger technology as a catalyst for open innovation adoption among small and medium-sized enterprises. Journal of High Technology Management Research, 32(1), 100405. https://doi.org/10.1016/j.hitech.2021.100405

[11] Inomata, S., & Hanaka, T. (2023). Measuring exposure to network concentration risk in global supply chains: Volume versus frequency. Structural Change and Economic Dynamics, 68, 177-193. https://doi.org/10.1016/j.strueco.2023.10.002

[12] Latsiou, A. C., Nygård, A. R., Katsikas, S., & Lambrinoudakis, C. (2025). Never trust - always verify: Assessing the cybersecurity trustworthiness of suppliers in the digital supply chain. Procedia Computer Science, 254, 98-107. https://doi.org/10.1016/j.procs.2025.02.068

[13] Li, J., & Kassem, M. (2021). Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction. Automation in Construction, 132, 103955. https://doi.org/10.1016/j.autcon.2021.103955

[14] Ouassou, E. H., Onyeaka, H., Tamasiga, P., & Bakwena, M. (2024). Carbon transparency in global supply chains: The mediating role of institutional and innovative capacity. Energy Strategy Reviews, 53, 101405. https://doi.org/10.1016/j.esr.2024.101405

[15] Poo, M. C. P., Wang, T., & Yang, Z. (2024). Global food supply chain resilience assessment: A case in the United Kingdom. Transportation Research Part A, 181, 104018. https://doi.org/10.1016/j.tra.2024.104018

[16] Rahimi, M., Maghsoudi, M., & Shokouhyar, S. (2024). The convergence of IoT and sustainability in global supply chains: Patterns, trends, and future directions. Computers & Industrial Engineering, 197, 110631. https://doi.org/10.1016/j.cie.2024.110631

[17] Shiraishi, C. S. H., Roriz, C. L., Carocho, M., Prieto, M. A., Abreu, R. M. V., Barros, L., & Heleno, S. A. (2024). Blockchain revolution in food supply chains: A positive impact on global food loss and waste. Food Chemistry, 467, 142331. https://doi.org/10.1016/j.foodchem.2024.142331

[18] Strazzullo, S. (2024). Fostering digital trust in manufacturing companies: Exploring the impact of industry 4.0 technologies. Journal of Innovation & Knowledge, 9(4), 100621. https://doi.org/10.1016/j.jik.2024.100621

[19] Tiwari, S., Sharma, P., Choi, T. M., & Lim, A. (2023). Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. Transportation Research Part E, 170, 103012. https://doi.org/10.1016/j.tre.2022.103012

[20] Wang, H., Yu, S., Yang, Y., Wang, M., & Zhou, P. (2025). Assessing carbon emissions along global supply chains from technology perspective: A network production decomposition analysis. Ecological Economics, 233, 108582. https://doi.org/10.1016/j.ecolecon.2025.108582