Journal of Information Systems Engineering and Management
2021, 6(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Digital Supply Chain Resilience: A Conceptual Framework for IoT and Blockchain Integration

Gokul Joshi[1], Goraj Joshi[2], Ankit Sharma[3]

Nottingham Trent University[1], T A Pai Management Institute[2], State University of New York[3]

United Kingdom[1], India[2], United States of America[3]

ARTICLE INFO

Received: 18 Apr 2021

Accepted: 22 June 2021

ABSTRACT

The COVID-19 pandemic exposed structural fragilities in globally dispersed supply chains, highlighting persistent gaps in multi-tier visibility, disruption detection, and interorganizational coordination under extreme uncertainty. While digital technologies such as the Internet of Things (IoT) and blockchain are frequently proposed as resilience enablers, existing research largely examines them in isolation and lacks a mechanism-based theoretical integration. Drawing on supply chain resilience theory, organizational information processing theory (OIPT), and transaction cost economics (TCE), this paper develops a conceptual framework that explains how IoT-enabled sensing and blockchain-enabled governance jointly enhance digital supply chain resilience. The framework introduces the concept of verifiable event anchoring, a mechanism linking physical event detection to shared, auditable governance structures, thereby simultaneously expanding information processing capacity and reducing transaction hazards. The model theorizes how integration improves visibility and coordination reliability, enabling absorptive, adaptive, and recovery capabilities under disruption. Six mechanism-based propositions are developed to guide empirical testing, along with boundary conditions related to asset specificity, compliance criticality, and ecosystem governance. The paper contributes a structured theoretical foundation for understanding how digital integration reshapes resilience in multi-tier supply networks.

Keywords: Digital supply chain; Supply chain resilience; Internet of Things (IoT); Blockchain; Industry 4.0; Information processing theory; Transaction cost economics; Supply chain visibility; Risk mitigation; Distributed ledger technology; Cold chain monitoring; Multi-tier supplier coordination; Smart contracts; COVID-19 disruption.

1.0 Introduction

The early months of 2020 have brought global supply chains into exceptional public and policy salience. Shortages of PPE, ventilators, and test-related supplies were reported by healthcare systems and highlighted by international organizations, with supply constraints and market distortions occurring simultaneously across multiple regions. Academic and practitioner discussions have similarly emphasized that medical supply chains embedded in global value chains can become brittle when exposed to synchronized disruptions in production, transportation capacity, and cross-border movement.

From a supply chain management perspective, the pandemic constitutes a disruption class characterized by uncertain duration, non-localized propagation, and concurrent shocks to supply, demand, and logistics

capacity. These features amplify known shortcomings of traditional supply chain designs that emphasize lean inventories, cost optimization, and limited redundancy, particularly when such designs are coupled with weak visibility beyond tier-one suppliers. Moreover, decision-makers frequently confront a dual problem: first, not knowing where disruptions originate in multi-tier networks; and second, lacking trusted, timely data for coordinating mitigation actions (e.g., reallocations, substitutions, or expedited transport) across organizational boundaries.

Digital infrastructure is increasingly positioned as a resilience enabler because it can expand the capacity to sense disruptions, interpret signals, and coordinate responses across firms. Editorial work on digital supply chains in 2020 underscores that digitization is not merely automation within a firm; it is the redesign of interorganizational information architectures that support end-to-end decision-making. Concurrently, the Industry 4.0 agenda has encouraged firms to deploy connected devices in manufacturing and logistics and to develop data-driven visibility into flows of materials, work-in-process, and finished goods. These developments are unfolding amid early-stage rollout of 5G networks, which, while not yet broadly mature, are expected to support higher device density and lower latency for some industrial and logistics use cases.

In parallel, enterprise blockchain initiatives in 2020 reflect a shift from speculative discourse toward selective pilots and early deployments in traceability and trade documentation. Notable examples include distributed-ledger networks for food traceability such as IBM Food Trust and global-shipping data-sharing platforms such as Trade Lens, built on permissioned architectures designed for multi-party collaboration. These initiatives remain constrained by adoption, governance, integration, and performance trade-offs typical of early-stage interorganizational systems.

Against this background, the objective of this conceptual paper is to develop a theory-grounded framework explaining how and through what mechanisms IoT and blockchain can be integrated to enhance digital supply chain resilience under pandemic-era uncertainty. Rather than asserting that "technology improves performance," the paper identifies specific causal pathways that connect technological capabilities to resilience dimensions, visibility, responsiveness, adaptability, trust-based coordination, and structural robustness, and develops research propositions suitable for future empirical testing in supply chain and operations management scholarship.

2.0 Literature Review

Digital supply chain research has increasingly emphasized the transformation of supply networks through interconnected data, digital platforms, and real-time decision support. In a 2020 editorial on digital supply chain management, digitization is framed as a shift in how supply chain actors coordinate through digital information structures, with attention to interoperability, data governance, and decision architectures rather than isolated IT implementations. COVID-19 underscores that these themes are not abstract: resilient responses depend on rapid access to accurate, shareable information about inventory positions, logistics constraints, and supplier capacity, including beyond direct contractual partners.

Supply chain resilience theory provides language for understanding these needs and for distinguishing resilience from related performance concepts. Foundational work frames resilience as the capability to withstand and recover from disruptions through combinations of preparation, response, and recovery [Christopher & Peck, 2004; Sheffi & Rice, 2005; Ponomarov & Holcomb, 2009]. The "absorb–adapt–recover" framing is particularly salient in 2020 because disruptions are not limited to single nodes; they propagate through network structures. Modeling studies of disruption propagation ("ripple effects")

highlight that the structural features of supply networks, recovery rates, and firm investments influence how disruptions diffuse and how quickly networks return toward stable operating states. COVID-19 has further motivated simulation-based studies of epidemic outbreaks as a specific risk type, characterized by non-stationary demand and capacity constraints and cross-regional contagion effects.

Within this resilience literature, visibility consistently appears as a critical enabling capability. However, visibility is often treated at a high level, with limited theorization of the digital mechanisms required to achieve reliable visibility across organizational boundaries, particularly in multi-tier contexts where data may be proprietary, heterogeneous, and strategically withheld. This gap becomes more acute in pandemic conditions, when the value of information increases and incentives for opportunism, hoarding, and market manipulation may rise.

IoT research in supply chain management has expanded rapidly and provides one important piece of this puzzle. A 2020 review and bibliometric study of IoT research in SCM and logistics documents the breadth of applications, tracking, monitoring, and automation across warehousing, transportation, and manufacturing, while also identifying challenges such as integration complexity, security, and data management. Empirically, IoT-enabled tracking and identification methods (including RFID, ultra-wideband, and related technologies) are being developed for Industry 4.0 asset and production tracking, reflecting growing technical feasibility but also ongoing concerns about reliability, scalability, and cost-effectiveness for widespread adoption. In resilience terms, IoT contributes primarily by increasing the timeliness and granularity of operational information, enabling detection of deviations such as temperature excursions, delays, or equipment anomalies before they cascade.

Blockchain research in supply chain management represents another strand of digitalization, with an emphasis on provenance, traceability, and interorganizational data integrity. A 2020 review on blockchain technology in supply chain operations identifies key features, including decentralized consensus, smart contracting, and cryptographic security, that can support transparency and visibility across parties, while also noting that implementation challenges remain significant. A systematic review of blockchain and supply chain management published in 2020 further reflects a growing body of work exploring potential use cases and value propositions, albeit often with limited empirical maturity and a need for clearer theoretical framing. Complementing academic coverage, early enterprise initiatives provide concrete examples: IBM's 2018 launch announcement for its food-traceability network emphasizes rapid trace-back, permissioned sharing, and an immutable record endorsed by multiple parties, illustrating how blockchain is positioned as a coordination infrastructure rather than merely a database. Shipping and trade documentation provide another example, as Maersk and IBM announced a blockchain-enabled shipping solution in 2018 with a broad early adopter program, reflecting an attempt to coordinate data exchange across ports, carriers, and other stakeholders.

Despite these advances, two integration gaps are evident as of 2020. First, blockchain-based traceability systems often confront the "physical–digital linkage" problem: a ledger can secure records, but it cannot, by itself, guarantee that recorded events accurately reflect physical conditions. Second, IoT systems can provide rich data streams but raise concerns about data tampering, inconsistent standards, and contested "single versions of truth" across organizations. These gaps are not merely technical; they imply under-theorized mechanisms linking digital infrastructures to resilience outcomes. In particular, much of the existing literature treats IoT and blockchain as parallel digital innovations rather than complementary components of unified information-processing and governance architecture. The result is a theoretical opportunity: to conceptualize IoT–blockchain integration as a mechanism that jointly increases information processing capacity (through sensing and analytics) and reduces interorganizational uncertainty and opportunism (through shared, auditable governance structures).

Contributions

This paper makes four primary contributions to the digital supply chain literature.

- First, it moves beyond technology-centric discussions by developing a mechanism-based integration framework that explains *how* IoT sensing and blockchain governance jointly generate resilience outcomes. Rather than treating digital technologies as isolated enablers, the framework identifies the causal pathways linking real-time data capture, verification logic, and interorganizational coordination.

- Second, the study introduces the concept of verifiable event anchoring, explaining how IoT-generated physical events can be cryptographically recorded on distributed ledgers to reduce information asymmetry and opportunism across multi-tier supply networks.

- Third, it integrates Organizational Information Processing Theory (OIPT) with resilience theory to demonstrate how digital integration enhances absorptive, adaptive, and restorative capacities under high environmental uncertainty.

- Finally, the paper specifies boundary conditions and governance moderators that explain when IoT–blockchain integration strengthens resilience and when it may fail due to ecosystem misalignment or weak institutional structures.

While prior digital supply chain research has examined IoT and blockchain largely as independent technological innovations, this paper advances theory by conceptualizing their integration as a dual-capacity architecture that simultaneously expands information processing capacity (OIPT) and reduces transaction hazards (TCE). The concept of verifiable event anchoring represents a novel mechanism linking physical event detection to interorganizational governance structures, thereby clarifying how digital technologies reshape both uncertainty management and coordination costs. By integrating information-processing and transaction-cost perspectives within the resilience outcome space, this framework moves digital supply chain theory beyond descriptive digitalization narratives toward a structured explanation of resilience-enhancing mechanisms.

3.0 Theoretical Foundations

This paper grounds the proposed framework in two complementary theoretical lenses: supply chain resilience theory and organizational information processing theory, with transaction cost economics as a secondary lens to explain governance and coordination effects. These theories are selected because COVID-19 exposes a dual challenge of (a) heightened uncertainty and equivocality in supply and demand conditions and (b) intensified interorganizational dependence, where decisions at one node affect outcomes across the network.

Supply chain resilience theory conceptualizes resilience as a set of capabilities enabling supply networks to prepare for, respond to, and recover from disruptions [Christopher & Peck, 2004; Sheffi & Rice, 2005; Ponomarov & Holcomb, 2009]. Importantly, resilience is multidimensional: it encompasses absorptive capacity (maintaining function under shock), adaptive capacity (reconfiguring to match new constraints), and recovery capacity (restoring or stabilizing operations after disruption). The pandemic context emphasizes that these capacities depend on visibility into upstream and downstream conditions and on coordination across organizational boundaries.

Research Article

Organizational information processing theory (OIPT) offers a mechanism-based explanation of how organizations cope with uncertainty. The central premise is that uncertain tasks require information processing, and performance depends on the fit between information processing needs (driven by uncertainty and interdependence) and information processing capacity (enabled by structures and information systems). A key implication for supply chains is that disruptions increase both the volume and the urgency of required information, while multi-tier networks increase equivocality because signals are distributed, incomplete, and sometimes contradictory. From an OIPT perspective, digital technologies contribute to resilience when they increase a supply chain's ability to acquire, transmit, interpret, and act on relevant information fast enough to reduce uncertainty and prevent disruption propagation.

Transaction cost economics (TCE) adds a complementary governance argument. TCE emphasizes transaction hazards arising from bounded rationality and opportunism, particularly under uncertainty and when asset specificity is high. Governance structures and contractual mechanisms are therefore selected to economize on transaction costs associated with monitoring, enforcement, and maladaptation [Williamson, 1979; Williamson, 1985]. Pandemic-era disruptions can be interpreted as conditions that increase transaction hazards: supply scarcity may incentivize opportunistic behavior, and the costs of verifying provenance, quality, and delivery commitments rise sharply. In this environment, technologies that reduce asymmetrical information and enable auditable, enforceable interorganizational commitments can reduce transaction costs and support more effective coordination.

Together, OIPT and TCE provide a coherent foundation for theorizing IoT–blockchain integration. IoT primarily expands information processing capacity by producing real-time, granular operational data, whereas blockchain primarily provides governance infrastructure that reduces information asymmetry and coordination costs by establishing shared, auditable records and rule-based validation of transactions. Supply chain resilience theory then specifies the outcome space: absorb, adapt, and recover, operationalized through constructs such as visibility, responsiveness, adaptability, coordination, and structural robustness.

4.0 Conceptual Framework Development

The proposed conceptual framework explains how IoT and blockchain capabilities, individually and in combination, enable digital supply chain resilience through mechanisms grounded in information processing and governance. The central logic is that resilience is enhanced when supply chains can detect disruptions early, interpret their implications accurately, coordinate mitigation actions across partners, and maintain trust in shared information during crisis conditions.

IoT capabilities in supply chains can be conceptualized as a set of sensing and connectivity resources that generate near-real-time data about assets, environments, and events. As documented in 2020 IoT SCM literature, industrial and logistics use cases include asset tracking, inventory visibility, condition monitoring (e.g., temperature, humidity), and equipment monitoring in production environments. These capabilities map to four operational functions that are particularly relevant to pandemic-era disruptions. First, real-time sensing captures the state of inventory, equipment, and shipments, reducing time delays in reporting. Second, event detection identifies deviations from planned conditions (e.g., a shipment delay exceeding tolerance, an unexpected temperature excursion, or an equipment anomaly). Third, environmental monitoring provides continuous oversight for temperature- and humidity-sensitive products, which is central for cold chain logistics of vaccines and biologics and for maintaining product integrity. Fourth, asset tracking supports the location visibility needed to reroute shipments, reallocate inventory, and maintain service continuity when transport networks face disruptions.

However, IoT-enabled information is not inherently trustworthy across organizational boundaries. Data can be incomplete, heterogeneous, or vulnerable to manipulation, and the integration of multi-party IoT data can produce disputes about which data source is authoritative. Moreover, the value of IoT data is limited if it remains confined within firm-level systems, since pandemic disruptions require coordination across manufacturers, logistics providers, distributors, and regulators.

Blockchain capabilities address a complementary challenge: establishing shared trust and auditability across organizations that do not fully trust one another or that have misaligned incentives. Enterprise blockchain platforms such as permissioned frameworks can provide immutability (tamper-evident records), decentralized validation (multi-party endorsement or consensus), distributed trust (no single firm unilaterally controls the record), auditability (traceable histories), and potentially smart contracts (code-based execution of predefined rules). Early industry initiatives illustrate how these features are intended to work in practice. For example, the 2018 launch communications around IBM's food traceability network emphasize permissioned sharing and rapid trace-back enabled by a shared ledger endorsed by multiple parties. In global shipping, the 2018 TradeLens announcement describes a platform designed to digitize and share shipment and documentation data across multiple parties, attempting to reduce paper-based frictions and improve near-real-time collaboration.

Yet, blockchain alone does not solve the resilience problem. First, blockchain records are only as accurate as the data entered, creating the well-known "garbage in, garbage out" limitation. Second, shared ledgers require governance agreements, data standards, and onboarding processes that are difficult to establish quickly, particularly under crisis pressure. Third, performance and scalability trade-offs, even in permissioned systems, require careful design choices regarding what information is stored on-chain versus off-chain. These limitations align with empirical work on blockchain adoption challenges, which identifies uncertainty about value, organizational readiness, and ecosystem participation as core barriers [Queiroz & Fosso Wamba, 2019].

The integration mechanism proposed in this paper treats IoT and blockchain as complementary modules in a unified architecture. IoT functions as the sensing layer that increases information processing capacity by generating timely, granular data; blockchain functions as the governance layer that increases the credibility and shareability of selected data across organizations. Integration can take the form of anchoring IoT sensor events (such as temperature readings, handoff confirmations, or equipment state changes) to a shared ledger, thereby ensuring that key events are time-stamped, auditable, and jointly validated. A 2020 proof-of-concept study in food-chain traceability illustrates this logic by integrating IoT devices for temperature monitoring with blockchain-based traceability, aiming to reduce reliance on centralized intermediaries.

Within the resilience outcome space, the framework links integrated capabilities to five interrelated resilience dimensions. Visibility refers to the ability to observe states and flows across the network, particularly beyond tier-one suppliers; IoT contributes by sensing and tracking, while blockchain contributes by enabling controlled sharing and ensuring record integrity. Responsiveness refers to how quickly the supply chain can detect and respond to disruptions; IoT contributes through early detection and alerts, while blockchain contributes by reducing data disputes and enabling faster coordination based on a shared record. Adaptability refers to the ability to reconfigure sourcing, logistics routes, and production plans under changed constraints; here, reliable multi-party data can reduce the time required to evaluate alternatives and to coordinate changes without excessive renegotiation. Trust-based coordination refers to collaboration among partners where information asymmetries and opportunism could otherwise lead to delays, hoarding, or contractual conflict; blockchain's auditability and shared validation reduce such hazards, especially in scarce markets. Structural robustness refers to the network's

Research Article

capacity to maintain function through redundancy, diversification, and controlled flexibility; while technology cannot create redundancy directly, it can enable better identification of critical nodes and faster execution of contingency plans by improving information availability and accountability.

The framework therefore emphasizes that IoT–blockchain integration is not a generic "digitalization" effect. Instead, it is a mechanism for improving the fit between information processing needs (which rise sharply under pandemic uncertainty) and information processing capacity, while simultaneously reducing transaction hazards and coordination costs in multi-party supply networks.

The framework assumes a mediated pathway in which digital integration enhances resilience primarily through improved visibility and reduced coordination friction. Visibility enables earlier disruption detection; reduced coordination friction accelerates collective response; together, these mechanisms support adaptive reconfiguration and recovery. Thus, resilience is not treated as a direct outcome of technology adoption, but as a capability emerging from improved information processing and governance alignment.

Construct Definitions and Conceptual Boundaries

To enhance conceptual clarity and empirical applicability, below we define the primary constructs used in the framework.

Table 1. Construct Definitions

Construct	**Definition**	**Theoretical Basis**
Supply Chain Resilience	The capability of a supply network to absorb, adapt to, and recover from disruptions while maintaining continuity of operations.	Christopher & Peck (2004); Ponomarov & Holcomb (2009)
Visibility	The accuracy, timeliness, and multi-tier accessibility of operational information across the supply network.	OIPT
Responsiveness	The speed with which disruption signals are detected, decisions are made, and corrective actions are executed.	OIPT
Adaptability	The ability to reconfigure sourcing, logistics, and production structures in response to environmental change.	Resilience theory
IoT Capability	The technological capacity to capture, transmit, and analyze real-time physical asset data through sensor-based monitoring systems.	Information processing capacity
Blockchain Governance Capability	The ability to validate, record, and enforce transaction rules through distributed ledger technologies and smart contracts.	TCE
Verifiable Event Anchoring	The integration mechanism by which IoT-generated physical events are cryptographically committed to blockchain systems to ensure tamper resistance and shared trust.	Integrated OIPT–TCE mechanism

Journal of Information Systems Engineering and Management
2021, 6(2)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The framework proposes a sequential mechanism. IoT systems generate real-time physical event data (e.g., temperature deviations, location changes, asset handovers). These events are filtered through validation protocols and selectively anchored onto blockchain systems, where immutability and distributed consensus establish shared trust.

The integration of sensing and verification reduces detection latency, minimizes information asymmetry, and enhances coordination reliability across supply chain tiers. These improvements strengthen visibility and responsiveness, which in turn enable adaptive reconfiguration and faster recovery during disruptions.

Figure 1 illustrates the sequential integration mechanism through which IoT-enabled real-time sensing generates physical event data (e.g., temperature deviations, location changes, asset handovers), which are validated and selectively anchored onto blockchain systems. The integration of sensing and distributed ledger governance reduces information asymmetry, enhances coordination reliability across supply chain tiers, and strengthens visibility, responsiveness, adaptability, and recovery capabilities.

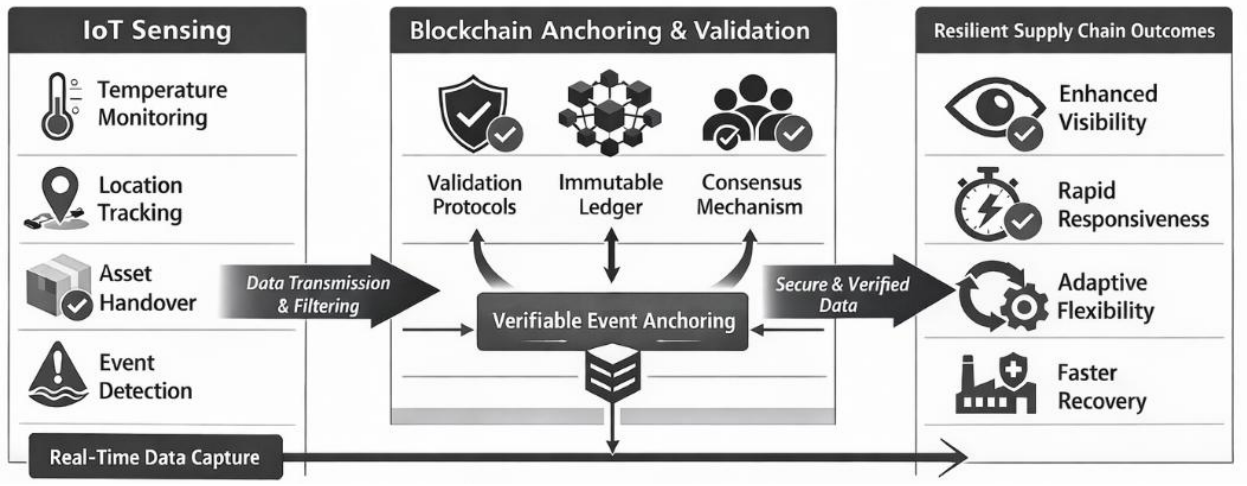

Figure 1. Mechanism-Based Framework of IoT–Blockchain Integration for Supply Chain Resilience.

Source: Authors' conceptualization.

5.0 Research Propositions

Proposition 1: Greater IoT-enabled real-time sensing capability is positively associated with supply chain absorptive capacity under high disruption uncertainty. IoT-enabled real-time sensing increases supply chain absorptive capacity by expanding information processing capacity under uncertainty. Under OIPT, disruptions increase information requirements because decision-makers need timely, accurate signals to prevent local failures from propagating. IoT deployments that provide continuous asset tracking and event detection reduce the latency between disruption onset and managerial awareness, thereby supporting the ability to absorb shocks through earlier corrective action (e.g., rerouting shipments, reallocating inventory, or isolating compromised lots). Accordingly, Proposition 1 states that, in supply chains characterized by high disruption uncertainty (such as pandemic conditions), greater IoT sensing capability is positively associated with resilience outcomes through improved visibility and faster responsiveness.

Proposition 2: Blockchain-enabled shared auditability is positively associated with trust-based coordination and reduced response time in multi-party supply chains experiencing crisis conditions. Blockchain-enabled immutability and decentralized validation reduce coordination delays by lowering information asymmetry and transaction hazards during disruptions. Under TCE, uncertainty and opportunism increase the costs of market transactions and interfirm coordination, as parties must invest in monitoring and enforcement to ensure compliance. Permissioned blockchain systems provide an auditable record endorsed by multiple parties, which can reduce disputes about shipment status, provenance, and handoffs. Therefore, Proposition 2 states that, in multi-party supply chains where verification and documentation costs rise during crises, blockchain-enabled shared auditability is positively associated with trust-based coordination and reduced response time, thereby supporting adaptive and recovery capacities.

Proposition 3: Integrated IoT–blockchain architectures are positively associated with multi-tier visibility and traceability beyond the independent effects of either technology alone. It advances the complementarity claim that integrating IoT event data with blockchain audit trails enhances multi-tier visibility more than deploying either technology alone. IoT systems can generate rich operational data, but cross-organization sharing can be limited by mistrust, inconsistent standards, and concerns about data manipulation. Blockchain systems can provide integrity and shared understanding, but they cannot directly observe physical conditions without trusted data inputs. Integration, anchoring key IoT events to a shared ledger, addresses both limitations by coupling sensing with verifiable recordkeeping. This mechanism is evident in 2020 proof-of-concept work integrating IoT temperature monitoring with blockchain traceability. Thus, Proposition 3 states that integrated IoT–blockchain architectures are positively associated with multi-tier visibility and traceability, particularly for products requiring condition control and provenance assurance.

Proposition 4: The positive relationship between IoT-enabled event detection and rapid response is strengthened when coupled with blockchain-based smart-contract enforcement mechanisms. It focuses on smart contracts as a conditional response mechanism that enhances responsiveness and recovery by automating predefined coordination actions. Permissioned blockchain platforms support the possibility of codifying process rules (e.g., release, hold, rework, recall initiation) that execute upon validated events, which can be interpreted as an information-processing mechanism that reduces coordination delays caused by manual verification and sequential approvals. When IoT event detection is integrated with blockchain validation, smart-contract logic can trigger alerts, documentation updates, or workflow handoffs without requiring that each organization independently reconcile records. Accordingly, Proposition 4 states that the effectiveness of IoT-enabled event detection for rapid response is strengthened when coupled with blockchain-based rule enforcement, leading to faster containment and recovery from disruptions.

Proposition 5: The positive relationship between IoT–blockchain integration and resilience outcomes is stronger in supply chains characterized by high asset specificity and compliance criticality. It introduces an important boundary condition: the resilience value of IoT–blockchain integration is greater in supply chains with high asset specificity and high compliance or quality criticality (e.g., pharmaceuticals, vaccines, and certain PPE categories) than in low-criticality commodity flows. Under TCE, asset specificity and uncertainty increase transaction hazards, motivating governance arrangements that reduce opportunism and safeguard relationship-specific investments. Cold chain contexts also impose strict condition requirements; vaccine and biologics potency depends on maintaining stipulated temperature ranges, and deviations can represent irreversible loss of quality. In such contexts, the value of trusted, auditable environmental monitoring is high. Therefore, Proposition 5 states that the positive relationship

between IoT–blockchain integration and resilience outcomes is stronger when (a) product integrity depends on controlled conditions and (b) stakeholders face high verification and liability risks.

Proposition 6: The resilience impact of IoT–blockchain integration is positively mediated by interorganizational governance quality and ecosystem participation breadth. It addresses ecosystem participation and governance as a necessary condition for realizing resilience benefits. Enterprise blockchain initiatives such as those in shipping and food traceability illustrate that value depends on onboarding multiple parties into a shared data-sharing environment. Adoption research indicates that organizational and ecosystem factors influence whether blockchain systems move beyond pilots, suggesting that technological capability alone is insufficient. Therefore, Proposition 6 states that the resilience impact of IoT–blockchain integration is mediated by interorganizational governance quality, including data standards alignment, access controls, and partner participation. Under weak governance, integration may increase complexity without producing commensurate improvements in visibility or responsiveness.

6.0 Managerial Implications

For managers operating in 2020's disruption environment, the framework suggests that IoT–blockchain integration should be pursued as a targeted resilience capability rather than as a broad transformation initiative. The pandemic has highlighted that the highest vulnerability often lies not in a firm's internal processes but in its inability to detect disruptions early in upstream tiers and to coordinate credible information exchange with logistics partners, regulators, and suppliers under uncertainty.

Cold chain monitoring provides a salient example. Vaccines and biologics typically require controlled temperature ranges, and literature on vaccine cold chain logistics emphasizes that potency losses from thermal compromise cannot be reversed, placing a premium on continuous monitoring and reliable documentation. Managers responsible for vaccine preparedness, recognizing that, as of mid-to-late 2020, large-scale COVID-19 vaccination is still emergent, can nonetheless adopt a forward-compatible approach: deploy IoT temperature and location sensors in storage and transport assets, while anchoring key custody and temperature events to a shared ledger accessible to authorized parties (e.g., manufacturers, 3PLs, public health agencies). This can reduce disputes about whether temperature excursions occurred and can accelerate corrective actions such as product quarantine and reallocation. The managerial emphasis should be on selective anchoring of critical events rather than storing full sensor streams on-chain, thereby addressing foreseeable performance and privacy constraints.

Multi-tier supplier traceability for critical inputs is another application aligned with 2020 realities. Global value chain analysis of medical supplies highlights interdependencies in production and trade that can contribute to shortages when demand surges and logistics impede replenishment. For managers seeking to reduce vulnerability to counterfeit or unreliable suppliers in high-scarcity markets, blockchain-based networks can provide a structured approach to documenting supplier credentials, certifications, and transaction histories, while IoT can provide physical verification signals (e.g., location tracking, tamper-evident sensor events) for shipments of critical materials. Early food traceability pilots integrating multiple parties around a shared ledger illustrate how trace-back time and collaboration can potentially be improved when participants agree on data-sharing rules and standardized identifiers. While direct translation to PPE or pharmaceuticals requires careful domain adaptation, the underlying coordination logic, shared auditability coupled with event capture, remains relevant.

In manufacturing equipment monitoring, managers can use IoT condition monitoring to detect anomalies that may threaten production continuity, particularly when spare parts lead times are uncertain and maintenance access may be constrained by workforce disruptions. Anchoring maintenance events and equipment condition exceptions to a permissioned ledger shared with key maintenance providers and critical suppliers can improve accountability for service-level commitments and create auditable records relevant to warranty, compliance, or insurance processes. This is most appropriate where multi-party coordination is required and where documentation disputes can slow recovery.

Recall management represents a further resilience-relevant domain. Blockchain-based traceability initiatives have been explicitly positioned as mechanisms to narrow recall scope by enabling rapid identification of affected lots and their distribution paths, as reflected in public descriptions of early food traceability systems and associated case analyses. IoT can complement this by providing condition data that supports root-cause analysis (e.g., identifying whether temperature excursions likely occurred during a particular transit segment). For managers, the implication is not that blockchain prevents quality failures, but that integrated digital records can reduce time-to-detection and time-to-targeted-response, core components of resilience.

Finally, risk detection and mitigation in logistics can be supported by integrating shipping documentation and event data across stakeholders. Trade documentation remains paper-intensive in many contexts, and pandemic disruptions highlight how delays can result from missing or inconsistent documentation. Early platforms in global shipping emphasize near-real-time data sharing among ports, carriers, and related actors, suggesting that the resilience value proposition is partly administrative: reducing coordination friction when logistics networks are stressed. Managers considering such platforms in 2020 should adopt an incremental implementation strategy focused on high-impact lanes and on data elements with the greatest coordination value, while anticipating that broad ecosystem adoption may be slow and contingent on governance, standards, and trust.

Across these applications, the managerial implication is clear: resilience gains arise not from adopting digital technologies as labels, but from deliberately designing integrated information architectures that enhance timely sensing, reduce ambiguity, and support credible interorganizational coordination under disruption.

Boundary Conditions and Failure Scenarios

Despite its potential, IoT–blockchain integration may fail to generate resilience benefits under certain conditions.

- First, low ecosystem participation reduces ledger effectiveness, as distributed validation requires broad stakeholder involvement.
- Second, weak data governance structures may undermine trust even when blockchain systems are implemented.
- Third, excessive data anchoring without strategic filtering may increase operational complexity and transaction costs.

These limitations highlight that digital technologies alone do not guarantee resilience; organizational alignment and governance maturity are critical enabling conditions.

7.0 Conclusion

This conceptual paper has developed a theory-grounded framework explaining how IoT and blockchain integration can enhance digital supply chain resilience in the pandemic context of 2020. COVID-19 has revealed vulnerabilities in global supply networks for essential medical products, highlighting multi-tier visibility gaps, limited event detection capacity, and coordination challenges under extreme uncertainty. In response, the paper argued that IoT and blockchain represent complementary components of a resilience-enabling infrastructure: IoT expands information processing capacity through real-time sensing and event detection, while blockchain provides distributed trust and auditability that can reduce transaction hazards and coordination friction in multi-party networks.

The theoretical contribution lies in specifying mechanisms rather than asserting generic digital benefits. By using OIPT to explain how technologies increase information processing capacity and reduce uncertainty, and by using TCE to explain how blockchain-based governance can reduce opportunism and verification costs, the paper links specific technological capabilities to resilience dimensions such as visibility, responsiveness, adaptability, trust-based coordination, and structural robustness. The six research propositions provide a structured agenda for empirical testing in future studies, including investigations of boundary conditions such as asset specificity, compliance criticality, and ecosystem governance.

Managerially, the paper argues for targeted, incremental adoption strategies grounded in 2020 technological maturity. Early enterprise pilots in food traceability and global shipping illustrate plausible pathways for blockchain-enabled collaboration, while 2020 IoT research underscores the expanding role of real-time sensing in logistics and manufacturing. The paper highlights realistic applications in cold chain monitoring, multi-tier traceability for critical inputs, equipment monitoring, and recall management, while emphasizing that these systems require careful design choices about data standards, access controls, and off-chain/on-chain architectures.

This study advances digital supply chain research by offering a theoretically grounded, mechanism-based framework for IoT–blockchain integration. By identifying causal pathways, governance moderators, and boundary conditions, the paper contributes a structured foundation for future empirical testing and managerial implementation. In doing so, it moves beyond technology optimism and provides a resilience-centered explanation of digital transformation in supply networks.

Future empirical studies can operationalize the proposed constructs to test complementarity effects and governance-mediated resilience mechanisms across industries and disruption contexts.

References

[1] World Health Organization. (2020, March 3). *Shortage of personal protective equipment endangering health workers worldwide*.

[2] Ivanov, D., & Dolgui, A. (2020). Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case. *Transportation Research Part E: Logistics and Transportation Review, 136*, 101922.

[3] Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1–14.

[4] Shashi, Centobelli, P., Cerchione, R., & Ertz, M. (2020). Cold chain time- and temperature-controlled transport of pharmaceuticals and vaccines. *Sustainability, 12*, Article 3709.

[5] World Customs Organization. (2020). *Seeing deeper into supply chains is key to overcoming disruptions*. WCO News, Issue 93.
[6] Büyüközkan, G., & Göçer, F. (2020). Digital supply chain: Literature review and a proposed framework for future research. *Supply Chain Forum: An International Journal*.
[7] Global mobile Suppliers Association. (2020). *5G stand-alone: August 2020 global status update*.
[8] Wagner, S. M., & Bode, C. (2017). An information processing perspective on supply chain risk management. *International Journal of Production Economics, 195*, 199–213.
[9] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain adoption challenges in supply chain: An empirical investigation. *International Journal of Production Economics, 210*, 1–12.
[10] Queiroz, M. M., & Wamba, S. F. (2019). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E, 129*, 1–23.
[11] Kouhizadeh, M., Saberi, S., & Sarkis, J. (2020). Blockchain technology for sustainable supply chain management: A systematic literature review and research agenda. *Sustainability, 12*(18), 7638.
[12] Williamson, O. E. (1979). Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics, 22*(2), 233–261.
[13] Ankit Sharma. (2020). Beyond cryptocurrency – More to blockchain.
[14] Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*.
[15] Casino, F., Dasaklis, T. K., & Patsakis, C. (2020). Combining blockchain and IoT: Food-chain traceability and transparency. *Energies, 13*(15), 3820.
[16] Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. *Journal of the British Blockchain Association, 1*(1).
[17] Sharma, A., & Sharma, A. (2019). Effect and impact of IoT (Internet of Thing) on supply chain management. *no. January*.
[18] Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., & Wamba, S. F. (2020). Big data analytics capability in supply chain agility: The moderating effect of organizational flexibility. *Management Decision, 58*(8), 1657–1676.
[19] Autry, C. W., & Griffis, S. E. (2008). Supply chain capital: The impact of structural and relational linkages on firm execution and innovation. *Journal of Business Logistics, 29*(1), 157–173.
[20] Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350.
[21] Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces, 4*(3), 28–36.
[22] Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research, 21*(4), 724–735.
[23] Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM, 63*(7), 80–90.
[24] Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management, 50*(3), 55–73.
[25] Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2.