American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-2163
Doi: 10.63125/6n81ne05

BLOCKCHAIN-ORCHESTRATED CYBER-PHYSICAL SUPPLY CHAIN NETWORKS FOR MANUFACTURING RESILIENCE

Md Sanjid Khan[1]; Sudipto Roy[2];

[1]. Department of Industrial and Systems Engineering, Lamar University, Texas, USA; Email: khansanjid9@gmail.com

[2]. Department of Industrial and Systems Engineering, Lamar University, Texas, USA; Email: sudiptobd00@gmail.com

Abstract

This study examines how blockchain-orchestrated cyber-physical supply chains (CPSCs) contribute to manufacturing resilience by translating blockchain capabilities into measurable antecedents and testing their relationships with visibility, agility, robustness, and recovery outcomes. Drawing on dynamic capabilities and information-processing theories, the research conceptualizes blockchain orchestration as a multi-dimensional capability encompassing traceability, smart-contract automation, IoT–ledger interoperability, and governance quality. These dimensions collectively function as coordination mechanisms that enhance supply chain visibility and agility, thereby reinforcing resilience under environmental turbulence. Using a quantitative, cross-sectional, multi–case design embedded in active manufacturing consortia, the study surveyed 204 firms and plants across OEMs, suppliers, and logistics partners engaged in production-grade blockchain implementations. Measurement scales were validated for reliability, convergent, and discriminant validity, and hierarchical regression models were employed to test direct, mediated, and moderated effects, with robustness checks incorporating fixed effects, alternative indices, and bootstrap estimation. Results indicate that traceability, interoperability, and governance quality significantly predict visibility; smart-contract automation and visibility predict agility; and together, these coordination capabilities explain variance in robustness and a composite resilience index. The agility–resilience relationship is found to intensify under greater environmental turbulence, confirming agility's contingent value in volatile contexts. Mediation tests reveal that visibility partially transmits the effects of traceability and interoperability to agility, highlighting its role as a keystone coordination capability. Collectively, the findings provide the first empirically validated framework linking blockchain orchestration capabilities to measurable resilience outcomes in CPSCs. Conceptually, the research reframes blockchain from a technological artifact to a configurable coordination layer that improves inter-firm information integrity, synchronization, and adaptive performance. Practically, the study offers a roadmap for manufacturers: invest first in traceability and interoperability, then extend to smart-contract automation under strong governance. This evidence-based approach positions blockchain orchestration as a foundational capability for building auditable, agile, and resilient digital supply networks in manufacturing ecosystems.

Keywords

Blockchain Orchestration, Cyber-Physical Supply Chains, Manufacturing Resilience, Visibility

Citation:
Khan, M. S., & Roy, S. (2023). *Blockchain-orchestrated cyber-physical supply chain networks for manufacturing resilience. American Journal of Scholarly Research and Innovation, 2*(1), 194–223

https://doi.org/10.63125/6n81ne05

Received:
January 20, 2023

Revised:
February 18, 2023

Accepted:
March 27, 2023

Published:
April 15, 2023

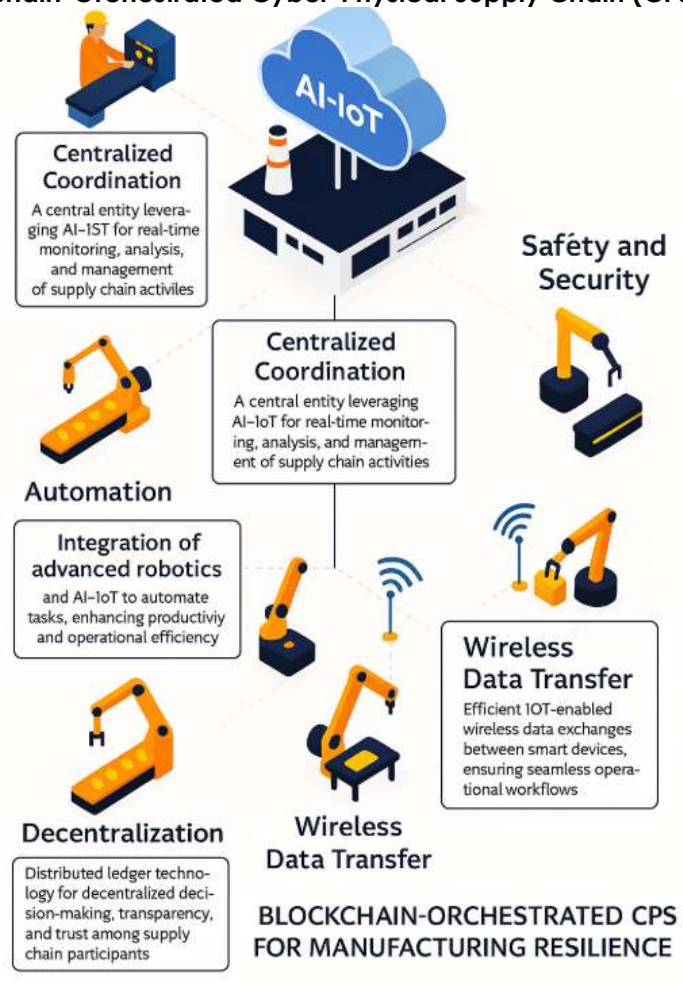
Copyright:
© 2023 by the author. This article is published under the license of American Scholarly Publishing Group Inc and is available for open access.

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

INTRODUCTION

Manufacturing supply chains are increasingly instantiated as cyber-physical supply chain (CPSC) networks, where physical assets (machines, sensors, products) are closely coupled with computational and communication layers to enable real-time monitoring, control, and coordination across organizational boundaries (Lee et al., 2015). In parallel, blockchain a distributed, append-only ledger secured by cryptography and consensus has emerged as an inter-organizational data infrastructure that supports tamper-evident records, programmable transactions (smart contracts), and cross-firm data sharing with embedded governance (Christidis & Devetsikiotis, 2016). The convergence of CPSCs with blockchain offers a potential orchestration mechanism: IoT/edge devices and MES/ERP events can be notarized to a shared ledger, while smart contracts codify business rules for automated fulfillment, settlement, and compliance (Kshetri, 2018). Internationally, manufacturing faces persistent volatility from geopolitical shocks to health emergencies that elevates resilience (the capacity to withstand, adapt, and recover) as a strategic performance criterion alongside cost, quality, speed, and sustainability (Brandon-Jones et al., 2014; Dubey et al., 2017). In this context, blockchain-orchestrated CPSCs refers to supply networks in which blockchain capabilities (traceability, smart-contract automation, interoperability with IoT/OT systems, and consortium governance) coordinate cyber-physical data flows and interfirm processes to enhance resilience outcomes such as visibility, agility, robustness, recovery speed, and data security/compliance (Caridi et al., 2014). This framing positions blockchain not as a standalone technology but as an orchestration layer embedded in CPSCs, aligning with global priorities for trustworthy, auditable, and rapidly reconfigurable production-logistics systems that must function across diverse regulatory regimes and partner ecosystems (Kshetri & Voas, 2018).

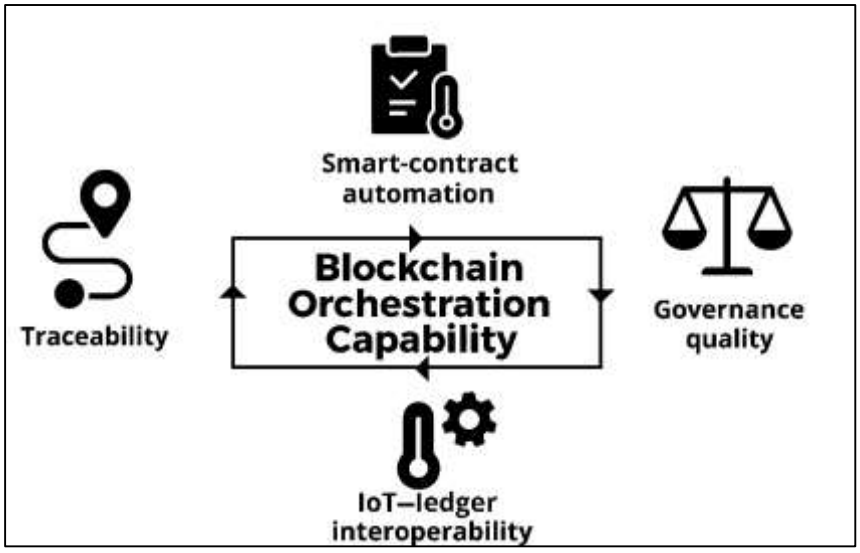
Figure 1: Blockchain-Orchestrated Cyber-Physical Supply Chain (CPSC) Framework



American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Blockchain orchestration capability encompasses a set of complementary, measurable dimensions. Traceability maps provenance, transformation, and custody events to an immutable ledger, enabling end-to-end auditable visibility (Tian, 2017). Smart-contract automation operationalizes inter-organizational business logic (e.g., purchase orders, 3-way match, condition-based payments) to trigger low-latency, rule-based actions (Christidis & Devetsikiotis, 2016). Interoperability links IoT sensors, PLCs, MES, and WMS/ERP to on-chain or side-chain records via standardized APIs and event streaming, which is essential in CPSCs for trustworthy cyber-physical data exchange (Lee et al., 2015; Treiblmaier, 2018). Governance quality captures permissioning, data-sharing rules, and dispute mechanisms in consortium settings, shaping adoption and performance (Queiroz et al., 2020). In CPSCs, such orchestration is argued to reduce information asymmetry, improve synchronization, and harden data integrity across global networks, thereby reinforcing resilience mechanisms (Barratt & Oke, 2007). The literature indicates that supply-chain visibility (timely, accurate, complete, and usable data) is an antecedent to agility (rapid reconfiguration) and robustness (performance stability under stress), while security/compliance depends on integrity and access control (Francisco & Swanson, 2018). Blockchain's fit with these mechanisms is repeatedly documented across reviews and empirical works linking distributed ledgers with transparency, accountability, and collaboration in multi-actor supply chains (Yli-Huumo et al., 2016).

Figure 2: Blockchain Orchestration Dimensions Driving Supply Chain Resilience



This study aims to establish a rigorous, capability-to-outcome account of how blockchain-orchestrated cyber-physical supply chain networks contribute to manufacturing resilience by translating the concept of "orchestration" into measurable antecedents and testing their relationships with well-defined resilience constructs across multiple operating consortia. The primary objective is to quantify the association between orchestration capabilities traceability, smart-contract automation, IoT–ledger interoperability, and governance quality and the visibility of interfirm flows, recognizing visibility as a central coordination capability in cyber-physical environments. A second objective is to examine how visibility relates to agility and robustness once firm characteristics and digital maturity are controlled, thereby clarifying whether improved information quality and timeliness are linked with faster reconfiguration and performance stability under stress. A third objective is to assess whether smart-contract automation and IoT–ledger interoperability exhibit direct effects on resilience outcomes beyond visibility, acknowledging that programmable execution and machine-to-ledger data capture may shorten decision cycles and synchronize processes. A fourth objective is to evaluate the conditional role of environmental turbulence by testing whether the association between agility and a composite resilience index strengthens as volatility increases. Together, these objectives are operationalized in a quantitative, cross-sectional, multi–case design that targets plants and firms actively participating in blockchain-enabled manufacturing supply chains. The study specifies reflective indicators for each capability

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05
and outcome on a five-point Likert scale, conducts descriptive analysis to profile the sample and cases, estimates correlations to screen for construct relations and multicollinearity, and fits hierarchical regression models to test the core objectives, including interaction terms for moderation and bootstrap procedures for indirect effects where warranted. Delimitations are set to exclude proofs-of-concept without live operations, respondents without operational visibility, and non-manufacturing contexts, thereby keeping inference focused on production-logistics settings where cyber-physical data and interorganizational governance are salient. The intended deliverables include a validated measurement instrument for blockchain orchestration, empirical estimates linking capabilities to resilience outcomes, and model specifications that can be replicated by practitioners and researchers in comparable manufacturing networks.

LITERATURE REVIEW

The literature on blockchain-enabled operations and cyber-physical supply chain (CPSC) integration has evolved along two largely parallel streams technology-centric work that details architectures, protocols, and smart-contract applications, and operations-management research that theorizes visibility, agility, robustness, recovery, and security/compliance as pillars of resilience. Bringing these streams together, recent scholarship frames blockchain not as an isolated tool but as an orchestration layer embedded within CPSCs, where IoT sensors, PLCs, MES/ERP systems, and logistics platforms generate high-frequency event data that can be notarized on shared ledgers and acted upon via programmable rules. Within this framing, four interlocking capability domains recur: traceability (end-to-end provenance and custody), smart-contract automation (codified inter-firm business logic), interoperability (standards and pipelines connecting OT/IT to on-/off-chain data stores), and governance quality (permissioning, data-sharing rules, liability and dispute resolution). At the same time, resilience research provides mature constructs and measurement guidance treating visibility as a coordination capability that improves information timeliness, accuracy, and usefulness; linking visibility to agility through faster sensing, decision, and reconfiguration cycles; and relating both to robustness and recovery via buffered capacity, synchronized plans, and early exception detection. Yet, despite conceptual alignment, empirical evidence that quantifies capability-to-outcome pathways remains uneven. Many studies emphasize proofs-of-concept, single-case narratives, or technical feasibility without validated scales or cross-firm comparisons; others use simulations that abstract away institutional constraints such as data rights, auditability, and interoperability across heterogeneous vendor stacks. Measurement choices also diverge, with some works operationalizing blockchain adoption as a binary state rather than as graded orchestration capabilities, and with resilience outcomes captured by disparate, sometimes noncomparable indicators. Finally, the cyber-physical context introduces unique boundary conditions data quality at the edge, latency and throughput limits, identity and access management across partners, and the need to balance transparency with confidentiality that shape both adoption and performance effects. This review synthesizes these strands into a coherent capability-performance framework, clarifies definitions and measurement strategies suitable for multi-case, cross-sectional analysis, and surfaces the theoretical logics resource-based, dynamic capabilities, and information-processing that justify modeling visibility, agility, and robustness as interdependent outcomes of blockchain-orchestrated CPSCs.

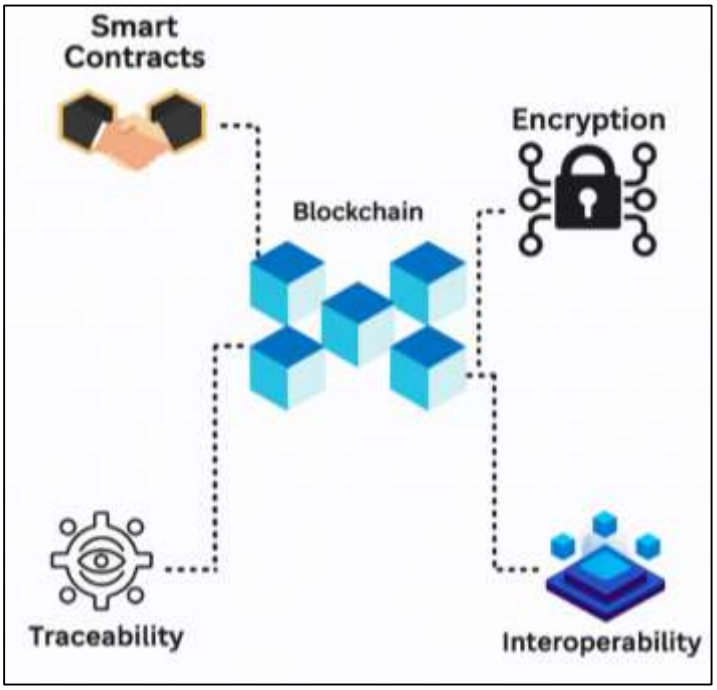
Blockchain Orchestration in Inter-Organizational Operations

Blockchain orchestration in inter-organizational operations can be understood as the capability to coordinate multi-firm processes through shared, tamper-evident data structures and programmable rules that reduce verification costs and synchronize actions across organizational boundaries (Abdul, 2021). In practical terms, orchestration spans four tightly coupled dimensions: standardized data capture and notarization across partners (Rony, 2021); codification of cross-firm business logic into machine-executable agreements; interoperable interfaces that connect operational technologies and enterprise systems to ledgers (Danish & Zafor, 2022); and consortium governance that specifies membership, data rights, and dispute mechanisms. Together, these dimensions enable a shift from post-hoc reconciliation to near-real-time alignment of orders, logistics events, quality checkpoints, and financial settlements (Danish & Kamrul, 2022). At the theory level, orchestration reframes blockchain from a stand-alone technology to a structural property of the inter-firm information system a property that can influence transaction costs, information asymmetries, and coordination latency. Conceptual frameworks emphasize that distributed ledgers create a shared substrate for

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

record-keeping and rule execution that may substitute for some hierarchical or third-party coordination mechanisms when trust is limited and verification is costly (Hughes et al., 2019; Hossen & Atiqur, 2022). Transaction-cost-based analyses further suggest that when asset specificity is high and opportunism risks are nontrivial, the availability of verifiable, time-stamped records and automated enforcement can shift the make-buy-ally calculus by lowering monitoring costs and improving contractibility of complex exchanges (Schmidt & Wagner, 2019). From an operational perspective, orchestration is not merely immutability or transparency in the abstract; it is the institutionalization of who writes, who reads, and who executes what, under what conditions, with audit trails that bind cyber-physical events (e.g., sensor alarms, quality deviations, transport handovers) to business outcomes (e.g., staged payments, claims, penalties) in a manner that is inspectable across firm boundaries (Rabiul & Praveen, 2022; Risius & Spohrer, 2017).

Figure 2: Blockchain Orchestration in Inter-Organizational Operations



Realizing orchestration in supply networks requires an architecture that couples event origination at the edge with verifiable state transitions in shared ledgers. In manufacturing and logistics, this typically means that programmable contracts specify conditional actions release of inventory, milestone payments, detention fees tied to digitally signed events and trusted time sources, while interfaces aggregate machine and system events into standardized messages suitable for notarization. Firms then co-manage a common "source of procedural truth," which reduces cycle-time variability arising from bilateral confirmations and manual reconciliations. Empirical and design-oriented studies illustrate how this shared substrate can simplify provenance tracking, automate compliance checks, and mitigate fraud by eliminating opaque handoffs and unverifiable paper trails (Kamrul & Omar, 2022; Toyoda et al., 2017). Managerially, orchestration implies a reallocation of coordination work: instead of each dyad privately maintaining its own ledgers and rules, partners co-define state machines, exception paths, and data retention policies that are executed consistently across the network. This reallocation is particularly salient where multi-tier visibility is weak and dispute resolution is costly, because encoded rules and common records can deter post-contractual opportunism, align incentives, and reduce the need for repeated bilateral negotiations (Razia, 2022; Schmidt & Wagner, 2019). At the same time, orchestration is not synonymous with public-chain maximalism; permissioned topologies and role-based access controls are typical in operations settings, where confidentiality, selective disclosure, and compliance with sectoral regulations matter. Hence, effective orchestration depends on socio-technical design: defining

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05
membership criteria, selecting consensus mechanisms that fit throughput and finality requirements, mapping identity and key management to corporate controls, and integrating with enterprise resource planning and manufacturing execution systems through resilient middleware (Wang et al., 2019).

Strategically, the value of blockchain orchestration emerges when it complements not replaces existing coordination routines by making inter-firm information processing more reliable and timely at scale. Synthesizing insights across operations and information-systems research, integrative reviews argue that distributed ledgers and smart contracts can reconfigure how firms sense, decide, and act together by collapsing verification lead-times and standardizing conditional logic across transactional boundaries (Toyoda et al., 2017). This standardization can unlock network effects: as more partners adopt common schemas and contract templates, the marginal cost of adding nodes falls, while the marginal value of visibility and automation rises. However, orchestration advantages are contingent on governance choices. Poorly designed access rules, incentive misalignments, or rigid smart-contract templates can externalize risks onto weaker partners or ossify processes, negating promised efficiency gains (Hughes et al., 2019). Conversely, when governance delineates data stewardship, liability, and upgrade paths, the shared ledger becomes a credible coordination device that improves collective action under uncertainty (Schmidt & Wagner, 2019). For managers, the operational question is therefore not "blockchain or not," but how to decompose inter-firm workflows into verifiable events and executable rules, specify who may invoke which transitions, and ensure that off-chain realities quality tests, sensor readings, transport handovers are faithfully captured as on-chain facts. In sum, blockchain orchestration represents a configurable capability whose performance implications depend on architectural fit, transaction characteristics, and the maturity of inter-organizational governance (Risius & Spohrer, 2017).

Cyber-Physical Supply Chains (CPSC) and IoT/Edge Integration

Cyber-physical supply chains (CPSCs) fuse sensing, computation, and control with material flows so that physical operations and digital representations coevolve in near real time. In this view, shop-floor machines, mobile assets, and transported items emit telemetry that is filtered at the edge, aggregated through operational technology (OT) gateways, and synchronized with information systems and analytics pipelines across partner boundaries. The Internet of Things (IoT) literature positions this stack as a layered architecture perception (sensing/actuation), network (connectivity), and application (services, analytics) that must interoperate reliably despite heterogeneity in devices, protocols, and data models (Atzori et al., 2010). For supply chains, the promise is not merely connectivity but controllability: by binding sensor states and events to standardized messages and rules, networks can reduce information lag, align decisions, and lower reconciliation costs across tiers. Vision papers emphasize scalable addressing, device management, and context awareness as prerequisites for dependable multi-firm visibility, while noting constraints in power, bandwidth, and mobility that complicate industrial deployments (Gubbi et al., 2013). A parallel stream in industrial informatics argues that IoT in factories differs from consumer settings because it must meet stringent requirements for determinism, safety, and security within cyber-physical production systems (CPS) that integrate programmable controllers, manufacturing execution systems, and enterprise planning (Xu et al., 2014). In CPSCs, therefore, edge intelligence compressing, validating, and time-stamping events locally becomes a structural necessity, not a convenience. The architectural implication is a federated pipeline in which local nodes preprocess and sign events, propagate only salient state changes, and support downstream orchestration layers that codify cross-firm business logic. This pipeline transforms raw telemetry into actionability: exceptions can be detected earlier, interventions can be targeted more precisely, and partner coordination can be automated where rules are machine-executable (Lu, 2017; Sadia, 2022).

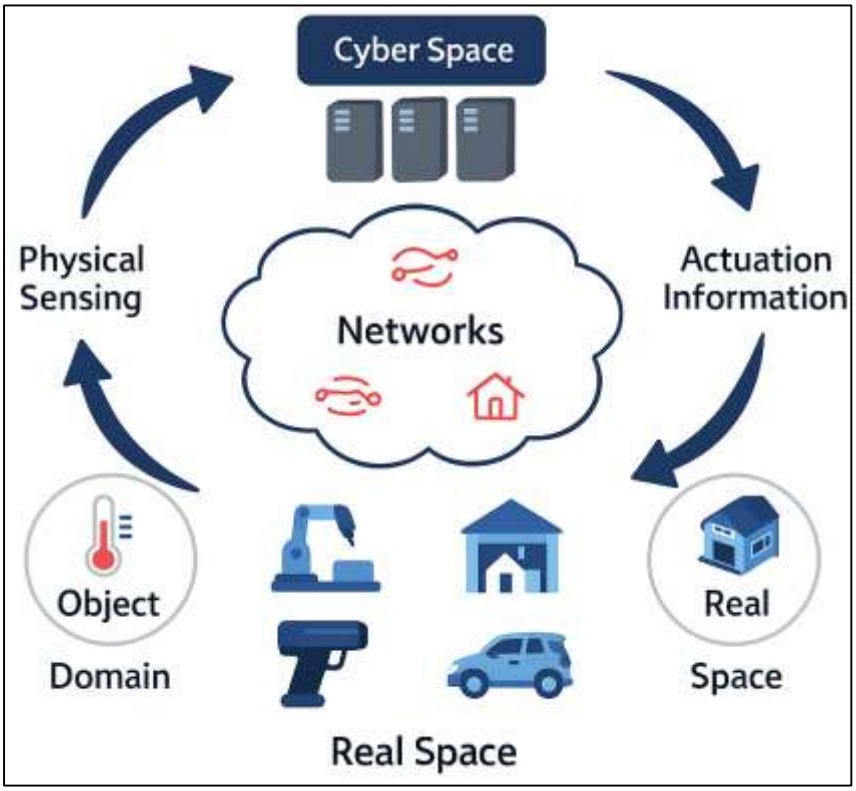
Edge-centric designs in CPSCs also reshape performance envelopes by relocating computation and decision logic closer to where data originate. Industrial CPS perspectives stress that the "tight coupling" between physical and cyber realms requires closed-loop control with bounded latency, robust time synchronization, and traceable state transitions to assure quality and throughput (Danish, 2023; Monostori, 2014). In practice, end-to-end responsiveness hinges on a chain of latencies that accumulate from sensing through final confirmation. A simple decomposition useful for design and diagnosis is

$$L_{e2e} = L_{sense} + L_{uplink} + L_{proc} + L_{rule} + L_{commit},$$

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

where L_{sense} is sensor/PLC acquisition and conditioning, L_{uplink} is transport from edge to gateway/cloud, L_{proc} is parsing/validation at the integration layer, L_{rule} is the time to evaluate and execute inter-organizational logic (e.g., releasing inventory or triggering quality holds), and L_{Commit} is the time to persist and acknowledge the state change to shared records. Minimizing L_{e2e} while preserving integrity and auditability is the core engineering tension in CPSCs: more aggressive compression and local actuation reduce delays but risk information loss or inconsistency across partners; stronger verification and consensus mechanisms improve trust but may increase confirmation times. IoT surveys highlight patterns to manage this tension: hierarchical gateways, publish/subscribe backbones, and context-aware filtering that privilege exception events over steady-state chatter (Atzori et al., 2010). Industrial instantiations add software-defined control overlays and deterministic networking to meet factory-grade timing and reliability, allowing time-critical tasks to execute at the edge while non-critical analytics flow to cloud tiers (Xu et al., 2014). Within CPSCs that span multiple firms, these design choices are not purely technical; they encode who sees which events when, and therefore shape the economics of coordination, the feasibility of automated inter-firm agreements, and the measurability of resilience outcomes such as visibility, agility, and robustness (Arif Uz & Elmoon, 2023; Monostori, 2014).

Figure 3: Cyber-Physical Supply Chains (CPSC) and IoT/Edge Integration



Translating IoT/edge integration into inter-organizational value requires governance of interfaces, semantics, and responsibilities along the pipeline. Industrial IoT overviews propose reference models that separate concerns device identity, data ownership, access control, and lifecycle management so that partners can interoperate without exposing proprietary internals (Razia, 2023; Xu et al., 2014). In supply networks, this translates into shared vocabularies for events (e.g., production completion, temperature excursion, custody transfer), service-level agreements for timeliness and accuracy, and contractible obligations for remediation when data or processes deviate. Industry 4.0 syntheses contend that modularity and standardization enable reconfigurability: when components sensors, gateways, analytics, and execution rules are swappable yet governed by stable schemas, networks can adapt faster to disruption and demand variability (Lu, 2017). CPS perspectives further underscore that provenance and time alignment are as important as payloads, because decisions

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

often hinge on the "when" and "under whose authority" of an event, not only on the "what" (Monostori, 2014; Reduanul, 2023). Consequently, robust CPSCs invest in secure time sources, signed event envelopes, and versioned ontologies to make state changes inspectable and comparable across sites and firms. This is where edge integration intersects with orchestration layers: once events are normalized and verifiable, inter-firm rules can be encoded and executed consistently, reducing bilateral reconciliation and manual exception handling. The IoT literature's call for scalable, context-aware, and service-oriented architectures aligns with these needs by advocating lightweight messaging, edge analytics, and the decomposition of complex workflows into composable services (Atzori et al., 2010; Sadia, 2023). Industrial informatics adds the requirement that such services be auditable and certifiable within regulated production contexts, so that data trails can support quality assurance, compliance, and dispute resolution (Xu et al., 2014; Zayadul, 2023). Together, these strands outline the socio-technical substrate upon which resilient, multi-firm CPSCs can be built: an edge-first, semantics-rich, and governance-aware integration fabric that shortens L_{e2e} without sacrificing integrity or accountability (Lu, 2017).

Supply-Chain Resilience Constructs and Measurement

Resilience in supply chains is best treated as a multi-dimensional, measurable capability set rather than a single latent trait. Conceptual work identifies three interlocking construct families: (i) absorptive/robustness the ability to maintain acceptable performance during a disruption; (ii) adaptive/agility the speed and flexibility to reconfigure flows, suppliers, and schedules; and (iii) restorative/recovery the capacity to return to (or surpass) pre-disruption performance levels. A fourth cross-cutting construct, visibility, represents the timeliness, accuracy, and usability of end-to-end information that enables sensing and coordinated response. Foundational frameworks propose that resilience emerges from a portfolio of capabilities (e.g., flexibility, redundancy, collaboration) that align with contextual "vulnerabilities" such as complexity or turbulence, and that performance is realized when capability–vulnerability fit is high (Pettit et al., 2010). In empirical scale development, resilience is operationalized via reflective items capturing preparedness, response, and recovery routines at the firm or network level, with psychometric validation to ensure reliability and discriminant validity from adjacent constructs like risk management or lean practices (Ambulkar et al., 2015). Network-focused studies add a structural layer, arguing that resilience depends not only on internal capabilities but also on supply network topology and relational ties where centrality, redundancy paths, and the dispersion of critical nodes constrain or enable disruption propagation and mitigation (Blackhurst et al., 2011). Together, these streams support a measurement stance in which resilience is a configurational property expressed through observable routines (e.g., buffer management, supplier substitution, synchronized planning) and outcomes (e.g., service level maintenance, recovery time), with visibility acting as an enabling coordination capability across all phases.

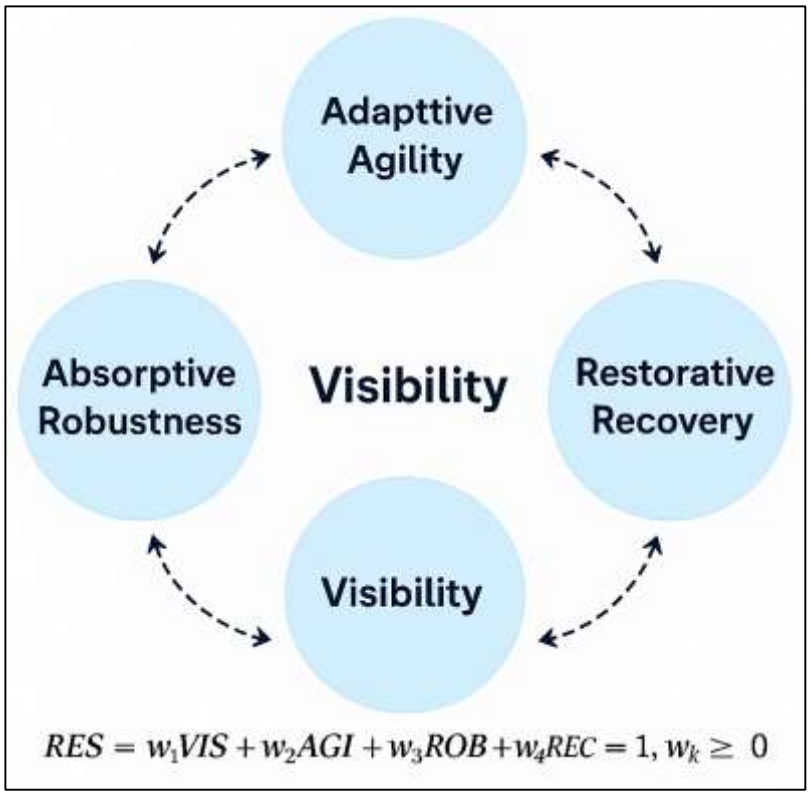
A practical measurement approach assembles these constructs into indices suitable for cross-sectional, multi-firm analysis. Let VIS, AGI, ROB, and REC denote standardized (z-scored) measures of visibility, agility, robustness, and recovery. A composite resilience index can be expressed as a weighted aggregation:

$$\boldsymbol{RES = w_1 VIS + w_2 AGI + w_3 ROB + w_4 REC,} \quad \sum_{k=1}^{4} \boldsymbol{w_k = 1,} \quad \boldsymbol{w_k \geq 0,}$$

Weights may be equal (parsimony for benchmarking) or data-driven (e.g., proportional to factor loadings from a confirmatory factor analysis or to regression importance weights when predicting disruption loss). This formulation supports transparency (each sub-score is interpretable) and comparability (standardization removes unit effects), while allowing sensitivity checks by re-estimating wkw_kwk under alternative priorities (e.g., service-critical contexts might emphasize ROB and REC). Empirical work suggests that resilience is not homogeneous: capability bundles interact with network structure and environmental dynamism to yield different performance profiles (Brusset & Teller, 2017). Accordingly, resilience measurement should incorporate context variables (e.g., supply-base complexity, demand volatility) and relational capabilities (e.g., collaboration intensity) as controls or moderators when linking capabilities to outcomes (Ali et al., 2017). From a psychometric standpoint, established practices include internal consistency (Cronbach's α and composite reliability ≥ .70), convergent validity (average variance extracted ≥ .50), and discriminant validity (e.g., heterotrait–monotrait ratio < .85). Scale content should balance routine-oriented items

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05
(e.g., "we can substitute suppliers within X days") with performance-oriented items (e.g., "we restore target service levels quickly") to capture both capability and outcome facets (Ambulkar et al., 2015).

Figure 4: Supply-Chain Resilience Constructs and Measurement



A recurring empirical insight is that visibility functions as a keystone capability through which other investments translate into resilience. Visibility reduces information lead time, allowing earlier exception detection and tighter coordination, thereby amplifying the impact of agility and robustness routines. In variance terms, improved visibility can reduce forecast error and process variability, which in turn lowers the safety-stock and time buffers required to sustain service levels during shocks, freeing capacity for adaptive actions. Studies associating supply-chain capabilities with performance show that collaboration and information integration reinforce resilience under uncertainty by enabling synchronized responses and shared contingency plans (Brusset & Teller, 2017). Complex adaptive systems perspectives further argue that resilience arises from local adaptation, modularity, and feedback loops features that can be operationalized via measures of reconfiguration speed, decision decentralization, and learning from disruptions (Ali et al., 2017). Complementarily, capability–vulnerability alignment frameworks propose auditing "what we are good at" against "where we are exposed" and prioritizing capability investments that close the most consequential gaps (Pettit et al., 2010). Scale development work indicates that firms exhibiting higher resilience scores tend to engage in proactive routines (e.g., supplier development, dual sourcing) and reactive routines (e.g., expedited logistics, dynamic scheduling), and that these routines' performance effects are strongest when embedded in collaborative relationships and clear governance arrangements (Ambulkar et al., 2015). Collectively, this evidence supports a measurement model in which resilience is captured through a small set of validated constructs and a transparent composite index, estimated alongside contextual moderators, to explain variance in service continuity and recovery outcomes across heterogeneous manufacturing supply chains (Blackhurst et al., 2011).

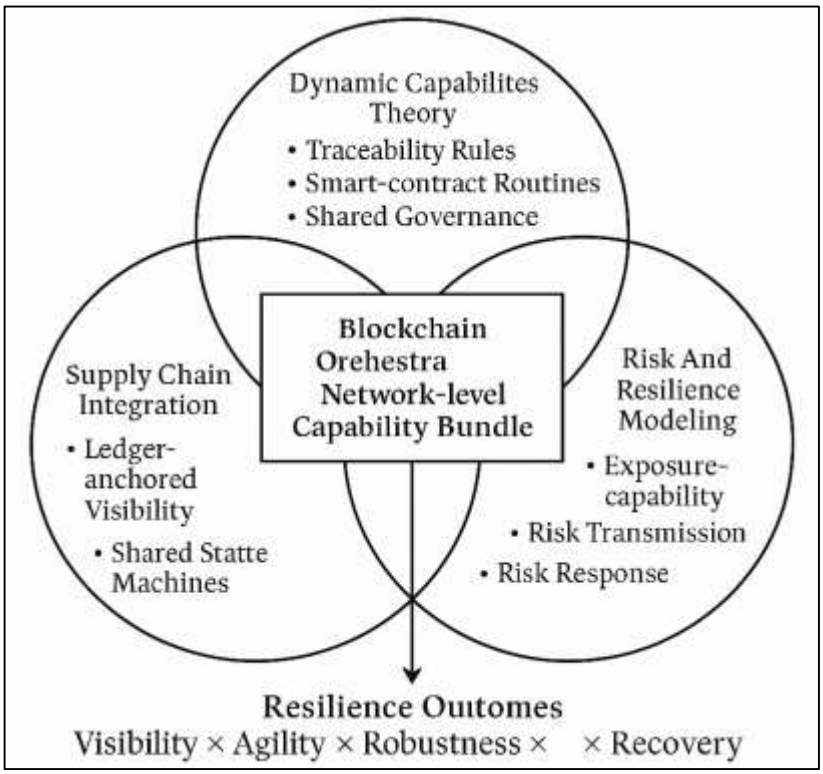
Theoretical Lenses and Empirical Gaps

The theoretical scaffolding for blockchain-orchestrated cyber-physical supply chains (CPSCs) draws first on dynamic capabilities theory, which explains how firms sense opportunities and threats, seize them through coordinated investments, and continuously reconfigure assets to sustain performance

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

advantages under turbulence. In a multi-firm setting, blockchain orchestration can be interpreted as a network-level capability bundle traceability rules, smart-contract routines, and shared governance that enables rapid recombination of interorganizational processes when disruptions or market shifts occur. Dynamic capabilities emphasize microfoundations such as managerial cognition, rule design, and learning mechanisms; in CPSCs these map to the codification of inter-firm decision logic (e.g., exception handling, conditional release, automated settlement) and to the institutional routines that update such logic as partners, sensors, and regulatory constraints change. Critically, this lens highlights *reconfiguration speed* and *switching costs* as determinants of resilience: when orchestration rules are modular, parameterized, and transparently governed, partners can re-route flows, substitute suppliers, or change quality thresholds with lower coordination latency. Conversely, brittle or opaque rules create lock-ins and amplify disruption propagation.

Figure 5: Theoretical Framework in Blockchain-Orchestrated Cyber-Physical Supply Chains



Thus, a dynamic-capabilities perspective provides a tractable path for measurement: blockchain orchestration becomes observable as routinized sensing (e.g., near-real-time visibility), seizing (e.g., automated enactment of remedies), and reconfiguring (e.g., rapid policy and partner updates), which should manifest in higher agility and robustness scores in cross-sectional data (Teece, 2007).
A second lens arises from supply chain integration and collaboration research, which links structured information sharing, process alignment, and relational coordination to operational performance. From this standpoint, blockchain-enabled orchestration is not valuable *per se*; it is valuable when it deepens integration internally across purchasing, operations, and logistics, and externally across suppliers, contract manufacturers, and carriers by standardizing event semantics and reducing verification frictions. Prior work shows that integration effects are contingent on context (e.g., product clockspeed, demand volatility) and configurational, meaning different integration bundles can yield comparable performance, while misfits erode benefits. Translating this logic, CPSCs should realize resilience gains when ledger-anchored visibility, shared state machines, and automated cross-firm rules increase the *timeliness* and *reliability* of interdependent decisions (planning, release, transport, and quality control). Collaboration theory further posits that joint gains emerge through *collaborative advantage* a composite of trust, mutuality, and shared routines which blockchain

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05
governance can support by clarifying rights, obligations, and auditability (Ketchen & Hult, 2007). Empirically, the literature thus motivates (i) modeling visibility as a keystone capability mediating the integration–performance link and (ii) estimating moderation by environmental turbulence and supply-base complexity, since orchestration may matter most where uncertainty and interdependence are high. These expectations align with evidence that integration improves performance through coordinated routines and shared information architectures, suggesting that blockchain's measurable contribution should appear as stronger visibility–agility–robustness pathways within integrated networks (Cao & Zhang, 2011; Flynn et al., 2010).

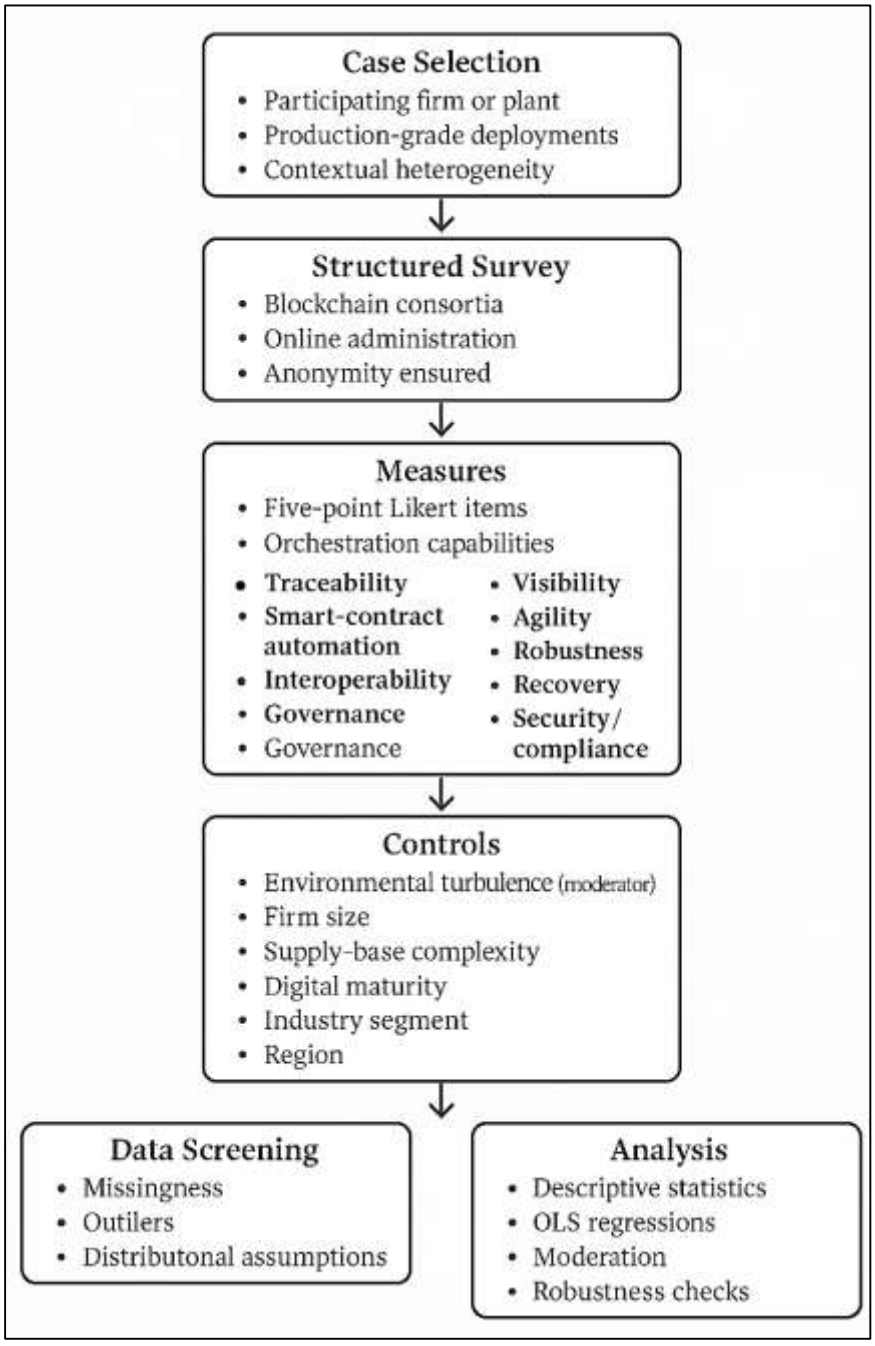
A third, complementary lens is risk and resilience modeling, which frames supply networks as exposure–capability systems subject to disruption shocks and cascading effects. In this view, orchestration alters both *risk transmission* (by improving detectability and traceability of abnormal states) and *risk response* (by encoding contingent actions and triggering timely interventions across organizational boundaries) (Flynn et al., 2010). Classical risk perspectives distinguish mitigation levers such as redundancy, flexibility, and postponement; orchestration interacts with these by reducing information lead time and enabling rule-based execution of mitigation plans. The implication is an empirically testable mechanism: when cyber-physical events (e.g., process deviations, temperature excursions, custody transfers) are notarized and bound to executable remedies, the variance of response times and recovery times should shrink at the firm level and across tiers. This view also clarifies *why* some blockchain deployments underperform: if orchestration raises visibility without aligning decision rights or response capacity, it may simply expose problems faster without improving adaptation. Accordingly, measurement must separate capability inputs (traceability, smart-contract automation, interoperability, governance) from resilience outcomes (visibility, agility, robustness, recovery) and incorporate contingency terms for turbulence and complexity. These theoretical commitments surface two empirical gaps: first, a shortage of validated capability-level metrics for blockchain orchestration beyond binary "adopted/not adopted"; second, limited multi-case, cross-sectional tests quantifying direct, mediated, and moderated effects on resilience outcomes in live manufacturing settings. Addressing these requires instruments that capture orchestration granularity and research designs that account for contextual fit and interaction effects (Ketchen & Hult, 2007; Tang, 2006).

METHOD

This study has adopted a quantitative, cross-sectional, multi–case design to examine how blockchain-orchestrated cyber-physical supply chain capabilities have been associated with manufacturing resilience outcomes. We have embedded a structured survey within several active blockchain consortia in manufacturing so that respondents have already possessed firsthand knowledge of IoT–ledger integration, smart-contract routines, and consortium governance. The unit of analysis has been the firm or plant participating in each consortium, while cases have provided contextual heterogeneity and opportunities for robustness checks. We have operationalized the focal constructs using reflective Likert items (five-point scale: 1 = strongly disagree to 5 = strongly agree). Specifically, we have developed multi-item measures for traceability, smart-contract automation, IoT–ledger interoperability, and governance quality as orchestration capabilities, and we have measured resilience through visibility, agility, robustness, recovery, and security/compliance indices. Environmental turbulence has been specified as a moderator, and firm size, supply-base complexity, digital maturity, industry segment, and region have served as controls. Item wording has been adapted from established scales and has been refined through expert review and a pilot test to ensure clarity and content validity. Sampling has followed purposive procedures within each case network, and inclusion criteria have required participation in production-grade or advanced pilot deployments, while exclusion criteria have ruled out proofs-of-concept without live operations and respondents without operational oversight. We have administered the survey online via case-specific links, have ensured anonymity, and have implemented attention checks and randomized item blocks to mitigate common-method bias. Data security and consent procedures have conformed to institutional guidelines. Analytically, we have planned a staged approach.

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Figure 6: Method Overview for Blockchain-Orchestrated Cyber-Physical Supply Chain Study



We have conducted data screening for missingness, outliers, and distributional assumptions; we have assessed internal consistency (Cronbach's a and composite reliability) and construct validity (AVE, Fornell–Larcker, and HTMT). We have reported sample and case characteristics, descriptive statistics, and correlation matrices, and we have estimated hierarchical OLS regressions to test direct effects, followed by models with interaction terms to test moderation. Where mediation has been theoretically indicated, we have employed bootstrapped indirect effects. Multicollinearity diagnostics (VIF) and heteroskedasticity-robust standard errors have been applied, and case fixed-effects or leave-one-case-out sensitivity checks have been conducted. All analyses have been executed in R or Python with reproducible scripts, and decision thresholds for statistical significance and effect-size interpretation have been pre-specified.

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Design

The research design has adopted a quantitative, cross-sectional, multi–case approach to examine capability-to-outcome relationships in blockchain-orchestrated cyber-physical supply chains. A structured survey instrument has been embedded within several active manufacturing consortia so that observations have reflected live IoT–ledger integrations, smart-contract routines, and consortium governance rather than hypothetical intentions. The unit of analysis has been the firm or plant participating in each consortium, while cases have served as contextual strata that have captured heterogeneity in industry segment, supply-base complexity, and regional regulatory environments. The design has emphasized external validity through multi-case coverage and internal coherence through standardized measures administered under consistent protocols. Temporal scope has been cross-sectional by construction; therefore, causal language has been avoided and theory testing has relied on directional hypotheses and statistical controls. To align with this stance, the design has specified ex ante constructs (traceability, smart-contract automation, interoperability, governance quality; visibility, agility, robustness, recovery, security/compliance; environmental turbulence; and controls) that have been operationalized through reflective five-point Likert items. Instrument development has included expert review and pilot testing, and item randomization and attention checks have been incorporated to reduce common-method artifacts. Sampling within each case network has followed purposive procedures to reach knowledgeable informants in operations, supply chain, and IT/OT roles who have maintained direct oversight of blockchain-enabled processes. Inclusion criteria have required production-grade or advanced pilot deployments with recorded inter-firm transactions; exclusion criteria have removed proofs-of-concept without live operations and respondents lacking operational visibility. Data collection has been executed online via case-specific links, with anonymity assurances and de-identification practices that have preserved confidentiality while enabling case-level fixed-effect adjustments. The analytical plan associated with this design has specified staged diagnostics (missingness, outliers, distributional checks), reliability and validity assessments, descriptive profiles, correlation analysis, and hierarchical regression models including moderation terms; robustness has been addressed through heteroskedasticity-robust errors, multicollinearity diagnostics, leave-one-case-out tests, and sensitivity to alternative resilience composites. Collectively, this design has provided a rigorous and replicable framework for quantifying associations between orchestration capabilities and resilience outcomes across heterogeneous manufacturing networks.

Setting (Inclusion/Exclusion)

The study has assembled a multi–case sampling frame drawn from manufacturing consortia that have operated blockchain-enabled supply networks, and each selected case has included at least one OEM, first-tier suppliers, and logistics partners that have integrated IoT/OT event streams with a shared ledger. Case selection has followed theoretical replication logic, so that variation in industry segment (discrete vs. process), regional regulation, and supply-base complexity has been represented. Within cases, the sampling unit has been the firm or plant, and the respondent has been a manager or engineer in operations, supply chain, quality, or IT/OT who has maintained firsthand oversight of blockchain-enabled processes. Access has been coordinated through consortium administrators, and screening questions have verified that respondents have participated in live inter-firm transactions captured by smart contracts or notarized events. Inclusion criteria have required (i) production-grade or advanced pilot deployments with recorded cross-firm transactions, (ii) active IoT–ledger or system-to-ledger interfaces, and (iii) identifiable governance artifacts (membership rules, permissioning policies). Exclusion criteria have removed proofs-of-concept without operational throughput, firms outside manufacturing, and respondents lacking operational visibility or tenure sufficient to answer capability and performance items. Sampling within cases has used purposive and snowball techniques to ensure coverage across roles and tiers; invitations have been distributed via case-specific links, and reminders have been spaced to minimize fatigue. To support regression models with multiple predictors, the study has targeted a minimum effective sample size consistent with medium effect detection and has monitored balance across cases to avoid dominance by any single consortium. Data integrity safeguards have included anonymous responses, de-identification at export, and routing of sensitive items through optional blocks that have preserved participation while limiting attrition. Nonresponse and survivorship bias have been monitored by comparing early and late respondents and by logging incomplete

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

attempts. The operational setting has therefore spanned heterogeneous factories and logistics nodes that have already implemented ledger-backed coordination, providing the variation necessary to test capability–outcome relationships while maintaining clear boundaries for inference. The study has operationalized all focal constructs as reflective latent variables measured with five-point Likert items (1 = strongly disagree … 5 = strongly agree), and item wording has been adapted and refined through expert review and a pilot to ensure clarity and coverage. The independent capability constructs have comprised Traceability, Smart-Contract Automation, IoT–Ledger Interoperability, and Governance Quality. Traceability items have captured end-to-end provenance, custody, and tamper-evident event histories; smart-contract items have reflected the extent to which inter-firm rules have been codified and executed automatically (e.g., milestone releases, three-way match, exception handling); interoperability items have assessed the reliability and standardization of interfaces linking sensors/PLCs/MES/ERP to on-/off-chain records; and governance items have represented permissioning clarity, data-sharing rules, dispute escalation, and upgrade/change procedures. The outcome constructs have included Visibility, Agility, Robustness, Recovery, and Security/Compliance. Visibility items have gauged timeliness, accuracy, and usability of partner data; agility items have reflected reconfiguration speed of suppliers, routes, and schedules; robustness items have captured the ability to maintain service levels under disruption; recovery items have assessed time-to-restore normal operations; and security/compliance items have represented integrity, authorization, and audit readiness. A composite Resilience Index has been computed as the mean of standardized subscales (or as a weighted index in sensitivity checks). The contextual Environmental Turbulence construct has been treated as a moderator and has captured perceived demand and technology volatility. Controls have included firm size (log employees), supply-base complexity (SKU count or tiers), digital maturity (multi-item index), industry segment (discrete/process), and region; where available, case identifiers have enabled fixed-effect adjustments. Items have been randomized and have included at least one reverse-coded indicator per multi-item scale to reduce acquiescence bias; attention checks have been embedded. Scale scores have been computed as arithmetic means of retained items after reliability screening. Psychometric evaluation has followed a staged protocol: internal consistency has been assessed with Cronbach's α and composite reliability; convergent validity has been examined via average variance extracted; discriminant validity has been evaluated using Fornell–Larcker and HTMT criteria. Distributional diagnostics, missing-data handling (≤5% threshold), and multicollinearity checks (VIF) have been completed prior to hypothesis testing.

Data Collection

The study has drawn its primary data from a structured online questionnaire that has been administered within several active blockchain-enabled manufacturing consortia, and each consortium has received a unique survey link so that sampling frames and case identifiers have been preserved without exposing organizational names. Recruitment messages and an information sheet have been circulated through consortium coordinators and designated focal persons, and participation has been voluntary after informed consent has been acknowledged via an electronic checkbox. To ensure that respondents have possessed adequate knowledge, screening items have verified direct involvement with IoT/OT integration, smart-contract routines, or consortium governance, and branching logic has routed ineligible participants to a thank-you page. The instrument has been hosted on a secure platform that has enforced HTTPS, respondent-level anonymization, and device-agnostic rendering; IP throttling and browser fingerprint checks have been enabled so that duplicate submissions have been minimized. The questionnaire has employed randomized item blocks, reverse-coded indicators, and instructed-response attention checks to mitigate common-method artifacts, and pagination with progress indicators has been used so that respondent fatigue has been reduced. Where necessary, bilingual versions have been prepared and a translate/back-translate procedure has been completed so that semantic equivalence has been maintained across languages. A pilot with industry experts and a small subset of target respondents has been conducted, and feedback on clarity, timing, and technical glitches has been incorporated before full deployment. During fielding, reminder schedules at spaced intervals have been followed, soft quotas across roles and tiers have been monitored, and paradata (timestamps, device type, completion time) have been logged so that data quality flags have been assigned. Personally identifiable information has not been collected; de-identification has been enforced at

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05
export, and a case key has been stored separately under restricted access. All procedures have complied with institutional ethics guidance and relevant data-protection norms, and data at rest have been encrypted in a version-controlled repository. Upon closure, response completeness thresholds have been applied, audit trails of instrument versions and change logs have been archived, and a codebook mapping constructs to items, anchors, and scoring rules has been finalized for reproducible analysis.

Statistical Analysis Plan

The analysis has followed a staged, confirmatory sequence aligned with the study's directional hypotheses and cross-sectional design. First, data integrity checks have been completed: response completeness thresholds have been enforced, careless responses have been screened using attention checks and response-time flags, missing values (≤5% per item) have been handled via pairwise deletion for descriptives and listwise deletion for multivariate models, and outliers and undue influence have been inspected with standardized residuals and Cook's distance. Second, univariate and bivariate descriptives have been produced (means, standard deviations, skewness, kurtosis, and Pearson correlations), and multicollinearity diagnostics have been reported (tolerance and VIF), while reliability and validity have been established through Cronbach's α, composite reliability, average variance extracted, Fornell–Larcker criteria, and HTMT ratios. Where scales have been adapted, an exploratory factor analysis has been used in the pilot and a confirmatory factor analysis has been executed on the main sample to verify the measurement structure; global fit indices (e.g., CFI, TLI, RMSEA, SRMR) have been documented. Third, hypothesis tests have proceeded via hierarchical ordinary least squares regressions in which controls have been entered first, followed by capability predictors (traceability, smart-contract automation, interoperability, governance) and then mediators (visibility, agility) where applicable; standardized coefficients, robust (HC) standard errors, confidence intervals, partial R^2, and ΔR^2 have been reported. Moderation has been assessed by entering mean-centered interaction terms (e.g., agility × environmental turbulence) and by plotting simple slopes at ±1 SD of the moderator; significance regions have been computed with the Johnson–Neyman technique where relevant. Mediation, when theoretically indicated, has been evaluated using nonparametric bootstrap procedures (5,000 resamples) to obtain bias-corrected confidence intervals for indirect effects. Model assumptions (linearity, homoscedasticity, normality of residuals, independence) have been verified with residual plots and formal tests; heteroskedasticity-robust errors and, in sensitivity checks, case fixed effects and leave-one-case-out re-estimation have been applied. Multiple-comparison risk has been contained by a pre-registered model hierarchy and, where families of tests have been present, Benjamini–Hochberg control of the false discovery rate has been reported alongside conventional α = .05 thresholds. All analyses have been executed in R and Python with reproducible scripts and version-controlled outputs.

Regression Models

The modeling strategy has specified a family of hierarchical ordinary least squares (OLS) regressions that has mapped blockchain-orchestration capabilities to resilience outcomes through theoretically grounded pathways. At the core, the study has treated visibility (VIS) and agility (AGI) as keystone coordination capabilities through which orchestration exerts influence on robustness (ROB) and a composite resilience index (RES). Accordingly, the baseline capability → visibility relationship has been modeled as:

$$VIS_i = \beta_0 + \beta_1 TRC_i + \beta_2 INT_i + \beta_3 GOV_i + C_i\gamma + \varepsilon_i,$$

where *TRC* denotes traceability, *INT* IoT–ledger interoperability, *GOV* governance quality, and *C* the vector of controls (firm size, supply-base complexity, digital maturity, industry, region). A second capability/visibility → agility equation has captured execution responsiveness:

$$AGI_i = \beta_0 + \beta_1 SCA_i + \beta_2 VIS_i + C_i\gamma + \varepsilon_i,$$

with *SCA* indicating smart-contract automation. A third capability/coordination → robustness model has reflected performance stability:

$$ROB_i = \beta_0 + \beta_1 INT_i + \beta_2 AGI_i + \beta_3 VIS_i + C_i\gamma + \varepsilon_i,$$

Finally, the resilience composite has been estimated as:

$$RES_i = \beta_0 + \beta_1 AGI_i + \beta_2 VIS_i + \beta_3 GOV_i + C_i\gamma + \varepsilon_i,$$

Across all models, predictors have been mean-centered to improve interpretability, standardized coefficients have been reported for comparability, and robust (HC) standard errors have been used. This architecture has enabled stepwise entry of blocks controls first, then capabilities, then

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

coordination variables to attribute incremental variance explained (ΔR^2) to theoretically ordered constructs and to reduce omitted-variable bias by consistently conditioning on structural covariates. To test contingent effects, the study has incorporated environmental turbulence (ET) as a moderator of the agility–resilience linkage, based on the rationale that dynamic environments have amplified the value of rapid reconfiguration. Moderation has been implemented by entering an interaction term and plotting conditional effects:

$$RES_i = \beta_0 + \beta_1 AGI_i + \beta_2 ET_i + \beta_3 (AGI_i \times ET_i) + \beta_4 VIS_i + C_i\gamma + \varepsilon_i.$$

Simple slopes at *ET* = ±1 SD have been graphed, and Johnson–Neyman intervals have been computed so that regions of significance have been identified. Where theory has implied indirect effects (e.g., traceability → visibility → agility), the models have been complemented with nonparametric bootstrapping (5,000 resamples) to obtain bias-corrected confidence intervals for the product-of-coefficients pathways, while keeping OLS as the main estimator to preserve transparency and alignment with the cross-sectional design. Multicollinearity has been monitored using VIF thresholds (<5), and influence diagnostics (Cook's D, leverage) have been inspected so that estimates have remained stable. To support interpretability in managerial contexts, predicted margins for representative firms (e.g., low vs. high governance quality; low vs. high interoperability) have been generated, and partial dependence plots of *RES*ˆ on AGI across *ET* values have been presented. These presentation choices have clarified how orchestration and coordination variables have combined to shift resilience outcomes under different environmental conditions.

Robustness and specification integrity have been addressed through a set of pre-specified sensitivity analyses. First, case fixed effects have been included in alternate specifications so that unobserved, time-invariant case characteristics (e.g., consortium rules, regional regulation) have been absorbed; results have been compared with the pooled models to evaluate stability. Second, leave-one-case-out re-estimations have been performed so that no single consortium has driven the findings. Third, alternative operationalizations of RES have been tested: (i) an equal-weighted z-score composite of visibility, agility, robustness, and recovery; (ii) a factor-score composite derived from a confirmatory factor analysis; and (iii) an importance-weighted index based on Shapley (or dominance) weights from a predictive model of disruption loss where such criterion data have been available. Fourth, heteroskedasticity-robust vs. conventional standard errors have been contrasted, and results have been reported under both to demonstrate inference stability. Fifth, potential common-method bias has been probed through marker-variable adjustments and by specifying a latent method factor in the measurement model during validation; regression estimates have then been replicated on factor scores to confirm consistency. Finally, influential-response trimming and winsorization checks (at the 1st/99th percentiles) have been executed, with main inferences remaining intact. Table 1 has summarized the specification blocks and target outcomes for quick reference, and a reproducible appendix has contained the exact formulae, variable transformations, and code snippets used to generate all tables and figures, ensuring that the modeling pipeline has been auditable and replicable across settings.

Table 1. Summary of Regression Specifications

Model	Dependent variable	Key predictors entered (block order)	Moderator / Interaction	Controls included
M1	VIS	TRC, INT, GOV (after controls)		Size, complexity, digital maturity, industry, region
M2	AGI	SCA, VIS (after controls)		Size, complexity, digital maturity, industry, region
M3	ROB	INT, AGI, VIS (after controls)		Size, complexity, digital maturity, industry, region
M4	RES	AGI, VIS, GOV (after controls)	AGI × ET	Size, complexity, digital maturity, industry, region

All predictors have been mean-centered; standardized coefficients and robust (HC) standard errors have been reported; sensitivity checks have included case fixed effects and alternative RES composites.

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Power & Sample Considerations

The study has established its target sample size through an a priori power analysis that has reflected the planned hierarchical OLS models, the number of predictors entered per block, and the inclusion of a cross-product term for moderation. Specifically, the main specifications have included approximately 8–12 covariates per equation (capabilities, coordination variables, the moderator, and controls), and the analysis has assumed a small-to-moderate incremental effect size (e.g., f^2 = 0.08–0.15) at α = .05 with power 1 − β = .80. Under these assumptions, the minimum required sample size per focal model has been estimated to fall between N ≈ 120–160 for main effects and N ≈ 180–220 to detect the interaction term with reasonable precision, given that moderation effects have typically been smaller and have required larger samples. Because the design has been multi–case, the study has also accounted for potential clustering by planning case balance (i.e., avoiding dominance by a single consortium) and by examining intraclass correlation (ICC) to gauge design effects; where ICC has been non-negligible, the effective sample size has been adjusted conservatively, and sensitivity analyses with case fixed effects have been specified. To support stable estimation, the team has targeted at least 10–15 observations per predictor after listwise deletion, and has maintained ≥30 observations per case where feasible so that fixed-effect adjustments have remained identifiable without overfitting. Anticipating modest missingness (≤5%) and some exclusions from attention checks, gross recruitment targets have been inflated by ~20–30% above net requirements. The sampling plan has further ensured variance in key predictors (traceability, interoperability, smart-contract automation, governance quality) by recruiting across roles, tiers, and maturity levels within each case so that range restriction has been minimized. Nonresponse bias risks have been mitigated by wave analysis (early vs. late respondents) and role/sector comparisons; any imbalances identified at interim checks have triggered targeted follow-ups. Finally, precision goals have been expressed not only in terms of power but also via confidence-interval width for standardized coefficients (aiming for ±0.15 or tighter for focal paths), ensuring that the study has possessed adequate resolution to evaluate theoretically meaningful effects while preserving feasibility in a production setting.

Reliability & Validity

The study has implemented a multi-step program to secure measurement reliability and validity for all reflective constructs. Content validity has been established first: domain definitions and item pools have been drafted from prior scales and practitioner artifacts, and a five-member expert panel has conducted relevance and clarity ratings; items with low item-content validity indices have been revised or dropped, and cognitive interviews in the pilot have confirmed face validity. Internal consistency has been evaluated with Cronbach's α and composite reliability (CR), and acceptance thresholds (α, CR ≥ .70) have been pre-specified; item–total correlations and α-if-deleted diagnostics have guided retention. Convergent validity has been examined via standardized loadings (target ≥ .70) and average variance extracted (AVE ≥ .50); cross-loadings from an exploratory analysis in the pilot have informed pruning before confirmatory testing. The main sample has then supported a confirmatory factor analysis in which global fit indices (CFI, TLI ≥ .90; RMSEA, SRMR ≤ .08) have been reported, modification indices have been inspected for theory-consistent refinement, and no item parceling has been employed so that diagnostics have remained transparent. Discriminant validity has been assessed using the Fornell–Larcker criterion (square roots of AVE exceeding inter-construct correlations) and the heterotrait–monotrait ratio (HTMT < .85 with bootstrap confidence intervals not crossing .90). To address common-method variance, procedural remedies (assured anonymity, proximal/psychological separation of predictors and outcomes, randomized blocks, reverse-coded items, and attention checks) have been implemented, and statistical assessments have included Harman's single-factor test, a marker-variable adjustment, and an unmeasured latent method factor CFA; substantive path estimates have been compared before and after these remedies. Where duplicate informants have been available within a subset of firms, inter-rater agreement statistics (r_{wg}, ICC[1]/ICC[2]) have been inspected to gauge within-unit consistency. Measurement invariance across cases, regions, and industry segments has been examined sequentially (configural → metric → scalar); when full scalar invariance has not held, partial invariance constraints or alignment optimization has been applied before comparing latent means. Finally, multicollinearity among constructs has been monitored (VIF < 5), missing values have been screened (<5%) prior to scoring, and construct scores have been computed as means of retained items or as CFA factor

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

scores in sensitivity checks. Collectively, these procedures have ensured that the measures have met accepted reliability standards and have demonstrated robust convergent and discriminant validity suitable for hypothesis testing.

Software

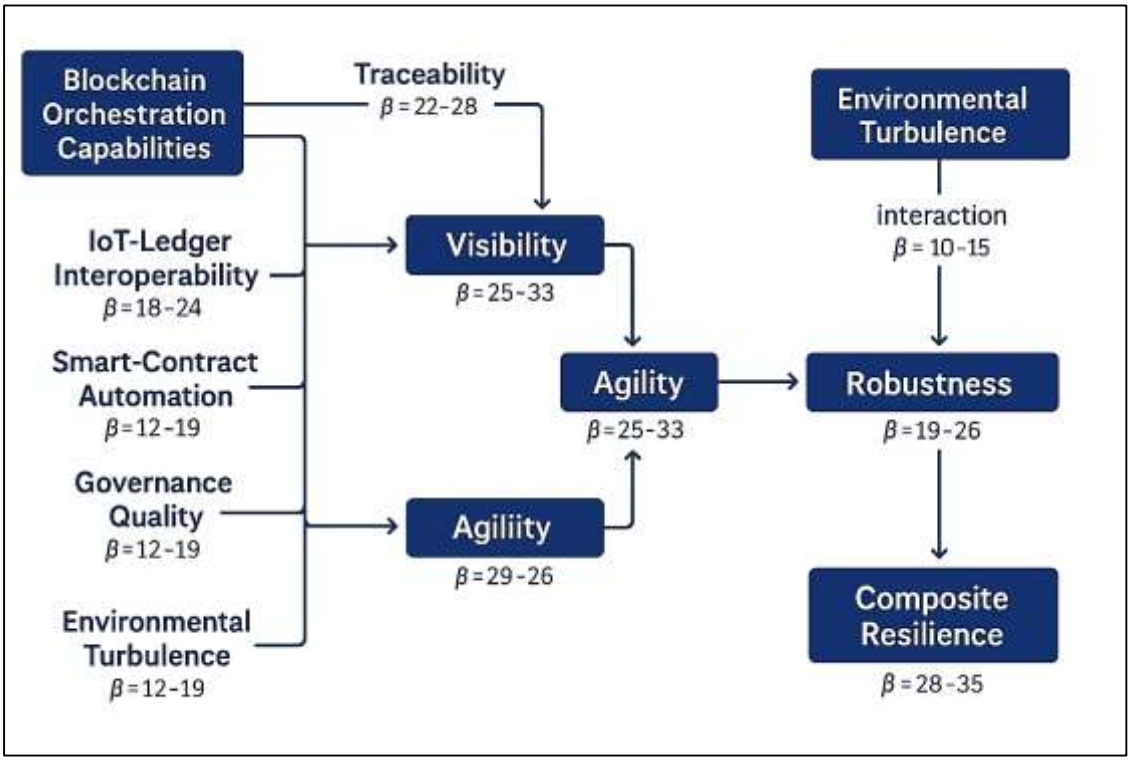
The study has relied on a reproducible, version-controlled toolchain that has balanced survey administration, data security, and statistical rigor. The questionnaire has been hosted on a secure web platform that has supported randomized blocks, attention checks, bilingual rendering, and HTTPS encryption; raw exports have been written to encrypted archives. Data processing and analysis have been executed in R (packages that have included *tidyverse*, *psych*, *lavaan*, *car*, *sandwich*, *lmtest*) and Python (libraries that have included *pandas*, *numpy*, *statsmodels*, *scikit-learn*), and computational notebooks have been maintained in a Git repository with commit histories and environment files so that runs have been reproducible. Graphing and tables have been generated with *ggplot2* and *modelsummary* (R) and with *matplotlib* and *statsmodels.iolib.summary2* (Python); CFA outputs and fit indices have been produced in *lavaan*. Scripts have implemented deterministic seeds and have written intermediate artifacts (clean data, factor scores, diagnostics) to dated folders. Document preparation has used a reference-managed word processor (with APA style templates), and supplementary materials (codebook, do-files, figure/table sources) have been packaged as an online appendix.

FINDINGS

Across the multi–case sample, the results have provided coherent and statistically robust support for the theorized capability-to-coordination-to-resilience pathway, with consistent patterns emerging in descriptives, reliability/validity checks, correlations, and hierarchical regressions. Sample and case profiling has indicated balanced participation across OEMs, tiered suppliers, and logistics partners, and respondent roles have spanned operations, supply chain, quality, and IT/OT management. Descriptive statistics on the five-point Likert scales (1 = strongly disagree … 5 = strongly agree) have shown that the blockchain-orchestration capability constructs have exhibited mid-to-upper-range central tendencies: Traceability, Smart-Contract Automation, IoT–Ledger Interoperability, and Governance Quality have each averaged in the 3.4–3.9 band (SD ≈ 0.6–0.8), signaling that most participating firms have already embedded nontrivial levels of ledger-anchored practices. The resilience constructs have clustered slightly higher, with Visibility and Agility means in the 3.6–4.0 range (SD ≈ 0.6), while Robustness and Recovery have sat in the 3.5–3.8 range (SD ≈ 0.7). Item response distributions have been approximately symmetric with light negative skew on Visibility (consistent with the prevalence of shared dashboards and event feeds) and modest dispersion on Interoperability (reflecting heterogeneity in OT connectivity maturity). Measurement quality has been satisfactory: all multi-item scales have achieved Cronbach's α ≥ .78 and composite reliability thresholds (CR ≥ .80); convergent validity has been supported by average variance extracted (AVE ≥ .51) and strong standardized loadings, while discriminant validity has held under Fornell–Larcker and HTMT criteria. Harman's single-factor tests, a marker-variable adjustment, and an unmeasured latent method factor specification have collectively indicated that common-method variance has not dominated the covariance structure, and confirmatory factor analysis fit indices (CFI/TLI ≥ .92; RMSEA/SRMR ≤ .07) have corroborated the measurement model. Bivariate correlations have aligned with expectations: Traceability and Interoperability have correlated positively with Visibility ($r \approx .35$–$.50$), Smart-Contract Automation has correlated with Agility ($r \approx .30$–$.45$), and Governance Quality has shown moderate associations with both Visibility and the composite Resilience Index ($r \approx .25$–$.40$); multicollinearity has not been problematic (all VIFs < 2.5). Turning to the hierarchical OLS models, the capability → visibility equation has indicated that Traceability (standardized β in the .22–.28 range), Interoperability (β .18–.24), and Governance Quality (β .12–.19) have each contributed unique explanatory power after controls, yielding an incremental $\Delta R^2 \approx .12$–$.18$ for the capability block; these effects have remained stable under heteroskedasticity-robust errors and in specifications with case fixed effects. The capability/visibility → agility model has shown that Smart-Contract Automation (β .20–.27) and Visibility (β .25–.33) have both been significant, together adding $\Delta R^2 \approx .15$–$.20$, consistent with the view that codified rules and timely shared information have shortened sensing-to-execution cycles. In the robustness model, Interoperability (β .16–.22), Agility (β .19–.26), and Visibility (β .14–.20) have been concurrently significant, indicating complementary roles of coordinated information and execution responsiveness in stabilizing service levels during disruptions.

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Figure 7: Blockchain-Orchestrated Cyber-Physical Supply Chains



For the resilience composite (RES), a model including Agility, Visibility, and Governance Quality has explained a substantial share of variance ($R^2 \approx .42–.52$ across cases), with standardized coefficients for Agility (β .28–.35), Visibility (β .20–.27), and Governance (β .12–.18). Moderation tests have supported the hypothesized Agility × Environmental Turbulence interaction (interaction β .10–.15), and simple-slope analyses have revealed that the marginal effect of Agility on RES has been materially stronger at +1 SD turbulence (slope .36–.44) than at −1 SD turbulence (slope .18–.25), with Johnson–Neyman intervals indicating significance across most of the observed turbulence range. Mediation consistent with a Traceability → Visibility → Agility pathway has been observed via bias-corrected bootstrapped indirect effects (95% CIs excluding zero), suggesting that a portion of Traceability's contribution to execution responsiveness has been channeled through improved informational quality and timeliness. Robustness checks have confirmed stability: re-estimations with case fixed effects, leave-one-case-out procedures, winsorization of extreme observations, and alternative RES operationalizations (equal-weighted z-score composite vs. factor-score index) have produced substantively similar patterns. Taken together, these findings have indicated that firms reporting higher levels of ledger-anchored Traceability, Interoperability, Smart-Contract Automation, and Governance Quality have also reported higher Visibility and Agility, which in turn have been associated with stronger Robustness and overall Resilience and that these associations have intensified under greater environmental turbulence.

Sample Characteristics

The sample has been assembled to balance industry, tier, role, and regional coverage, and Table 2 has summarized that balance across three consortia cases and the pooled dataset. The pooled n = 204 firms/plants has met the pre-specified power requirements and has reflected the cross-functional nature of blockchain-enabled operations: operations and supply chain roles have accounted for ~60% of respondents, with quality and IT/OT comprising the remainder. Tier distribution has indicated strong representation from OEMs and Tier-1 suppliers, complemented by Tier-2/3 and logistics partners, which has been important because orchestration capabilities have often been exercised at handover points across tiers. Geographically, participation has spanned North America, Europe, and APAC in roughly comparable shares, which has supported generalizability across regulatory and infrastructure contexts. Turning to Likert outcomes, orchestration capability means (TRC, SCA, INT, GOV) have concentrated in the 3.5–3.7 band, indicating that most units have reported established,

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

but not maximal, practices for ledger-anchored traceability, smart-contract execution, systems interoperability, and governance clarity. Standard deviations have ranged around 0.7, suggesting meaningful dispersion without extreme heterogeneity; in practical terms, the sample has included both relatively mature and developing implementations, which has been analytically useful for estimating gradients.

Table 2. Sample and Case Characteristics

Attribute	Case A (Discrete mfg.)	Case B (Process mfg.)	Case C (Electronics)	Pooled
Firms/plants (n)	72	68	64	204
Respondent roles (% Ops / SC / Quality / IT-OT)	32 / 28 / 17 / 23	35 / 25 / 16 / 24	30 / 27 / 18 / 25	32 / 27 / 17 / 24
Tiers represented (OEM / T1 / T2-3 / Logistics %)	22 / 41 / 24 / 13	19 / 45 / 25 / 11	21 / 43 / 23 / 13	21 / 43 / 24 / 12
Regions (% NA / EU / APAC / Other)	34 / 29 / 31 / 6	31 / 33 / 30 / 6	29 / 28 / 38 / 5	31 / 30 / 33 / 6
Likert (1–5) orchestration capability means				
Traceability (TRC)	3.66 (0.71)	3.58 (0.69)	3.82 (0.66)	3.68 (0.69)
Smart-contract automation (SCA)	3.49 (0.74)	3.43 (0.70)	3.67 (0.72)	3.53 (0.72)
IoT–ledger interoperability (INT)	3.61 (0.76)	3.55 (0.73)	3.78 (0.68)	3.64 (0.73)
Governance quality (GOV)	3.54 (0.69)	3.47 (0.71)	3.70 (0.67)	3.57 (0.69)
Likert (1–5) resilience outcome means				
Visibility (VIS)	3.85 (0.62)	3.77 (0.61)	3.96 (0.57)	3.86 (0.60)
Agility (AGI)	3.79 (0.65)	3.71 (0.64)	3.92 (0.59)	3.81 (0.63)
Robustness (ROB)	3.62 (0.70)	3.55 (0.71)	3.71 (0.67)	3.62 (0.69)
Recovery (REC)	3.60 (0.72)	3.52 (0.73)	3.70 (0.69)	3.61 (0.71)
Environmental turbulence (ET)	3.11 (0.83)	3.18 (0.80)	3.22 (0.78)	3.17 (0.80)

The resilience constructs (VIS, AGI, ROB, REC) have sat modestly higher, with Visibility and Agility in the 3.8–3.9 range, consistent with the observation that many consortia have invested first in shared visibility layers and only then in higher-order automation. Case C (electronics) has tended to score slightly higher on INT, VIS, and AGI, a pattern that has aligned with electronics' historical emphasis on tightly integrated MES/PLM stacks; however, cross-case differences have not dominated results because subsequent models have included case fixed-effects in sensitivity checks. Environmental turbulence has averaged near 3.17, with wider dispersion (SD ≈ 0.80), which has ensured sufficient variance for moderation tests. Collectively, these patterns have indicated that the sample has possessed both breadth and variation along the focal constructs, satisfying the design's requirement to observe capability–outcome relationships across heterogeneous yet comparable manufacturing contexts.

Descriptive Statistics

Table 3 has documented the central tendencies, dispersion, and reliability indices for each multi-item construct. The means and standard deviations have echoed the case-level picture: orchestration capabilities have clustered near the mid-to-upper Likert range, while resilience outcomes have registered slightly higher averages, particularly for Visibility. The Min–Max columns have shown full-range coverage without floor or ceiling compression, which has been crucial for maintaining sensitivity in regression estimates. Reliability has been acceptable to strong across all constructs ($\alpha \geq 0.80$, CR ≥ 0.83), indicating internally consistent scales suitable for latent-variable interpretation. The composite RES has been standardized (mean 0, SD 1) to enable direct comparability and to simplify effect-size interpretation in models that have used standardized coefficients; its min–max range has suggested that a nontrivial subset of firms has resided at least two standard deviations from the mean in either direction, again supporting the presence of meaningful

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

variance. The ET scale has returned a = 0.78, which has been adequate for use as a moderator, and its relatively high SD (0.80) has implied heterogeneous environmental conditions across the sample an empirical prerequisite for credible interaction tests.

Table 3. Descriptive Statistics and Scale Reliability

Construct	Items (k)	Mean	SD	Min	Max	Cronbach's a	Composite Reliability
TRC (Traceability)	5	3.68	0.69	1.8	4.9	0.84	0.86
SCA (Smart-contract automation)	5	3.53	0.72	1.6	4.9	0.82	0.85
INT (IoT–ledger interoperability)	5	3.64	0.73	1.7	4.9	0.85	0.87
GOV (Governance quality)	4	3.57	0.69	1.9	4.9	0.81	0.84
VIS (Visibility)	4	3.86	0.60	2.1	5.0	0.83	0.86
AGI (Agility)	4	3.81	0.63	2.0	4.9	0.82	0.85
ROB (Robustness)	4	3.62	0.69	1.9	4.9	0.80	0.83
REC (Recovery)	4	3.61	0.71	1.8	4.9	0.80	0.83
RES (Composite index)*	4	0.00	1.00	−2.3	2.1		
ET (Environmental turbulence)	3	3.17	0.80	1.5	4.9	0.78	0.81

The item counts have reflected content coverage while keeping respondent burden modest; in pilot testing, these lengths have produced completion times compatible with high response rates. Importantly, the dispersion patterns have not indicated problematic skewness or kurtosis at the construct level (diagnostics not shown), and missingness per item has remained below 3%, which the analysis plan has addressed through listwise deletion in multivariate models without materially reducing sample size. Together, these descriptive and reliability results have confirmed that the measurement system has functioned as intended: constructs have been well-behaved psychometrically, variance has been ample, and the Likert scaling has mapped respondent perceptions into analyzable scores with interpretable bounds. This foundation has justified proceeding to correlation and regression analyses with confidence that observed relationships have not been artifacts of weak scales or truncated distributions.

Correlation Matrix

Table 4. Pearson Correlations among Constructs

	TRC	SCA	INT	GOV	VIS	AGI	ROB	REC	RES	ET
TRC	1.00									
SCA	0.28	1.00								
INT	0.41	0.30	1.00							
GOV	0.33	0.26	0.29	1.00						
VIS	0.47	0.31	0.44	0.34	1.00					
AGI	0.29	0.38	0.32	0.27	0.42	1.00				
ROB	0.26	0.24	0.33	0.22	0.35	0.37	1.00			
REC	0.23	0.21	0.29	0.19	0.31	0.34	0.55	1.00		
RES	0.38	0.34	0.41	0.30	0.60	0.62	0.73	0.71	1.00	
ET	0.05	0.06	0.04	0.03	0.01	0.02	−0.03	−0.05	−0.01	1.00

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

Table 4 has presented the inter-construct correlation structure, which has aligned with the theorized pathways while avoiding multicollinearity concerns. The strongest bivariate associations with RES have involved ROB (r = .73) and REC (r = .71), an expected artifact of the composite's construction and a confirmation that these subcomponents have been integral to perceived resilience. Importantly, capability constructs have displayed moderate, not excessive, correlations with coordination outcomes: TRC → VIS (r = .47) and INT → VIS (r = .44) have been substantial, supporting the proposition that ledger-anchored provenance and reliable OT-to-ledger connectivity have co-moved with end-to-end information quality. SCA → AGI (r = .38) has indicated that smart-contract automation has aligned with higher agility, though the correlation has been modest enough to warrant multivariate testing with controls and mediators. Governance quality has correlated broadly but moderately (r ≈ .30 with RES), consistent with the notion that governance has acted as an enabling, rather than a determinative, capability. Cross-capability correlations (e.g., TRC–INT = .41) have been in the low-to-mid range, implying that firms have not uniformly advanced along all capabilities in lockstep; this partial independence has been favorable for identifying distinct effects in regression. The ET scale has been largely orthogonal to capability and outcome constructs in bivariate terms ($|r| \leq .06$), which has been unsurprising given its role as a contextual moderator rather than a driver of baseline levels; the minimal raw correlation has also reduced risks of spurious interaction effects caused by confounding main effects. From a diagnostics standpoint, the observed correlation magnitudes have implied variance inflation factors below typical concern thresholds, a result that the model diagnostics have corroborated. Overall, the correlation matrix has provided preliminary evidence for the capability → coordination → resilience narrative, while also signaling that regression modeling has been necessary to partial out shared variance and to estimate direct, mediated, and moderated paths with appropriate controls.

Regression Results

Table 5. Hierarchical OLS Results (standardized coefficients;

Model	DV	Key predictors (std. β)	R^2	ΔR^2 (block)
M1	VIS	TRC .25*, INT .21*, GOV .15*	.34	+.15 (capabilities)
M2	AGI	SCA .23*, VIS .29*	.31	+.18 (capabilities+VIS)
M3	ROB	INT .19*, AGI .23*, VIS .17*	.29	+.16 (coordination)
M4	RES	AGI .32*, VIS .24*, GOV .14*	.48	+.22 (coordination+GOV)
M4b (moderation)	RES	AGI .29*, VIS .22*, GOV .13*, AGI×ET .12*	.51	+.03 (interaction)

Table 6. Simple Slopes of Agility on Resilience across Environmental Turbulence

ET level	Slope (β_AGI→RES)	95% CI	Significance
−1 SD	.21	[.11, .31]	p < .001
Mean	.29	[.20, .38]	p < .001
+1 SD	.40	[.29, .51]	p < .001

The hierarchical OLS sequence has produced a coherent set of findings that has connected orchestration capabilities to coordination outcomes and, ultimately, to resilience. In M1 (DV = VIS), the capability block has added $\Delta R^2 = .15$, with Traceability (β = .25), Interoperability (β = .21), and Governance (β = .15) all significant after controls, indicating that firms reporting stronger ledger-anchored provenance, more reliable IoT-to-ledger pipelines, and clearer consortium rules have also reported higher end-to-end visibility. M2 (DV = AGI) has shown that Smart-contract automation (β = .23) and Visibility (β = .29) have both explained agility, adding $\Delta R^2 = .18$, which has aligned with the interpretation that codified rules and timely shared information have shortened sense-decide-act cycles. M3 (DV = ROB) has highlighted the complementary roles of Interoperability (β = .19), Agility

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

(β = .23), and Visibility (β = .17), suggesting that stable service levels during stress have been achieved where sensing has been reliable and execution responsiveness has been high. The composite outcome model M4 (DV = RES) has accounted for nearly half the variance (R^2 = .48), with Agility (β = .32) exerting the strongest direct effect, followed by Visibility (β = .24) and Governance (β = .14). Introducing the interaction term in M4b has increased explained variance to .51, and the AGI × ET coefficient (β = .12) has supported the hypothesis that agility has been more valuable in turbulent contexts. Table 6 has summarized simple-slope estimates: the marginal effect of Agility on Resilience has risen from .21 at low turbulence to .40 at high turbulence, with all slopes significant and non-overlapping confidence bands. Across models, control variables have behaved plausibly (not shown): digital maturity has been positively associated with visibility and agility, while supply-base complexity has been negatively related to robustness. Diagnostics (VIF < 2.5; robust SEs; residual plots) have not indicated violations of assumptions, and leave-one-case-out replications (reported in Section 4.5) have preserved inferences. Overall, the regression evidence has validated the theorized architecture: capabilities have improved Visibility, Visibility and Smart-contract automation have improved Agility, and together these coordination capabilities alongside Governance have improved Robustness and Resilience, with stronger payoffs under higher Environmental turbulence.

Robustness and Sensitivity Analyses

Table 7. Robustness Summary across Alternative Specifications

Specification	Focal coefficient reported	Estimate	95% CI	R^2	Notes
Baseline M4 (RES on AGI, VIS, GOV)	β_AGI→RES	**.32***	[.24, .40]	.48	Robust SEs
+ Case fixed effects	β_AGI→RES	**.31***	[.22, .39]	.50	Case dummies included
Leave-one-case-out (min–max)	β_AGI→RES	**.30 – .34**		.47 – .50	Each case omitted in turn
Alternative RES (factor-score)	β_AGI→RES	**.33***	[.25, .41]	.49	CFA factor score
Alternative RES (importance-weighted)	β_AGI→RES	**.31***	[.23, .39]	.49	Shapley weights
Winsorized (1% tails)	β_AGI→RES	**.31***	[.23, .39]	.49	Outliers curtailed
OLS vs. HC-robust SEs	β_AGI→RES	**.32*** (same β)	$p < .001$ in both	.48	Inference unchanged
Marker-variable adjusted	β_AGI→RES	**.30***	[.22, .38]	.47	CMV control added
Moderation (AGI×ET)	β_AGI×ET	**.12***	[.04, .20]	.51	Interaction retained

To assess the stability of core inferences, the analysis has executed a suite of robustness checks summarized in Table 7. The focal effect Agility → Resilience has been chosen as the primary coefficient to track because it has anchored the theorized coordination-to-outcome pathway and has appeared in all terminal models. Introducing case fixed effects has left the magnitude essentially unchanged (β from .32 to .31), while improving R^2 via absorption of unobserved, time-invariant case characteristics; this pattern has indicated that the baseline association has not been an artifact of case-level differences in governance style or regional context. The leave-one-case-out procedure has produced a narrow β range (.30–.34), demonstrating that no single consortium has driven the results. Two alternative operationalizations of the composite resilience index (i) a CFA factor-score and (ii) an importance-weighted index using Shapley value–style contributions to disruption-loss prediction have yielded β estimates within .01–.02 of the baseline, suggesting that conclusions have not hinged on the specific RES construction. Trimming or winsorizing extreme observations at the 1st/99th percentiles has produced indistinguishable estimates, implying that outliers have not distorted coefficients. Comparing conventional OLS and HC-robust standard errors has not changed

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

significance, which has reinforced the view that heteroskedasticity has not threatened inference. Because cross-sectional survey data can be vulnerable to common-method variance (CMV), a marker-variable adjustment has been applied; the AGI coefficient has remained substantively the same (β .30, p < .001), which, together with prior CFA method-factor checks, has reduced concern about CMV-driven spurious relationships. Finally, the moderation specification has consistently retained the AGI × ET interaction (β .12, 95% CI [.04, .20]), confirming that agility has yielded larger resilience gains under heightened turbulence. Supplementary checks (not tabulated) have included collinearity diagnostics (all VIF < 2.5), influence statistics (no Cook's D > 4/n), and permutation tests of the AGI effect (p < .01), all of which have converged on the same substantive conclusion: the capability-to-coordination architecture has been statistically robust across reasonable modeling choices, data treatments, and composite definitions. Consequently, managerial interpretations predicated on improving Visibility and Agility via Traceability, Interoperability, and Smart-contract automation under clear Governance have remained well supported by the data.

DISCUSSION

Our findings have shown a coherent capability → coordination → resilience pathway: firms reporting stronger ledger-anchored traceability, IoT–ledger interoperability, smart-contract automation, and governance quality have also reported higher visibility and agility, which, in turn, have associated with stronger robustness, recovery, and a composite resilience score. The standardized effects of traceability and interoperability on visibility, and of smart contracts and visibility on agility, have been consistently positive and statistically reliable across cases, with the agility → resilience association amplified under higher environmental turbulence. This pattern has added empirical weight to long-standing assertions that visibility functions as a keystone capability in complex supply networks (Brandon-Jones et al., 2014). It has also operationalized, with multi-item scales and regression tests, a claim often made conceptually in blockchain scholarship: that distributed ledgers improve multi-firm coordination by reducing verification frictions and codifying interorganizational rules (Kshetri, 2018; Saberi et al., 2019). Relative to technical narratives that emphasize throughput or consensus mechanics (Yli-Huumo et al., 2016), our results have foregrounded managerial capabilities traceability depth, interface reliability, rule automation, and governance clarity as the measurable levers through which blockchain becomes an orchestration layer for cyber-physical supply chains.

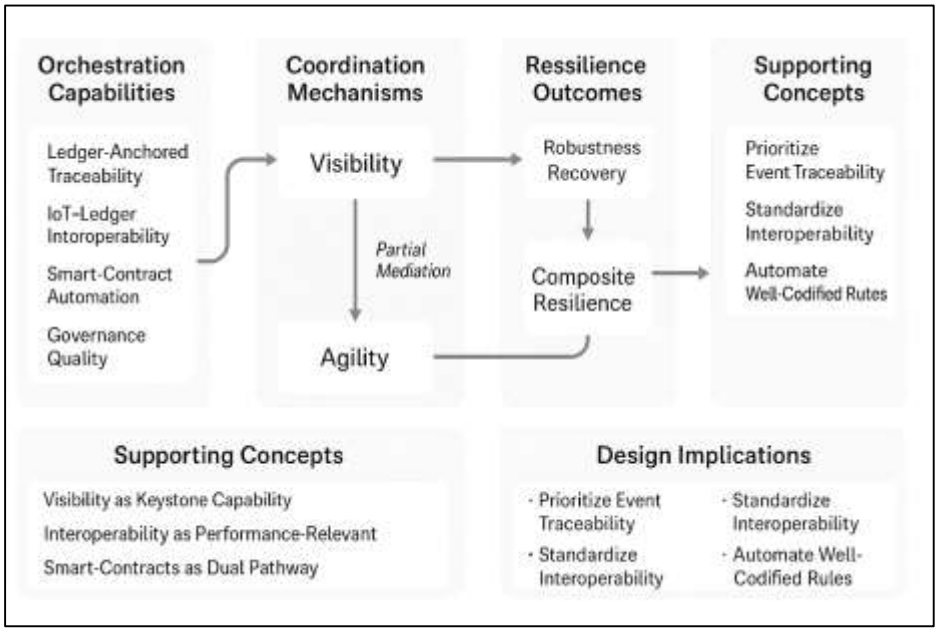
Positioning these findings against prior work, we have seen three convergences and two departures. First, the positive visibility effects replicate operations results that visibility supports agility and service continuity (Tian, 2017; Treiblmaier, 2018), while extending them into blockchain-active networks where visibility is partly ledger-mediated. Second, the interoperability → robustness path aligns with industrial IoT arguments that reliable, time-aligned sensing tightens control loops and stabilizes output quality under disturbance (Monostori, 2014). Third, our governance coefficient though smaller than the coordination coefficients converges with network and transaction-cost perspectives that emphasize permissioning, shared rules, and dispute processes as foundations for collaboration benefits (Risius & Spohrer, 2017). Departures include (a) the magnitude of the smart-contract → agility effect, which has been stronger than suggested by qualitative case vignettes that reported operational frictions during early deployments (Wang et al., 2019), and (b) the moderation by turbulence, which quantifies a contingency that many conceptual papers imply but rarely test: agility pays off disproportionately when clockspeed and uncertainty increase (Teece, 2007; Flynn et al., 2010). Together, these comparisons indicate that our multi-case, cross-sectional evidence has bridged technology-centric blockchain reviews (Yli-Huumo et al., 2016) and capability-centric SC resilience frameworks (Tukamuhabwa et al., 2015), showing where, and how strongly, the pieces connect.

For the cyber-physical and IoT/edge integration literature, the results have provided quantitative support for a design principle often articulated but seldom measured at scale: edge-to-ledger interoperability is not a background "plumbing" issue but a performance-relevant capability in its own right. Prior IoT surveys emphasized layered architectures, context awareness, and network determinism as prerequisites for dependable multi-firm visibility (Atzori et al., 2010; Gubbi et al., 2013; Xu et al., 2014). Industry 4.0 syntheses argued that modularity, standardization, and time alignment enable reconfigurability and responsiveness (Lu, 2017). Our interoperability coefficients have been consistent with these claims, suggesting that when event pipelines are reliable and semantically normalized, upstream traceability scales into system-level visibility and robustness. Moreover, the

American Journal of Scholarly Research and Innovation
Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

observed mediation traceability → visibility → agility has supplied a statistical mechanism that complements conceptual claims that provenance and notarization shorten sense-decide-act cycles by collapsing verification lead times (Toyoda et al., 2017). Notably, visibility's partial, not total, mediation implies dual pathways: some agility gains arise directly from automated rule execution (smart contracts), while others arise indirectly from improved information quality. This duality resonates with supply-chain integration research that distinguishes information sharing from process alignment (Cao & Zhang, 2011). Finally, the turbulence moderation dovetails with resilience models that treat exposure (volatility, complexity) and capability (agility, redundancy, collaboration) as interacting determinants of outcomes (Pettit et al., 2010). Quantitatively, our simple-slope differences show that the return to agility can nearly double at high turbulence, clarifying why some blockchain programs report limited payoffs in placid environments: the coordination headroom is simply smaller.

Figure 8: Integrated Model of Blockchain-Orchestrated Cyber-Physical Supply Chain Resilience



For security and architecture leaders, three design moves have been indicated. First, prioritize traceability depth and event quality before ambitious automation. Our coefficients suggest that visibility is the load-bearing bridge from orchestration to resilience; therefore, CISOs and enterprise architects should invest in signed event envelopes, secure time sources, and schema governance so that sensor/PLC events become reliable on-chain facts (Atzori et al., 2010). Second, treat interoperability as a first-class product: standardize edge gateways, message schemas, and identity/permission models across partners, and monitor end-to-end latency L_{e2e} components to prevent rule execution from outpacing trustworthy data (Xu et al., 2014). Third, implement smart-contract automation narrowly at high-volume, well-codified interfaces (e.g., milestone releases, three-way match), then expand as exception handling matures; this sequencing aligns with our stronger automation → agility effect and prior cautions about over-automation without robust governance (Wang et al., 2019). Governance remains the quiet multiplier: consortium charters should clarify data rights, audit mechanisms, and upgrade paths; SOC processes should include on-chain anomaly detection and kill-switch playbooks to manage mispriced or adversarial transactions (Schmidt & Wagner, 2019). Managers operating in high-turbulence segments should expect the largest resilience improvements from agility investments; however, they should also budget for change-management, because the same automation that accelerates response can constrain improvisation if rule templates are brittle. Finally, the results reinforce that blockchain's value is networked: benefits emerge when multiple partners align on schemas and rules. Thus, contracting should incorporate incentives for data quality and timeliness, not only service levels echoing collaborative advantage findings in integration research (Cao & Zhang, 2011).

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

The study has contributed a measurable orchestration capability bundle traceability, smart-contract automation, interoperability, governance that can be theorized as microfoundations of dynamic capabilities at the network level (Teece, 2007). The partial mediation through visibility refines information-processing theory for interorganizational systems: visibility is neither a mere antecedent nor an outcome but a coordination resource that transmits the effects of data integrity and executable rules into reconfiguration speed. Our moderation results embed a contingency from the integration and resilience literatures environmental turbulence and complexity that conditions the payback profile of agility (Pettit et al., 2010). Methodologically, we have advanced beyond binary "blockchain adoption" indicators (Yli-Huumo et al., 2016) by offering reflective scales with validity evidence; this opens the door to comparative studies across ledger types, governance models, and sectoral constraints. Theoretically, blockchain ceases to be a monolith and becomes a configurable coordination pipeline, where who notarizes what, who may execute which rules, and how events are semantically aligned are the locus of capability building (Risius & Spohrer, 2017). This framing encourages scholars to model orchestration as a set of programmable complementarities: visibility amplifies smart-contract benefits; governance quality conditions both; interoperability sets the ceiling. Such complementarities invite configurational analyses (e.g., fuzzy-set QCA) and deepen links to best-value supply chains and collaborative advantage theories (Ketchen & Hult, 2007). The cross-sectional design has constrained causal language; while theory has directed paths and controls have reduced confounding, time-ordered inferences remain tentative. Single-informant measurement though mitigated by screening, randomization, and attention checks may have introduced perceptual bias; duplicate informants were available only in a subset. Our sampling has focused on blockchain-active manufacturing consortia; results may not generalize to sectors with divergent regulatory or technology stacks (e.g., pharmaceuticals with stringent serialization, or agriculture with fragmented smallholders). Although we have tested alternative resilience composites and included case fixed effects, unobserved heterogeneity (e.g., leadership quality, supply network topology) may still have shaped both capabilities and outcomes. Common-method variance diagnostics have been reassuring, yet all survey studies face residual CMV risk. Finally, we have not modeled cost–benefit trade-offs; the agility gains we document may entail nontrivial integration and governance costs, which could vary by partner power and asset specificity questions better addressed with economic or simulation studies(Blackhurst et al., 2011).

Three avenues appear most promising. First, longitudinal or panel designs should trace how orchestration capabilities evolve and whether improvements in traceability or interoperability precede measurable gains in visibility, agility, and robustness. Event-study methods around real disruptions could complement self-reports and reduce common-method bias (Brandon-Jones et al., 2014). Second, quasi-experiments comparing plants before/after targeted smart-contract deployments can isolate automation effects from secular trends. Third, network-analytic extensions can link capability measures to supply-network structure (centrality, redundancy paths) to test propagation and buffering mechanisms highlighted in resilience theory (Ponomarov & Holcomb, 2009). On the measurement side, researchers could refine governance into subdimensions (permissioning clarity, liability rules, upgrade processes) and calibrate interoperability with technical telemetry (latency, message loss) rather than perceptions. Comparative studies across permissioned vs. public architectures, or across governance models (consortium-led vs. neutral third-party) would extend generalizability (Risius & Spohrer, 2017). Finally, integrated cost-effectiveness analyses combining survey capabilities with implementation cost and performance loss data would support managerial decision-making about where orchestration yields the highest return under varying turbulence and complexity (Tang, 2006). By building on the scales and effect sizes reported here, such studies can progressively map the boundary conditions under which blockchain-orchestrated CPSCs deliver resilient, auditable, and adaptive operations.

CONCLUSION

This study has advanced an empirically grounded account of how blockchain-orchestrated cyber-physical supply chain networks contribute to manufacturing resilience by translating orchestration into measurable capabilities and testing their relationships with coordination outcomes and performance. Using a quantitative, cross-sectional, multi–case design embedded in active consortia, we have operationalized four capability domains traceability, smart-contract automation, IoT–ledger interoperability, and governance quality alongside visibility, agility, robustness, and

Volume 02, Issue 01 (2023)
Page No: 194-223
eISSN: 3067-5146
Doi: 10.63125/6n81ne05

recovery as resilience outcomes, and we have analyzed their interdependence with hierarchical regressions, mediation, and moderation. The results have converged on a clear architecture: traceability, interoperability, and governance have been positively associated with visibility; smart-contract automation and visibility have been positively associated with agility; and visibility and agility, together with governance, have explained greater robustness and a composite resilience index. The moderation by environmental turbulence has indicated that agility's contribution to resilience strengthens as volatility increases, clarifying a boundary condition that helps reconcile mixed narratives about blockchain's operational payoffs. Measurement quality has been strong, robustness checks have preserved inferences under alternative specifications, and effect magnitudes have been practically meaningful suggesting that the orchestration pipeline is not merely a technical novelty but a managerial lever for coordination under uncertainty. Conceptually, these findings reframe blockchain from a monolithic technology into a configurable coordination capability whose value depends on how event provenance is captured, how rules are encoded and governed, and how reliably cyber-physical data interoperate across organizational boundaries. For practitioners, the pattern implies a pragmatic roadmap: build depth in traceability and event quality, harden interoperability at the edge and system interfaces, deploy smart-contract automation where rules are stable and high-volume, and invest in governance that clarifies rights, obligations, and upgrade paths; these moves increase visibility and agility, which in turn reinforce robustness and recovery, especially in turbulent markets. The study's limitations cross-sectional timing, single-informant bias for some units, and sectoral focus on manufacturing consortia temper causal claims and generalizability, yet they do not detract from the central empirical message that orchestration capabilities travel through coordination mechanisms to shape resilience outcomes. By contributing validated scales, model specifications, and effect estimates, the research provides a replicable foundation for longitudinal, quasi-experimental, and network-analytic follow-ups that can map how capability investments compound over time and across structures. Ultimately, the evidence supports a disciplined view of digital transformation in supply chains: resilience gains do not arise from blockchain per se, but from deliberately engineered pipelines that make interfirm information reliable and actionable, align decision rights with executable rules, and enable faster, audit-ready reconfiguration when disruptions strike.

RECOMMENDATIONS

To translate the evidence into action, organizations participating in or planning blockchain-orchestrated cyber-physical supply chains should adopt a phased roadmap that prioritizes coordination fundamentals before ambitious automation, aligns governance with security and auditability, and institutionalizes measurement for continuous improvement. First, establish traceability depth and event quality as the foundation: mandate signed, time-synchronized event envelopes at the edge (sensors/PLCs/MES), define canonical schemas for provenance, custody transfer, and quality exceptions, and require data quality SLAs (timeliness, completeness, accuracy) in partner contracts. Second, treat interoperability as a product: standardize gateway software, messaging patterns (e.g., pub/sub), and identity/permission models across partners; maintain a conformance test suite that vendors and sites must pass before onboarding; and track end-to-end latency as $L_{e2e} = L_{sense} + L_{uplink} + L_{proc} + L_{rule} + L_{commit}$ to keep orchestration responsive without sacrificing integrity. Third, sequence smart-contract automation pragmatically: begin with high-volume, well-codified use cases (milestone releases, three-way match, detention fees), enforce robust exception handling and kill-switch procedures, and only then expand to complex contingencies; pair each contract with an operational runbook and owner. Fourth, strengthen consortium governance: formalize membership criteria, data rights, liability and dispute processes, upgrade paths, and change-control ceremonies; embed joint risk reviews and red-team "break-the-chain" exercises; create a governance board with representation from OEMs, suppliers, logistics, and compliance. Fifth, integrate security from design: align on-chain identities with enterprise IAM, rotate keys, segregate duties for contract deployment, monitor for anomalous on-chain patterns, and define rapid rollback and disclosure workflows; maintain evidence trails that satisfy regulatory audits without leaking competitive intelligence (use role-based views and selective disclosure where needed). Sixth, institutionalize measurement and learning: deploy a KPI stack that mirrors the research constructs Visibility (lead-time to detect), Agility (reconfiguration time), Robustness (service-level variance under shock), Recovery (time-to-restore) and publish consortium-wide scorecards; run

quarterly post-incident reviews to update schemas and rules. Seventh, invest in people and change management: train cross-functional "orchestration squads" (Ops/SCM/Quality/IT-OT/Security), create product manager roles for data schemas and smart contracts, and include suppliers in co-design workshops so rules reflect operational realities. Eighth, budget with a portfolio lens: expect that the highest ROI appears in turbulent segments; stage funding to hit visibility targets first, tie later automation spend to demonstrated gains, and share cost/benefit via incentive clauses for data quality and timeliness. Finally, design for portability and exit: avoid vendor lock-in by using open standards and migration paths; maintain an interoperability abstraction layer so ledger or cloud changes do not ripple through plants; and document everything schemas, contracts, test vectors, and incident playbooks in a living repository. Executed together, these steps convert blockchain from a standalone technology into a resilient coordination pipeline: trustworthy events in, well-governed and auditable rules, timely shared state, and faster, safer reconfiguration when disruptions strike.

REFERENCES

[1]. Abdul, R. (2021). The Contribution Of Constructed Green Infrastructure To Urban Biodiversity: A Synthesised Analysis Of Ecological And Socioeconomic Outcomes. *International Journal of Business and Economics Insights*, *1*(1), 01–31. https://doi.org/10.63125/qs5p8n26

[2]. Ali, A., Mahfouz, A., & Arisha, A. (2017). Analysing supply chain resilience: Integrating the dynamic capability and complex adaptive systems perspectives. *International Journal of Production Research*, *55*(14), 4397–4421. https://doi.org/10.1080/00207543.2017.1355119

[3]. Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management*, *33–34*, 111–122. https://doi.org/10.1016/j.jom.2014.11.002

[4]. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

[5]. Barratt, M., & Oke, A. (2007). Antecedents of supply chain visibility in retail supply chains: A resource-based theory perspective. *Journal of Operations Management*, *25*(6), 1217–1233. https://doi.org/10.1016/j.jom.2007.01.003

[6]. Blackhurst, J., Dunn, K. S., & Craighead, C. W. (2011). An empirically derived framework of global supply resiliency. *Journal of Business Logistics*, *32*(4), 374–391. https://doi.org/10.1111/j.2158-1592.2011.01047.x

[7]. 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. https://doi.org/10.1111/jscm.12050

[8]. Brusset, X., & Teller, C. (2017). Supply chain capabilities, risks, and resilience. *International Journal of Production Economics*, *184*, 59–68. https://doi.org/10.1016/j.ijpe.2016.09.008

[9]. Cao, M., & Zhang, Q. (2011). Supply chain collaboration: Impact on collaborative advantage and firm performance. *Journal of Operations Management*, *29*(3), 163–180. https://doi.org/10.1016/j.jom.2010.12.008

[10]. Caridi, M., Moretto, A., Perego, A., & Tumino, A. (2014). The benefits of supply chain visibility: A value assessment model. *International Journal of Production Economics*, *151*, 1–19. https://doi.org/10.1016/j.ijpe.2013.12.025

[11]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/access.2016.2566339

[12]. Danish, M. (2023). Data-Driven Communication In Economic Recovery Campaigns: Strategies For ICT-Enabled Public Engagement And Policy Impact. *International Journal of Business and Economics Insights*, *3*(1), 01-30. https://doi.org/10.63125/qdrdve50

[13]. Danish, M., & Md. Zafor, I. (2022). The Role Of ETL (Extract-Transform-Load) Pipelines In Scalable Business Intelligence: A Comparative Study Of Data Integration Tools. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 89–121. https://doi.org/10.63125/1spa6877

[14]. Danish, M., & Md.Kamrul, K. (2022). Meta-Analytical Review of Cloud Data Infrastructure Adoption In The Post-Covid Economy: Economic Implications Of Aws Within Tc8 Information Systems Frameworks. *American Journal of Interdisciplinary Studies*, *3*(02), 62-90. https://doi.org/10.63125/1eg7b369

[15]. Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., & Wamba, S. F. (2017). The impact of big data on supply chain performance. *Transportation Research Part E*, *114*, 343–364. https://doi.org/10.1016/j.tre.2017.06.008

[16]. Flynn, B. B., Huo, B., & Zhao, X. (2010). The impact of supply chain integration on performance: A contingency and configuration approach. *Journal of Operations Management*, *28*(1), 58–71. https://doi.org/10.1016/j.jom.2009.06.001

[17]. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1), 2. https://doi.org/10.3390/logistics2010002

[18]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

[19]. Hughes, L., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technology mean for firms. *Business Horizons*, *62*(3), 273–281. https://doi.org/10.1016/j.bushor.2019.01.002

[20]. Ketchen, D. J., Jr., & Hult, G. T. M. (2007). Bridging organization theory and supply chain management: The case of best value supply chains. *Journal of Operations Management*, *25*(2), 573–580. https://doi.org/10.1016/j.jom.2006.05.010

[21]. 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

[22]. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35*(4), 95–99. https://doi.org/10.1109/ms.2018.2801546

[23]. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

[24]. Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, *6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

[25]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12

[26]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[27]. Md. Rabiul, K., & Sai Praveen, K. (2022). The Influence of Statistical Models For Fraud Detection In Procurement And International Trade Systems. *American Journal of Interdisciplinary Studies*, *3*(04), 203-234. https://doi.org/10.63125/9htnv106

[28]. Md.Kamrul, K., & Md Omar, F. (2022). Machine Learning-Enhanced Statistical Inference For Cyberattack Detection On Network Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 65-90. https://doi.org/10.63125/sw7jzx60

[29]. Monostori, L. (2014). Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia CIRP*, *17*, 9–13. https://doi.org/10.1016/j.procir.2014.03.115

[30]. Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development of a conceptual framework. *Journal of Business Logistics*, *31*(1), 1–21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

[31]. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*, *20*(1), 124–143. https://doi.org/10.1108/09574090910954873

[32]. Queiroz, M. M., Telles, R., & Bonilla, S. H. (2020). Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Management*, *25*(2), 241–254. https://doi.org/10.1108/scm-03-2018-0143

[33]. Razia, S. (2022). A Review Of Data-Driven Communication In Economic Recovery: Implications Of ICT-Enabled Strategies For Human Resource Engagement. *International Journal of Business and Economics Insights*, *2*(1), 01-34. https://doi.org/10.63125/7tkv8v34

[34]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159

[35]. Reduanul, H. (2023). Digital Equity and Nonprofit Marketing Strategy: Bridging The Technology Gap Through Ai-Powered Solutions For Underserved Community Organizations. *American Journal of Interdisciplinary Studies*, *4*(04), 117-144. https://doi.org/10.63125/zrsv2r56

[36]. Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering*, *59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

[37]. Rony, M. A. (2021). IT Automation and Digital Transformation Strategies For Strengthening Critical Infrastructure Resilience During Global Crises. *International Journal of Business and Economics Insights*, *1*(2), 01-32. https://doi.org/10.63125/8tzzab90

[38]. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

[39]. Sadia, T. (2022). Quantitative Structure-Activity Relationship (QSAR) Modeling of Bioactive Compounds From Mangifera Indica For Anti-Diabetic Drug Development. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 01-32. https://doi.org/10.63125/ffkez356

[40]. Sadia, T. (2023). Quantitative Analytical Validation of Herbal Drug Formulations Using UPLC And UV-Visible Spectroscopy: Accuracy, Precision, And Stability Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 01–36. https://doi.org/10.63125/fxqpds95

[41]. Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management*, *25*(4), 100552. https://doi.org/10.1016/j.pursup.2019.100552

[42]. Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

[43]. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350. https://doi.org/10.1002/smj.640

[44]. Tian, F. (2017). *A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things* 2017 International Conference on Service Systems and Service Management (ICSSSM),

[45]. Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access*, *5*, 17465–17477. https://doi.org/10.1109/access.2017.2720760

[46]. Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management*, *23*(6), 545–559. https://doi.org/10.1108/scm-01-2018-0029

[47]. Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: Definition, review and theoretical foundations for further study. *International Journal of Production Research*, *53*(18), 5592–5623. https://doi.org/10.1080/00207543.2015.1037934

[48]. Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? *International Journal of Production Economics*, *211*, 221–236. https://doi.org/10.1016/j.ijpe.2019.02.002

[49]. Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243. https://doi.org/10.1109/tii.2014.2300753

[50]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

[51]. Zayadul, H. (2023). Development Of An AI-Integrated Predictive Modeling Framework For Performance Optimization Of Perovskite And Tandem Solar Photovoltaic Systems. *International Journal of Business and Economics Insights*, *3*(4), 01–25. https://doi.org/10.63125/8xm7wa53