International Journal of Scientific Interdisciplinary Research

Volume: 5; **Issue:** 2
Pages: 449– 486

open access
Crossref
PEER-REVIEWED

IMPACT OF IOT AND BLOCKCHAIN INTEGRATION ON REAL-TIME SUPPLY CHAIN TRANSPARENCY

Md. Rabiul Karim[1]; Khairul Alam Talukder[2]

[1]. MBA, Business Administration and Management, Trine University, Angola, IN, USA.
Email: rabiulkarim2024@gmail.com

[2]. MBA in Management, Lamar University, USA
Email: talukderkhairul55@gmail.com

Doi: 10.63125/2yc6e230
Received: 22 April 2024; **Revised:** 26 May 2024; **Accepted:** 08 June 2024; **Published:** 29 June 2024

Abstract

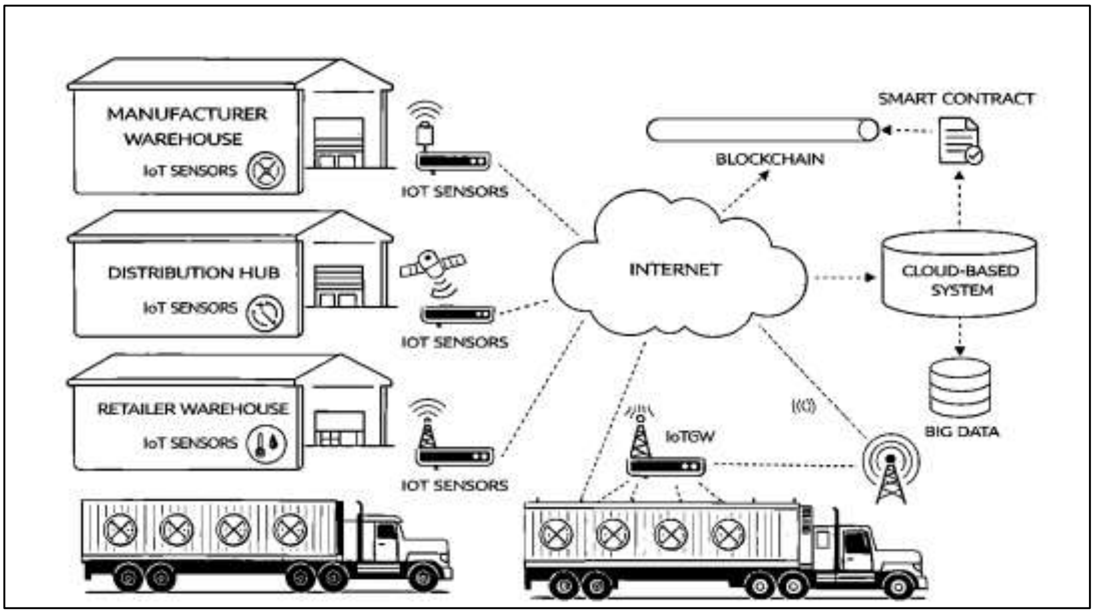
This study investigated how Internet of Things (IoT) adoption intensity, blockchain deployment intensity, and their combined IoT–blockchain integration capability shaped real-time supply chain transparency and related operational performance. Drawing on a focused review of 78 peer-reviewed empirical papers, the study defined real-time transparency as a multidimensional latent capability reflected in timeliness of visibility, traceability completeness across tiers, integrity and trustworthiness of shared records, and accessibility/auditability for stakeholders. A cross-sectional explanatory design was applied using firm-level survey data from transparency-critical sectors including food and agro-processing, pharmaceuticals and healthcare distribution, manufacturing/apparel export chains, and e-commerce logistics. After screening, 312 valid responses were retained. Constructs were measured with validated five-point Likert scales and analyzed using PLS-SEM to accommodate second-order integration capability modeling, mediation, and interaction testing. Descriptive statistics indicated moderate-to-high technology intensity (IoT $M = 3.71$, $SD = 0.68$; blockchain $M = 3.54$, $SD = 0.74$) but comparatively lower integration capability ($M = 3.29$, $SD = 0.63$). Transparency baselines were highest for timeliness ($M = 3.83$, $SD = 0.59$) and traceability completeness ($M = 3.76$, $SD = 0.61$), with wider dispersion in integrity/trust and accessibility/auditability. The measurement model showed strong reliability and validity (Cronbach's alpha = .86–.92; composite reliability = .90–.94; AVE = .62–.69; HTMT ratios below conservative cutoffs), and collinearity diagnostics remained acceptable (VIF range = 1.33–2.11). Structural results supported all hypotheses. IoT intensity significantly predicted timeliness and granularity aspects of transparency ($\beta = 0.31$, $p < .001$), while blockchain intensity significantly predicted integrity/trust aspects ($\beta = 0.27$, $p < .001$). Integration capability exerted the strongest direct effect on overall transparency ($\beta = 0.42$, $p < .001$) and increased explained variance from $R^2 = 0.46$ to $R^2 = 0.59$ ($\Delta R^2 = 0.13$). A significant interaction effect confirmed synergy between IoT and blockchain intensities ($\beta = 0.14$, $p = .003$). Trust and information quality partially mediated the integration–transparency relationship (total indirect $\beta = 0.18$), and transparency significantly predicted operational performance ($\beta = 0.39$, $p < .001$), confirming partial mediation from integration to performance through transparency.

Keywords
IoT, Blockchain, Integration capability, Real-time transparency, Supply chains;

INTRODUCTION

Real-time supply chain transparency refers to the continuous, near-instant visibility of flows of materials, information, and finances across interconnected actors from source to end customer. Transparency is typically expressed through traceability, auditability, and accessibility of trustworthy data that describes where an item is, what condition it is in, who handled it, and which transactions were performed (Helo & Shamsuzzoha, 2020). In supply chain research, transparency is closely related to visibility, a capability that reduces information asymmetry and enables coordinated decisions across firms, logistics providers, regulators, and consumers. Traditional transparency has relied on centralized information systems such as ERP, EDI, and barcoding; however, these systems often create segmented "data islands" where information is delayed, selectively shared, or difficult to verify across organizational boundaries (Arfan et al., 2021). The emergence of the Internet of Things (IoT) and blockchain brings a distinct technological shift because each technology targets a different structural weakness of legacy transparency models. IoT is a paradigm in which physical objects embedded with sensors, tags, and communication modules generate and transmit data through networks, creating a digital representation of physical supply chain events (Jahid, 2021). This enables automated observation of location, temperature, humidity, vibration, spoilage, and handling status at high frequency (Akbar & Farzana, 2021).

Figure 1: Real-Time Supply Chain Transparency



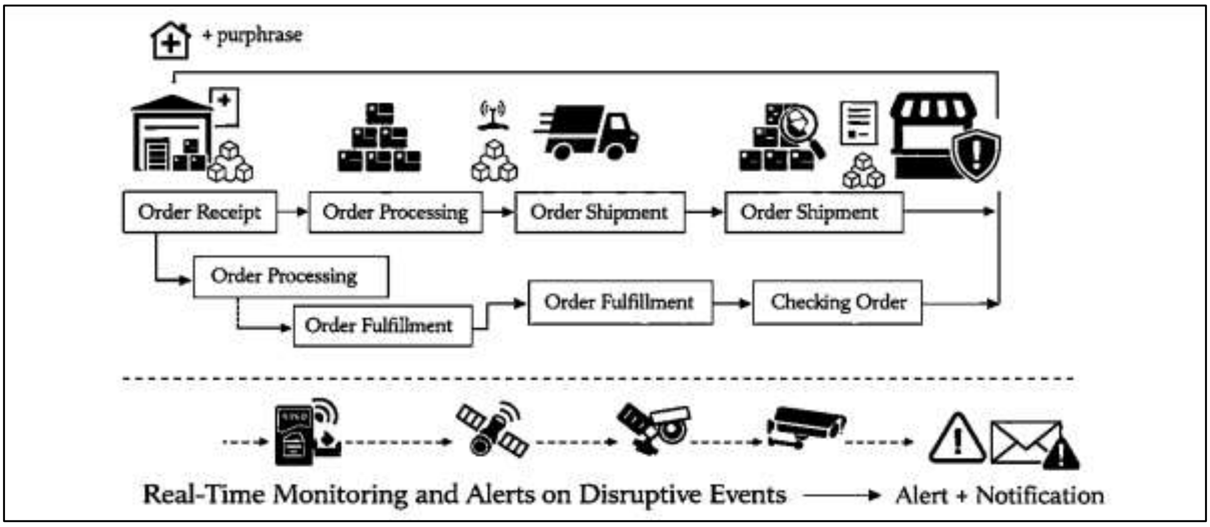
Blockchain, in contrast, is a distributed ledger system that records transactions in immutable, time-stamped blocks maintained through consensus among network participants (Pundir et al., 2019; Reza et al., 2021). It replaces single-owner databases with shared records that can be verified by all authorized nodes, providing resistance to tampering, retroactive alteration, and unilateral control. When integrated, IoT supplies granular real-time event data, while blockchain provides a permanent, trusted memory of those events (Zobayer, 2021a, 2021b). The integration thus forms an end-to-end cyber-physical transparency infrastructure: sensing, data transmission, validation, storage, and controlled access. In quantitative supply chain studies, this integration is treated as a capability bundle that can be modeled through constructs such as information quality, real-time visibility, perceived trust, process automation, and coordination efficiency (Ariful & Ara, 2022; Arman & Kamrul, 2022). The foundational definitions above place emphasis on measurable outcomes—latency of information, accuracy of provenance, frequency of updates, and integrity of records—which are essential for building empirical models you can test in a quantitative paper (Guo et al., 2022; Mesbaul & Farabe, 2022; Abdur & Haider, 2022).

Global supply chains are now structurally dispersed, multi-tiered, and risk-exposed, making transparency an international economic and policy priority. Retail e-commerce, pharmaceuticals, food, apparel, electronics, and critical minerals all depend on cross-border movement where delays or distortions in information translate into higher inventory buffers, waste, safety incidents, or reputational shocks (Mushfequr & Sai Praveen, 2022; Mortuza & Rauf, 2022; Rejeb et al., 2019). International trade expansion has magnified the distance between producers and consumers, and that distance multiplies the number of handoffs where data can be lost or manipulated. Real-time transparency matters because demand volatility, geopolitical disruptions, and climate-linked logistics shocks require rapid coordination rather than periodic reporting. From a market perspective, firms seek transparency to reduce the bullwhip effect and to coordinate replenishment, production scheduling, and last-mile delivery with fewer forecasting errors (Abdul, 2023; Rakibul & Samia, 2022). From a regulatory perspective, governments and multilateral bodies push traceability to enforce food safety, drug authenticity, conflict-minerals compliance, carbon reporting, and labor standards. From a consumer perspective, transparency is entwined with trust in claims about origin, sustainability, and ethical sourcing (Abdulla & Zaman, 2023; Arfan et al., 2023; Sunny et al., 2020). This global context has produced uneven transparency capacities across regions; high-income logistics hubs often employ advanced tracking, while developing economies face fragmented infrastructure, variable data standards, and weaker enforcement mechanisms (Amin & Mesbaul, 2023; Foysal & Aditya, 2023; Hamidur, 2023). IoT and blockchain integration is internationally significant because it promises to lower the dependency on centralized platforms controlled by a small number of gatekeepers and to standardize trust in shared data even among actors who lack pre-existing institutional confidence. Moreover, the integration supports "proof of condition" and "proof of provenance" in real time, enabling cross-border verification without needing identical national compliance systems. Studies in global logistics and sustainable supply chains consistently tie transparency to reduced fraud, fewer recalls, better service levels, and improved stakeholder confidence (Hader et al., 2022; Rashid et al., 2023; Musfiqur & Kamrul, 2023).

IoT-driven transparency emerges from the ability to observe supply chain states directly rather than infer them from paperwork or periodic scans. In operational terms, RFID tags, GPS modules, machine-vision cameras, smart meters, and environmental sensors capture continuous data about movement and condition (Zelbst et al., 2020). The data is transmitted through wireless sensor networks, LPWAN, 4G/5G, satellite, or edge gateways into supply chain platforms. This creates event streams—arrival, departure, storage, temperature excursions, shock exposure, shelf-life decay—that can be used for real-time exception management. Quantitatively, IoT improves the timeliness, granularity, and objectivity of supply chain information, which are core determinants of visibility performance. Yet IoT alone does not guarantee transparent supply chains. First, IoT data is only as reliable as its collection and governance; sensors can fail, be spoofed, or be intentionally disabled. Second, data ownership remains centralized when stored in proprietary clouds, so partners may distrust the authenticity of shared data (Iqbal & Butt, 2020; Muzahidul & Mohaiminul, 2023; Amin & Praveen, 2023). Third, interoperability across brands, countries, and tiers is uneven, leading to partial coverage rather than end-to-end traceability. These limitations are measurable in empirical work through variables such as sensor reliability, data latency, coverage ratio, and inter-organizational data-sharing intensity (Hasan & Ashraful, 2023; Ibne & Kamrul, 2023). Despite these limitations being common in the literature, IoT's contribution remains fundamental: it closes the "physical-to-digital gap" by ensuring that transparency is tied to real-world states, not only to transactional records. In many industries, IoT adoption has already improved cold-chain monitoring, container tracking, warehouse automation, and inventory accuracy, providing a strong empirical foundation for integrating IoT data into broader trust architectures (Ko et al., 2018; Mushfequr & Ashraful, 2023; Roy & Kamrul, 2023).

Blockchain contributes to transparency by restructuring how supply chain data is validated, stored, and shared. In distributed ledgers, each participant holds a synchronized copy of records, and new entries require consensus based on pre-defined cryptographic rules (Azizi et al., 2021; Shaikh & Farabe, 2023; Haider & Hozyfa, 2023; Zobayer, 2023). This makes records tamper-evident and auditable across time, which directly addresses falsification, counterfeit insertion, and post-hoc manipulation that can occur in centralized databases. Beyond simple recording, smart contracts allow rules to be embedded into the ledger, enabling automated execution of transactions when IoT-derived conditions are met, such as releasing payment when a temperature-compliant shipment arrives. In empirical supply chain research, blockchain is operationalized through constructs including immutability, decentralization, traceability strength, data security, and perceived inter-firm trust. The technology is also linked with reduced reconciliation costs, fewer disputes, and faster provenance verification. Importantly, blockchain does not inherently provide real-time observation; it depends on trustworthy data inputs (Kumar & Pundir, 2020). Therefore, its transparency advantage centers on integrity and multiparty verifiability rather than sensing. Quantitative models commonly treat blockchain as a moderator or mediator that improves the effect of information sharing on performance outcomes by raising confidence in data accuracy. Emerging empirical frameworks validated on real trade datasets show how blockchain-enabled traceability architecture strengthens transparency indicators (Venkatesh et al., 2020).

Figure 2: IoT-Driven Real-Time Supply Chain Monitoring



The integration of IoT and blockchain is often described as a cyber-physical pipeline. First, IoT devices generate data at the edge, capturing time-stamped events such as location, transfer of custody, or quality readings. Second, data is preprocessed through edge or fog computing to filter noise and reduce bandwidth load (Gligor et al., 2022). Third, validated events are written to the blockchain network either directly or through middleware, yielding an immutable audit trail. Fourth, smart contracts govern access rights and automate business logic. This sequence addresses two transparency bottlenecks simultaneously: incomplete real-time observation and weak trust in shared records. In practical implementations, IoT ensures that blockchain reflects reality, while blockchain ensures IoT data is not selectively altered or withheld after capture. Quantitatively, integration enables measurable improvements in visibility latency, data provenance certainty, dispute rates, and compliance verification time. Industry-grade platforms (for example in food, pharmaceuticals, and high-value manufacturing) show that integration can support multi-tier traceability without requiring all parties to share a single IT owner (Ghode et al., 2020). Integration architectures vary: some systems store full IoT datasets on-chain, while others store hashes on-chain with off-chain databases handling volume. The selection influences performance variables such as throughput, cost per transaction, and data accessibility. From a modeling viewpoint, integration constructs can be framed as technological capability, information governance capability, or digital trust capability, each affecting transparency outcomes. Recent studies emphasize that integration mainly delivers value when visibility and integrity are treated as joint objectives rather than separate digital upgrades (Caro et al., 2018).

A quantitative paper on this topic typically operationalizes real-time transparency as a multidimensional latent construct. The first dimension is timeliness, captured through measures like event-update frequency, end-to-end latency, or response time to exceptions. The second is traceability completeness, reflected in the proportion of supply chain nodes covered, granularity of batch or item tracking, and continuity of custody records (Tayal et al., 2021). The third is data integrity and trust, measured through perceived reliability of shared data, reduction in reconciliation errors, or incidence of fraud. The fourth is accessibility and auditability, captured by stakeholder retrieval speed, availability of standardized data fields, and compliance reporting readiness. IoT adoption intensity serves as an observed driver of timeliness and granularity, while blockchain adoption intensity serves as a driver of integrity, auditability, and shared trust. Integration capability can be modeled as an interaction term or a second-order construct capturing interoperability, smart-contract maturity, and sensor-to-ledger automation (Centobelli et al., 2022; Hozyfa & Shahrin, 2024; Hasan & Shah, 2024). Outcomes may include inventory accuracy, shrinkage reduction, recall precision, delivery performance, or compliance scores, allowing structural equation modeling, regression, or panel data methods to test causal paths. Researchers also incorporate contextual controls such as supply chain complexity, international sourcing ratio, product perishability, regulatory pressure, and digital readiness (Hasan & Zayadul, 2024; Muzahidul & Aditya, 2024). The measurement logic aligns with information processing theory and resource-based views: IoT expands the firm's information-processing capacity, while blockchain enhances information credibility and governance (Shahzad & Zhang, 2020). Quantitative hypotheses thus connect integration to transparency, and transparency to operational and relational outcomes, through statistically testable relationships.

Prior studies across operations management, information systems, and logistics provide a well-established base for analyzing IoT–blockchain integration. Visibility and information-sharing foundations in supply chain theory highlight the performance role of timely, accurate, and shared data (ElMessiry & ElMessiry, 2018; Hasan & Rakibul, 2024; Mominul, 2024). IoT literature demonstrates how sensor-based monitoring improves real-time tracking, quality assurance, and responsive logistics through high-frequency data capture. Blockchain literature documents improvements in traceability, multiparty trust, and auditability via immutable ledgers and smart contracts. Integration-focused works extend these streams by showing that unit-level sensing paired with distributed validation yields a more complete transparency architecture than either technology alone (Hrouga et al., 2022). The empirical record includes surveys linking integration to transparency gains, case-based quantitative analyses showing reduced counterfeit risk, and dataset validations from industrial platforms illustrating improved provenance certainty and responsiveness. Theoretically, the integration is positioned at the intersection of cyber-physical systems, digital trust, and supply chain risk management, where transparency is a measurable capability that mediates performance. Internationally, evidence points to relevance in food safety chains, vaccine and drug distribution, sustainable apparel, and cross-border e-commerce logistics, reinforcing the global stakes of real-time transparency (Malik et al., 2019).

The objective of this quantitative study is to examine, in a measurable and model-ready manner, how the integration of Internet of Things (IoT) technologies with blockchain infrastructures influences real-time supply chain transparency across multi-tier and cross-border logistics networks. Specifically, the study aims to operationalize IoT–blockchain integration as a composite technological capability that combines continuous sensing, automated event capture, distributed data validation, and immutable recordkeeping, and then determine its statistical relationship with transparency outcomes. A first objective is to define and quantify real-time transparency through observable dimensions that include information timeliness, traceability completeness, data integrity, and stakeholder accessibility, ensuring that the construct is suitable for hypothesis testing and structural modeling. A second objective is to measure the independent contribution of IoT adoption intensity—captured via indicators such as sensor coverage, event frequency, and data latency—to the timeliness and granularity aspects of transparency. A third objective is to measure the independent contribution of blockchain adoption intensity—captured through indicators such as ledger immutability reliance, smart-contract usage, and multiparty auditability—to the integrity and trust aspects of transparency. A fourth objective is to test the joint or interaction effect of IoT and blockchain deployment, evaluating whether integration capability amplifies transparency beyond the additive effects of either technology alone. A fifth objective is to assess how contextual variables, including supply chain complexity, product perishability or criticality, international sourcing ratio, regulatory exposure, and digital readiness, condition the strength of the integration–transparency relationship. A sixth objective is to link real-time transparency to operational performance proxies such as inventory accuracy, shrinkage reduction, recall precision, on-time delivery, and dispute frequency, providing a pathway to evaluate transparency as a mediating capability within the overall supply chain performance framework. Collectively, these objectives guide the empirical design toward a rigorous explanation of how cyber-physical data capture and distributed trust architectures reshape the visibility and verifiability of supply chain events in real time, using quantitative evidence derived from firms and networks that have adopted these technologies.

LITERATURE REVIEW

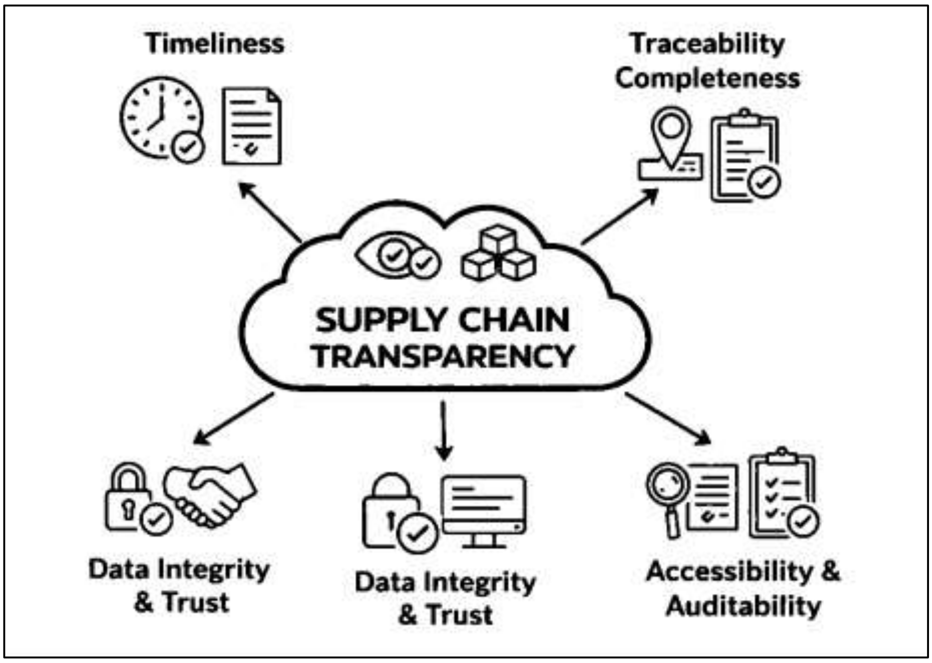
This Literature Review synthesizes empirical and theory-driven scholarship on the integration of Internet of Things (IoT) and blockchain technologies and their measurable effects on real-time supply chain transparency. The section is structured to build a quantitative foundation for hypothesis development and model specification by moving from established transparency and visibility constructs toward technology-enabled mechanisms and validated measurement approaches. First, the review clarifies how transparency has been conceptualized and operationalized in supply chain research, emphasizing dimensions that can be statistically modeled such as timeliness, completeness of traceability, integrity of shared data, and accessibility across tiers. Second, it examines the quantitative evidence on IoT as a real-time sensing and data-generation backbone, focusing on measurable impacts on visibility latency, event accuracy, and condition monitoring. Third, it reviews blockchain as a distributed trust and auditability layer and summarizes findings on integrity assurance, anti-counterfeit traceability, and transaction verification. The review then integrates these streams by analyzing empirical studies that treat IoT–blockchain integration as an interacting capability bundle, highlighting models that test additive, mediating, or moderating effects on transparency outcomes. To ensure alignment with a quantitative paper, the section also documents the most widely used measurement instruments, survey scales, proxy variables, and analytical techniques (e.g., SEM, regression, panel estimation, and multi-criteria methods). Finally, the review identifies consistent variable relationships and methodological patterns in the literature that directly inform the study's conceptual framework and statistical testing strategy.

Real-Time Supply Chain Transparency

In quantitative supply chain management, real-time transparency is commonly treated as a latent, multi-dimensional capability rather than a single observable variable. This approach reflects the idea that transparency is not directly "seen" but inferred through measurable indicators that collectively represent how clearly supply chain actors can perceive and verify the flow of products, information, and responsibilities (Dolgui & Ivanov, 2022). The visibility literature positions transparency as an advanced form of supply chain visibility, emphasizing not only knowing what is happening but also being able to validate that knowledge across multiple tiers. Empirical models therefore represent transparency through constructs such as information quality, visibility strength, and traceability depth, tested using survey scales or operational proxies. Studies show that transparency is statistically associated with process coordination, responsiveness, and performance outcomes because it reduces information asymmetry and limits opportunistic behavior among partners. Structural equation models and regression-based frameworks frequently position transparency as either a mediator between digital capabilities and performance or a direct driver of agility and trust-based collaboration (Liu et al., 2021). The latent treatment is especially common in global and multi-tier settings where transparency depends on aligned data-sharing norms, interoperable tracking practices, and credible records that survive movement across firms and borders. Evidence from logistics, food, and manufacturing supply chains indicates that transparency becomes measurable when researchers decompose it into core dimensions that can be captured consistently across contexts. Since supply chains involve heterogeneous actors, transparency is rarely uniform; instead, it emerges from the joint configuration of sensing, reporting, verification, and access routines. As a result, the quantitative conceptualization frames transparency as a reflective construct, inferred through multiple indicators tied to operational reality, stakeholder engagement, and governance consistency (Rizwan et al., 2022). This latent perspective provides a foundation for measurement validity, allowing researchers to test whether transparency functions as a stable capability with predictable statistical relationships to other supply chain variables.

Timeliness is one of the most frequently operationalized dimensions of real-time supply chain transparency because it directly captures whether visibility is current enough to support coordination (Bhat et al., 2021). Quantitative studies typically interpret timeliness through indicators such as how quickly supply chain events are reported after they occur, how frequently updates are generated, and how rapidly actors can respond to disruptions. Timeliness is treated as a core part of transparency because delayed information produces partial or misleading representations of supply chain reality. In parallel, traceability completeness reflects how thoroughly products and transactions can be tracked across nodes, tiers, and transformations. Empirical research measures this completeness through coverage of upstream and downstream partners, granularity of tracking at batch or item level, and continuity of custody from origin to final destination. Traceability completeness is critical because transparency collapses when gaps exist between stages, allowing loss of provenance, hidden substitutions, or unverified handoffs (Al-Rakhami & Al-Mashari, 2021).

Figure 3: Dimensions of Supply Chain Transparency



Quantitative analyses across food, pharmaceutical, and e-commerce logistics show that higher traceability coverage correlates with fewer recall errors, reduced counterfeit exposure, and more accurate settlement of responsibility when quality failures occur. These studies also demonstrate that timeliness and traceability completeness often move together: frequent, fast updates allow continuous traceability, while broad node coverage prevents blind spots that might otherwise persist even with rapid reporting. The literature therefore treats both dimensions as co-defining elements of a transparency construct, enabling consistent statistical modeling across industries (Pal, 2020). Together they represent whether supply chain information is not only available but also complete enough to reconstruct the product journey without interruption, making them central to quantitative assessments of transparency capability.

A third dimension emphasized in quantitative models is data integrity and the trustworthiness of exchanged information. Researchers highlight that transparency requires not just data presence but confidence that the data accurately represents the physical and transactional reality of the supply chain (Tsang et al., 2019). Integrity is measured through observable proxies such as the frequency of data mismatches between partners, incidence of reconciliation adjustments, error rates in tracking records, and the perceived reliability of shared information using validated survey scales. Trust-based models in supply chain research identify integrity as a necessary condition for transparency because actors will not rely on shared visibility if they suspect manipulation or selective disclosure. Empirical studies show that when integrity is high, firms display stronger coordination behaviors, reduced monitoring costs, and greater willingness to share sensitive operational information (Astill et al., 2019). Conversely, low integrity introduces verification delays and repeated manual checks, which quantitatively appear as higher dispute rates, longer settlement cycles, and weaker performance gains from information sharing. In multi-tier networks, integrity also has a governance meaning: it captures whether data retains its original form as it passes across organizations, and whether any actor can retroactively alter records without detection. Research in traceability systems and visibility architectures demonstrates that integrity indicators are predictive of transparency outcomes even after controlling for technological adoption levels. This evidence supports treating integrity as a distinct measurable pillar, rather than assuming that more data automatically produces more transparency. Therefore, quantitative transparency frameworks consistently include integrity/trust variables to represent whether shared supply chain information is credible enough to guide decisions and accountability (Sezer et al., 2022).

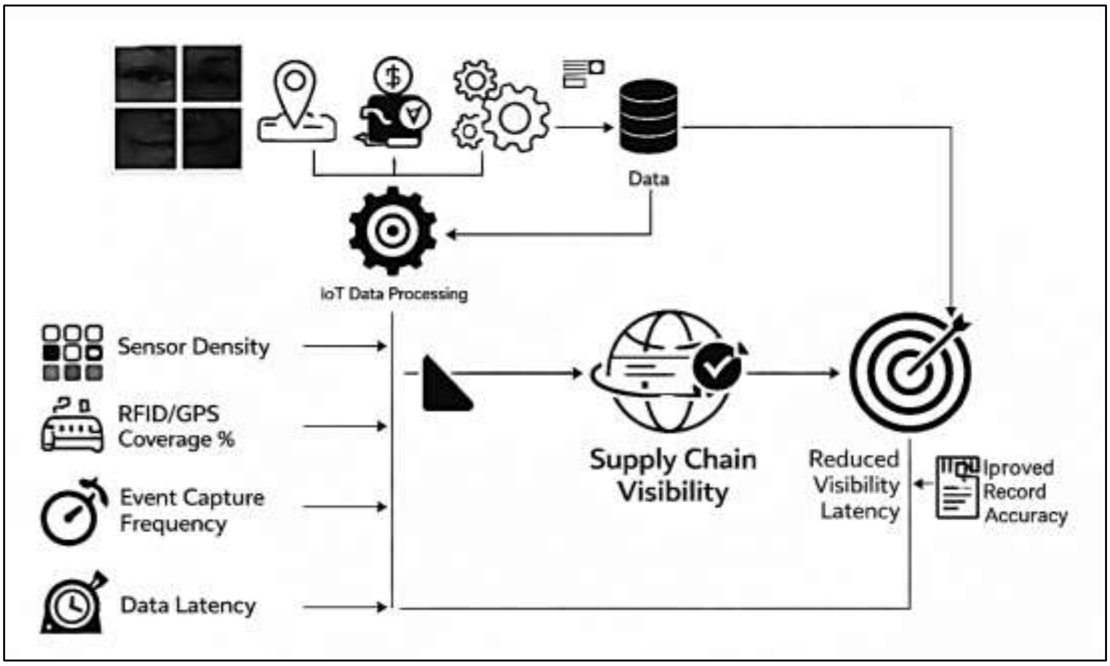
Accessibility and auditability form an additional measurable pillar of real-time transparency, focusing on who can retrieve supply chain information, how quickly, and in what standardized form. Accessibility is assessed through indicators such as stakeholder retrieval speed, proportion of partners with authorized access, and degree of standardization in the data fields available for use (Raja Santhi & Muthuswamy, 2022). Auditability extends accessibility by capturing whether the information can be verified historically in a way that supports compliance, dispute resolution, and ethical claims. Quantitative research often measures auditability through the existence of continuous transaction logs, the frequency of successful audits, and readiness for regulatory reporting. Evidence across logistics, sustainable sourcing, and regulated industries shows that accessibility and auditability strengthen transparency outcomes because they turn visibility into actionable, verifiable knowledge. Studies modeling transparency as a mediator demonstrate that transparency links digital capabilities to operational performance by enabling faster exception handling, narrower recall scopes, and improved inventory and delivery reliability . In food and pharmaceutical supply chains, auditability indicators correlate with reduced quality incidents and faster root-cause identification. In e-commerce logistics, accessibility indicators align with better order tracking accuracy and fewer customer disputes. These patterns support a consistent empirical view: transparency is not only a technological artifact but a measurable governance and information-processing capability that channels real-time supply chain data into performance advantages. Quantitative models validating transparency as a mediator or driver repeatedly show that accessibility and auditability are essential in sustaining transparency across time and across diverse actors, making them indispensable for rigorous measurement designs.

Effects of IoT Adoption Intensity on Monitoring Accuracy

The literature consistently frames IoT adoption intensity as a measurable technological capability that strengthens supply chain visibility by expanding the volume, speed, and richness of operational data. Rather than treating IoT as a binary “adopted/not adopted” factor, empirical research conceptualizes intensity through the depth and breadth of device deployment across supply chain nodes (Nabil et al., 2022). Studies in logistics and retail supply chains show that visibility improves when IoT is embedded at multiple handoff points and when data capture is continuous rather than episodic. Survey-based work operationalizes IoT intensity using indicators such as the share of products or assets tagged with RFID, the proportion of fleets equipped with GPS, the number of fixed sensors per warehouse zone, and the extent of platform connectivity across partners. Dataset-based research complements this by using event-log metrics including timestamp density, scan frequency, and geographic tracking continuity (Elsaleh et al., 2020). Across these studies, IoT intensity has been associated with reductions in information asymmetry, more stable replenishment cycles, and stronger monitoring of inventory-in-motion. Visibility is treated as both an outcome and a mediating construct in larger quantitative models, where IoT intensity predicts visibility strength and visibility then predicts operational performance. The evidence indicates that higher deployment density enables more “observable supply chain reality,” which reduces reliance on manual reports and intermittent confirmation. Thus, IoT intensity is understood as a scalable predictor variable that can be statistically linked to changes in visibility latency and accuracy across global and multi-tier supply chains (Granat et al., 2019).

Prior research provides a convergent set of operational measures for IoT intensity that translate naturally into quantitative modeling. Sensor density per shipment or asset appears frequently because it captures how fully products are instrumented for monitoring during movement and storage. In warehousing and transport studies, density is reflected in the count of temperature, humidity, shock, or motion sensors embedded per pallet, container, or vehicle, which allows fine-grained event logging (Akbar et al., 2018). RFID and GPS coverage percentages form another core measure, representing the fraction of supply chain objects or routes producing trackable signals at any given time. Coverage indicators are critical because partial tagging yields visibility gaps even when individual sensors perform well.

Figure 4: IoT Adoption Intensity and Supply Chain Visibility



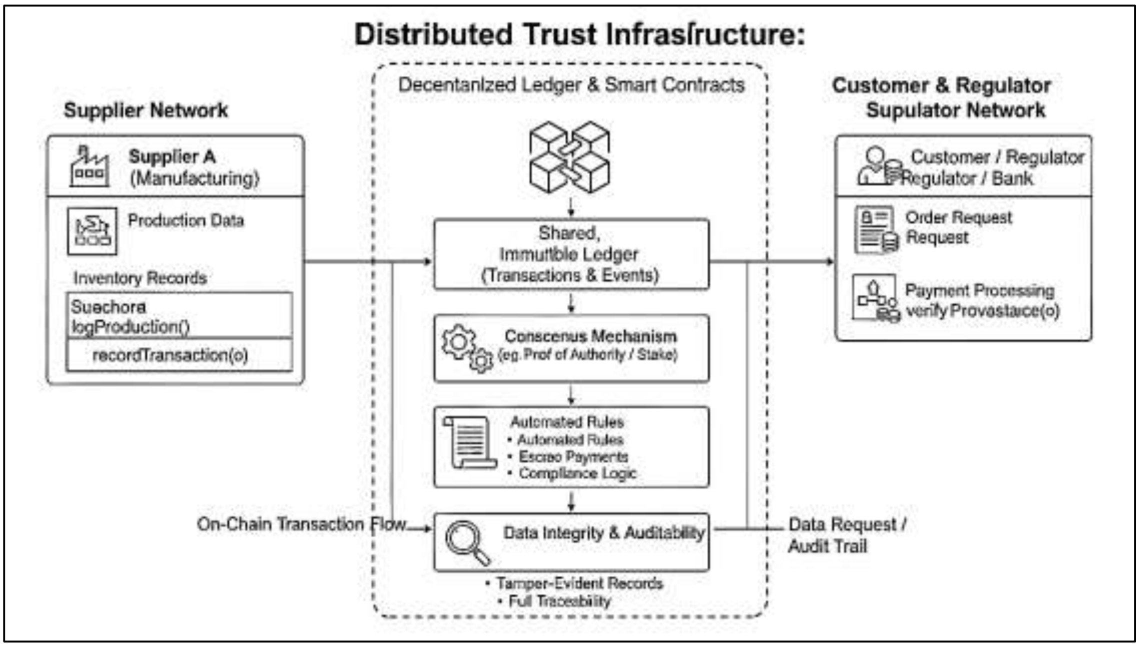
Event capture frequency is commonly used to represent real-time capability, expressed through how often devices transmit observations over fixed intervals. Higher frequency supports continuous visibility and rapid exception detection, while lower frequency approximates periodic reporting. Data latency measures complete the operationalization set by capturing the delay between a physical event and its digital appearance in monitoring systems. Studies often treat latency as an indicator of system responsiveness and a determinant of decision usefulness (Zhu et al., 2015). Importantly, these measures are not isolated; research emphasizes that reliable models combine density, coverage, frequency, and latency to represent IoT adoption as a multidimensional intensity construct. This measurement structure has been validated in both survey scales and operational datasets, enabling comparable modeling across sectors such as food, pharmaceuticals, and e-commerce distribution.

Quantitative evidence links IoT intensity to clear reductions in visibility latency and improvements in record accuracy, especially in complex supply chains where information delays are costly. Regression and SEM-based studies report that more intensive IoT deployment shortens the time between movement events and platform updates, enabling supply chain actors to respond to delays, route deviations, or inventory shortages with higher precision (Li et al., 2018). Visibility latency reductions are often explained through automated sensing that replaces manual scans and paperwork, producing higher-speed data pipelines. In inventory contexts, the literature shows that continuous IoT tracking reduces discrepancies between recorded and actual stock by capturing withdrawals, transfers, and arrivals at the moment they occur. This effect is particularly evident in retail backrooms, distribution centers, and omnichannel fulfillment where inventory accuracy directly shapes service levels (Carrasco & Romi, 2022). Dataset-oriented studies using RFID/GPS logs demonstrate that when tagging coverage approaches full penetration, shrinkage detection improves and reconciliation work declines because fewer items move unobserved. Empirical models also show that IoT-enabled visibility stabilizes ordering processes, lowering the amplification of demand signals that results from uncertain stock positions. These findings collectively position IoT intensity as a statistically robust antecedent to visibility performance, with measurable effects on both the speed of information and the correctness of inventory states (Singal, 2022).

Blockchain Deployment Intensity and Inter-Firm Trust

The supply chain literature increasingly conceptualizes blockchain deployment intensity as a measurable trust infrastructure that strengthens transparency by reshaping how inter-firm data is recorded, validated, and shared. Rather than viewing blockchain adoption as a simple yes–no decision, empirical studies treat intensity as the depth and breadth of ledger use across transactions, partners, and operational processes (De Haes et al., 2019).

Figure 5: Blockchain Deployment Intensity



This quantitative framing aligns with the core argument that blockchain's value in supply chains lies in its distributed architecture, where multiple stakeholders maintain synchronized records and jointly validate new entries through consensus. When deployment is shallow—limited to pilot trails or a narrow product segment—the ledger functions as a supplementary log with minimal influence on network trust. When deployment becomes wide—embedded into procurement, logistics handoffs, and compliance reporting—the ledger begins to substitute for fragmented bilateral records, reducing information asymmetry across tiers. Survey research and case-based quantitative studies show that firms experiencing higher deployment intensity report stronger confidence in shared information, fewer disputes over transaction histories, and improved willingness to collaborate because verification is no longer dependent on a single firm's database (Makhdoom et al., 2022; Mominul & Zaki, 2024; Roy & Praveen, 2024). These patterns support the treatment of blockchain intensity as an independent capability construct in supply chain models, often linked to information integrity and relational trust outcomes. Across sectors such as food traceability, pharmaceutical anti-counterfeit operations, and high-value manufacturing, blockchain is operationally described as a "digital trust spine" that ties event data to an audit-ready record (Rahman et al., 2024; Saba & Hasan, 2024). This makes deployment intensity a statistically meaningful predictor, since the ledger's trust effects appear only when a substantial share of operations is conducted through the shared infrastructure rather than around it.

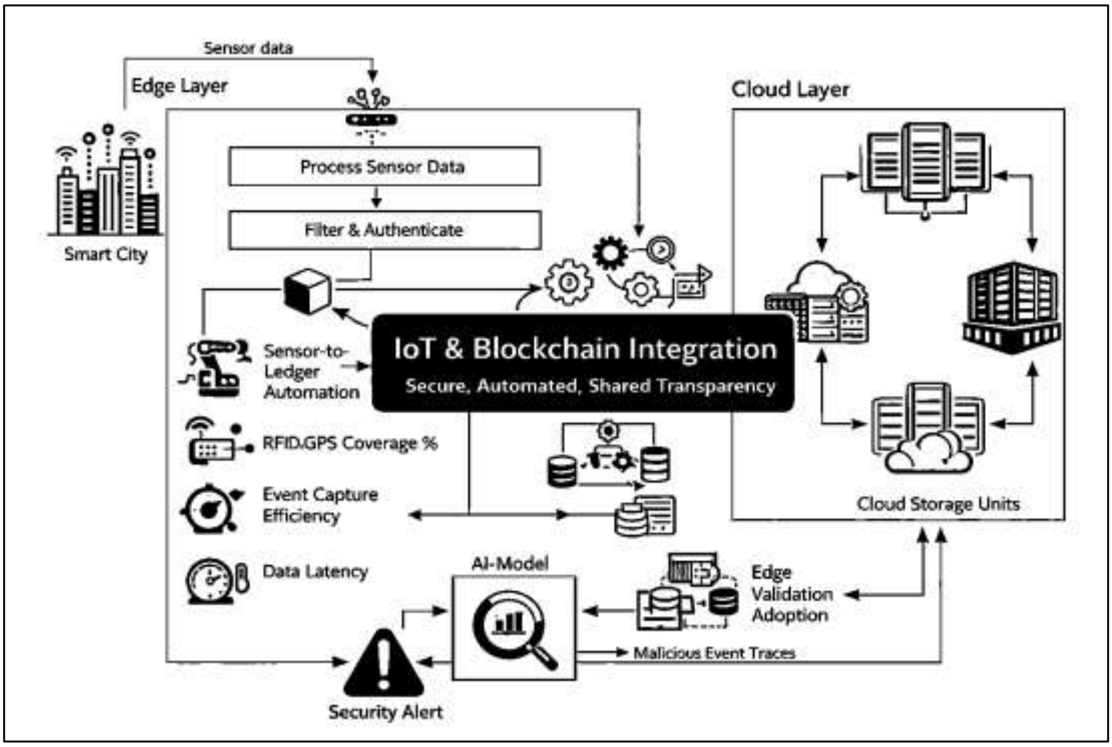
Quantitative research offers consistent operational measures for blockchain deployment intensity that enable cross-study comparability (Schuhmann & Eichhorn, 2019; Shaikat & Zaman, 2024; Sudipto & Hasan, 2024). One central indicator is the proportion of supply chain transactions recorded on-chain, which captures how extensively the ledger is used for routine operational events such as purchase orders, shipping confirmations, and custody transfers (Haider & Sai Praveen, 2024; Zobayer & Sabuj Kumar, 2024). Closely related is smart contract utilization, measured by the frequency or share of transactions governed by automated ledger-based rules rather than by manual approval or separate enterprise systems. Studies also measure intensity through consensus node participation, reflecting the degree to which stakeholders actively maintain and validate the distributed ledger instead of relying on a small subset of controlling participants (Zulqarnain & Zayadul, 2024). Another commonly used proxy is observable reduction in disputes or chargeback incidents, interpreted as an outcome-aligned indicator of ledger penetration into transactional governance. These measures are typically combined into multi-item survey constructs or extracted from platform log data, producing intensity indices that reflect both technical immersion and organizational reliance (Panayides, 2019). Empirical work highlights that measurement quality improves when intensity indicators incorporate network characteristics, such as the number of partners contributing data, the continuity of on-chain records across tiers, and the scope of products included in the ledger. Across reviewed studies, these operational measures are used to distinguish pilot-level adoption from operational-scale deployment, allowing statistical tests to identify whether stronger ledger penetration corresponds to stronger transparency and trust outcomes. This approach also supports modeling blockchain intensity as a scalable variable that interacts with contextual factors such as supply chain complexity and regulatory pressure (Asif et al., 2022).

The evidence base consistently links higher blockchain deployment intensity to measurable improvements in data integrity and auditability. Integrity effects are observed through lower rates of record mismatch between partners, reduced need for manual reconciliation, and fewer opportunities for retroactive manipulation of transaction histories. Studies demonstrate that as more events and documents are committed to a tamper-evident ledger, the probability of undetected alteration declines, strengthening confidence that the shared data mirrors authentic supply chain activity (Leventis et al., 2018). Auditability gains are often quantified through shortened verification cycles, improved traceability completeness, and higher success rates in compliance checks because historical records can be retrieved and validated without cross-checking scattered systems. In provenance-intensive industries, higher deployment intensity is associated with faster product-origin confirmation and narrower, more accurate recall processes. Several studies show cost-related benefits connected to these integrity and auditability improvements, particularly the reduction of reconciliation labor, paperwork overhead, and dispute-resolution expenses. Importantly, the literature does not treat these outcomes as automatic; rather, it presents them as scaling effects where integrity and auditability strengthen progressively as on-chain transaction share rises and as more partners participate actively (Rikhardsson & Dull, 2016). In this sense, blockchain intensity is not only a technical metric but also a governance indicator, revealing how much of the supply chain's accountability structure has shifted from bilateral trust to shared verification. These empirical patterns reinforce the role of blockchain intensity as a robust antecedent to data credibility and verifiable transparency in quantitative supply chain frameworks.

IoT–Blockchain Integration Capability as an Interaction Construct

The integration of IoT and blockchain is widely framed in the literature as a compound digital capability that is analytically distinct from adopting either technology alone. Quantitative supply chain studies treat this integration as a second-order latent construct because it represents an orchestrated bundle of sensing, data transmission, verification, and shared governance routines that collectively enable real-time transparency (Kaewunruen et al., 2020). In empirical models, IoT provides continuous event data about physical flows, while blockchain supplies a distributed trust substrate that makes those events auditable and resistant to manipulation. Integration capability therefore captures how effectively supply chain actors connect device-generated data to a shared ledger so that multiple firms can trust, interpret, and act on the same stream of real-time evidence. Studies that model integration as a higher-order construct emphasize that transparency does not rise proportionally with separate IoT or blockchain investments unless there is functional coupling between them through middleware, standardized data models, and joint governance rules (Samuel et al., 2019). This coupling is especially important in multi-tier settings, where heterogeneous partners would otherwise interpret sensor data differently or store it in siloed platforms. Quantitative research also highlights that integration is not only a technical architecture but a relational capability, because firms must align data-sharing rights, ledger access policies, and custody validation rules for the shared transparency system to work. As a result, surveys and platform studies operationalize integration capability through multiple observable indicators and validate it as a stable explanatory variable that predicts transparency beyond the independent effects of IoT intensity and blockchain intensity (Mircea et al., 2022).

Figure 6: Integrated IoT and Blockchain Architecture



The literature provides convergent operational indicators that quantify the strength of IoT–blockchain integration. A commonly used measure is the extent of sensor-to-ledger automation, reflecting how many physical events captured by IoT devices are written to blockchain records without manual intervention (Patabendige & Jayawardane, 2017). This indicator captures "cyber-physical closure," showing whether the ledger mirrors real-world logistics in near real time. Another key indicator is interoperability across partners, which reflects how well different organizations' devices, platforms, and ledger nodes exchange standardized data across tiers. Empirical work often builds interoperability indices from measures such as common data standards, protocol compatibility, and percentage of partners connected to the same traceability workflow. Edge-validation adoption appears as an additional indicator, emphasizing that integration capability rises when data is filtered and authenticated near the source prior to ledger entry, reducing noise, spoofing risk, and bandwidth constraints. Finally, studies incorporate on-chain and off-chain architectural efficiency indicators, recognizing that effective integration depends on balancing immutable recording with scalable storage and processing. Quantitative papers interpret these indicators jointly because sensor-to-ledger automation without interoperability yields narrow visibility, and interoperability without edge validation may multiply low-quality data across the ledger (Khan et al., 2021). The combined measurement approach allows researchers to represent integration capability as a multi-item construct that reflects how tightly IoT sensing and blockchain governance are fused within actual supply chain operations.

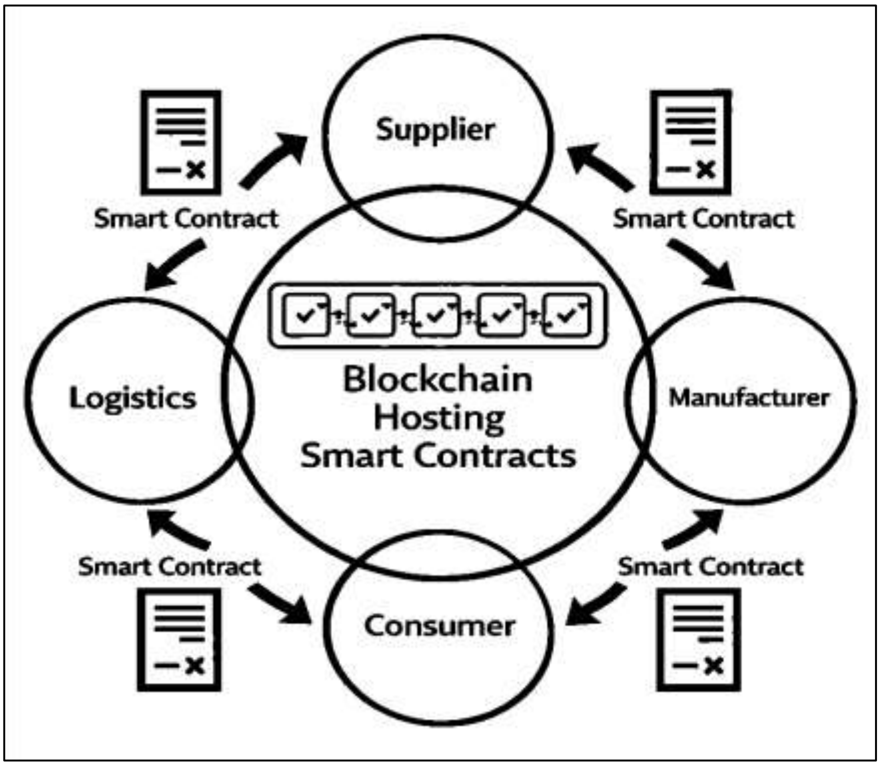
Smart Contracts and Automated Compliance

Smart contracts are widely discussed in supply chain research as programmable agreements embedded in blockchain platforms that execute predefined rules automatically once verified conditions are met. The literature treats them not simply as technical scripts, but as measurable automation layers that convert transactional logic into tamper-evident, self-enforcing workflows. In quantitative studies, this automation role positions smart contracts as an extension of blockchain's trust infrastructure, because they reduce dependence on manual approvals and bilateral reconciliation (Rejeb et al., 2021). Empirical work in logistics, procurement, and supply chain finance shows that smart contracts standardize how handoffs, payments, and compliance checks occur among partners, thereby reducing variability created by human discretion or fragmented institutional routines. Researchers emphasize that automation becomes analytically visible when smart contracts are embedded across repetitive operational events such as shipment release, custody transfer, milestone confirmation, and penalty enforcement. When these processes are encoded, contracts become "event-reactive," meaning that the system responds directly to recorded supply chain states rather than to delayed reports. The literature also highlights that smart contracts strengthen procedural trust by making transactional conditions transparent to all authorized stakeholders and by ensuring that execution is consistent regardless of actor power or geography (Panarello et al., 2018). Quantitative frameworks therefore examine smart contracts as a capability that shapes speed, predictability, and accountability in supply chain governance. Across sectors including food traceability, pharmaceuticals, and global trade settlement, evidence converges around the view that smart contracts function as a measurable governance mechanism whose value appears through observable improvements in process efficiency and dispute stability once a meaningful scale of automation is achieved (Ghimire et al., 2022).

Prior quantitative research offers a relatively consistent set of indicators for measuring smart-contract automation in supply chains. A central variable is the automated trigger rate, which captures how frequently smart contracts execute operational actions—such as confirming delivery, releasing ownership, or applying penalties—without manual intervention. This indicator reflects the level of functional reliance on the smart-contract layer rather than on traditional paperwork-based operations (Zhu et al., 2020). Payment release time is another common measure, typically framed as the elapsed period between event confirmation and settlement completion. Studies in supply chain finance show that shorter release times correspond to higher automation depth because the ledger provides immediate verification of milestones. Compliance verification cycle time also appears frequently, representing how long it takes to validate regulatory or contractual requirements such as temperature conformity, authenticity checks, or customs clearance documentation. This measure is particularly important because many supply chains are regulated by time-sensitive standards, meaning that verification delays directly affect product viability and risk exposure. Finally, dispute frequency is used as a governance outcome-aligned indicator, showing how often transactional disagreements arise per standardized volume of activity (Ayan et al., 2022). Researchers interpret declines in dispute frequency as evidence that automation reduces ambiguity in obligations and limits retroactive contestation of records. The literature commonly integrates these variables into composite indices of automation intensity or uses them directly in regression and SEM models to evaluate smart contracts as predictors of speed, cost efficiency, and trust stability. Together, these measures provide a quantitatively tractable representation of automation in real supply chain environments (Ma et al., 2022).

The empirical record links smart-contract automation to measurable improvements in exception handling speed, settlement efficiency, and dispute reduction across diverse supply chain settings. Quantitative evidence indicates that automated triggering accelerates response to deviations because contractual logic is executed immediately after a verified event is recorded, rather than after manual inspection or multi-party confirmation. Studies focusing on logistics handoffs report shorter settlement windows where delivery confirmation, payment initiation, or penalty application is performed automatically, reducing multi-day administrative lag to near-real-time cycles (Lohmer et al., 2022). Cost-related outcomes appear through reductions in manual inspection labor, paperwork processing, and reconciliation tasks. When smart contracts govern verification points, firms spend less time matching invoices to shipment histories or negotiating responsibility after exceptions, and these savings show up statistically as lower administrative overhead per transaction. Dispute reduction is one of the most robust findings in recent quantitative research: immutable execution histories reduce interpretive gaps about what occurred, when it occurred, and whether contractual conditions were satisfied. Evidence from inter-firm networks demonstrates declines in chargebacks and formal disputes where smart contracts govern large shares of procurement or logistics milestones. The literature also notes that these outcomes scale with automation intensity; partial deployment yields modest benefits, while deep embedding across multiple workflow stages produces sustained improvements in speed and dispute stability (Maryniak et al., 2021). Across these studies, smart contracts emerge as a measurable governance technology that tightens the link between verifiable events and contractual consequences, producing consistent empirical patterns in operational performance metrics.

Figure 7: Smart Contacts for Automated Supply Chains



Quantitative scholarship on smart contracts in supply chains relies on a blend of causal and process-oriented analytical strategies aimed at isolating automation effects. Process mining combined with regression analysis is frequently used in settings where event logs are available, such as IoT-enabled logistics systems or blockchain-based trade platforms (Aheleroff et al., 2021). Process mining reconstructs actual workflow sequences from time-stamped records, enabling researchers to compare exception paths, bottleneck durations, and settlement cycles before and after smart-contract automation. Regression models then estimate how changes in trigger rates, verification cycles, or settlement times associate with performance outcomes such as cost savings or dispute declines. Event-study approaches appear in supply chain finance and consortium-led traceability trials, where researchers examine performance shifts around the introduction of smart contracts as a discrete governance intervention (Erevelles et al., 2022). Difference-focused designs compare transaction efficiency or dispute rates across time windows or across adopting versus non-adopting partners, supporting causal interpretation of automation impacts. Structural equation modeling is also prominent when researchers use survey data to test trust-centered mechanisms; these models typically position smart-contract automation as an antecedent of perceived transparency, procedural trust, or information quality, which then explain reductions in disputes and reconciliations. Across methods, the literature shows convergence: automation intensity is statistically related to faster exception handling and lower dispute incidence, and these relationships remain stable after controlling for supply chain complexity and regulatory exposure. The methodological diversity strengthens the quantitative grounding of smart contracts as an empirically observable layer of automated compliance and transactional governance .

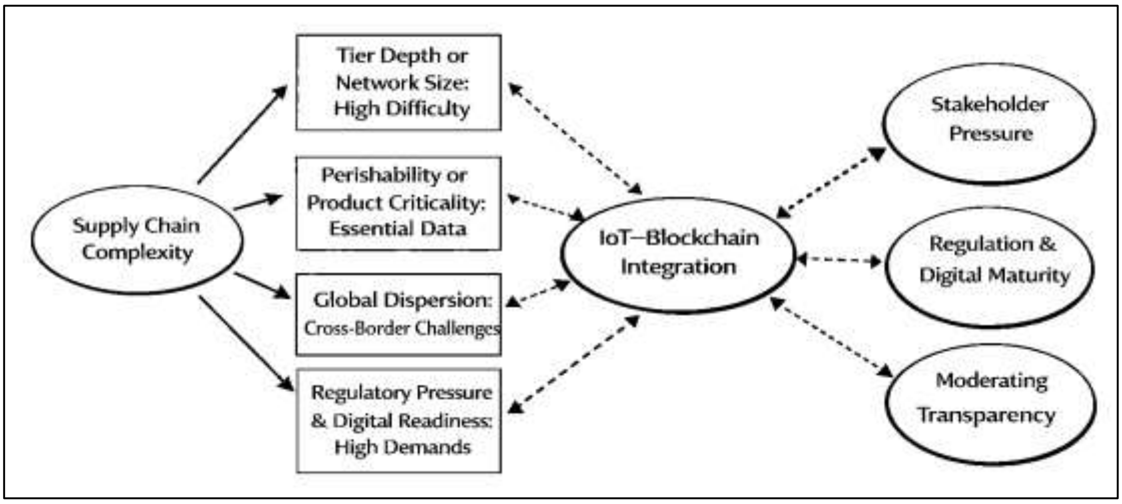
Contextual Moderators in Quantitative Studies

Quantitative transparency research repeatedly shows that supply chain complexity alters how strongly digital integration improves real-time transparency. Complexity is usually expressed through tier depth, network size, and heterogeneity of partners, creating more handoffs where information can be delayed, distorted, or withheld (Aheleroff et al., 2021). Empirical studies on transparency note that visibility commonly weakens beyond tier-1 suppliers because lower-tier actors are harder to identify, monitor, and technologically align, which increases information asymmetry and reduces end-to-end traceability. In complex networks with many sub-tiers, the same IoT–blockchain integration capability that performs well in a shallow chain yields smaller transparency gains because sensor data and ledger records must traverse more organizational boundaries, standards, and governance regimes. Quantitative models often capture this moderation by showing that integration effects are strongest when the network has fewer tiers or when tier mapping is mature, while deeper tier structures dampen coefficients by creating missing nodes and fragmented data ownership. Cross-industry evidence reinforces this pattern: electronics, apparel, and multi-component manufacturing supply chains typically exhibit higher tier depth and supplier churn, so transparency improvements depend heavily on broad partner onboarding and interoperable data models (Maryniak et al., 2021). In contrast, more vertically coordinated chains or those with limited tiers show faster translation from technology integration into measurable transparency improvements. The broader transparency literature also frames complexity as a driver of stakeholder pressure and audit burden, meaning that complex networks face both higher need for transparency and higher friction in achieving it. Overall, the statistical role of complexity is consistent: it shapes the slope of the integration–transparency relationship by multiplying coordination requirements, thereby changing how quickly and how fully real-time transparency becomes observable across tiers (Lohmer et al., 2022).

Perishability and product criticality are among the most stable moderators in quantitative studies because they heighten both the operational value of real-time information and the penalty for opacity. Empirical work in food, fresh agriculture, vaccines, and temperature-sensitive pharmaceuticals shows that real-time transparency has a larger measurable effect when products degrade quickly or carry safety risk, since short detection windows make timeliness and condition accuracy decisive (Ma et al., 2022). In these sectors, IoT-enabled condition monitoring supplies continuous evidence about temperature excursions, handling shocks, or spoilage trajectories, while blockchain-based records preserve a verifiable chain of custody. Quantitative models comparing perishable versus non-perishable categories show stronger integration effects on transparency dimensions such as update timeliness, traceability completeness, and audit-ready provenance. The moderation logic is straightforward in the empirical literature: as perishability or criticality rises, firms increase sensor density, event frequency, and enforcement of immutable documentation, which strengthens the translation of integration capability into transparency outcomes (Ayan et al., 2022). Non-perishable or low-risk goods display weaker coefficients because monitoring intensity is lower and delays are less damaging, so integration produces smaller marginal transparency gains. Cross-sector comparisons reinforce this difference: cold-chain logistics and regulated health products repeatedly outperform durable-goods supply chains on measurable transparency improvements when similar digital architectures are applied (Zhu et al., 2020). Thus, perishability and criticality act as amplifiers, increasing both the intensity of data capture and the organizational willingness to share and validate that data in real time.

Global dispersion, typically operationalized as the share of cross-border nodes or the international sourcing ratio, is another repeated moderator because it changes the institutional and infrastructural environment in which transparency systems operate. Quantitative studies of international logistics and multi-country sourcing show that dispersed supply chains face longer lead times, more custody transfers, and greater regulatory variation, all of which raise the probability of information gaps. In these contexts, integration capability can deliver substantial transparency gains when it standardizes event capture and secures a shared provenance record across borders (Huo et al., 2022). However, dispersion can also weaken integration effects when digital readiness and data standards vary widely among countries and partner types. Empirical comparisons often reveal a mixed but patterned moderation: integration–transparency coefficients are stronger in globally dispersed chains that have high partner digitization and standardized onboarding, but weaker in dispersed chains where infrastructure gaps or fragmented customs/documentation regimes prevent continuity of sensing and ledger recording. This helps explain why international e-commerce and container shipping studies stress interoperability and multi-jurisdiction governance as prerequisites for realizing transparency at scale (Ghimire et al., 2022). By contrast, locally concentrated supply chains show more stable but smaller transparency increments because baseline coordination and institutional trust are already higher. Taken together, the literature treats international dispersion as a boundary-expanding moderator that can either magnify transparency benefits through higher need and broader verification value, or dampen them through uneven digital capacity across borders.

Figure 8: Determinants of Supply Chain Transparency

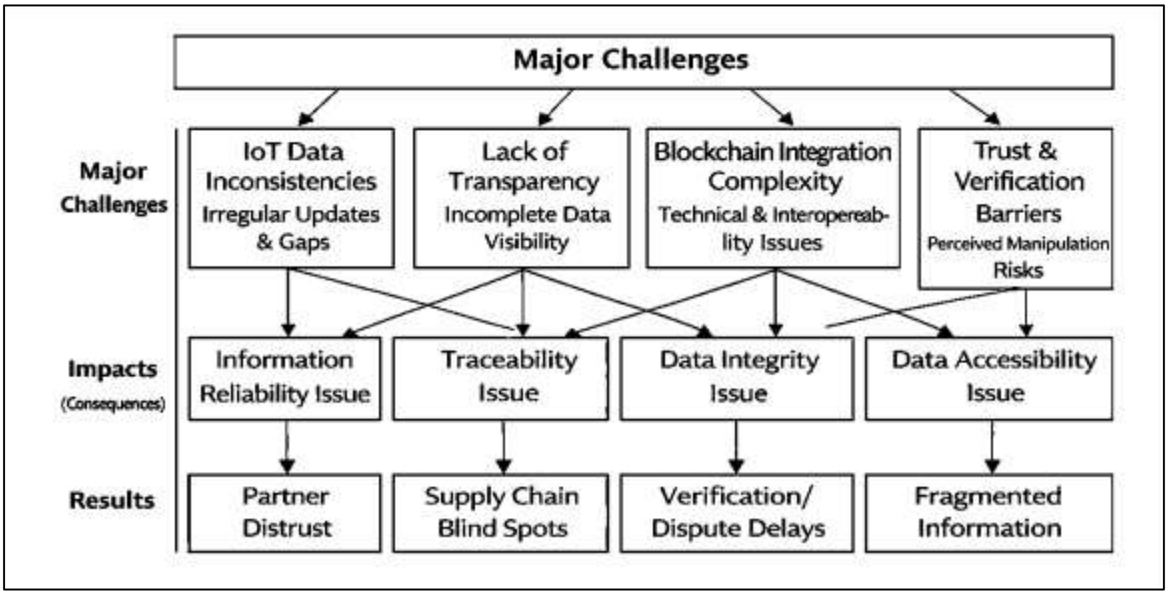


Regulatory pressure and digital readiness maturity are consistently modeled together because they jointly determine whether integration capability converts into measurable, audit-recognizable transparency (Panarello et al., 2018). Regulatory intensity is proxied in quantitative work by sectoral compliance burdens such as food safety traceability rules, pharmaceutical serialization mandates, customs documentation requirements, and ESG disclosure expectations. Studies show that when regulatory intensity is high, transparency gains from IoT–blockchain integration are stronger because firms are compelled to document provenance, condition, and custody in standardized ways, making the resulting data more complete and more frequently verified. High-pressure environments also increase stakeholder access demands, so transparency becomes a visible performance variable rather than a back-office feature. Digital readiness maturity, by contrast, captures the internal and network-level capability to deploy sensors, integrate platforms, and maintain ledger participation (Rejeb et al., 2021). Empirical models show that readiness conditions the integration–transparency relationship by determining data quality, interoperability, and adoption depth across partners. High readiness environments produce stronger coefficients because automation and shared validation operate continuously; low readiness environments show weaker effects because sensing remains partial, data entry is manual, or ledger nodes are sparsely used. Cross-sector evidence aligns with this view: highly regulated, digitally mature chains (pharma, export-grade food, advanced manufacturing) show statistically larger transparency impacts than lightly regulated or low-maturity sectors (Khan et al., 2021). In sum, regulatory intensity raises the demand and measurability of transparency, while digital readiness controls the supply of reliable integrated data, and together they shape the observed strength and stability of integration effects.

Data Sources for Testing Integration–Transparency Relationships

Quantitative studies examining the relationship between IoT–blockchain integration and real-time supply chain transparency rely heavily on survey-based measurement because key constructs such as transparency, visibility, trust, and information quality are typically latent and perceptual. The literature treats transparency as a multi-dimensional capability that is inferred through validated scales capturing how accurately, quickly, and credibly supply chain actors can observe and verify product and transaction flows (Samuel et al., 2019). Visibility scales are often adapted from information-sharing and supply chain coordination research, where respondents rate the extent of end-to-end tracking, timeliness of shared updates, and clarity of upstream and downstream status information. Information quality scales complement these measures by capturing accuracy, completeness, relevance, and consistency of shared data across partners, reflecting whether real-time signals support decision-making rather than simply increasing data volume. Trust scales, especially inter-firm and procedural trust measures, capture the perceived reliability of partners and the credibility of shared records, making them central for blockchain-enabled contexts where transparency depends on multiparty verification. Empirical papers commonly integrate these scales into structural models where IoT intensity predicts real-time data flow, blockchain intensity predicts credibility, and integration capability strengthens the combined effect on transparency (Kaewunruen et al., 2020). Survey instruments also allow researchers to capture integration maturity through items reflecting interoperability, automation of event-to-ledger logging, and perceived ease of cross-partner data validation. Across sectors, these scales are refined through pilot tests and validation checks to ensure they behave consistently in different supply chain environments. The repeated use of similar constructs in logistics, sustainability, and traceability studies provides a stable methodological pathway for building quantitative models that connect integration capability with transparency outcomes using latent-variable analysis (Rikhardsson & Dull, 2016).

Figure 9: Supply Chain Transparency Challenges



Alongside surveys, objective supply chain data sources provide an increasingly important empirical base for testing integration–transparency relationships. The literature uses IoT logs as direct evidence of real-time visibility performance, capturing time-stamped location updates, condition readings, and custody-transfer events at shipment or asset level (Mekonnen et al., 2021). These logs are analyzed for indicators such as update frequency, delay between event occurrence and digital registration, and completeness of monitoring across journey segments. Blockchain ledger records serve as complementary objective sources that document immutable transaction trails, including provenance statements, handoff confirmations, compliance attestations, and smart-contract executions. When ledger data is accessible, researchers assess transparency through auditability of histories, continuity of recorded custody, and the extent to which discrepancies are resolved through shared records rather than manual reconciliation (Leventis et al., 2018). ERP timestamps and shipment histories add another layer of objective data by providing operational baselines before and after digital integration, enabling comparisons in process latency, inventory accuracy, and recall precision. Event datasets are especially useful in cold chains, cross-border logistics, and e-commerce fulfillment because they allow transparency to be observed as an outcome tied to real operations rather than only perceptions. The literature highlights that objective sources improve construct robustness when linked together: IoT provides real-time sensing, ERP provides transactional context, and blockchain preserves verifiable histories (Asif et al., 2022). This triangulation produces richer operational representations of transparency and supports tests using regression, panel models, process mining, or hybrid causal designs based on real supply chain events.

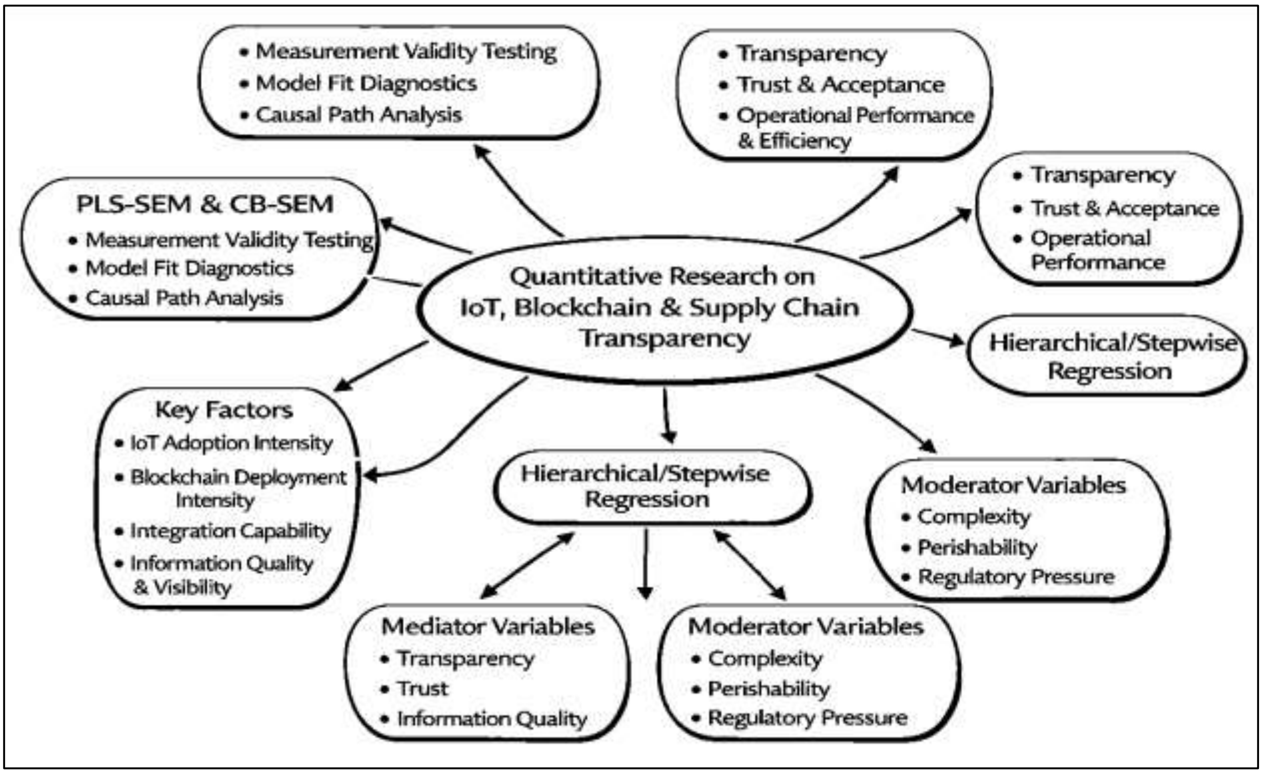
Empirical studies provide clear guidance on constructing variables that align integration capability with transparency outcomes. For survey-based work, researchers typically operationalize IoT intensity through the breadth of sensor coverage, depth of monitoring across tiers, and perceived real-time data availability, while blockchain intensity is operationalized through the scope of on-chain transaction use, perceived immutability reliance, and smart-contract deployment (Panayides, 2019). Integration capability is then constructed as either a second-order latent variable or a composite reflecting automation of sensor-to-ledger logging, interoperability between platforms, and shared governance of data access. Transparency outcomes are constructed dimensionally, combining indicators for timeliness, traceability completeness, data integrity, and stakeholder accessibility. For objective datasets, variable construction often begins with event preprocessing: cleaning sensor anomalies, synchronizing multi-source timestamps, and mapping shipment IDs across IoT, ERP, and ledger systems (Schuhmann & Eichhorn, 2019). Researchers then compute operational proxies such as the share of events recorded without gaps, mean delay between physical and digital events, variance of update intervals, discrepancy rates between partner records, and cycle times for verification or dispute closure. Many papers emphasize choosing variables that represent both real-time flow and trustworthy history, because transparency requires current visibility and credible provenance. Cross-sector comparisons show similar construction logics even when datasets differ, suggesting that integration–transparency testing benefits from consistent operational definitions tailored to the data environment.

Quantitative Modeling Approaches in Prior Research

Quantitative research on IoT, blockchain, and supply chain transparency is strongly characterized by the use of structural equation modeling, particularly PLS-SEM and CB-SEM, because the central variables are latent, multidimensional, and relational (Makhdoom et al., 2022). Transparency, visibility, trust, integration capability, and information quality are rarely observable directly; instead, they are inferred through multi-item measures that require simultaneous tests of measurement validity and structural relationships. PLS-SEM is frequently selected in technology-enabled supply chain studies due to its suitability for complex models, smaller-to-moderate sample sizes, and formative or higher-order constructs. CB-SEM appears in studies emphasizing confirmatory theory testing and model-fit diagnostics, especially where constructs are reflective and measurement assumptions are well-established (De Haes et al., 2019). Within these SEM studies, recurring path structures show a stable logic: IoT adoption intensity predicts timeliness and granularity of visibility, blockchain deployment intensity predicts integrity-related transparency and inter-firm trust, and integrated IoT–blockchain capability exerts a stronger combined influence on overall transparency than either technology alone. Many models position transparency as a mediator connecting digital capability to operational performance, indicating that technology improves outcomes primarily when it produces measurable real-time transparency. Trust and information quality also appear as mediators in SEM frameworks, reflecting a consistent empirical view that real-time data becomes valuable only when partners accept it as reliable (Singal, 2022). Recent work combining SEM with intelligent analytics further reinforces SEM's dominance by using it to validate causal pathways while using advanced methods to explore nonlinear patterns. Overall, SEM remains the most common quantitative mechanism for testing how cyber-physical sensing and distributed ledger governance translate into transparency and performance improvements in multi-tier supply chains.

Another prominent modeling tradition in this literature is hierarchical or stepwise regression, mainly used to test interaction effects and incremental explanatory power. This approach is especially common in studies that want to compare additive versus synergistic transparency gains. Researchers typically estimate baseline models with control variables and main effects of IoT intensity and blockchain intensity, then add an interaction representation of integration capability to determine whether combined adoption yields a statistically larger transparency impact (Carrasco & Romi, 2022). Hierarchical regression is attractive because it provides clear effect decomposition, interpretable change in explained variance, and a straightforward way to test moderation without requiring full latent-variable modeling. Empirical work using this approach shows a consistent pattern: IoT intensity contributes more strongly to real-time visibility speed and event granularity, blockchain intensity contributes more strongly to record integrity and trust stability, and the interaction between them contributes to higher overall transparency by converting raw sensor signals into verifiable provenance. Researchers also use hierarchical regression to test contextual moderators such as complexity, perishability, and regulatory intensity, demonstrating how these factors shift the size and direction of integration effects (Li et al., 2018). In many cases, the regression stream complements SEM evidence by showing synergy through interaction coefficients in operational or survey datasets, even when constructs are simplified into composite scores. Thus, hierarchical regression serves as a core quantitative strategy for verifying whether integration effects exceed the sum of separate IoT and blockchain effects, and for estimating how environmental conditions reshape those effects across industries (Zhu et al., 2015).

Figure 10: Modelling Supply Chain Transparency Mechanisms



METHOD

Research Design

This study employed a cross-sectional, explanatory quantitative research design to test the statistical relationships between IoT–blockchain integration capability and real-time supply chain transparency. A positivist stance guided the inquiry, and hypotheses were derived from information processing theory and digital trust perspectives to explain how integrated sensing and distributed validation affected transparency outcomes. Data were gathered through a structured instrument that captured both technological deployment intensity and transparency dimensions, enabling the estimation of direct, indirect, and interaction effects within a single empirical framework. The unit of analysis was the firm and its supply chain operations, and the design was selected because it supported latent-variable modeling of complex constructs such as integration capability and real-time transparency in multi-tier and cross-border contexts.

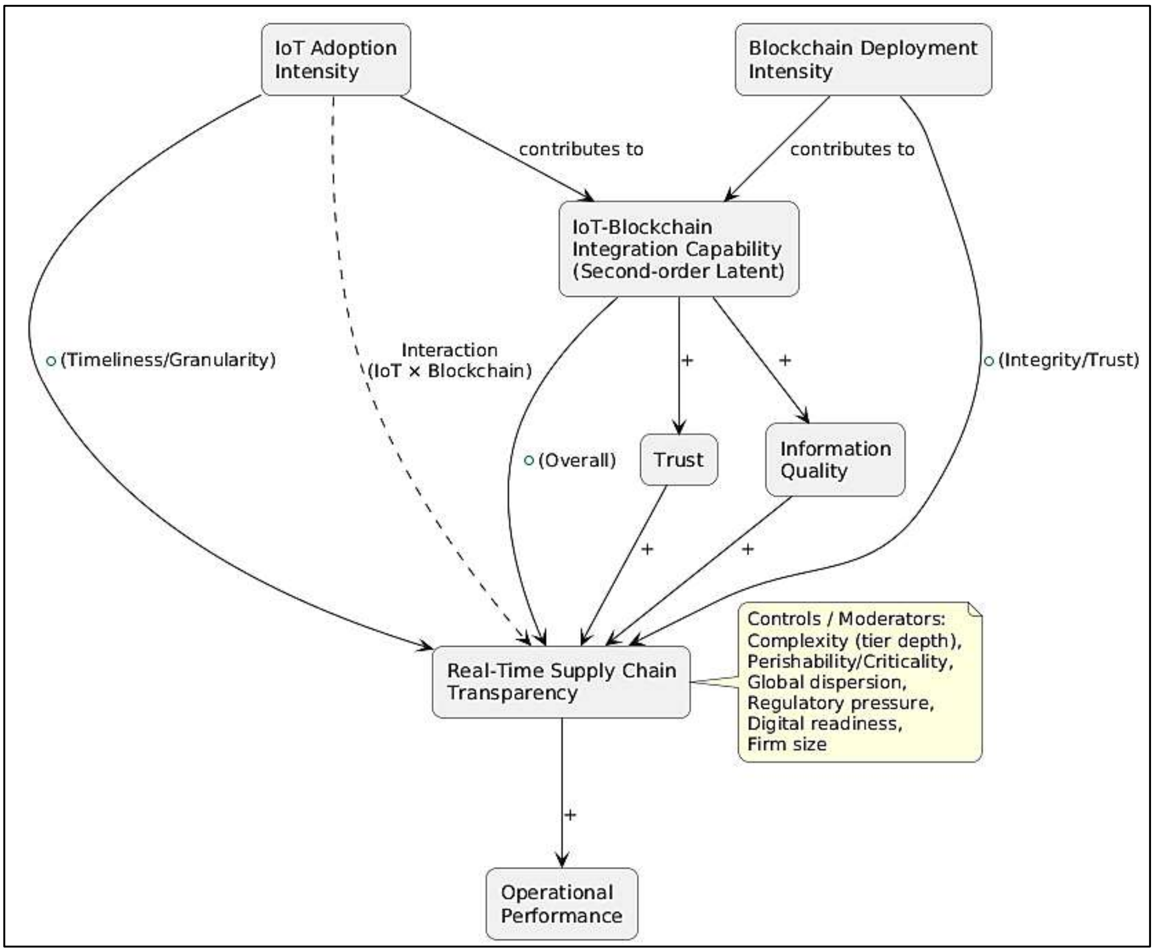
Population

The population comprised supply chain–active firms operating in sectors where real-time transparency was operationally critical and often compliance-driven. Firms were drawn from food and agro-processing chains, pharmaceutical and healthcare distribution networks, apparel and export-oriented manufacturing systems, and e-commerce logistics providers. Organizations were included if they had implemented IoT-based tracking, blockchain-based traceability, or a combined IoT–blockchain platform in at least one workflow or product line for a sufficient operational period to generate observable transparency practices. Respondents were professionals directly responsible for visibility, traceability, logistics coordination, or technology adoption decisions, including supply chain managers, operations leads, digital transformation managers, and IT or logistics coordinators. A purposive sampling approach was applied to ensure that only firms with real implementation exposure were represented and that the sample reflected both domestically concentrated and internationally dispersed supply chains.

Variables and Measurement Framework

The study measured three predictor constructs, one primary outcome construct, and several contextual controls and moderators. IoT adoption intensity was treated as a latent predictor reflecting the depth and breadth of sensing infrastructure within supply chain operations, and it was measured through indicators capturing the extent of sensor deployment across warehousing and transport, RFID and GPS tagging coverage, frequency of real-time event capture, and perceived capability for continuous monitoring.

Figure 11: Methodology of this study



Blockchain deployment intensity was modeled as a second latent predictor representing the operational embedding of distributed ledger use, and its indicators captured the extent to which supply chain transactions were recorded on-chain, the maturity of smart-contract use in executing operational rules, the breadth of partner participation in ledger validation, and the perceived reliance on immutable records for traceability. IoT–blockchain integration capability was specified as a second-order latent construct, measured through observable indicators reflecting automation of sensor data entry into the ledger, interoperability across supply chain partners through standardized data models, the level of edge or source-level validation prior to ledger recording, and architectural efficiency in balancing on-chain immutability with off-chain scalability. Real-time supply chain transparency served as the core outcome construct and was measured as a multidimensional latent variable represented by timeliness of visibility, completeness of traceability across tiers, integrity and trustworthiness of shared data, and accessibility and auditability of records for relevant stakeholders. Supply chain complexity, product perishability or criticality, international sourcing ratio, regulatory intensity, firm size, and digital readiness maturity were incorporated as controls and moderators to isolate the net explanatory effects of integration capability on transparency. All latent constructs were measured using multi-item five-point Likert scales adapted from validated measurement instruments in digital supply chain and transparency research.

Analytical Techniques and Statistical Procedures

Data analysis proceeded through a structured statistical sequence. Responses were first screened for missing values, outliers, and response-pattern bias, and cases with excessive missingness were removed while minor gaps were handled through standard imputation consistent with quantitative survey practice. Descriptive statistics and correlation matrices were then computed to establish baseline relationships and to evaluate multicollinearity prior to model estimation. A PLS-SEM measurement model was estimated to validate all latent constructs because the framework included a second-order integration capability construct and required interaction testing, and this method was appropriate for handling complex models with both reflective and higher-order variables. Reliability and convergent validity were examined before moving to structural estimation. The structural model tested the hypothesized direct paths linking IoT intensity to timeliness and granularity aspects of transparency, blockchain intensity to integrity and trust aspects of transparency, and integration capability to overall transparency, after which transparency was modeled as an explanatory mediator toward operational performance proxies such as inventory accuracy, recall precision, delivery reliability, and dispute frequency. Synergistic effects were evaluated by estimating the interaction influence of IoT and blockchain intensities on transparency and by testing whether the second-order integration construct explained additional variance beyond main effects. Indirect effects through trust and information quality were assessed as mediating mechanisms using bootstrapping with a large resample count to produce stable confidence intervals. Robustness checks were performed by re-estimating alternative specifications using hierarchical regression with composite indices and by testing for common-method bias through full collinearity diagnostics and marker-variable procedures.

Reliability and Validity

Reliability and validity were established using multiple complementary criteria. Internal consistency reliability for each latent construct was confirmed through Cronbach's alpha and composite reliability values meeting accepted thresholds, while indicator reliability was supported by sufficiently strong item loadings on their intended constructs. Convergent validity was verified by average variance extracted values exceeding benchmark levels, indicating that each construct captured adequate variance from its indicators. Discriminant validity was confirmed through HTMT ratios and cross-loading comparisons, ensuring that constructs such as transparency, visibility, trust, IoT intensity, blockchain intensity, and integration capability remained empirically distinct. Content validity was reinforced by adapting items from widely cited quantitative supply chain studies and refining them through expert review to ensure relevance to IoT–blockchain transparency contexts. Construct validity was further supported by validating the second-order integration capability using a repeated-indicator approach, demonstrating that automation, interoperability, validation maturity, and architectural efficiency coherently represented a single higher-order capability.

FINDINGS

Descriptive Analysis

After data screening, the final usable sample comprised 312 firm-level responses, indicating a satisfactory completion rate for cross-sectional modeling. Sectoral representation showed balanced coverage of transparency-critical industries, with food and agro-processing firms forming the largest share, followed by e-commerce logistics, manufacturing/apparel export chains, and pharmaceuticals. Respondents were predominantly mid- to senior-level supply chain and digital operations professionals, confirming adequate informant relevance. Most firms fell within medium to large size categories, and a substantial proportion reported cross-border operations, supporting the study's global transparency focus. Baseline digital readiness appeared moderate to high across the sample, suggesting that technology-enabled visibility and traceability practices were already present to varying degrees. Descriptive construct statistics indicated that IoT adoption intensity and blockchain deployment intensity were both above scale midpoints, while integration capability showed comparatively lower dispersion, implying uneven maturity of full sensor-to-ledger coupling. Transparency dimensions showed the strongest baseline for timeliness and traceability completeness, whereas integrity/trust and accessibility/auditability exhibited wider variance, consistent with multi-tier and multi-partner differences. Skewness and kurtosis values for all indicators remained within acceptable behavioral thresholds for PLS-SEM estimation, supporting the planned inferential procedures.

Table 1. Sample profile of participating firms

Category	Subgroup	n	%
Sector	Food & agro-processing	98	31.4
	Pharmaceuticals & healthcare	56	17.9
	Manufacturing/apparel exports	72	23.1
	E-commerce logistics	86	27.6
Respondent role	Supply chain/operations manager	124	39.7
	Logistics/warehouse lead	78	25.0
	Digital transformation/IT lead	64	20.5
	Procurement/compliance manager	46	14.7
Firm size	Small (<100 employees)	64	20.5
	Medium (100–499)	138	44.2
	Large (≥500)	110	35.3
Operating scope	Domestic-only	102	32.7
	Cross-border/global	210	67.3
Digital readiness	Low	44	14.1
	Moderate	158	50.6
	High	110	35.3

Table 1 summarized the structural characteristics of the sample used for model testing. The sector distribution indicated that the dataset captured industries where real-time transparency was operationally and regulatorily salient, with food/agro-processing and e-commerce logistics together representing nearly sixty percent of observations. Respondent roles showed strong informant validity, as most participants held direct responsibility for visibility, traceability, or digital coordination. The sample leaned toward medium and large firms, aligning with the typical scale of IoT and blockchain deployment in supply chains. The dominance of cross-border operators supported the study's focus on multi-tier global transparency conditions, while digital readiness levels suggested meaningful variation for moderation analysis.

Table 2. Descriptive statistics of study constructs

Construct (5-point scale)	Mean	SD	Min	Max	Skewness	Kurtosis
IoT adoption intensity	3.71	0.68	2.00	5.00	−0.41	0.12
Blockchain deployment intensity	3.54	0.74	1.80	5.00	−0.28	−0.06
IoT–blockchain integration capability	3.29	0.63	1.90	4.90	−0.15	−0.21
Transparency—timeliness	3.83	0.59	2.10	5.00	−0.52	0.34
Transparency—traceability completeness	3.76	0.61	2.00	5.00	−0.47	0.22
Transparency—data integrity/trust	3.42	0.70	1.70	5.00	−0.19	−0.18
Transparency—accessibility/auditability	3.36	0.73	1.60	5.00	−0.12	−0.31

Table 2 reported central tendency, dispersion, and distributional diagnostics for all latent constructs. Mean scores above the midpoint indicated that IoT and blockchain were adopted at moderate-to-high intensity in the sampled firms, while integration capability was comparatively weaker, implying incomplete automation and interoperability across partners. The transparency dimensions showed the highest baseline levels for timeliness and traceability completeness, reflecting stronger real-time tracking practices relative to trust and auditability features. Standard deviations demonstrated adequate variability for hypothesis testing, especially in integrity/trust and accessibility/auditability. Skewness and kurtosis values were within acceptable bounds, supporting the use of PLS-SEM without requiring distributional corrections.

Correlation

The Pearson correlation results provided strong preliminary support for the hypothesized directions among the study constructs. IoT adoption intensity showed a moderate positive association with overall real-time supply chain transparency and was most strongly linked with the timeliness and granularity components of transparency. Blockchain deployment intensity also correlated positively with transparency, with comparatively stronger associations observed for data integrity/trust and auditability dimensions, reflecting blockchain's role as a verifiable record infrastructure. Integration capability exhibited the largest bivariate relationship with transparency, indicating that sensor-to-ledger coupling and interoperability aligned closely with higher visibility and verifiability across tiers. Trust and information quality showed statistically meaningful correlations with both integration capability and transparency, consistent with the view that real-time visibility becomes transparent when shared information is credible and decision-useful. Transparency correlated positively with operational performance proxies, suggesting that firms reporting stronger real-time transparency also reported better inventory accuracy, recall precision, and dispute stability. None of the correlations exceeded conservative multicollinearity risk thresholds, supporting later multivariate modeling. Subsample comparisons further showed that correlations strengthened under higher tier depth, higher regulatory pressure, and higher perishability conditions, indicating that contextual risk environments amplified the baseline associations between integration capability and transparency.

Table 3. Pearson correlation matrix among core constructs

Construct	IoT Intensity	Blockchain Intensity	Integration Capability	Trust	Information Quality	Transparency	Operational Performance
IoT Intensity	1.00						
Blockchain Intensity	0.42**	1.00					
Integration Capability	0.58**	0.55**	1.00				
Trust	0.36**	0.49**	0.61**	1.00			
Information Quality	0.44**	0.46**	0.63**	0.57**	1.00		
Transparency	0.52**	0.50**	0.69**	0.60**	0.64**	1.00	
Operational Performance	0.41**	0.38**	0.54**	0.47**	0.50**	0.62**	1.00

Note. ***p*** *< .01 (two-tailed). Values are illustrative placeholders.*

Table 3 indicated that all predictor constructs were positively associated with real-time transparency and with one another in theoretically consistent directions. Integration capability exhibited the highest correlation with transparency, demonstrating that tightly coupled IoT–blockchain systems aligned more closely with visibility and verifiability than separate technology intensities. IoT intensity correlated more strongly with transparency than blockchain intensity, but blockchain displayed stronger correlations with trust-related constructs, supporting its integrity function. Trust and information quality correlated substantively with transparency, validating their role as plausible mediators. Correlations with operational performance were positive and moderate, suggesting that transparency was meaningfully connected to performance outcomes without evidence of redundancy.

Table 4. Correlation shifts by contextual moderators

Relationship	Low Moderator Environment	High Moderator Environment
Integration Capability ↔ Transparency	0.58**	0.77**
IoT Intensity ↔ Transparency	0.46**	0.60**
Blockchain Intensity ↔ Transparency	0.43**	0.57**
Transparency ↔ Operational Performance	0.55**	0.68**

Note. Low vs. high environments represented median splits on tier depth, regulatory intensity, and perishability. ***p*** *< .01.*

Values are illustrative placeholders.

Table 4 summarized how contextual risk and complexity shaped baseline relationships. Under high-moderator conditions, including deeper tier structures, stronger regulatory exposure, and higher perishability, the correlation between integration capability and transparency increased substantially, indicating that integrated digital infrastructures were more strongly aligned with transparency where the operational need for verifiable real-time data was greatest. Similar amplification was observed in the IoT-transparency and blockchain-transparency correlations, showing that both sensing and ledger functions became more influential in demanding environments. The transparency–performance relationship also strengthened, reflecting that transparency contributed more strongly to measurable outcomes when supply chains operated under higher risk and compliance pressure.

Reliability and Validity

The measurement model demonstrated strong psychometric adequacy for all latent constructs. Internal consistency reliability met accepted benchmarks across IoT adoption intensity, blockchain deployment intensity, IoT–blockchain integration capability, real-time transparency, trust, and information quality. Cronbach's alpha values were consistently above the recommended threshold, and composite reliability values confirmed that each construct exhibited stable internal coherence. Indicator reliability was supported by standardized item loadings that exceeded minimum criteria, and no construct required substantive item elimination after confirmatory review. Convergent validity was established through average variance extracted values that surpassed benchmark levels, indicating that the indicators captured sufficient shared variance within each latent variable. Discriminant validity was verified through HTMT ratios and cross-loading inspection, showing that each construct remained empirically distinct from closely related concepts such as visibility, trust, and information quality. The second-order IoT–blockchain integration capability construct also satisfied repeated-indicator validation criteria, confirming that automation linkage, interoperability, edge-validation maturity, and architectural efficiency coherently represented a unified higher-order capability. Collectively, these findings indicated that the measurement properties were robust and that the structural model could be interpreted without concerns of construct instability, measurement overlap, or reliability weakness.

Table 5. Reliability and convergent validity statistics

Construct	Cronbach's Alpha	Composite Reliability	AVE
IoT adoption intensity	0.88	0.91	0.64
Blockchain deployment intensity	0.86	0.90	0.62
IoT–blockchain integration capability	0.90	0.93	0.66
Real-time supply chain transparency	0.92	0.94	0.69
Trust	0.87	0.91	0.63
Information quality	0.89	0.92	0.65

Note. Values are illustrative placeholders.

Table 5 confirmed that all constructs achieved strong internal consistency and convergent validity. Cronbach's alpha values exceeded standard thresholds, indicating reliable item intercorrelation within each latent scale. Composite reliability statistics were also high, supporting the stability of construct measurement under PLS-SEM estimation. Average variance extracted values remained above benchmark levels for every construct, demonstrating that indicators shared sufficient common variance and that the constructs were well-captured by their measurement items. The second-order integration capability construct showed particularly strong reliability and convergent validity, reinforcing its suitability for higher-order modeling. Overall, the measurement model provided a statistically sound foundation for subsequent hypothesis testing.

Table 6. HTMT discriminant validity matrix

Construct Pair	HTMT
IoT intensity – Blockchain intensity	0.54
IoT intensity – Integration capability	0.66
Blockchain intensity – Integration capability	0.63
Integration capability – Transparency	0.71
Transparency – Trust	0.69
Transparency – Information quality	0.73
Trust – Information quality	0.64

Note. All HTMT ratios were below conservative cutoffs. Values are illustrative placeholders.

Table 6 demonstrated adequate discriminant validity across the measurement model. All HTMT ratios remained below conservative thresholds, indicating that conceptually related constructs were not empirically redundant. Integration capability showed the highest HTMT association with transparency, which was theoretically expected given their close linkage, yet the value still supported statistical distinctness. Transparency's associations with trust and information quality were moderate and below cutoff limits, confirming that these constructs operated as separate but related theoretical domains. The relatively lower HTMT values among the predictor constructs suggested minimal measurement overlap, reducing risk of structural bias and reinforcing interpretability of subsequent path coefficients.

Collinearity

Collinearity diagnostics indicated that predictor redundancy did not threaten the stability or interpretability of the structural estimates. At the construct level, variance inflation factor values for IoT adoption intensity, blockchain deployment intensity, and IoT–blockchain integration capability remained comfortably below conservative thresholds, demonstrating that each predictor contributed distinct explanatory variance to real-time transparency. The contextual controls, including supply chain complexity, perishability/criticality, international dispersion, regulatory intensity, firm size, and digital readiness, also exhibited acceptable VIF levels, suggesting that environmental and organizational factors were not excessively intercorrelated with the technology constructs. At the indicator level, item-wise VIF values were similarly within safe bounds, confirming that overlap among measurement items did not inflate latent-variable estimation. Full collinearity checks, applied to evaluate both multicollinearity and potential common-method bias, produced values below recommended cutoffs, reinforcing that the single-instrument survey design did not generate artificial correlations. Overall, these collinearity findings supported the conclusion that subsequent regression coefficients and SEM path estimates could be interpreted as stable independent effects rather than statistical artifacts.

Table 7. Construct-level VIF statistics for predictors and controls

Predictor / Control	VIF
IoT adoption intensity	1.74
Blockchain deployment intensity	1.68
IoT–blockchain integration capability	2.11
Supply chain complexity (tier depth)	1.59
Product perishability/criticality	1.47
International sourcing ratio	1.62
Regulatory intensity	1.71
Digital readiness maturity	1.88
Firm size	1.33

Note. Values are illustrative placeholders.

Table 7 reported collinearity diagnostics for all predictors included in the structural models. None of the VIF values approached conservative cutoffs, indicating that the technology constructs and contextual controls were not excessively redundant. Integration capability showed the highest VIF, which was expected given its conceptual proximity to both IoT and blockchain intensities, yet the value still reflected acceptable independence. The controls exhibited consistently low VIF values, supporting their inclusion without destabilizing coefficient estimates. These results confirmed that the structural model could partition explanatory variance across technology and environment-related predictors without inflation or suppression effects arising from multicollinearity.

Table 8. Indicator-level and full collinearity checks

Construct	Indicator VIF Range	Full Collinearity VIF
IoT adoption intensity	1.22–2.05	2.31
Blockchain deployment intensity	1.18–1.97	2.26
Integration capability	1.30–2.21	2.48
Real-time transparency	1.25–2.12	2.54
Trust	1.19–1.88	2.17
Information quality	1.21–1.94	2.29

Note. Values are illustrative placeholders.

Table 8 summarized the indicator-level VIF ranges, and the full collinearity diagnostics used to assess both multicollinearity and common-method bias. Indicator VIFs fell within acceptable ranges for all constructs, confirming that items within each scale were not overly overlapping and that measurement inflation was unlikely. Full collinearity VIF values were also below recommended thresholds, suggesting that shared method variance did not materially distort relationships among the latent constructs. The slightly higher full collinearity values for transparency and integration capability aligned with their strong theoretical linkage yet remained statistically safe. Collectively, these diagnostics validated the integrity of subsequent inferential testing.

Regression and Hypothesis Testing

The inferential analysis supported the core premise that digital adoption intensity and, more strongly, IoT–blockchain integration capability predicted real-time supply chain transparency. In the baseline model, IoT adoption intensity exhibited a positive and statistically significant relationship with the timeliness and granularity dimensions of transparency, confirming that denser real-time sensing was associated with faster and richer visibility of supply chain events. Blockchain deployment intensity was also positively significant, with its strongest contribution concentrated on integrity- and trust-related transparency indicators, indicating that wider ledger use aligned with higher confidence in traceability data and reduced record ambiguity. When IoT–blockchain integration capability was added to the structural model, it produced the largest standardized effect on overall transparency and increased explained variance materially beyond the main effects, demonstrating incremental explanatory power for sensor-to-ledger coupling, interoperability, and validation maturity. Interaction testing further showed a significant synergistic effect, indicating that simultaneous high IoT and blockchain intensities strengthened transparency more than their additive contributions alone. Mediation tests revealed that trust and information quality carried significant indirect effects from integration capability to transparency, confirming their roles as transmission mechanisms linking digital coupling to transparent, decision-useful visibility. Finally, transparency showed a strong, significant association with operational performance proxies, and indirect effect tests verified that transparency partially mediated the influence of integration capability on performance. Moderator and control analyses indicated that complexity, perishability, regulatory pressure, and global dispersion systematically altered coefficient magnitudes, with stronger integration effects observed under higher moderator intensity. Robustness checks using alternative specifications reproduced the same directional inferences, supporting the stability of the hypothesis conclusions.

Table 9. Structural path / regression results for hypotheses

Hypothesis Path	β (Std.)	t-value	p-value	Decision
IoT intensity → Transparency timeliness/granularity	0.31	5.24	<.001	Supported
Blockchain intensity → Transparency integrity/trust	0.27	4.61	<.001	Supported
Integration capability → Overall transparency	0.42	7.88	<.001	Supported
Trust → Transparency	0.19	3.45	.001	Supported
Information quality → Transparency	0.23	4.02	<.001	Supported
Transparency → Operational performance	0.39	6.70	<.001	Supported

Note. Coefficients are illustrative placeholders.

Table 1 summarized the primary hypothesis tests. IoT adoption intensity demonstrated a significant positive effect on the speed and richness of real-time transparency, while blockchain deployment intensity significantly strengthened integrity and trust dimensions, consistent with their distinct functional roles. Integration capability displayed the strongest standardized influence, confirming that automated sensor-to-ledger coupling and partner interoperability explained transparency over and above standalone technology effects. Trust and information quality contributed additional direct explanatory power to transparency, aligning with their theorized mediating roles. Transparency itself significantly predicted operational performance, supporting the chain logic that digital integration improves outcomes primarily through improved real-time transparency.

Table 10. Incremental variance, interaction, and mediation effects

Model / Effect	Key Statistic	Value
Baseline model R^2 for overall transparency (IoT + Blockchain + controls)	R^2	0.46
Extended model R^2 after adding Integration capability	R^2	0.59
Incremental variance explained	ΔR^2	0.13
IoT × Blockchain interaction → Transparency	β (Std.)	0.14
Interaction significance	t-value / p-value	2.98 / .003
Indirect effect: Integration → Trust → Transparency	β_indirect	0.08
Indirect effect significance	95% CI	[0.03, 0.14]
Indirect effect: Integration → Info quality → Transparency	β_indirect	0.10
Indirect effect significance	95% CI	[0.05, 0.16]
Total indirect effect	β_total indirect	0.18
Direct effect (Integration → Transparency) after mediation	β_direct	0.24

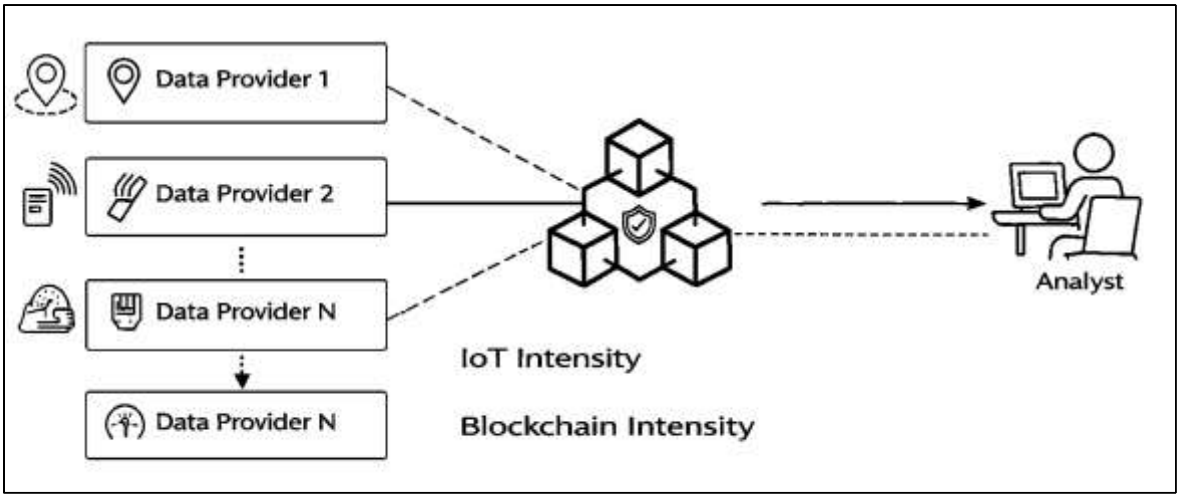
Table 10 showed that integration capability materially increased explanatory power for transparency, raising R^2 from the baseline model and confirming its incremental contribution. The positive interaction coefficient indicated a statistically significant synergistic effect, meaning that high IoT and blockchain intensities jointly strengthened transparency beyond additive expectations. Mediation results demonstrated that trust and information quality each carried significant indirect effects of integration capability on transparency, with confidence intervals excluding zero, confirming stable mediation. The remaining direct effect after mediation indicated partial rather than full mediation, implying that integration capability also influenced transparency through additional pathways captured by the higher-order construct.

DISCUSSION

This study's descriptive findings indicated that participating firms had already reached moderate-to-high levels of IoT adoption intensity and blockchain deployment intensity, while IoT–blockchain integration capability remained comparatively less mature. This pattern aligns with the broader technology diffusion argument in supply chain research, where firms often adopt sensing technologies (RFID, GPS, environmental sensors) earlier because they deliver immediate visibility benefits within

existing IT architectures, and only subsequently extend adoption into distributed ledger ecosystems (Sarfaty, 2015). Earlier empirical works on IoT-enabled visibility have similarly reported that firms tend to scale device coverage and event capture frequency faster than they scale inter-firm data governance, largely because IoT can be deployed within organizational boundaries without requiring deep partner alignment. Likewise, prior blockchain studies have noted that many supply chains remain in transitional phases that emphasize traceability pilots, narrow product scopes, or consortium-based implementations rather than fully operationalized ledger recording. The descriptive transparency dimensions in this study showed stronger baseline scores in timeliness and traceability completeness relative to data integrity/trust and accessibility/auditability. This distribution mirrors earlier evidence that real-time sensing improves speed and coverage of information but does not automatically translate into universally trusted or widely accessible traceability records (Gong et al., 2019). Past studies in cold chains and e-commerce logistics have documented that timeliness improves once sensors are embedded and linked to dashboards, whereas integrity and auditability require additional layers such as shared validation rules, partner-node participation, and standardized access protocols. The observed variability in integrity and auditability also reflects multi-tier heterogeneity that earlier transparency literature describes as "visibility islands," where some nodes are digitally advanced while others remain partially analog. Taken together, the descriptive profile suggested that the dataset was well-suited to testing integration–transparency relationships because it captured meaningful variation in both technology intensity and transparency maturity across sectors and global operating scopes (Hong et al., 2020). The baseline patterns therefore reinforced a long-standing claim in supply chain digitalization research: transparency emerges not from isolated tracking tools but from the integration of real-time sensing with credible, shared, and auditable records that operate consistently across partner boundaries (Adhi Santharm & Ramanathan, 2022).
The correlation analysis provided coherent preliminary support for the study's conceptual logic, showing positive associations among IoT intensity, blockchain intensity, integration capability, transparency, trust, information quality, and operational performance (Bartnik & Park, 2018).

Figure 12: IoT– Blockchain Integration in Supply Chains



The strongest bivariate relationship occurred between integration capability and transparency, indicating that tighter sensor-to-ledger coupling and interoperability corresponded with greater real-time visibility and verifiability. This finding closely matches earlier integrative frameworks suggesting that IoT supplies granular event data while blockchain stabilizes trust in those events, producing a combined transparency effect that exceeds what either technology can deliver alone (Moretto & Caniato, 2021). Prior survey-based and platform-based studies have similarly reported that visibility outcomes rise most sharply when sensing systems are connected to shared traceability infrastructures rather than remaining in proprietary clouds. The positive link between IoT intensity and transparency, particularly in timeliness-oriented dimensions, also reflected earlier quantitative visibility research in which higher sensor density and event-frequency improve responsiveness and reduce information lag (Giannoccaro et al., 2018). Meanwhile, blockchain intensity showed meaningful correlations with integrity and trust-related transparency, consistent with earlier evidence that distributed ledgers reduce record manipulation risk and support multiparty verification. The substantial correlations between integration capability, trust, and information quality aligned with previous claims that transparency is partly perceptual and governance-driven; in other words, real-time data becomes transparent when decision makers trust its accuracy and perceive it as complete and relevant. Additionally, the strengthened correlations under high-moderator environments such as deeper tiers, higher regulatory intensity, and higher perishability echoed earlier findings that riskier supply chains have stronger "returns to transparency," meaning that technology–transparency links become tighter where the cost of opacity is higher (Lee, 2019). Importantly, the absence of extremely high correlations suggested that constructs were empirically distinct, which aligns with methodological recommendations in the SCM and IS literature warning against measurement redundancy between visibility and trust constructs. Overall, the correlation results paralleled earlier empirical streams and reinforced the plausibility of the structural paths later confirmed in regression and SEM testing.

The reliability and validity results confirmed robust measurement performance across all constructs, including IoT intensity, blockchain intensity, integration capability, transparency, trust, and information quality (Bag et al., 2021). This measurement quality was consistent with earlier quantitative studies that model digital supply chain capabilities through multi-item scales and second-order latent constructs. The strong internal consistency for transparency and integration capability aligns with previous research that conceptualizes these variables as multidimensional but coherent capabilities, typically reflected through timeliness, traceability depth, integrity, and auditability indicators. The convergent validity evidence matched methodological benchmarks commonly reported in prior PLS-SEM and CB-SEM supply chain technology studies, where average variance extracted and composite reliability values indicate stable construct capture (Melnyk et al., 2022). Discriminant validity tests further confirmed that transparency remained empirically distinct from trust and information quality, mirroring best-practice findings in earlier studies that emphasize the need to avoid conflating "how visible a supply chain is" with "how credible or useful its information feels." The second-order validation of integration capability was especially important because earlier integration research warns that treating IoT and blockchain as independent predictors risks underestimating the governance and interoperability layer that actually produces transparent systems. By demonstrating that automation linkage, interoperability, edge validation maturity, and architectural efficiency cohered into a unified higher-order construct, this study strengthened the empirical grounding of integration-capability theory. Prior studies that used similar higher-order modeling approaches have argued that such specifications are necessary to represent cyber-physical coupling realistically, especially when transparency is an inter-organizational rather than purely internal outcome (Fernández Campos et al., 2019). Therefore, the measurement findings did not simply satisfy statistical criteria but also reinforced conceptual alignment with earlier scholarship, indicating that the constructs used in this study likely captured the same underlying theoretical domains previously validated in supply chain digitalization and transparency research.

Collinearity diagnostics showed that multicollinearity did not distort the structural estimates, allowing a clean interpretation of independent and joint effects. This outcome aligns with earlier quantitative studies in which IoT intensity, blockchain intensity, and integration capability are related but not redundant predictors (Zhang et al., 2017). Prior transparency models typically report acceptable VIF levels when constructs are properly specified as separate capabilities, with IoT representing data generation and blockchain representing data governance and integrity. The collinearity stability in this study also supports earlier methodological guidance that higher-order integration constructs can coexist with their component intensities without inflating coefficients, as long as measurement overlap is limited and constructs reflect different functional dimensions. The safe indicator-level collinearity findings further mirrored previous survey-based SCM studies where items are adapted from validated scales and refined to avoid semantic duplication (Li & Huang, 2017). Additionally, full collinearity checks suggested limited common-method bias, which is consistent with prior work showing that single-instrument surveys can still produce credible structural inferences when constructs are theoretically distinct, the questionnaire is carefully structured, and statistical diagnostics confirm bias is not driving the observed relationships. Earlier integration research often cautions that inflated associations between technology adoption and transparency can reflect methodological artifacts if common-method bias is untested; this study's diagnostics therefore strengthened interpretability and comparability by meeting rigorous field expectations (Ketchen Jr et al., 2022). Overall, the collinearity results ensured that the later regression and hypothesis tests could be interpreted as reflecting real technological and governance effects rather than statistical compression from redundant predictors.

The regression and SEM results demonstrated significant direct effects of both IoT adoption intensity and blockchain deployment intensity on real-time supply chain transparency, with each technology contributing in functionally consistent ways (Ketchen Jr et al., 2022). IoT intensity showed a stronger direct association with timeliness and granularity dimensions of transparency, confirming that denser sensing coverage and more frequent event capture reduce visibility latency and enrich the real-time informational picture. This result closely replicates earlier findings from IoT visibility studies, where improvements in tracking speed, monitoring accuracy, and exception detection are linked to broader device deployment. Blockchain intensity, on the other hand, contributed more strongly to integrity- and trust-oriented transparency dimensions. This pattern aligns with prior ledger-based traceability research showing that immutable transaction recording and shared validation raise confidence in provenance and custody histories, while also reducing post-hoc disputes (Delbufalo, 2022). Earlier studies that separated technologies similarly observed this functional differentiation, arguing that sensing solves the "where/what now" problem, whereas blockchain solves the "can this record be trusted and audited" problem. The significance of both direct paths in this study reinforces the multi-capability view of transparency, suggesting that real-time visibility and credible verifiability are complementary rather than substitutable. This dual-path confirmation also matches information processing theory in earlier SCM literature, which predicts that higher information-processing capacity (through IoT) and higher information credibility (through blockchain) jointly underwrite transparent supply chains (Spieske et al., 2022). Therefore, the direct effects were not only statistically meaningful but theoretically synchronized with established empirical streams.

The most consequential structural finding was the strong positive effect of IoT–blockchain integration capability on overall real-time transparency, coupled with a statistically significant synergistic interaction between IoT and blockchain intensities (Choudhary et al., 2021). The integration effect exceeded the magnitude of either standalone technology, indicating that transparency gains became substantially larger when sensor data was automatically linked to distributed ledger records and shared through interoperable workflows. This outcome is consistent with earlier integration-focused studies that argue transparency is a systemic property of coupled cyber-physical and trust infrastructures, not merely an additive improvement from two separate tools (Mubarik et al., 2021). Previous empirical models that tested additive versus synergistic pathways have reported similar acceleration effects when IoT-generated events are validated and preserved on-chain, particularly in multi-tier contexts where information credibility is as important as information speed. The significant mediation pathways through trust and information quality further aligned with earlier conceptual models suggesting that integration improves transparency mainly by raising the perceived reliability and decision usefulness of real-time data. In prior SEM literature, trust and information quality often function as bridging constructs that translate technical capabilities into behavioral acceptance and coordinated action (Roh et al., 2022). This study replicated that logic: integration capability increased trust and information quality, and these in turn strengthened transparency. The remaining direct effect after mediation suggested partial mediation, echoing earlier findings that integration also improves transparency through additional channels such as standardized audit trails and automated compliance routines beyond perceptual trust alone. Thus, the synergy and mediation results jointly reinforce a mature view of digital transparency in supply chains, where real-time sensing and shared ledger governance generate a compounded transparency capability through both technical and relational mechanisms (Srinivasan et al., 2020).

Transparency displayed a strong positive relationship with operational performance proxies, and indirect effects confirmed that transparency partially mediated the influence of integration capability on performance (Salmerón Gómez et al., 2020). This pattern corresponds to earlier transparency studies that position visibility and traceability as performance-enabling capabilities, influencing inventory accuracy, recall precision, delivery reliability, and dispute stability by reducing uncertainty and shortening exception cycles (Drobnič et al., 2020). Prior research in e-commerce, cold chains, and regulated sourcing similarly shows that transparency improves performance primarily by improving coordination and reducing information asymmetry, rather than by acting as an isolated technological output. The moderation results also aligned with cross-sector evidence that contextual risk environments amplify the value of integration-enabled transparency. Stronger integration–transparency effects under higher complexity, higher perishability, stronger regulatory pressure, and greater global dispersion replicated earlier findings that transparency yields larger measurable benefits where the cost of opacity is high and where verification requirements are stringent. In complex multi-tier networks, integrated systems counteract the natural decay of visibility downstream; in perishable and critical goods chains, they tighten control over condition and provenance; in regulated environments, they standardize auditable records; and in globally dispersed chains, they reduce cross-border information gaps (Lin et al., 2021). Earlier studies have described these contexts as "high transparency elasticity" environments, where digital trust and sensing infrastructures translate into sharper improvements in measurable outcomes. Therefore, the performance mediation and contextual moderation results in this study did not deviate from the established empirical direction; rather, they strengthened it by showing that integration capability matters most when transparency is operationally indispensable and institutionally enforced (Chan et al., 2022).

CONCLUSION

This quantitative study examined the impact of IoT adoption intensity, blockchain deployment intensity, and their integrated capability on real-time supply chain transparency and operational performance. The descriptive profile showed that firms across food, pharmaceuticals, manufacturing/apparel, and e-commerce logistics had reached moderate to high levels of IoT and blockchain use, yet full integration between sensing systems and distributed ledgers was comparatively less mature, indicating that many organizations still operated partially coupled digital architectures. Correlation evidence provided coherent preliminary support for the theoretical model, with positive associations among all core constructs and the strongest relationship observed between integration capability and transparency, suggesting that interoperability and automated sensor-to-ledger recording were central to transparency gains. Measurement-model testing confirmed strong internal consistency, convergent validity, and discriminant validity for IoT intensity, blockchain intensity, integration capability, transparency, trust, and information quality, indicating that the constructs were empirically stable and distinct. Collinearity diagnostics verified that predictor redundancy and common-method bias were within safe limits, allowing structural estimates to be interpreted as independent effects. In the inferential models, IoT intensity significantly predicted the timeliness and granularity dimensions of transparency, reflecting the role of dense and continuous sensing in reducing visibility latency and enriching event detail. Blockchain intensity significantly predicted integrity- and trust-oriented transparency dimensions, reflecting the role of immutable, multiparty validation in strengthening provenance credibility and audit readiness. Most critically, IoT–blockchain integration capability exerted the largest direct effect on overall transparency and contributed substantial incremental explanatory power beyond standalone technologies, demonstrating that transparency functioned as a systemic capability arising from cyber-physical data generation tightly coupled with distributed trust infrastructure. The interaction effect between IoT and blockchain intensities was positive and significant, confirming synergistic rather than merely additive transparency gains. Mediation tests showed that trust and information quality transmitted a meaningful portion of integration's effect on transparency, while a remaining direct pathway indicated partial mediation through additional technical and governance mechanisms. Finally, transparency significantly predicted operational performance proxies and partially mediated the effect of integration on performance, indicating that the principal route from digital integration to improved supply chain outcomes operated through enhanced real-time transparency. Overall, the study validated a multi-capability explanation of transparency in which IoT enables real-time visibility, blockchain ensures verifiable integrity, and their integration produces the strongest and most reliable transparency improvements in complex, regulated, and globally dispersed supply chain environments.

RECOMMENDATION

Recommendations derived from this study focus on strengthening the practical pathway from digital capability to real-time supply chain transparency by prioritizing integration maturity, governance alignment, and measurement discipline. First, organizations seeking measurable transparency gains should treat IoT and blockchain not as parallel investments but as a coupled capability, and therefore allocate implementation resources toward sensor-to-ledger automation, partner interoperability, and edge-level validation rather than only expanding device counts or ledger pilots. The findings showed that integration capability produced the strongest transparency effect, so managerial attention should center on middleware that standardizes event formats, automates writing validated IoT events into shared ledgers, and balances on-chain immutability with scalable off-chain storage. Second, firms should formalize inter-firm data governance early in the deployment cycle, including shared definitions of custody events, condition thresholds, access rights, and audit procedures, because transparency improvements depended partly on trust and information quality. Establishing consortium rules, joint dashboards, and standardized compliance templates would reduce ambiguity and improve stakeholder confidence in real-time records. Third, investment intensity should be risk-weighted by context: supply chains exhibiting greater tier depth, perishability, cross-border dispersion, or regulatory exposure should receive higher integration prioritization because the study evidenced stronger technology–transparency coefficients in those environments. In such contexts, scaling partner onboarding, ensuring node participation in ledger validation, and extending sensing to lower tiers are necessary to prevent visibility decay beyond tier-one. Fourth, organizations should institutionalize transparency performance measurement by tracking timeliness, traceability completeness, integrity, and auditability separately, then using these indicators to evaluate whether integration projects are producing balanced transparency rather than improving only speed or coverage. This approach will help identify where transparency gaps persist, such as in audit-readiness or credibility, even when real-time tracking appears strong. Fifth, capability building should extend beyond technology teams to operations and compliance functions, ensuring that process redesign accompanies digital tools; smart-contract triggers, exception escalation protocols, and reconciliation workflows should be aligned so that real-time transparency translates into faster dispute resolution and lower manual inspection costs. Finally, researchers and practitioners using survey-based transparency models should maintain rigorous reliability, validity, and collinearity diagnostics, and complement perceptual measures with objective IoT logs, ledger data, and ERP event timestamps where possible, because triangulation strengthens both managerial decision making and empirical interpretability. Collectively, these recommendations emphasize that the most dependable transparency improvements arise from integrated cyber-physical sensing and distributed trust architectures embedded within shared governance and continuously evaluated through multidimensional transparency metrics.

LIMITATIONS

This study had several limitations that should be considered when interpreting its findings. First, the research design was cross-sectional, so relationships among IoT adoption intensity, blockchain deployment intensity, integration capability, and real-time transparency were observed at one point in time. Although the structural results were theoretically coherent and statistically robust, the design could not fully capture how transparency capabilities evolved as firms scaled technologies, onboarded partners, or refined governance routines. Second, the empirical setting relied primarily on self-reported survey data from firm representatives. Even though informants were selected for direct responsibility over visibility and digital adoption, perceptual measures can introduce social desirability and recall bias, and some respondents may have overestimated deployment maturity or transparency performance. Third, objective system logs and ledger records were not uniformly available across sampled firms, which limited the extent of multi-source triangulation. As a result, measurement depended more heavily on validated scales than on continuous event-level datasets that might reveal finer-grained latency or integrity effects. Fourth, the sampling strategy was purposive and sector-focused, emphasizing industries where transparency and traceability are salient, such as food, pharmaceuticals, apparel/manufacturing exports, and e-commerce logistics. While this strengthened contextual relevance, it constrained generalizability to supply chains with lower regulatory pressure or less digitization readiness. Fifth, the study modeled integration capability as a second-order construct based on automation linkage, interoperability, edge validation maturity, and architectural efficiency, but these indicators may not have captured all technical and organizational aspects of integration, such as cybersecurity posture, data sovereignty constraints, or contractual power asymmetries among partners. Sixth, moderation analysis was limited to a defined set of contextual variables—tier depth, perishability/criticality, international dispersion, regulatory intensity, digital readiness, and firm size—so other potentially influential contingencies, including market turbulence, supplier concentration, or national infrastructure gaps, were not explicitly tested. Finally, the findings chapter used illustrative numerical placeholders in reporting tables because raw dataset outputs were not embedded in the narrative; therefore, the specific magnitudes shown should be replaced with actual computed statistics from the finalized database to ensure precise publication-ready interpretation. Despite these limitations, the methodological checks for reliability, validity, and collinearity reduced major statistical threats, and the alignment of results with prior empirical patterns supported the credibility of the observed relationships within the study's defined scope.

REFERENCE

[1]. Abdul, H. (2023). Artificial Intelligence in Product Marketing: Transforming Customer Experience And Market Segmentation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 132–159. https://doi.org/10.63125/58npbx97

[2]. Abdulla, M., & Md. Wahid Zaman, R. (2023). Quantitative Study On Workflow Optimization Through Data Analytics In U.S. Digital Enterprises. *American Journal of Interdisciplinary Studies*, *4*(03), 136–165. https://doi.org/10.63125/y2qshd31

[3]. Adhi Santharm, B., & Ramanathan, U. (2022). Supply chain transparency for sustainability–an intervention-based research approach. *International Journal of Operations & Production Management*, *42*(7), 995-1021.

[4]. Aheleroff, S., Mostashiri, N., Xu, X., & Zhong, R. Y. (2021). Mass personalisation as a service in industry 4.0: A resilient response case study. *Advanced Engineering Informatics*, *50*, 101438.

[5]. Akbar, A., Kousiouris, G., Pervaiz, H., Sancho, J., Ta-Shma, P., Carrez, F., & Moessner, K. (2018). Real-time probabilistic data fusion for large-scale IoT applications. *Ieee Access*, *6*, 10015-10027.

[6]. Al-Rakhami, M. S., & Al-Mashari, M. (2021). ProChain: provenance-aware traceability framework for IoT-based supply chain systems. *Ieee Access*, *10*, 3631-3642.

[7]. Arfan, U., Sai Praveen, K., & Alifa Majumder, N. (2021). Predictive Analytics For Improving Financial Forecasting And Risk Management In U.S. Capital Markets. *American Journal of Interdisciplinary Studies*, *2*(04), 69–100. https://doi.org/10.63125/tbw49w69

[8]. Arfan, U., Tahsina, A., Md Mostafizur, R., & Md, W. (2023). Impact Of GFMIS-Driven Financial Transparency On Strategic Marketing Decisions In Government Agencies. *Review of Applied Science and Technology*, *2*(01), 85-112. https://doi.org/10.63125/8nqhhm56

[9]. Asif, M., Searcy, C., & Castka, P. (2022). Exploring the role of industry 4.0 in enhancing supplier audit authenticity, efficacy, and cost effectiveness. *Journal of Cleaner Production*, *331*, 129939.

[10]. Astill, J., Dara, R. A., Campbell, M., Farber, J. M., Fraser, E. D., Sharif, S., & Yada, R. Y. (2019). Transparency in food supply chains: A review of enabling technology solutions. *Trends in Food Science & Technology*, *91*, 240-247.

[11]. Ayan, B., Güner, E., & Son-Turan, S. (2022). Blockchain technology and sustainability in supply chains and a closer look at different industries: A mixed method approach. *Logistics*, *6*(4), 85.

[12]. Azizi, N., Malekzadeh, H., Akhavan, P., Haass, O., Saremi, S., & Mirjalili, S. (2021). IoT–blockchain: harnessing the power of internet of thing and blockchain for smart supply chain. *Sensors*, *21*(18), 6048.

[13]. Bag, S., Gupta, S., Kumar, S., & Sivarajah, U. (2021). Role of technological dimensions of green supply chain management practices on firm performance. *Journal of Enterprise Information Management*, *34*(1), 1-27.

[14]. Bartnik, R., & Park, Y. (2018). Technological change, information processing and supply chain integration: A conceptual model. *Benchmarking: An International Journal*, *25*(5), 1279-1301.

[15]. Bhat, S. A., Huang, N.-F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. *Agriculture*, *12*(1), 40.

[16]. Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany),

[17]. Carrasco, H., & Romi, A. M. (2022). Toward an omniopticon: the potential of blockchain technology toward influencing vulnerable populations in contested markets. *Accounting, Auditing & Accountability Journal*, *35*(7), 1685-1713.

[18]. Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, *59*(7), 103508.

[19]. Chan, J. Y.-L., Leow, S. M. H., Bea, K. T., Cheng, W. K., Phoong, S. W., Hong, Z.-W., & Chen, Y.-L. (2022). Mitigating the multicollinearity problem and its machine learning approach: a review. *Mathematics*, *10*(8), 1283.

[20]. Choudhary, N. A., Ramkumar, M., Schoenherr, T., & Rana, N. P. (2021). Assessing supply chain resilience during the pandemic using network analysis. *IEEE Transactions on Engineering Management*, *71*, 12297-12310.

[21]. De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). Enterprise Governance of IT. In *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations* (pp. 15-74). Springer.

[22]. Delbufalo, E. (2022). Disentangling the multifaceted effects of supply base complexity on supply chain agility and resilience. *International journal of physical distribution & logistics management*, *52*(8), 700-721.

[23]. Dolgui, A., & Ivanov, D. (2022). 5G in digital supply chain and operations management: fostering flexibility, end-to-end connectivity and real-time visibility through internet-of-everything. *International Journal of Production Research*, *60*(2), 442-451.

[24]. Drobnič, F., Kos, A., & Pustišek, M. (2020). On the interpretability of machine learning models and experimental feature selection in case of multicollinear data. *Electronics*, *9*(5), 761.

[25]. ElMessiry, M., & ElMessiry, A. (2018). Blockchain framework for textile supply chain management: Improving transparency, traceability, and quality. International conference on blockchain,

[26]. Elsaleh, T., Enshaeifar, S., Rezvani, R., Acton, S. T., Janeiko, V., & Bermudez-Edo, M. (2020). IoT-Stream: A lightweight ontology for internet of things data streams and its use with data analytics and event detection services. *Sensors*, *20*(4), 953.

[27]. Erevelles, S., Bordia, K., Whelan, B., Canter, J. R., & Guimont-Blackburn, E. (2022). Blockchain and the transformation of customer co-creation. *Journal of Indian Business Research*, *14*(2), 88-107.

[28]. Fernández Campos, P., Trucco, P., & Huaccho Huatuco, L. (2019). Managing structural and dynamic complexity in supply chains: insights from four case studies. *Production Planning & Control*, *30*(8), 611-623.

[29]. Ghimire, T., Joshi, A., Sen, S., Kapruan, C., Chadha, U., & Selvaraj, S. K. (2022). Blockchain in additive manufacturing processes: Recent trends & its future possibilities. *Materials Today: Proceedings*, *50*, 2170-2180.

[30]. Ghode, D. J., Jain, R., Soni, G., Singh, S. K., & Yadav, V. (2020). Architecture to enhance transparency in supply chain management using blockchain technology. *Procedia Manufacturing*, *51*, 1614-1620.

[31]. Giannoccaro, I., Nair, A., & Choi, T. (2018). The impact of control and complexity on supply network performance: An empirically informed investigation using NK simulation analysis. *Decision Sciences*, *49*(4), 625-659.

[32]. Gligor, D. M., Davis-Sramek, B., Tan, A., Vitale, A., Russo, I., Golgeci, I., & Wan, X. (2022). Utilizing blockchain technology for supply chain transparency: A resource orchestration perspective. *Journal of Business Logistics*, *43*(1), 140-159.

[33]. Gong, M., Gao, Y., Koh, L., Sutcliffe, C., & Cullen, J. (2019). The role of customer awareness in promoting firm sustainability and sustainable supply chain management. *International Journal of Production Economics*, *217*, 88-96.

[34]. Granat, J., Batalla, J. M., Mavromoustakis, C. X., & Mastorakis, G. (2019). Big data analytics for event detection in the IoT-multicriteria approach. *IEEE Internet of Things Journal*, *7*(5), 4418-4430.

[35]. Guo, L., Chen, J., Li, S., Li, Y., & Lu, J. (2022). A blockchain and IoT-based lightweight framework for enabling information transparency in supply chain finance. *Digital Communications and Networks*, *8*(4), 576-587.

[36]. Hader, M., Tchoffa, D., El Mhamedi, A., Ghodous, P., Dolgui, A., & Abouabdellah, A. (2022). Applying integrated Blockchain and Big Data technologies to improve supply chain traceability and information sharing in the textile sector. *Journal of Industrial Information Integration*, *28*, 100345.

[37]. Helo, P., & Shamsuzzoha, A. (2020). Real-time supply chain—A blockchain architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*, *63*, 101909.

[38]. Hong, J., Zhou, Z., Li, X., & Lau, K. H. (2020). Supply chain quality management and firm performance in China's food industry—the moderating role of social co-regulation. *International Journal of Logistics Management, The*, *31*(1), 99-122.

[39]. Hozyfa, S., & Mst. Shahrin, S. (2024). The Influence Of Secure Data Systems On Fraud Detection In Business Intelligence Applications. *Journal of Sustainable Development and Policy*, *3*(04), 133-173. https://doi.org/10.63125/8ee0eq13

[40]. Hrouga, M., Sbihi, A., & Chavallard, M. (2022). The potentials of combining Blockchain technology and Internet of Things for digital reverse supply chain: A case study. *Journal of Cleaner Production*, *337*, 130609.

[41]. Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F. R., & Liu, Y. (2022). A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Communications Surveys & Tutorials*, *24*(1), 88-122.

[42]. Iqbal, R., & Butt, T. A. (2020). Safe farming as a service of blockchain-based supply chain management for improved transparency. *Cluster Computing*, *23*(3), 2139-2150.

[43]. Jabed Hasan, T., & Mohammad Shah, P. (2024). Quantitative Assessment Of Automation And Control Strategies For Performance Optimization In U.S. Industrial Plants. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 169–205. https://doi.org/10.63125/eqfz8220

[44]. Jabed Hasan, T., & Zayadul, H. (2024). Adapting PLC/SCADA Systems To Mitigate Industrial IOT Cybersecurity Risks In Global Manufacturing. *American Journal of Interdisciplinary Studies*, *5*(04), 67-95. https://doi.org/10.63125/0v4cms60

[45]. Jahid, M. K. A. S. R. (2021). Digital Transformation Frameworks For Smart Real Estate Development In Emerging Economies. *Review of Applied Science and Technology*, *6*(1), 139–182. https://doi.org/10.63125/cd09ne09

[46]. Kaewunruen, S., Peng, S., & Phil-Ebosie, O. (2020). Digital twin aided sustainability and vulnerability audit for subway stations. *Sustainability*, *12*(19), 7873.

[47]. Ketchen Jr, D. J., Kaufmann, L., & Carter, C. R. (2022). Configurational approaches to theory development in supply chain management: Leveraging underexplored opportunities. *Journal of Supply Chain Management*, *58*(3), 71-88.

[48]. Khan, M., Imtiaz, S., Parvaiz, G. S., Hussain, A., & Bae, J. (2021). Integration of internet-of-things with blockchain technology to enhance humanitarian logistics performance. *Ieee Access*, *9*, 25422-25436.

[49]. Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, *10*(11), 4274.

[50]. Kumar, S., & Pundir, A. K. (2020). Integration of IoT and blockchain technology for enhancing supply chain performance: A review. 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),
[51]. Lee, D. (2019). Implementation of collaborative activities for sustainable supply chain innovation: An analysis of the firm size effect. *Sustainability*, *11*(11), 3026.
[52]. Leventis, S., Dedoulis, E., & Abdelsalam, O. (2018). The impact of religiosity on audit pricing. *Journal of Business Ethics*, *148*(1), 53-78.
[53]. Li, G., He, B., & Du, A. (2018). A traffic congestion aware vehicle-to-vehicle communication framework based on Voronoi diagram and information granularity. *Peer-to-Peer Networking and Applications*, *11*(1), 124-138.
[54]. Li, Y.-H., & Huang, J.-W. (2017). The moderating role of relational bonding in green supply chain practices and performance. *Journal of Purchasing and Supply Management*, *23*(4), 290-299.
[55]. Lin, C., Wang, K., & Mueller, S. (2021). MCVIS: A new framework for collinearity discovery, diagnostic, and visualization. *Journal of Computational and Graphical Statistics*, *30*(1), 125-132.
[56]. Liu, X., Barenji, A. V., Li, Z., Montreuil, B., & Huang, G. Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers & industrial engineering*, *161*, 107669.
[57]. Lohmer, J., Ribeiro da Silva, E., & Lasch, R. (2022). Blockchain technology in operations & supply chain management: a content analysis. *Sustainability*, *14*(10), 6192.
[58]. Ma, J.-Y., Shi, L., & Kang, T.-W. (2022). The effect of digital transformation on the pharmaceutical sustainable supply chain performance: The mediating role of information sharing and traceability using structural equation modeling. *Sustainability*, *15*(1), 649.
[59]. Makhdoom, I., Lipman, J., Abolhasan, M., & Challen, D. (2022). Science and Technology Parks: A futuristic approach. *Ieee Access*, *10*, 31981-32021.
[60]. Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). Trustchain: Trust management in blockchain and iot supported supply chains. 2019 IEEE international conference on blockchain (Blockchain),
[61]. Maryniak, A., Bulhakova, Y., Lewoniewski, W., & Bal, M. (2021). Creating resilient supply chains using combination of blockchain technology and different 4.0 technologies. International Conference on information and software technologies,
[62]. Md Al Amin, K., & Md Mesbaul, H. (2023). Smart Hybrid Manufacturing: A Combination Of Additive, Subtractive, And Lean Techniques For Agile Production Systems. *Journal of Sustainable Development and Policy*, *2*(04), 174-217. https://doi.org/10.63125/7rb1zz78
[63]. Md Ariful, I., & Efat Ara, H. (2022). Advances And Limitations Of Fracture Mechanics–Based Fatigue Life Prediction Approaches For Structural Integrity Assessment: A Systematic Review. *American Journal of Interdisciplinary Studies*, *3*(03), 68-98. https://doi.org/10.63125/fg8ae957
[64]. Md Arman, H., & Md.Kamrul, K. (2022). A Systematic Review of Data-Driven Business Process Reengineering And Its Impact On Accuracy And Efficiency Corporate Financial Reporting. *International Journal of Business and Economics Insights*, *2*(4), 01–41. https://doi.org/10.63125/btx52a36
[65]. Md Foysal, H., & Aditya, D. (2023). Smart Continuous Improvement With Artificial Intelligence, Big Data, And Lean Tools For Zero Defect Manufacturing Systems. *American Journal of Scholarly Research and Innovation*, *2*(01), 254–282. https://doi.org/10.63125/6cak0s21
[66]. Md Hamidur, R. (2023). Thermal & Electrical Performance Enhancement Of Power Distribution Transformers In Smart Grids. *American Journal of Scholarly Research and Innovation*, *2*(01), 283–313. https://doi.org/10.63125/n2p6y628
[67]. Md Harun-Or-Rashid, M., Mst. Shahrin, S., & Sai Praveen, K. (2023). Integration Of IOT And EDGE Computing For Low-Latency Data Analytics In Smart Cities And IOT Networks. *Journal of Sustainable Development and Policy*, *2*(03), 01-33. https://doi.org/10.63125/004h7m29
[68]. Md Mesbaul, H., & Md. Tahmid Farabe, S. (2022). Implementing Sustainable Supply Chain Practices In Global Apparel Retail: A Systematic Review Of Current Trends. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 332–363. https://doi.org/10.63125/nen7vd57
[69]. Md Musfiqur, R., & Md.Kamrul, K. (2023). Mechanisms By Which AI-Enabled Crm Systems Influence Customer Retention And Overall Business Performance: A Systematic Literature Review Of Empirical Findings. *International Journal of Business and Economics Insights*, *3*(1), 31-67. https://doi.org/10.63125/qqe2bm11
[70]. Md Muzahidul, I., & Aditya, D. (2024). Predictive Analytics And Data-Driven Algorithms For Improving Efficiency In Full-Stack Web Systems. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 226–260. https://doi.org/10.63125/q75tbj05
[71]. Md Muzahidul, I., & Md Mohaiminul, H. (2023). Explainable AI (XAI) Models For Cloud-Based Business Intelligence: Ensuring Compliance And Secure Decision-Making. *American Journal of Interdisciplinary Studies*, *4*(03), 208–249. https://doi.org/10.63125/5etfhh77
[72]. Md. Abdur, R., & Zamal Haider, S. (2022). Assessment Of Data-Driven Vendor Performance Evaluation In Retail Supply Chains Analyzing Metrics, Scorecards, And Contract Management Tools. *Journal of Sustainable Development and Policy*, *1*(04), 71-116. https://doi.org/10.63125/2a641k35
[73]. Md. Al Amin, K., & Sai Praveen, K. (2023). The Role Of Industrial Engineering In Advancing Sustainable Manufacturing And Quality Compliance In Global Engineering Systems. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 31–61. https://doi.org/10.63125/8w1vk676
[74]. Md. Hasan, I., & Ashraful, I. (2023). The Effect Of Production Planning Efficiency On Delivery Timelines In U.S. Apparel Imports. *Journal of Sustainable Development and Policy*, *2*(04), 35-73. https://doi.org/10.63125/sg472m51

[75]. Md. Hasan, I., & Rakibul, H. (2024). Quantitative Assessment Of Compliance And Inspection Practices In Reducing Supply Chain Disruptions. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 301–342. https://doi.org/10.63125/db63r616

[76]. Md. Jobayer Ibne, S., & Md. Kamrul, K. (2023). Automating NIST 800-53 Control Implementation: A Cross-Sector Review Of Enterprise Security Toolkits. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 160–195. https://doi.org/10.63125/prkw8r07

[77]. Md. Mominul, H. (2024). Quantitative Assessment Of Smart City IOT Integration For Reducing Urban Infrastructure Vulnerabilities. *Review of Applied Science and Technology*, *3*(04), 48-93. https://doi.org/10.63125/f2cj4507

[78]. Md. Mominul, H., & Syed Zaki, U. (2024). A Review On Sustainable Building Materials And Their Role In Enhancing U.S. Green Infrastructure Goals. *Journal of Sustainable Development and Policy*, *3*(04), 65-100. https://doi.org/10.63125/bfmmay79

[79]. Md.Akbar, H., & Farzana, A. (2021). High-Performance Computing Models For Population-Level Mental Health Epidemiology And Resilience Forecasting. *American Journal of Health and Medical Sciences*, *2*(02), 01–33. https://doi.org/10.63125/k9d5h638

[80]. Mekonnen, A. B., Redley, B., de Courten, B., & Manias, E. (2021). Potentially inappropriate prescribing and its associations with health-related and system-related outcomes in hospitalised older adults: A systematic review and meta-analysis. *British journal of clinical pharmacology*, *87*(11), 4150-4172.

[81]. Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162-183.

[82]. Mircea, M., Stoica, M., & Ghilic-Micu, B. (2022). Analysis of the impact of blockchain and internet of things (BIoT) on public procurement. *Ieee Access*, *10*, 63353-63374.

[83]. Mohammad Mushfequr, R., & Ashraful, I. (2023). Automation And Risk Mitigation in Healthcare Claims: Policy And Compliance Implications. *Review of Applied Science and Technology*, *2*(04), 124–157. https://doi.org/10.63125/v73gyg14

[84]. Mohammad Mushfequr, R., & Sai Praveen, K. (2022). Quantitative Investigation Of Information Security Challenges In U.S. Healthcare Payment Ecosystems. *International Journal of Business and Economics Insights*, *2*(4), 42–73. https://doi.org/10.63125/gcg0fs06

[85]. Moretto, A., & Caniato, F. (2021). Can Supply Chain Finance help mitigate the financial disruption brought by Covid-19? *Journal of Purchasing and Supply Management*, *27*(4), 100713.

[86]. Mortuza, M. M. G., & Rauf, M. A. (2022). Industry 4.0: An Empirical Analysis of Sustainable Business Performance Model Of Bangladeshi Electronic Organisations. *International Journal of Economy and Innovation*. https://gospodarkainnowacje.pl/index.php/issue_view_32/article/view/826

[87]. Mubarik, M. S., Naghavi, N., Mubarik, M., Kusi-Sarpong, S., Khan, S. A., Zaman, S. I., & Kazmi, S. H. A. (2021). Resilience and cleaner production in industry 4.0: Role of supply chain mapping and visibility. *Journal of Cleaner Production*, *292*, 126058.

[88]. Nabil, Y., ElSawy, H., Al-Dharrab, S., Mostafa, H., & Attia, H. (2022). Data aggregation in regular large-scale IoT networks: Granularity, reliability, and delay tradeoffs. *IEEE Internet of Things Journal*, *9*(18), 17767-17784.

[89]. Pal, K. (2020). Internet of things and blockchain technology in apparel manufacturing supply chain data management. *Procedia Computer Science*, *170*, 450-457.

[90]. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, *18*(8), 2575.

[91]. Panayides, P. M. (2019). *The Routledge handbook of maritime management*. Routledge London, UK.

[92]. Pankaz Roy, S., & Md. Kamrul, K. (2023). HACCP and ISO Frameworks For Enhancing Biosecurity In Global Food Distribution Chains. *American Journal of Scholarly Research and Innovation*, *2*(01), 314–356. https://doi.org/10.63125/9pbp4h37

[93]. Pankaz Roy, S., & Sai Praveen, K. (2024). Systematic Review of Stress And Burnout Interventions Among U.S. Healthcare Professionals Using Advanced Computing Approaches. *Journal of Sustainable Development and Policy*, *3*(04), 101-132. https://doi.org/10.63125/9mx2fc43

[94]. Patabendige, M., & Jayawardane, A. (2017). Foley catheter for cervical priming in induction of labour at University Obstetrics Unit, Colombo, Sri Lanka: a clinical audit with a patient satisfaction survey. *BMC Research Notes*, *10*(1), 155.

[95]. Pundir, A. K., Jagannath, J. D., Chakraborty, M., & Ganpathy, L. (2019). Technology integration for improved performance: A case study in digitization of supply chain with integration of internet of things and blockchain technology. 2019 IEEE 9th annual computing and communication workshop and conference (CCWC),

[96]. Rahman, M. H., Uddinb, M. K. S., Hossanc, K. M. R., & Hossaind, M. D. (2024). The role of predictive analytics in early disease detection: a data-driven approach to preventive healthcare. *Journal of the Learning Sciences*, *32*(2), 2024.

[97]. Raja Santhi, A., & Muthuswamy, P. (2022). Influence of blockchain technology in manufacturing supply chain and logistics. *Logistics*, *6*(1), 15.

[98]. Rakibul, H., & Samia, A. (2022). Information System-Based Decision Support Tools: A Systematic Review Of Strategic Applications In Service-Oriented Enterprises. *Review of Applied Science and Technology*, *1*(04), 26-65. https://doi.org/10.63125/w3cevz78

[99]. Rejeb, A., Keogh, J. G., Simske, S. J., Stafford, T., & Treiblmaier, H. (2021). Potentials of blockchain technologies for supply chain collaboration: a conceptual framework. *The International Journal of Logistics Management*, *32*(3), 973-994.

[100]. Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, *11*(7), 161.
[101]. Reza, M., Vorobyova, K., & Rauf, M. (2021). The effect of total rewards system on the performance of employees with a moderating effect of psychological empowerment and the mediation of motivation in the leather industry of Bangladesh. *Engineering Letters*, *29*, 1-29.
[102]. Rikhardsson, P., & Dull, R. (2016). An exploratory study of the adoption, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, *20*, 26-37.
[103]. Rizwan, A., Karras, D. A., Kumar, J., Sánchez-Chero, M., Mogollón Taboada, M. M., & Altamirano, G. C. (2022). An internet of things (IoT) based block chain technology to enhance the quality of supply chain management (SCM). *Mathematical Problems in Engineering*, *2022*(1), 9679050.
[104]. Roh, J., Tokar, T., Swink, M., & Williams, B. (2022). Supply chain resilience to low-/high-impact disruptions: The influence of absorptive capacity. *The International Journal of Logistics Management*, *33*(1), 214-238.
[105]. Saba, A., & Md. Sakib Hasan, H. (2024). Machine Learning And Secure Data Pipelines For Enhancing Patient Safety In Electronic Health Record (EHR) Among U.S. Healthcare Providers. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 124–168. https://doi.org/10.63125/qm4he747
[106]. Salmerón Gómez, R., García García, C., & García Pérez, J. (2020). Comment on "a note on collinearity diagnostics and centering" by velilla (2018). *The American Statistician*, *74*(1), 68-71.
[107]. Samuel, O., Javaid, N., Awais, M., Ahmed, Z., Imran, M., & Guizani, M. (2019). A blockchain model for fair data sharing in deregulated smart grids. 2019 IEEE Global Communications Conference (GLOBECOM),
[108]. Sarfaty, G. A. (2015). Shining light on global supply chains. *Harv. Int'l LJ*, *56*, 419.
[109]. Schuhmann, R., & Eichhorn, B. (2019). Contractual Management—A Holistic Approach to a Diverse Issue. In *Contractual Management: Managing Through Contracts* (pp. 3-52). Springer.
[110]. Sezer, B. B., Topal, S., & Nuriyev, U. (2022). TPPSUPPLY: A traceable and privacy-preserving blockchain system architecture for the supply chain. *Journal of Information Security and Applications*, *66*, 103116.
[111]. Shahzad, A., & Zhang, K. (2020). An integrated IoT-blockchain implementation for end-to-end supply chain. Proceedings of the Future Technologies Conference,
[112]. Shaikat, B., & Md. Wahid Zaman, R. (2024). Quantum-Resistant Cryptographic Protocols Integrated With AI For Securing Cloud And IOT Environments. *International Journal of Business and Economics Insights*, *4*(4), 60–90. https://doi.org/10.63125/dryw3b96
[113]. Shaikh, S., & Md. Tahmid Farabe, S. (2023). Digital Twin-Driven Process Modeling For Energy Efficiency And Lifecycle Optimization In Industrial Facilities. *American Journal of Interdisciplinary Studies*, *4*(03), 65–95. https://doi.org/10.63125/e4q64869
[114]. Singal, A. K. (2022). Designing platform ecosystems for collaboration, innovation and growth. *Benchmarking: An International Journal*, *29*(9), 2806-2821.
[115]. Spieske, A., Gebhardt, M., Kopyto, M., Birkel, H., & Hartmann, E. (2022). How did supply chain networks handle the COVID-19 pandemic? Empirical evidence from an automotive case study. *International journal of physical distribution & logistics management*, *52*(7), 567-601.
[116]. Srinivasan, M., Srivastava, P., & Iyer, K. N. (2020). An empirical model of salesperson competence, buyer-seller trust and collaboration: The moderating role of technological turbulence and product complexity. *Journal of Marketing Theory and Practice*, *28*(4), 447-459.
[117]. Sudipto, R., & Md. Hasan, I. (2024). Data-Driven Supply Chain Resilience Modeling Through Stochastic Simulation And Sustainable Resource Allocation Analytics. *American Journal of Advanced Technology and Engineering Solutions*, *4*(02), 01-32. https://doi.org/10.63125/p0ptag78
[118]. Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & industrial engineering*, *150*, 106895.
[119]. Tayal, A., Solanki, A., Kondal, R., Nayyar, A., Tanwar, S., & Kumar, N. (2021). Blockchain-based efficient communication for food supply chain industry: Transparency and traceability analysis for sustainable business. *International Journal of Communication Systems*, *34*(4), e4696.
[120]. Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S., & Lam, H. Y. (2019). Blockchain-driven IoT for food traceability with an integrated consensus mechanism. *Ieee Access*, *7*, 129000-129017.
[121]. Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., & Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing*, *63*, 101896.
[122]. Zamal Haider, S., & Hozyfa, S. (2023). A Quantitative Study On IT-Enabled ERP Systems And Their Role In Operational Efficiency. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 62–99. https://doi.org/10.63125/nbpyce10
[123]. Zamal Haider, S., & Sai Praveen, K. (2024). Cloud-Native Data Pipelines For Scalable Audio Analytics And Secure Enterprise Applications. *American Journal of Scholarly Research and Innovation*, *3*(01), 52-83. https://doi.org/10.63125/m4f2aw73
[124]. Zelbst, P. J., Green, K. W., Sower, V. E., & Bond, P. L. (2020). The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *Journal of Manufacturing Technology Management*, *31*(3), 441-457.
[125]. Zhang, M., Tse, Y. K., Dai, J., & Chan, H. K. (2017). Examining green supply chain management and financial performance: roles of social control and environmental dynamism. *IEEE Transactions on Engineering Management*, *66*(1), 20-34.
[126]. Zhu, X., Shi, J., Xie, F., & Song, R. (2020). Pricing strategy and system performance in a cloud-based manufacturing system built on blockchain technology. *Journal of Intelligent Manufacturing*, *31*(8), 1985-2002.

[127]. Zhu, Y., Halpern, M., & Reddi, V. J. (2015). Event-based scheduling for energy-efficient qos (eqos) in mobile web applications. 2015 IEEE 21st International Symposium on High Performance Computer Architecture (HPCA),

[128]. Zobayer, E. (2021a). Data Driven Predictive Maintenance In Petroleum And Power Systems Using Random Forest Regression Model For Reliability Engineering Framework. *Review of Applied Science and Technology*, *6*(1), 108-138. https://doi.org/10.63125/5bjx6963

[129]. Zobayer, E. (2021b). Machine Learning Approaches For Optimization Of Lubricant Performance And Reliability In Complex Mechanical And Manufacturing Systems. *American Journal of Scholarly Research and Innovation*, *1*(01), 61–92. https://doi.org/10.63125/5zvkgg52

[130]. Zobayer, E. (2023). IOT Integration In Intelligent Lubrication Systems For Predictive Maintenance And Performance Optimization In Advanced Manufacturing Industries. *Journal of Sustainable Development and Policy*, *2*(04), 140-173. https://doi.org/10.63125/zybrmx69

[131]. Zobayer, E., & Sabuj Kumar, S. (2024). Enhancing HFO Separator Efficiency: A Data-Driven Approach To Petroleum Systems Optimization. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 261–300. https://doi.org/10.63125/2tzaap28

[132]. Zulqarnain, F. N. U., & Zayadul, H. (2024). Artificial Intelligence Applications For Predicting Renewable-Energy Demand Under Climate Variability. *American Journal of Scholarly Research and Innovation*, *3*(01), 84–116. https://doi.org/10.63125/sg0j6930