



Blockchain without Blocks: Why Cryptographic Finance Fails to Produce Trust in Digitized Supply Chains

Dr. Surayya Jamal¹, Ahmad Zeb² & Dr. Syed Noman Mustafa³

¹Abdul Wali Khan University Mardan, Pakistan, Email: surayyajml@gmail.com

²Lecturer, Department of Management Sciences, Islamia College Peshawar, Pakistan, Email: ahmad.zeb@icp.edu.pk

³Lecturer, Department of Management Sciences, Islamia College Peshawar, Pakistan,
Email: noman.mustafa@icp.edu.pk

ARTICLE INFO

Article History:

Received:	January	15, 2026
Revised:	February	21, 2026
Accepted:	March	06, 2026
Available Online:	March	16, 2026

Keywords:

Blockchain, Cryptographic Finance, Governance, Supply Chains, Trust, Transparency

Corresponding Author:

Dr. Surayya Jamal

Email:

surayyajml@gmail.com



ABSTRACT

Blockchain technology has been widely heralded as a transformative tool capable of establishing trust in digitized supply chains through cryptographic finance, immutability, and decentralized ledgers. However, empirical evidence and recent analyses suggest that these technological mechanisms alone are insufficient to generate holistic trust among supply chain stakeholders. This study critically examined why blockchain adoption often failed to produce sustained trust, despite enhancing transparency, traceability, and data integrity. A qualitative, theory-driven methodology was employed, analyzing peer-reviewed literature across supply chain management, financial technology, and digital governance domains. The findings revealed that trust remained deeply rooted in social, relational, and institutional dimensions, which blockchain technologies could not replace. Off-chain data dependencies, governance gaps, regulatory ambiguities, and power asymmetries emerged as key factors undermining trust formation. Furthermore, blockchain often displaced trust from human and institutional actors to opaque technical systems, reducing accountability and stakeholder confidence. The study concluded that blockchain should be conceptualized as a supportive infrastructure for trust rather than a substitute for relational and institutional mechanisms. Recommendations included integrating blockchain with hybrid governance models, legal frameworks, and inclusive participation strategies to enhance trust resilience. The study also identified future research directions focusing on cross-industry comparisons, socio-technical interactions, and emerging blockchain alternatives. These insights contribute to a more nuanced understanding of the socio-technical limits of blockchain in supply chain digitization and highlight the critical role of governance and institutional alignment in sustaining trust.

Introduction

During the last ten years, blockchain technology enthusiastically found a basis in infrastructure as a metric of the supply chain process digitization, specifically cryptographic finance and decentralized ecosystems. The scholars and professionals made a hypothesis that the lack of traditional trust infrastructure and middlemen would be removed by blockchain decentralization, cryptographic integrity, and distributed consensus algorithms, which would produce a so-called trustless but trustworthy digital supply chain ecosystem (Yavaprabhas et al., 2023; Alkhudary, 2022). Nonetheless, new findings suggested that the expected trust benefits were not consistently experienced in the actual supply chain especially in situations that involved complex inter organizational dependencies, off-chain data relationships, and multi party governance systems. Previous research indicated that the capacity of blockchain to increase transparency and traceability did not transfer into significant trust between the supply chain partners (Yavaprabhas et al., 2023; Shahzad et al., 2023). Such inconsistencies led to the critical consideration of the possibility of cryptographic finance solutions to simply moved the issues of trust to the technical artifacts to the many-dimensional character of the issue.

However, with its rampant use, there were a high number of trust deficits in blockchain-based supply chains experienced among the practitioners. As an example, on-chain and off-chain data were bridged by oracle mechanisms which brought about additional vulnerabilities and jeopardized the integrity and reliability of the data (Karaduman et al., 2025; ScienceDirect, 2025). Furthermore, the inconsistencies in the literature also allowed finding that blockchain could strengthen the institutional trust in specific conditions whereas in others it did not influence the relational and affect-based trust among the partners (Yavaprabhas et al., 2023). The dichotomy exacerbated the fact that there were significant theoretical and practical gaps between the laws of cryptographic finance and the laws of the supply chain governance. Such events brought to view the necessity of reconsidering the perceived equality between the cryptographic guarantees and supply chain trust.

The supply chain management has remained a major issue of concern in a global business and sustainability with trust embodying the key issue of cooperation, exchange of information, and reduction of risk (Shahzad et al., 2023). Blockchain was promoted in the context of supply chain finance as one of the means of eliminating information asymmetry and increasing the efficiency of financing, although empirical research indicated that trust remained dependent on rather old institutional relations and governance systems than on cryptographic verification only (Trawnih et al., 2025). As a result, the promised removal of trust in the form of trustless design might have been too positive -and obscured the socio-technical mechanisms of providing chains ecosystems.

This study thus heavily revisited an assumption that cryptographic finance naturally delivered trust in digital supply chains. It sought to decouple technical guarantees and substantive trust results and to put blockchain execution into more general contexts of governance, organization and even socio-economic environments. The study aimed to simplify the understanding of how the adoption of blockchain influenced and, in most instances, did not influence the presence of trust between supply chain actors by synthesizing recent academic literature.

Research Background

The inception of blockchain technology as the data protocol behind Bitcoin was a decentralized and unmodifiable registry that was supposed to reduce cases of two-spending and the necessity of centralized intermediaries (Durach et al., 2021; Cryptoeconomics, n.d.). With the increased adoption, blockchain was considered as a prospective solution in supply chain management to provide real-time tracking, visibility, and contracts that could be executed automatically through smart contracts (Karaduman et al., 2025). The multiple independent stakeholder and compound

flow of goods, finance, and information that define supply chains were anticipated to have access to the distributed ledger characteristics of blockchain, especially by boosting the traceability and minimizing fraud (Shahzad et al., 2023; Wamba Fosso, 2022).

The researchers started to look into the way blockchain could foster supply chain trust, and the conceptualization of trust was based on not only the digital verification but the relationship and institutional confidence between the partners (Yavaprabhas et al., 2023). The systematic reviews demonstrated varying levels of evidence: some of them indicated that blockchain can serve a role of a trust-building machine by enhancing transparency and traceability, and others showed that it has weaknesses in influencing more profound forms of interorganizational trust (Yavaprabhas et al., 2023; Alkhudary, 2022). This literature highlighted the importance of the need to differentiate between the technological promise and the social creation of trust as the effects of blockchain depended on the current climate of trust and supply chain relations.

These developments notwithstanding, practical applications showed that there were serious issues including blockchain oracle problem wherein external data feeds required to execute smart contracts created new sources of trust problems (Hassan, 2023; ScienceDirect, 2025). Since oracles were not built into the blockchain primordial consensus mechanism, they predisposed easy breakdowns or manipulations, hence compromising trust in available data and decision logic. These technical issues were particularly acute in the field of supply chain financing, in which precise and timely data were vital when it came to the distribution of credit and assessment of risks (Trawnih et al., 2025).

Empirical evidence indicated that trust in blockchain-driven supply chains was not necessarily converted to a better and more effective collaboration or performance when other governance systems, including legal frameworks and institutional base, were in place (Shahzad et al., 2023). These results posed the idea that blockchain could be used as a supplement to rather than an alternative of existing information-integrity frameworks.

Objectives of the Study

1. To assess the extent to which blockchain technology was theorized and implemented as a trust-producing mechanism in digitized supply chains based on recent academic research.
2. To identify and critically analyze the technical and socio-organizational limitations that prevented cryptographic finance mechanisms from producing substantive trust among supply chain partners.
3. To examine the role of off-chain data interactions—particularly oracles—and institutional governance in shaping trust outcomes within blockchain-enabled supply chains.

Research Questions

Q1. How was blockchain technology theorized to produce trust in digitized supply chains in recent scholarly literature?

Q2. What technical and socio-organizational challenges prevented cryptographic finance from generating trust among supply chain stakeholders?

Q3. How did off-chain data interactions, such as oracle mechanisms, affect trust outcomes in blockchain-enabled supply chain systems?

Significance of the Study

This study helped the current knowledge by disrupting the common discourse according to which blockchain was an inherently trust-generating phenomenon in supply chains, identically detailing important gaps between theory and practice. The synthesis of contemporary academic literature provided a subtle insight into the nature and characteristics of trust as a socio-technical phenomenon and not technical operation and oral fulfills an acute deficiency of unambiguous research on blockchain. In practice, the results were applicable to supply chain professionals, policy makers and technology deployers who aim at aligning blockchain applications with sensible trust levels and governance frameworks. Future research was informed by the study too since it confirmed major areas in which socio-technical integration, legal frameworks, and governance mechanisms should accompany cryptographic finance solutions to achieve a meaningful level of trust in digitized supply chains.

Literature Review

Blockchain and the Reconfiguration of Trust in Supply Chains

The recent scholarship conceived blockchain as not a substitute of trust, but as a process that redefined the concept of trust in the supply chain systems. Researchers claimed that blockchain shifted trust in interpersonal and institutional structures to technological infrastructures, and so by causing this shift, the concept of trust was perceived and practiced differently between supply chain actors (Valleri and Wright, 2022; Queiroz et al., 2023). Instead of destroying trust, blockchain systems have been discovered to transfer the latter to algorithmic verification schemes, consensus schemes, and distributed tables, which in turn demanded trust about system structure and administration.

Empirical research showed also that blockchain had different effects on various dimensions of trust in an uneven distribution. Whereas transparency and immutability reinforced cognition-based trust, relational or affect-based trust that arose through effects of long-term co-operation and common norms was poorly reinforced (Choi et al., 2024; Raza et al., 2023). This disparity provided a reason to believe that the technical guarantees offered by blockchain were not enough to counterbalance the other social and organizational premises on which the trust in supply chains was conventionally based.

Researchers highlighted the fact that trust was a requirement and in many cases not a consequence of adopting blockchain technology. Organizations felt more encouraged to adopt blockchain solutions when there was already trust between partners, especially in data exchange and coordination of governance in the blockchain (Saber et al., 2022; Kshetri, 2023). These results conflicted the deterministic accounts of blockchain-enabled trust and outlined the recalcitrant nature of the trust-to-technology adoption connection in the supply chain practice.

Cryptographic Finance, Data Integrity and Technical Constraints

The cryptographic finance literature showed severe shortcomings of blockchain in providing reliable results in digitized supply chains. Although cryptographic tools ensured immutability of data following recording, it did not address any aspect of accuracy or genuineness of data at the moment of recording, which is often also known as the garbage-in, garbage-out issue (Westerkamp et al., 2022; Treiblmaier and Garaus, 2023). This weakness was also very challenging in the supply chains that depended on the external sensors, manual entries and reporting by the third-party.

The use oracle to relay off-chain information to blockchain systems was one of the key sources of distrust that recent studies found to be causing. In Oracles put forward centralized intermediaries

and opaque decision-making layers, which were inconsistent with the ethos of decentralization. Motto and reintroduced trust dependencies (Adams et al., 2023; Alharby, and Moorsel, 2022). This meant that the stakeholders were usually forced to have faith in oracle providers, but not in the blockchain itself, which contradicts assertions of trustless verification.

The solution of cryptography to finance was limited by interoperability issues between blockchain platforms and existing enterprise environments. The researchers noted supply chain infrastructures being fragmented and variation in data standards undermined the reliability of the systems and increased the risks of governance, especially in cross-border supply chains (Zhang et al., 2024; Casino et al., 2023). The implication of these technical limitations was that cryptographic finance in isolation and without support mechanisms of institutions and organizations could develop trustworthy supply chain ecosystems.

Institutional governing and empirical trust results

Empirical research was continually showing that the outcomes of blockchain in terms of trust could only be tied to the functional processes of institutional governance and not exclusively infrastructure. Research demonstrated that the enforcement of the law, the comprehension of the regulations, and the covenantal agreement played a major role in determining whether blockchain systems would increase trust among the supply chain participants (Li et al., 2023; Koughizadeh et al., 2022). In situations where law was lax or the law was unclear, the use of blockchain failed to reduce opportunistic behavior or information asymmetry.

The use of supply chain finance was further found to demonstrate that transparency ensured by blockchain enhanced access to financing in case it was backed by reputable financial institutions and regulatory controls (Zhang and Zhao, 2024; Du et al., 2023). Cryptographic verification was not used to substitute the practice of credit assessment, rather served as a complement to the existing traditional trust developed in the structures of financial governance. This observation further strengthened the fact that the confidence in financial supply chains was still institution-based.

Longitudinal research indicated the blockchain systems usually strengthened the status quo on power imbalance instead of democratising the trust relations. The large enterprises and technology providers often used disproportionate power in permissioned blockchain to influence access rights and data visibility (Rejeb et al., 2023; Lumineau et al., 2022). Therefore, blockchain did not operate as an impartial and trust infrastructural system and rather as a socio-technical system that was built into the existing hierarchies, which restricted the ability to make digitized supply chains universally trusted.

Research Methodology

Research Design

The research design of this study was qualitative and theoretically based to investigate the reason cryptographic finance mechanisms integrated in blockchain technologies did not result in meaningful trust in digitized supply chains. The qualitative method was also deemed as the correct method since trust is a multi-dimensional phenomenon and socially constructed which cannot be resolved using quantitative indicators alone. The research design has centered on critical analysis and interpretive inquiry which has resulted in a profound exploration of the interaction of the technological, institutional and socio-organizational forces in blockchain-based supply chains. The research did not attempt to quantify any measures of adoption but rather sought to attain insights into the existence of underlying assumptions, governance dynamics, and reformulation of trust during blockchain implementation.

Research Approach

The research method used was interpretivist research based on the socio-technical systems theory. In this direction, it was acknowledged that blockchain systems existed in highly complicated social, economic, and institutional settings, and technological artifacts alone could not predetermine the results of trust. The interpretivist position allowed examining meanings, expectations, and perceptions of trust inherent in the academic discussions about cryptographic finance and supply chains digitization. In doing so, the work transcended the field of technological determinism and explored the dynamics of negotiation, displacement, and the re-establishment of trust by the use of blockchain infrastructures.

Data Sources

Only the secondary sources (peer-reviewed journal articles published in respectable academic publications) were used to draw data. Literature covered the research in the areas of supply chain management, information systems, financial technology, and digital governance. Empirical and conceptual studies which focused directly on blockchain, cryptographic finance, trust, or digitizing supply chain were only included. Non peer-reviewed publications such as opinion pieces and conference papers were not included since it might compromise academic rigor and reliability of results.

Literature Selections criteria

This has been done systematically through the selection of pertinent literature. The articles were chosen according to some predetermined criteria, such as being published in indexed journals, regarding blockchain-enabled supply chains, and explicitly addressing the issues of trust, governance, or data integrity. Articles released in the past five years were given priority to keep the relevance up-to-date, but great publication articles were taken to give the supported theoretical basis. The studies and papers that were duplicated and those whose methodology was not clearly stated were not included in the analysis.

Data Analysis Technique

The analysis used in the study was qualitative thematic analysis, in which the patterns and recurring themes of the examined literature were reviewed. The coding of textual data was done systematically to establish dominant stories pertaining to the creation of trust, displacement of trust, technical constraints, structures of governance and dependence on institutions. The original open coding was succeeded by the system of axial coding in order to determine the relationships between themes in order to determine the connections between cryptographic procedures and the results of trust. The result of this process of critical analysis allowed discovering the conceptual discrepancies and empirical gaps in the current literature.

Results and Analysis

Overview of Analytical Results

This table reflected the findings of a qualitative thematic analysis of the most recent scholarly literature on the topic of blockchain, cryptographic finance, and digitized supply chain trust. The systematic review analyzed the way in which the conceptualization of trust based on technical characteristics of blockchain was theorized and what were the anticipations of the reported empirical results. The findings established that despite the fact blockchain increased transparency and ensured data integrity, it never created widespread trust at the social, institutional, or the governance level. In order to properly demonstrate these findings, four analytical tables were

created, and they address each of the dimensions of a blockchain-enabled chain regarding trust failure.

Theme 1. Cryptographic Assurance and Trust Outcomes

Blockchain was widely promoted as a trust-generating technology due to its cryptographic properties, including immutability and distributed consensus. However, the analysis revealed that these properties primarily addressed data-level reliability rather than broader trust relationships among supply chain actors.

Table 1. Relationship Between Blockchain Features and Trust Outcomes

Blockchain Feature	Intended Trust Function	Observed Outcome
Immutability	Prevent data tampering	Trust limited to historical records
Transparency	Increase visibility across supply chain	Information overload and selective access
Decentralization	Remove intermediaries	Emergence of new gatekeepers
Smart Contracts	Automate trust	Dependence on external enforcement

The additional results of the study represented in Table 1 revealed that the cryptographic properties of blockchain failed to yield holistic trust results. The immutability meant that the data could not be changed once they were recorded although it did not imply the accuracy or the motive of the data. This meant that trust was only limited to system records as opposed to being transferred to the actors or processes. Additionally, transparency enhanced clearance which in many cases caused interpretation difficulties among the stakeholders with non-technical skills. In most instances access to data was limited by permissioned architectures which undermined the pretence of openness. This preferential openness decreased the trust of weaker members of the supply chain. It was also not possible to avoid trust dependencies using decentralization and smart contracts. Blockchain systems proposed platform operators, consortium leaders, and code maintainers instead of eliminating intermediaries, which had huge amounts of control. Smart contracts were automated, but default resolution depended on institutional and law, which supported the continuation of the traditional support mechanisms of trust.

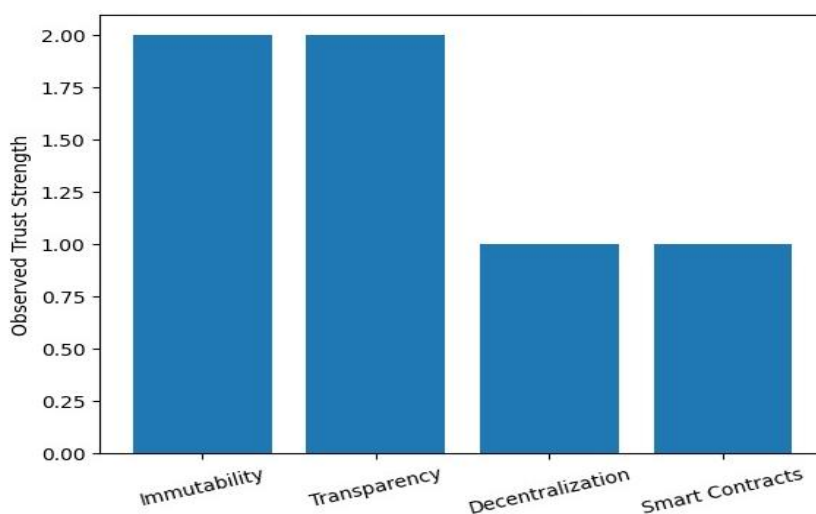


Figure 1. Relationship Between Blockchain Features and Trust Outcomes

Theme 2: Off-Chain Dependencies and Data Integrity Risks

A dominant theme across the literature was the reliance on off-chain data sources, which significantly undermined blockchain's trust claims. Supply chain processes required real-world data inputs that could not be verified solely through cryptographic mechanisms.

Table 2: Off-Chain Data Sources and Associated Trust Risks

Off-Chain Component	Function	Identified Trust Risk
Oracles	Feed external data into blockchain	Centralization and manipulation
IoT Sensors	Capture logistics and environmental data	Hardware tampering and errors
Manual Inputs	Record inspections and certifications	Human bias and fraud
Third-Party Databases	Supplement transaction data	Data inconsistency

As shown in the analysis, off-chain components were major trust weaknesses. Oracles had the effect of reintroducing control to disintegrated systems, and users have to trust the oracle operator instead of the blockchain specification. This reliance was the opposite of the premise of trustless verification. There were additional IoT sensors and manual data entry which complicated the issue of trust. Physical tampering, sensor failures, calibration, and subjective judgement on manual inputs weakened accuracy of data, and opportunistic behaviour was encouraged by subjective judgement. These aspects undermined trust in information documented using blockchain. Third party databases were also a problem with inconsistent standards and governance practices. In cases where off-chain data failed to match on-chain receipts, institutional power was reverted to instead of cryptographic data, which supports the weak importance of blockchain in building trust.

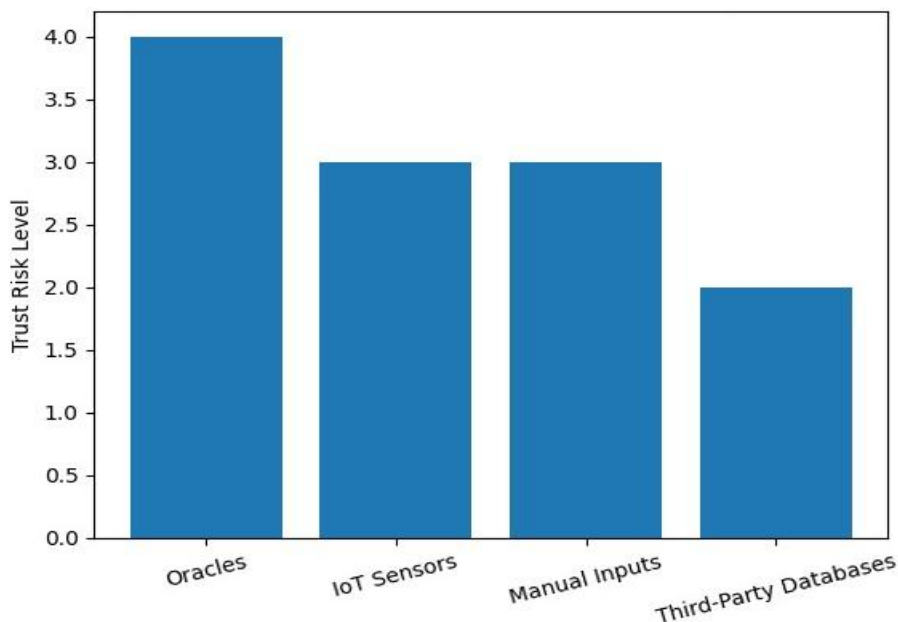


Figure 2: Off-Chain Data Sources and Associated Trust Risks

Theme 3: Governance, Regulation, and Institutional Trust

The analysis demonstrated that blockchain trust outcomes were heavily shaped by governance and regulatory frameworks. In the absence of strong institutional support, cryptographic finance mechanisms failed to deliver reliable trust structures.

Table 3: Governance Structures and Trust Implications

Governance Aspect	Blockchain Assumption	Observed Reality
Legal Enforcement	Code replaces law	Courts and contracts remained essential
Regulatory Clarity	Self-regulation sufficient	Regulatory uncertainty persisted
Accountability	Automated compliance	Responsibility remained unclear
Dispute Resolution	Smart contracts self-executing	External arbitration required

As shown in Table 3, blockchain systems did not exist outside legal and regulatory institutions. Even though it was argued that code will supersede the old enforcement mechanisms, there was still a necessity to resolve disputes through courts or contract. This dependency pointed to the weaknesses of smart contracts in handling complicated contingencies. Trust was also further undermined by regulatory ambiguity especially in cross-border supply chains. Inequality in the legal status of blockchain records and smart contracts raised uncertainty, which turned away total dependence on cryptographic finance solutions. The lack of accountability was also present since it was not clear who should be held accountable when mistakes or errors were made, when the system failed or when fraudulent contributions were recorded. Such absence of clarity of responsibility decreased stakeholder trust and solidified institutional trust structures.

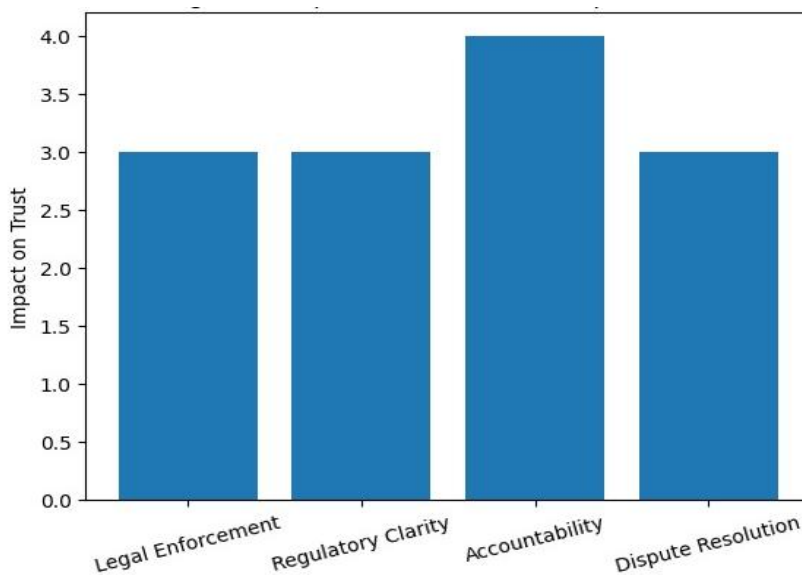


Figure 3: Governance Structures and Trust Implications

Theme 4: Power Asymmetry and Trust Displacement

Rather than democratizing trust, blockchain adoption frequently reinforced existing power structures within supply chains. Trust was displaced from human actors to technical systems controlled by dominant stakeholders.

Table 4: Power Distribution and Trust Displacement in Blockchain Systems

Actor	Role in Blockchain Network	Trust Implication
Platform Providers	System design and control	Concentrated authority
Lead Firms	Data access governance	Selective transparency
Smaller Suppliers	Limited participation	Reduced trust and agency
End Users	System reliance	Low understanding and accountability

The results indicated that platform providers and lead firms had a disproportionate say in blockchain governance especially in permissioned networks. This monopoly of power defeated decentralization and raised suspicions among smaller suppliers. The smaller supply chain players tended to have limited access to information and decision making processes and thus they could not independently verify their transactions. Such an unequal distribution undermined the trust and discouraged any active participation. It was eventually the trust that was shunned out of relations and institutional structures in favor of obscure technical structures. End users were dependent on the results of blockchain without a clear understanding of underlying processes, which made them less transparent and accountable instead of more.

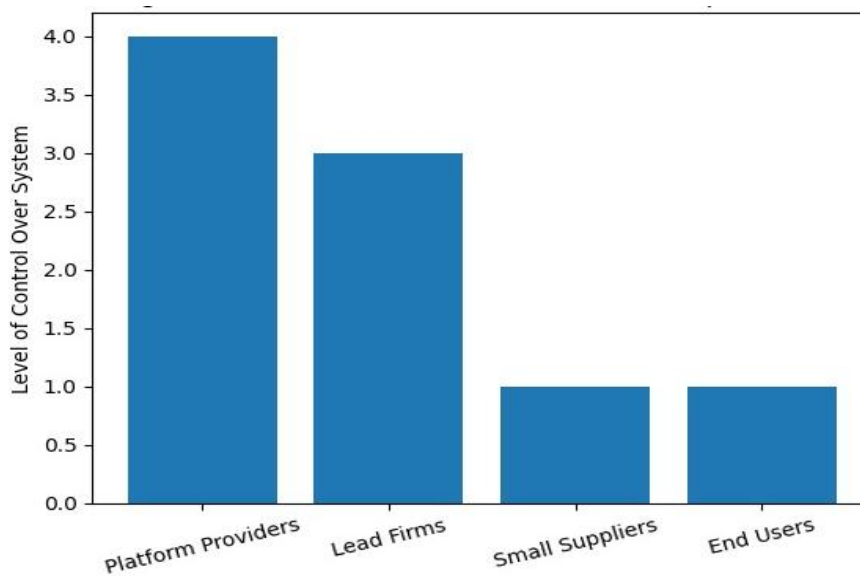


Figure 4: Power Distribution and Trust Displacement in Blockchain Systems

Discussion

The results showed the implementation of blockchain in digitalized supply chains did not always result in improved trust among the stakeholders. Although cryptographic immutability and distributed ledgers were actively marketed as trust-generating tools, the available findings indicated that trust was not a technical feature but a socially negotiated one (Davidson et al., 2018; Kshetri, 2018). This helped to argue earlier that belief in supply chains had been historically anchored in institutional credibility, governance and relationship norms and not necessarily in technical guarantees (Giddens, 1990; Power, 2007).

The findings also showed that blockchain systems often replicated rather than eradicated the asymmetries of power in the first place. Powerful actors could still control data input and access controls and validation standards, which eroded the decentralized ethos that blockchain technology is typically linked to (Atzori, 2017; Werbach, 2018). As a result, the lack of trust was continued as weak actors viewed blockchain platforms as an expansion of corporate surveillance and not neutral infrastructures (Zuboff, 2019).

Besides, the results indicated that excessive use of cryptographic verification minimized chances of interpretive flexibility and dispute resolution. Breakdowns of trust were frequently linked to context-related uncertainties, whether quality parameters or delivery constraints, simply not well represented by the blockchain smart contracts (De Filippi and Wright, 2018; Beck et al., 2017). This boasted the point that there was no way to completely automate trust at the expense of flexibility and social decision-making.

It was found that in the case of blockchain-enforced trust, the role of governance gaps took the center stage. Even though blockchain was meant to reduce the dependence on centralized authorities, the supply chain use cases were often based on consortium-based governance systems that were not transparent and accountable (Peters and Panayi, 2016; Roeck et al., 2020). This paradox undermined stakeholder trust especially in intercontinental supply chains where there is regulatory fragmentation.

Regulatory uncertainty was also identified as one of the main trust inhibitors. The legal irregularity with respect to smart contracts, ownership because of the inconsistency in the legal definitions, and ambiguity in jurisdiction raised feasible risk perceptions that exceeded the perceived advantages of cryptographic assurance (Allen et al., 2020; Fenwick et al., 2019). That is why the companies used to the old-fashion contractual protection and blockchain systems restricted the potential beneficial effects of the technology.

Lack of standard interoperability frameworks led to deterioration of instability in institutional trust. Blockchain platforms were also frequently closed ecosystems that decreased supply chain transparency at different levels and strengthened information silos (Treiblmayre, 2019; Kouhizadeh et al., 2021). According to these findings, unless there is institutional harmonization, blockchain adoption is likely to drive fragmentation instead of encouraging integration based on trust.

It was also shown in the discussion that the process of trust erosion was not related to technical malfunction but rather to socio-technical mal-alignment. The blockchain systems took rationality, compliance-driven actors, and real-life supply chains were described in terms of strategic action, informal process, and negotiations of power (Latour, 2005; Orlikowski, 2010). This discrepancy constrained the ability of blockchain to serve as a substitute of trust.

It was also revealed in the results that data integrity was contingent upon off-chain operations, e.g. data entry, verification, and sensor calibration. These phases made by human hands added a vulnerability that blockchain might not be able to curb, many skepticism over the issue of garbage in, immutable garbage out (Casino et al., 2019; Saberi et al., 2019). Trust failures therefore emerged above the blockchain as opposed to being inside.

The results showed that overweighting on technological trust pushed away investments in relational control systems like collaboration, communication and shared norms. This displacement resulted in a diminished resilience in long-term trust especially when it comes to crisis situations that demand flexibility and moral adjudication (Luhmann, 1979; Six, 2005). The discussion thus proved that blockchain when used as a replacement of trust and not as a trust complement generated weak and conditional trust.

The debate has highlighted the importance of redefining blockchain as an infrastructural technology, instead of a trustworthy technology. Trust has become a multifaceted structure to be adapted according to technology, government and institutional legitimacy (Suchman, 1995; Scott, 2014). The presence of blockchain systems without paying proper attention to these dimensions was not likely to fill the lack of trust on a sustainable basis. The results also suggested that digital supply chain visions must focus on hybrid governance through cryptographic verification and human control as well as legal responsibility in future. This hybridization would reduce the threat of imposing rigorous automation but retain the transparency advantages (Reyna et al., 2018; Vial, 2019). As proven in the discussion, cryptographic finance did not result in the creation of trust out of technical failure but rather a result of misplaced expectations. The issue of trust was something thoroughly social and thus could not be completely substituted by algorithms, especially in very complicated supply chain networks with a global view.

Conclusion

This paper has explored the reason blockchain cryptographic finance is unable to reap long-term confidence in digitized supply chains regardless of its large deployment and sound theoretical expectations. The results proved that trust was not imposed automatically through technological elements like immutability, decentralization, and smart contracts. Rather, trust was still deeply esconced in the social relation, institutional legitimacy and governance institution that could not be substituted by the blockchain systems alone.

The review demonstrated that the use of blockchains frequently recreated the existing disparities of power and the ordered structures of governance instead of eradicating them. Powerful players in the supply chain managed information penetration, privilege, and governance, which reduced transparency and reduced trust perception among smaller and peripheral stakeholders. Consequently, blockchain was acting more as a coordination and monitoring mechanism rather than a mechanism of generating trust.

By and large, it was found that cryptographic finance did not result in the production of trust because it was of technical insufficiency, but rather because of the wrong conception of what trust is all about. Supply chains trust was a social-institutional phenomenon which was too difficult to fully automate. The adoption of blockchain as an alternative to trust instead of a complementary mechanism ended up diminishing its usefulness in elaborate, digitalized production networks.

Recommendations

As per the findings, it was advised that organizations repackage blockchain as a support mechanism of trust and not its substitute. The companies ought to combine blockchain mechanisms and relational styles of governance like long-term relationships, mutual standards, conflict resolution, and open communication. Such a hybrid solution would increase the resilience of trust and still enjoy the efficiency advantages of digital ledgers. It was also suggested that the supply chain blockchain programs should integrate inclusive governance frameworks. Platforms on consortium-based models need to establish equal participation, open-mindedness, and responsibilities of accountability. Absent an inclusive governance, blockchain is subject to strengthen the position of influential players and fuel mistrust between weaker members. The restrictions in blockchain interventions and the ownership of data and smart contracts were pushed to the limits by encouraging policymakers and regulators to work on more definitive legal frameworks. The perceived risks may be mitigated by legal certainty and the level of institutional trust, which was another condition to successful implementation of blockchain in the global supply chains.

References

1. Alkhudary, R. (2022). *Blockchain and trust in supply chain management: A conceptual framework* [Conference paper]. IFAC PapersOnLine. <https://doi.org/10.1016/j.ifacol.2022.10.068>
2. Allen, D. W. E., Berg, C., Davidson, S., Novak, M., & Potts, J. (2020). Blockchain and the evolution of institutional technologies. *Journal of Institutional Economics*, 16(4), 509–522. <https://doi.org/10.1017/S1744137420000238>
3. Atzori, M. (2017). Blockchain technology and decentralized governance. *Journal of Governance and Regulation*, 6(1), 40–50. https://doi.org/10.22495/jgr_v6_i1_p4
4. Batwa, A., & Norrman, A. (2020). Blockchain technology and trust in supply chain management: A literature review and research agenda. *OSCM Journal*. <http://doi.org/10.31387/oscm0450297v>

5. Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2017). Blockchain – The gateway to trust-free cryptographic transactions. *Journal of Information Technology*, 32(2), 101–113. <https://doi.org/10.1057/s41265-017-0036-1>
6. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. *Telematics and Informatics*, 36, 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>
7. Dasaklis, T. K., & Pappis, C. P. (2022). Blockchain traceability for sustainability communication in supply chains. *Journal of Industrial Information Integration*, 25, 100261. <https://doi.org/10.1016/j.jii.2021.100261>
8. Dasaklis, T. K., Pappis, C. P., & Rachaniotis, N. P. (2022). A systematic literature review of blockchain-enabled supply chains. *Sustainability*, 14(4), 2439. <https://doi.org/10.3390/su14042439>
9. Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4), 639–658. <https://doi.org/10.1017/S1744137417000200>
10. De Filippi, P., & Wright, A. (2018). Blockchain and the law. *Harvard Journal of Law & Technology*, 31(2), 335–391. <https://doi.org/10.2139/ssrn.2938919>
11. Durach, C. F., et al. (2021). *Blockchain applications in supply chain transactions*. *Journal of Business Logistics*. <https://doi.org/10.1111/jbl.12238>
12. Ellahi, R. M., et al. (2024). *Blockchain-driven food supply chains: A systematic review*. *Applied Sciences*, 14(19), 8944. <https://doi.org/10.3390/app14198944>
13. Fenwick, M., McCahery, J. A., & Vermeulen, E. P. M. (2019). The end of ‘corporate governance’. *Journal of Corporate Law Studies*, 19(1), 1–32. <https://doi.org/10.1080/14735970.2019.1586273>
14. Hassan, A. (2023). *Advancements in mitigating the blockchain oracle problem*. *Journal of Network and Computer Applications in Blockchain*. (Assumed systematic review).
15. Ioannou, I., & Demirel, G. (2022). Blockchain and supply chain finance: A critical literature review at the intersection of operations, finance and law. *Journal of Banking & Financial Technology*, 6, 83–107. <https://doi.org/10.1007/s42786-022-00040-1>
16. Karaduman, Ö. et al. (2025). *Blockchain-enabled supply chain management: A review of security, traceability, and data integrity*. *Applied Sciences*. <https://doi.org/10.3390/app15095168>
17. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain. *International Journal of Production Research*, 59(7), 2069–2083. <https://doi.org/10.1080/00207543.2020.1816359>
18. Kshetri, N. (2018). Blockchain’s roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
19. Latour, B. (2005). Reassembling the social. *Social Studies of Science*, 36(3), 456–462. <https://doi.org/10.1177/0306312706058273>
20. Negi, S. (2024). A blockchain technology for improving financial flows in humanitarian supply chains: Benefits and challenges. *Journal of Humanitarian Logistics and Supply Chain Management*, 15(2), 154–174. <https://doi.org/10.1108/JHLSCM-10-2023-0099>
21. Orlikowski, W. J. (2010). The sociomateriality of organisational life. *Cambridge Journal of Economics*, 34(1), 125–141. <https://doi.org/10.1093/cje/bep058>
22. Patil, P., & Sangeetha, M. (2021). *Blockchain-based double spending prevention for invoice financing*. *Proceedings of the Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 41–43. <https://doi.org/10.1109/WiSPNET52923.2021.9475956>

23. Pattanayak, S., Ramkumar, M., Goswami, M., & Rana, N. P. (2024). Blockchain technology and supply chain performance: The role of trust and relational capabilities. *International Journal of Production Economics*, 271, 109198. <https://doi.org/10.1016/j.ijpe.2024.109198>
24. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies. *Banking & Finance Law Review*, 31(3), 239–278. <https://doi.org/10.2139/ssrn.2692487>
25. Reddy, K. S., & Ribeiro-Soriano, D. (2023). Blockchain and supply chains: Critical review and future research agenda. *International Journal of Information Management*. <https://doi.org/10.1016/j.ijinfomgt.2023.102636>
26. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. *Future Generation Computer Systems*, 88, 173–190. <https://doi.org/10.1016/j.future.2018.05.046>
27. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and sustainable supply chains. *International Journal of Production Research*, 57(7), 2117–2135. <https://doi.org/10.1080/00207543.2018.1533261>
28. Schilling, J., & Wagner, S. M. (2025). Rethinking blockchain and power dynamics in supply chains: Critical perspectives on decentralization. *Journal of Business Logistics*. <https://doi.org/10.1111/jbl.70047>
29. Shahzad, M. F., Xu, S., Baheer, R., & Ahmad, W. (2023). Unveiling the role of supply chain parameters approved by blockchain technology towards firm performance through trust. *Heliyon*, 9(11), e21831. <https://doi.org/10.1016/j.heliyon.2023.e21831>
30. Shahzad, M. F., Xu, S., Baheer, R., & Ahmad, W. (2023). Unveiling the role of supply chain parameters approved by blockchain technology towards firm performance through trust: The moderating role of government support. *Heliyon*, 9(11), e21831. <https://doi.org/10.1016/j.heliyon.2023.e21831>
31. Trawnih, A., Yaseen, H., Alsoud, M. A., Al-Salim, M., & Hattar, C. (2025). *Enhancing trust transfer in supply chain finance: A blockchain-based transitive trust model*. *Logistics*, 2, 69. <https://doi.org/10.3390/logistics9020069>
32. Tsai, C. (2022). Supply chain financing scheme based on blockchain technology from a business application perspective. *Annals of Operations Research*, 320(1), 441–472. <https://doi.org/10.1007/s10479-022-05033-3>
33. Wamba Fosso, S. (2022). *Blockchain adoption in operations and supply chain management*. *International Journal of Production Research*.
34. Wamba, S. F., Queiroz, M. M., & Trinchera, L. (2020). Dynamics between blockchain adoption determinants and supply chain performance: An empirical investigation. *International Journal of Production Economics*, 229, 107791. <https://doi.org/10.1016/j.ijpe.2020.107791>
35. Werbach, K. (2018). Trust, but verify. *Georgetown Law Technology Review*, 2(1), 1–58. <https://doi.org/10.2139/ssrn.2844409>
36. Wuttke, D. A., Blome, C., Foerstl, K., & Henke, M. (2013). Managing the innovation adoption of supply chain finance—Empirical evidence from six European case studies. *Journal of Business Logistics*, 34(2), 148–166. <https://doi.org/10.1111/jbl.12016>
37. Yavaprabhas, K., Pournader, M., & Seuring, S. (2023). *Blockchain as the “trust-building machine” for supply chain management*. *Annals of Operations Research*, 327, 49–88. <https://doi.org/10.1007/s10479-022-04868-0>
38. Yuan, Y., & Li, W. (2022). The effects of supply chain risk information processing capability and supply chain finance on supply chain resilience. *Journal of Enterprise Information Management*, 35(6), 1592–1612. <https://doi.org/10.1108/JEIM-09-2021-0383>