sustainability

MDPI

Article

Blockchain as a Foundational Infrastructure for Collaborative Logistics: A Multi-Theoretical Lifecycle Framework

Yousra Chabba *, Moulay Ali El Oualidi and Mustapha Ahlaqqach

Laboratory of Advanced Research in Industrial & Logistic Engineering, Ecole Nationale Supérieure d'Electricité er de Mécanique, Hassan II University, Casablanca 20360, Morocco
* Correspondence: yousra.chabba@ensem.ac.ma

Abstract

Collaborative logistics offers substantial economic, environmental, and operational benefits, yet many collaborations fail to endure. This paper argues that blockchain should be understood not as an efficiency tool but as institutional infrastructure that supports trust, governance, coordination, and organizational memory across the collaboration lifecycle. Integrating transaction cost economics, network governance theory, the natural-resource-based view with dynamic capabilities, and socio-technical systems theory with the multi-level perspective, the paper develops a lifecycle framework spanning emergence, viability, and evolution. The analysis identifies three shifts in collaboration failure modes: from trust deficit to readiness paradox, from opacity-driven to rigidity-driven governance failures, and from relational inertia to capability–infrastructure desynchronization. Cross-theoretical synthesis identifies governance inversion as a potential divergence between technically constituted governance and socially constituted authority. The paper theorizes a potentially non-monotonic trajectory of governance effectiveness, in which reductions in monitoring and enforcement costs may be offset by adaptation, legitimacy, and governance-alignment costs as collaboration evolves. This bounded effectiveness thesis highlights the conditions under which blockchain may support or constrain collaborative governance. Four managerial recommendations and fifteen diagnostic questions provide a structured basis for deployment assessment, helping bridge the gap between optimization models and the organizational realities of collaborative logistics.

Keywords: blockchain; collaborative logistics; multi-theoretical framework; lifecycle analysis

Check for updates

Academic Editor: Ming Liu

Received: 3 September 2026
Revised: 18 September 2026
Accepted: 23 September 2026
Published: 25 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

1.1. The Collaborative Logistics Paradox

Contemporary logistics face a convergence of powerful and structural pressures that make inter-organizational collaboration not merely advantageous but increasingly necessary. First, economic intensification, manifested by margin compression, chronic asset underutilization and rising service expectations, has eroded the viability of isolated operational strategies [1]. Simultaneously, environmental mandates and sustainability commitments increasingly demand emissions reductions, as well as circular flows, and transparent performance accountability imposes coordination demands, rendering unilateral optimization structurally insufficient [2]. Escalating operational complexity, arising from geographic fragmentation, volatile demand, and multi-actor interdependencies, further compounds

these challenges. Together, these forces make collaborative logistics not merely desirable but an increasingly unavoidable structural imperative.

When sustained, collaboration delivers substantial operational, economic, and environmental value. Evidence consistently demonstrates cost reductions through shipment consolidation, improved vehicle utilization, significant reductions in empty running, measurable carbon footprint gains, and strategic access to new markets and capabilities [3–6]. Empirical evidence consistently confirms these benefits across transport pooling, joint warehousing, and collaborative distribution networks. The business case for logistics collaboration is, by now, well established across both horizontal and vertical partnership configurations. Yet the empirical record reveals a striking paradox.

The paradox is threefold. First, collaboration is proven beneficial. The evidence base for cost, efficiency, and sustainability gains is robust. Second, collaboration is widely recognized as necessary. Competitive and regulatory pressures leave firms with diminishing alternatives. Third, collaboration is empirically fragile. Most logistics collaborations struggle to persist beyond their initial years, frequently dissolving during early stabilization and governance phases [2,7]. Crucially, this fragility is not primarily a formation problem: collaborations often succeed in launching but fail in sustaining collective coordination over time, uncovering that collaboration is structurally unstable. This temporal failure pattern reveals not an execution deficit but rather a fundamental infrastructure deficit: the digital and institutional architectures supporting collaboration are systematically inadequate for sustaining collective coordination among independent organizations over time.

To resolve this paradox, collaboration must be conceptualized not as a static organizational arrangement, but as a dynamic socio-economic process unfolding across sequential phases: emergence, viability, and evolution. Each phase introduces distinct coordination challenges and governance requirements. This lifecycle perspective provides the analytical foundation for examining how infrastructures shape the formation, stabilization, and long-term sustainability of collaborative logistics systems.

1.2. Infrastructure Deficits Driving Collaboration Failure

Existing digital infrastructures address isolated coordination problems but fail to support collaborative governance across the full lifecycle. Enterprise systems such as ERP and TMS optimize intra-firm efficiency but reproduce hierarchical control structures that exacerbate power asymmetries when extended to inter-organizational settings [8]. Digital platforms and logistics marketplaces facilitate matchmaking and transactional exchange but centralize governance authority, creating strategic dependency and institutional lock-in for participating firms [9]. Data-sharing architectures, including APIs, EDI and emerging data spaces, enhance technical interoperability and visibility, yet provide no institutional trust layer, no governance automation, and no mechanism for incentive alignment across independent actors. Consequently, none of these infrastructures adequately supports the sustained collective governance required for long-term collaboration. Table 1 maps these deficits systematically across the collaboration lifecycle.

Three observations emerge. First, collaboration exhibits sequential dependency: infrastructure adequacy at each phase conditions the feasibility of subsequent stages. Second, existing solutions display cumulative insufficiency: while current solutions address fragments of individual phases, no infrastructure spans the full governance lifecycle. Third, a structural gap persists: prevailing infrastructures optimize transactions and visibility, not collaborative governance across time. This structural coordination deficit is particularly acute for novel collaborations lacking relational history, multi-actor sustainability systems requiring institutional trust and distributed accountability, and long-term inter-organizational alignment requiring adaptive rule-making and governance continuity [10].

This structural coordination vacuum opens space for investigating whether a qualitatively different infrastructure layer could address the lifecycle-spanning deficits that current solutions leave unresolved.

Table 1. Systematic Infrastructure Deficits Across the Collaboration Lifecycle.

Lifecycle Phase	Infrastructure Requirement	Current Solutions' Capability	Systematic Deficit
Emergence	Neutral coordination substrate; trust without prior relationships	Platforms offer matchmaking but impose proprietary governance; ERPs require bilateral integration	No infrastructure enables collaboration formation among independent actors without centralized authority or pre-existing trust
Viability & Governance	Transparent rules; equitable benefit distribution; opportunism control	Platforms centralize governance over time; APIs lack enforcement; ERPs serve dominant partner	Governance progressively concentrates in dominant actors; no mechanism prevents power asymmetry creep or ensures rule stability
Evolution & Sustainability	Adaptive governance; collective learning; modular reconfiguration	Rigid architectures resist modification; no persistent institutional memory across partner changes	Collaboration cannot evolve governance rules or absorb new partners without destabilizing existing arrangements

1.3. Blockchain as a Foundational Infrastructure Layer

Blockchain technology is conceptualized here not as a tool for optimizing existing supply chain processes but as a decentralized socio-technical infrastructure enabling shared governance, verifiable coordination, and institutional trust without centralized authority [9,11]. Its core architectural properties—distributed consensus, immutability, programmable governance through smart contracts, and transparent rule enforcement—enable collective coordination among independent actors without hierarchical control or bilateral dependence. Thus, it addresses, in principle, the very infrastructure deficits identified previously. Blockchain potentially enables collaboration models that otherwise cannot emerge or persist, rather than merely improving the efficiency of models that already function.

This positioning is deliberately bounded. Blockchain's effectiveness as a collaboration infrastructure is constrained by organizational readiness, pre-existing institutional regimes, regulatory uncertainty, and the inherent complexity of socio-technical system adoption [12,13]. The paper neither promotes blockchain as a universal solution nor dismisses its transformative potential. Instead, it investigates the conditions under which blockchain can serve as a foundational governance infrastructure for collaborative logistics across lifecycle stages.

1.4. Research Gap, Positioning, and Contributions

1.4.1. Research Gap

Existing research on blockchain in supply chain management concentrates on adoption drivers [12], performance impacts [11], and technical architecture design. These streams offer valuable insight into discrete dimensions of blockchain-enabled supply chains, but comparatively less attention has been given to how blockchain-mediated governance evolves as interorganizational collaborations move from formation to stabilization and subsequent adaptation. In particular, existing studies rarely integrate lifecycle dynamics, institutional fragility, and failure mechanisms within a single analytical framework, treating governance, adaptation, and technical architecture as separate concerns rather than as interdependent dimensions of one evolving process. This gap leaves the field without a framework for understanding why blockchain may sustain collaboration viability where conventional infrastructures fail.

1.4.2. Positioning

Table 2 positions this paper against representative prior studies across seven analytical dimensions, highlighting how this work departs from existing approaches.

Table 2. Compact Positioning Against Representative Prior Studies.

Dimension	Prior Studies	This Paper
Primary question	How does blockchain improve SC transparency or efficiency?	How does blockchain enable and sustain collaborative logistics across lifecycle stages?
Theoretical approach	Single-theory (TCE, TAM, TOE) or atheoretical	Sequential multi-theory: STS+MLP, TCE, NGT, NRBV+DC
View of collaboration	Assumed, static, or treated as background condition	Dynamic, fragile socio-technical process
Role of time	Implicit or secondary (adoption timing)	Central explanatory variable
Blockchain positioning	Technology for process automation and efficiency	Foundational governance infrastructure for collaboration
Failure analysis	Rarely addressed	Central theoretical construct
Core contribution type	Efficiency gains, barrier catalogues, adoption models	Lifecycle framework with failure mode transformation thesis

Note: Prior studies represented include [9,11–14], and [15].

1.4.3. Contributions

This paper makes four contributions. First, it conceptualizes blockchain as foundational institutional infrastructure rather than a process optimization technology, developing a lifecycle governance perspective in which blockchain's governance effects vary across Emergence, Viability, and Evolution, and identifying the institutional preconditions for sustainable collaborative optimization in interorganizational logistics arrangements. Second, it introduces failure mode transformation as a new analytical lens: blockchain does not eliminate collaboration fragility but transforms the location and nature of governance vulnerabilities across lifecycle stages. Third, through the integration of transaction cost economics, network governance theory, the natural-resource-based view combined with dynamic capabilities, and socio-technical systems theory with the multi-level perspective, it reveals a governance inversion and theorizes a potentially non-monotonic trajectory of governance effectiveness, conditioned by architectural and organizational boundary conditions. Fourth, it identifies these boundary conditions as a set of theoretical propositions for empirical testing, and translates them into a theory-derived diagnostic framework for practitioner blockchain deployment assessment.

2. Theoretical Foundations

2.1. Collaboration as a Dynamic Socio-Economic Process

Logistics collaboration cannot be reduced to transactional coordination or contractual alignment, but it is a socio-economic process to be constituted and sustained. It is relational, dynamic, and institutionally embedded, requiring ongoing negotiation of shared rules, mutual adaptation, and collective commitment among autonomous organizations. The empirical literature consistently documents this fragility: collaborative logistics arrangements face high failure rates not because they lack economic rationale but because the relational and governance infrastructure required to sustain them is difficult to build and maintain [3,5,16]. Understanding collaboration therefore demands analytical frameworks that treat it as a process unfolding over time, not as a structural choice made at a single point.

This temporal dimension is analytically consequential because early-stage challenges differ fundamentally from late-stage challenges. While initial formation revolves around partner selection, trust building, and commitment formation, later phases are dominated by governance drift, incentive erosion, power asymmetry, and institutional inertia. Most collaboration failures emerge not at formation but during governance stabilization and adaptation [2]. Static analysis, which evaluates collaboration at a snapshot in time, systematically underestimates three critical degradation mechanisms: governance drift, whereby agreed-upon rules progressively diverge from enacted practice; capability stagnation, whereby initial competencies fail to evolve with changing demands; and coordination fatigue, whereby the ongoing costs of maintaining collective action erode participants' commitment [17]. These observations justify treating time as a central analytical variable to capture how collaboration viability unfolds, degrades, and potentially renews across extended horizons.

This paper conceptualizes collaboration as unfolding across three meta-phases. Emergence concerns how collaboration forms among independent actors lacking prior relational ties. Viability and governance address how collective action is sustained through governance mechanisms that regulate opportunism, distribute value, and preserve legitimacy. Evolution and sustainability examines how collaboration adapts, renews, and maintains strategic relevance under shifting environmental, institutional, and technological conditions. Each phase introduces distinct coordination challenges, necessitating distinct but complementary theoretical lenses.

Two distinct notions of sustainability are relevant across this lifecycle, and the two should not be conflated. Collaboration sustainability refers to its durability which is the capacity of the interorganizational arrangement itself to survive, remain legitimate, and adapt as conditions change—a governance property of the collaboration. Sustainability outcomes refer to the environmental, social, and economic performance the collaboration is intended to generate—for example, emissions reduction, resource efficiency, or equitable value distribution among partners. These are causally connected rather than interchangeable: blockchain infrastructure shapes governance mechanisms, which in turn condition collaboration durability and adaptability; durability and adaptability then determine the collaboration's capacity to pursue and sustain its intended environmental, social, and economic outcomes over time. Where this paper labels the lifecycle's third meta-phase "evolution and sustainability," the term refers to the former sense—the durability and adaptive capacity of the governance arrangement itself—while sustainability outcomes are treated throughout as a downstream consequence that adaptive governance capacity makes possible but does not guarantee.

2.2. Blockchain as Socio-Technical Infrastructure

2.2.1. Blockchain as Institutional Technology

Blockchain should be conceptualized not as a transactional technology but as an institutional technology that performs core governance functions. It is a decentralized infrastructure that performs institutional functions: distributed trust generation through cryptographic verification, embedded governance enforcement through smart contracts, protocolized coordination through shared consensus mechanisms, and persistent institutional memory through immutable ledger records. The technology provides credible commitments, accountability, and enforcement mechanisms independently of centralized authority. In this sense, blockchain operates as a proto-institutional scaffold, a technical architecture that performs institutional trust functions prior to the emergence of relational trust [9]. By substituting algorithmic assurance for absent interpersonal confidence,

blockchain enables coordination among actors who lack pre-existing relationships, thereby facilitating the initial constitution of collaborative structures.

2.2.2. Blockchain Versus Existing Infrastructure Logics

The critical contrast between blockchain and existing digital infrastructures is not technical, centralized versus distributed databases, but institutional. ERP and TMS systems embed hierarchical control logics; when extended to inter-organizational settings, they reproduce the power asymmetries of the dominant firm [8]. Platform architectures centralize governance authority in the platform operator, creating strategic dependency for participants. APIs and data spaces improve technical interoperability but provide no governance layer: they enable data exchange without the safeguards, credible commitments, and enforcement mechanisms that sustain collaboration over time. Existing digital infrastructures, in short, address the informational dimensions of coordination costs but not their governance dimensions [18]. Blockchain's distinctive proposition is that it embeds governance directly into protocol: collective rule-making rather than hierarchical control, distributed authority rather than centralized platforms, and institutional trust embedded in code rather than technical interoperability alone.

2.2.3. Architectural Specification and Governance-Layer Flexibility

The institutional functions described above are not uniform across all blockchain architectures. This paper's claims concern specifically permissioned, consortium-governed blockchain environments of the kind relevant to interorganizational logistics collaborations—architectures in which membership and participation are controlled by the collaborating organizations rather than open to anonymous public actors. Such architectures typically combine controlled membership and identity management, channels or private data collections that restrict visibility of sensitive transactions to authorized subsets of participants, smart contracts encoding agreed rules, and endorsement policies specifying which parties must approve a transaction, a rule change, or a new member before it takes effect.

This architectural specificity exposes a distinction on which the remainder of the analysis depends. At the ledger level, historical records are tamper-evident and persistent: once validated and committed, a transaction cannot be silently altered or deleted. At the governance/application level, however, the rules that govern the network—smart contract logic, endorsement policies, membership criteria, access permissions—can be deliberately revised through the consortium's agreed governance procedures. Immutability of the record therefore does not imply immutability of governance: the layer designed to resist tampering is not the same layer that determines whether the network's rules can adapt.

The extent to which the governance layer can in fact be revised—how readily contracts can be upgraded, how membership and endorsement rules can be amended, and how much authority participants retain over such changes—is what this paper terms architectural flexibility. Architectural flexibility functions as a boundary condition on the relationship between blockchain-mediated codification and governance rigidity: where architectural flexibility is low, codified rules resist adaptation as circumstances change, sharpening the maladaptation risks discussed in Section 3.6; where architectural flexibility is high—through modular, upgradeable smart contracts and meta-governance procedures specifying how the network's own rules may be revised—codification can coexist with a meaningful capacity for controlled adaptation, as discussed further in Section 3.9. Codification and rigidity are therefore not equivalent: rigidity is conditional on architectural flexibility, not an inherent property of the ledger itself.

2.2.4. Data Provenance and the Limits of Ledger Verification

A related qualification concerns what a blockchain record can and cannot verify. The technology's institutional value rests on its capacity to preserve, once entered, a tamper-evident history of transactions and governance decisions. It does not verify the accuracy of information at the point of entry. Data reaches the ledger through a chain that originates outside it: a physical or organizational event occurs; it is captured through an ERP system, an IoT sensor, or a human operator; that input is, or is not, subject to some form of verification or submission governance; only then is it recorded on-chain, where it becomes immutable and auditable. Blockchain strengthens the integrity and traceability of the record once this chain is complete, but it cannot by itself guarantee the truthfulness, completeness, or accuracy of the underlying event report—a limitation well documented in the oracle-problem literature. This distinction qualifies claims made throughout the remainder of this paper: where blockchain is described as reducing information asymmetry or improving observability, the claim concerns the visibility and traceability of recorded transactions, conditional on the quality of data verification and submission governance upstream of the ledger—not a claim that inaccurate, incomplete, or manipulated data is thereby prevented from entering the record.

2.2.5. Mechanism Anchors

The lifecycle framework in Section 3 deploys four blockchain-enabled mechanisms, each addressing a specific infrastructure deficit identified in Table 1.

- Trust bootstrapping addresses the Emergence deficit: blockchain provides cryptographic verification that substitutes for absent relational trust, enabling coordination among actors without prior relationships or shared governance history.
- Governance automation addresses the Viability deficit: smart contracts operationalize agreed-upon rules as self-executing code, reducing the gap between agreed and enacted governance and functioning as self-enforcing safeguards against opportunism [9,13].
- Coordination verifiability addresses cross-phase accountability: a shared, tamper-evident ledger provides continuous performance records that substantially reduce post-record informational opacity at the governance interface, conditional on the input-verification and data-submission governance discussed in Section 2.2.4.
- Institutional persistence addresses the Evolution deficit: the immutable ledger creates permanent institutional memory in the form of a complete record of governance decisions, performance histories, and contractual evolution that persists across partner changes and organizational transitions.

These four mechanisms are the analytical building blocks through which Section 3 evaluates blockchain's lifecycle-spanning potential.

2.3. Multi-Theoretical Framework

Understanding blockchain-enabled collaborative logistics requires a multi-theoretical perspective because collaboration involves economic, relational, organizational, institutional, and technological dimensions that cannot be adequately captured by a single theoretical lens. Accordingly, this study draws on four complementary theoretical perspectives: Transaction Cost Economics [19], Network Governance Theory [20,21], the Natural Resource-Based View extended through Dynamic Capabilities perspectives [22,23], and Socio-Technical Systems theory integrated with the Multi-Level Perspective approaches [24,25]. These perspectives are not assigned one-to-one to the three lifecycle phases. Rather, they address different dimensions of the governance problem and remain analytically relevant throughout the lifecycle, while their relative salience may shift as the

dominant coordination problem changes from formation to stabilization and adaptation. Their application across the lifecycle is developed in Section 3.

2.3.1. Complementary Theoretical Lenses

The four perspectives provide distinct but complementary explanations of how blockchain-enabled collaborative arrangements may be formed, governed, and adapted. Table 3 summarizes their respective analytical questions, key constructs, contributions to the framework, and boundaries.

Table 3. Complementary theoretical lenses in the integrated framework.

Theoretical Perspective	Core Analytical Question	Key Constructs	Contribution to the Framework	Main Analytical Boundary
TCE [19]	How may blockchain alter the costs of monitoring, enforcement, coordination, and adaptation in interorganizational arrangements?	Bounded rationality, opportunism, asset specificity, uncertainty, frequency, transaction costs	Explains changes in transaction and governance costs associated with information, monitoring, verification, enforcement, and adaptation	Provides limited explanation of relational legitimacy, multilateral power relations, and broader socio-technical transition
NGT [20,21]	How may blockchain reshape governance among autonomous and interdependent actors?	Trust, legitimacy, reputation, collective sanctions, governance form, relational governance, power	Explains changes in trust, legitimacy, authority, relational coordination, and power distribution	Provides less direct explanation of transaction-cost structures and technological or organizational capability evolution
NRBV & DC [22,23]	How may blockchain-enabled governance influence organizational capabilities and adaptation over time?	Valuable resources, sensing, seizing, transforming, resource configurations, adaptation	Explains capability development, resource reconfiguration, strategic adaptation, and longer-term evolution	Provides less direct explanation of immediate governance mechanisms, relational authority, and transaction-level coordination
STS & MLP [24,25]	Under what socio-technical and institutional conditions may blockchain-enabled collaboration emerge and evolve?	Socio-technical alignment, niche, regime, landscape, institutional inertia, social and technical interaction	Explains contextual conditions, institutional embedding, socio-technical alignment, and transition dynamics	Provides less direct explanation of transaction costs and specific network-governance mechanisms

The perspectives therefore operate as complementary analytical lenses rather than sequential theoretical stages. TCE draws attention to how blockchain may redistribute monitoring, enforcement, coordination, and adaptation costs; NGT examines how these changes interact with trust, legitimacy, authority, and power among autonomous actors; NRBV/DC considers whether organizations possess and develop the capabilities required to adapt collaborative arrangements; and STS/MLP situates these processes within broader organizational, technological, and institutional contexts. Considering these dimensions jointly is important because a governance arrangement may, for example, reduce monitoring costs while generating concerns about legitimacy, or improve coordination while becoming difficult to adapt when organizational or environmental conditions change. The integrated perspective therefore treats blockchain not as an isolated efficiency technology but as an infrastructure whose governance effects depend on the interaction between technological properties, organizational capabilities, relational arrangements, and institutional context.

This integration also establishes an important distinction between theoretical lens and lifecycle phase. The three lifecycle phases—Emergence, Viability, and Evolution—represent temporal and organizational contexts in which different coordination problems become salient; they do not correspond to separate theories. Thus, all four perspectives may inform analysis within each phase, although their relative explanatory salience may vary. For example, socio-technical alignment and uncertainty may be particularly important when a collaboration is being established, while monitoring, enforcement, legitimacy, and authority

may become more prominent as the arrangement stabilizes. During longer-term evolution, capability development and socio-technical adaptation may become increasingly important.

2.3.2. Framework Development Approach

The framework was developed through a structured conceptual synthesis. The synthesis began from the focal problem of collaborative logistics arrangements that may remain institutionally and organizationally fragile despite the introduction of technologies intended to improve information sharing, coordination, monitoring, and trust. Relevant literature was considered across four complementary domains corresponding to distinct sources of this fragility: transaction and governance costs, relational and network governance, organizational capabilities and adaptation, and socio-technical and institutional alignment. The four theoretical perspectives were retained because each addresses a mechanism that is not fully captured by the other perspectives. Their combination therefore provides a broader explanatory basis for examining how blockchain-mediated governance can alter collaboration across time.

The synthesis proceeded by comparing the explanatory mechanisms and boundaries of the four perspectives and then examining how these mechanisms interact across the Emergence–Viability–Evolution lifecycle. Rather than treating the theories as independent explanations, the framework considers their intersections: transaction-cost changes may influence relational governance; governance arrangements may affect organizational capabilities and willingness to adapt; and both technological and organizational changes may be conditioned by wider socio-technical and institutional structures. This process led to the integrated framework presented in Figure 1, in which blockchain infrastructure influences governance mechanisms, governance mechanisms shape interorganizational outcomes, and these relationships evolve across the collaboration lifecycle. The framework also recognizes boundary conditions that may alter the strength or direction of these relationships, including architectural flexibility, governance–authority distribution, environmental uncertainty, task contractibility, relational embeddedness, and the quality and provenance of recorded data.

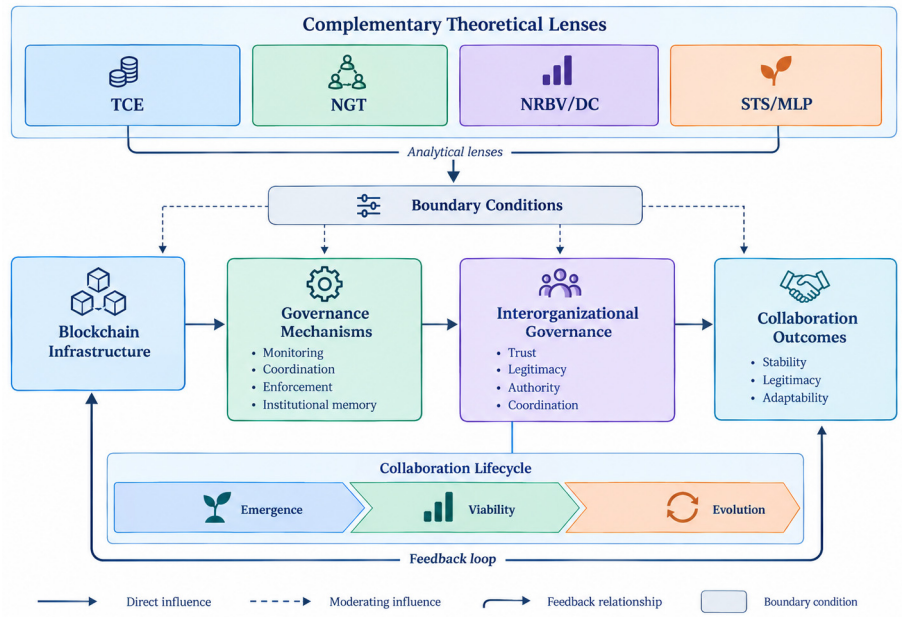


Figure 1. Integrated theoretical framework for blockchain-enabled collaborative logistics.

Importantly, the framework is conceptual rather than empirically validated. The relationships identified through the synthesis should therefore be understood as theoretical

mechanisms and propositions that require empirical examination rather than as established causal regularities. In particular, the lifecycle patterns and governance tensions developed later in the paper provide theoretical expectations about when blockchain-mediated governance may support or constrain collaboration; they do not imply that these effects occur uniformly across all blockchain architectures or collaborative settings.

The literature base was identified through targeted searches of peer-reviewed research on blockchain-enabled interorganizational collaboration, logistics and supply-chain collaboration, governance, organizational capabilities, and socio-technical transitions, with emphasis placed on studies that addressed coordination mechanisms, governance arrangements, organizational adaptation, or institutional context. Studies were retained for the synthesis when they provided a clearly articulated mechanism relevant to at least one of these dimensions or informed the boundary conditions of blockchain-enabled collaboration.

3. Blockchain Across the Lifecycle

The lifecycle framework developed in this study examines how blockchain-mediated governance interacts with the coordination problems of inter-organizational collaboration as they change over time. Rather than assigning one theoretical lens to each phase, the analysis applies the integrated framework developed in Section 2.3 across three meta-phases: Emergence, Viability, and Evolution. At each phase, the analysis identifies the dominant collaboration problem, examines what blockchain changes in the underlying governance arrangement, and considers which problems remain or may emerge as a consequence of that change.

This approach treats blockchain as a heterogeneous socio-technical infrastructure rather than as a uniform technology. Permissioned and permissionless architectures, different distributions of validation authority, privacy mechanisms, data-access arrangements, and different levels of smart-contract and governance upgradeability can generate substantially different governance conditions. The mechanisms developed below should therefore be understood as conditional rather than inherent properties of blockchain.

The cases discussed in this section are used as illustrative and comparative evidence, not as empirical tests of the theoretical propositions. In particular, the TradeLens case provides a detailed illustration of the interaction between technical architecture and institutional governance, while GSBN provides a same-industry contrast that helps identify a relevant boundary condition. The broader empirical implications and operationalization of the propositions are developed in Section 4.1.

Meta-Phase I: Emergence

3.1. Emergence: Formation and Socio-Technical Alignment

The emergence phase concerns the formation of collaboration among organizations that must coordinate while retaining separate interests, assets, capabilities, and decision rights. The formation problem therefore extends beyond the decision to adopt a technology. Prospective participants must agree on what information will be exchanged, how transactions will be coordinated, which rules will apply, who will possess decision rights, and how benefits, costs, and risks will be distributed.

These decisions simultaneously involve economic, relational, organizational, and socio-technical conditions. Transaction-related uncertainty and relationship-specific investments affect the expected cost of forming the collaboration. Relational conditions influence whether participants are willing to share information and accept collective rules. Organizational capabilities determine whether firms can absorb new technologies and modify established processes. Existing information systems, institutional arrangements,

and industry structures further influence whether a new collaborative infrastructure can be integrated into the prevailing socio-technical environment.

The emergence problem can therefore be characterized as one of alignment under uncertainty. A technically feasible infrastructure may remain difficult to establish when participants disagree about data ownership, governance authority, standards, value distribution, or the organizational changes required for participation. Conversely, external pressures such as regulatory requirements, supply disruptions, sustainability demands, or increasing coordination complexity may increase the perceived value of collective infrastructure and stimulate adoption.

3.2. Structural Barriers to Collaboration Formation

Three interconnected groups of barriers are particularly relevant.

First, relational barriers arise because prospective partners may lack a history of cooperation. Concerns about information disclosure, unequal benefit distribution, opportunistic behavior, and the absence of established conflict-resolution mechanisms can limit collective commitment [3,5].

Second, economic and organizational barriers arise from the costs and risks associated with creating a new collaborative arrangement. Organizations may need to invest in system integration, process redesign, specialized capabilities, or relationship-specific assets. These investments can create switching costs and increase concerns regarding opportunism or unequal appropriation of benefits [26].

Third, socio-technical barriers arise from the coexistence of the proposed infrastructure with incumbent systems and routines. ERP, EDI, TMS, proprietary platforms, and bilateral interfaces may already be deeply embedded in organizational processes. Their technical and institutional embeddedness can make the introduction of a new shared infrastructure difficult even when the latter promises improved coordination [25].

These barriers interact rather than operate independently. Low relational trust can increase the potential value of credible information-sharing mechanisms while simultaneously making organizations reluctant to share commercially sensitive information. Technical heterogeneity can increase the value of interoperability while increasing implementation costs. Strong incumbent infrastructures can reduce the immediate need for a new coordination layer while increasing the cost of introducing one.

The formation challenge is therefore not simply that collaboration is costly. Rather, the conditions that increase the potential value of a shared governance infrastructure may also increase the difficulty of establishing that infrastructure.

3.3. Blockchain Mechanisms and the Readiness Paradox

Blockchain can potentially modify several of these formation conditions. In permissioned architectures, authorized participants can share a common record while retaining controlled access to sensitive information. Cryptographic mechanisms can provide evidence that recorded transactions have not been altered after validation, while smart contracts can formalize selected rules that are sufficiently precise and stable.

Blockchain integrity should also be distinguished from the accuracy or completeness of the information submitted to the ledger. The infrastructure can preserve and make auditable a record after validation, but it does not independently establish that an ERP entry, sensor reading, shipment status, or human-submitted event accurately represents the underlying physical transaction. Data provenance, validation responsibilities, and mechanisms for governing erroneous or manipulated inputs therefore remain part of the collaboration's institutional governance.

These mechanisms may reduce reliance on some forms of interpersonal assurance for transactions that can be objectively verified. They may also improve the availability and traceability of recorded performance information and reduce some forms of bilateral reconciliation. However, these technical capabilities do not eliminate the organizational conditions required to establish the network.

Participants must still agree on membership, standards, data rights, validation responsibilities, governance procedures, and mechanisms for changing the system. They must also possess the technical and organizational capabilities required to integrate and operate the infrastructure.

This creates the Readiness Paradox proposed in this study: blockchain may have greater potential value when existing coordination mechanisms are weak, while the same conditions that create this potential value may make collective implementation more difficult. Low trust can increase the potential value of a shared verification infrastructure but also increase resistance to delegating authority or exposing information. Technical heterogeneity can increase the value of interoperability while simultaneously increasing the cost of achieving it.

The paradox should not be interpreted as implying that blockchain replaces trust. Rather, it suggests that the nature of the required governance capacity may change. Some assurance requirements concerning verifiable transactions may be partially transferred to technical mechanisms, while organizational readiness, collective rule-setting, technical compatibility, and governance capacity become more important.

This mechanism is also conditioned by architecture. A permissioned consortium with controlled membership and private data arrangements creates different adoption requirements from an open network. Likewise, architectures in which smart contracts and governance rules can be legitimately upgraded provide different adaptation possibilities from architectures in which these elements are highly constrained. Architectural flexibility therefore moderates the relationship between blockchain adoption and organizational readiness.

Technical feasibility should consequently be distinguished from organizational readiness. A blockchain implementation can demonstrate that heterogeneous participants, privacy requirements, and inter-organizational transactions can be represented within a given architecture without demonstrating that independent organizations would voluntarily adopt or sustain such an infrastructure [27]. This distinction is important because readiness is an organizational and institutional construct rather than a purely technical property.

Meta-Phase II: Viability and Governance

3.4. Viability: Monitoring, Enforcement and Relational Governance

Once collaboration has been established, the central governance problem changes from formation to sustained coordination. Participants must determine whether agreed obligations are being met, respond to deviations, resolve disputes, and maintain sufficient legitimacy for continued participation.

Blockchain can affect some of these functions directly. Shared records can improve traceability of selected events, while smart contracts can automate rules that are sufficiently precise and contractible. These mechanisms may reduce some monitoring and enforcement costs by reducing reliance on repeated bilateral reconciliation and by making selected transaction histories more consistently available to authorized participants.

However, improved monitoring does not eliminate the need for relational governance. Participants still have to decide who establishes the rules, who can modify them, who admits new members, how disputes are resolved, how benefits are distributed, and how exceptional situations are handled.

This creates a distinction between technical governance and institutional governance. Technical mechanisms determine how selected rules are executed and records maintained, whereas institutional governance determines who has authority to define, interpret, and change those rules.

The resulting governance problem is therefore not whether blockchain makes governance universally more effective. It is which governance functions are transferred to the technical infrastructure, which remain organizational or relational, and whether that allocation remains legitimate and adaptable over time.

3.5. Governance Fragilities in Ongoing Collaboration: TradeLens and GSBN

The TradeLens case provides a particularly useful illustration because it allows the interaction between transaction costs, network governance, and socio-technical structure to be examined within a single inter-organizational platform.

From a TCE perspective, the value proposition of TradeLens can be understood partly in terms of reducing information-exchange and reconciliation costs. Global shipping involves multiple carriers, terminals, shippers, freight forwarders, customs authorities, and other actors whose records and workflows have historically been fragmented. A shared and verifiable record can reduce the need for repeated bilateral reconciliation and improve the availability of information across organizational boundaries. The relevant theoretical mechanism is therefore a potential reduction in ex-post monitoring and coordination costs.

Yet this mechanism does not resolve the entire governance problem. Reducing the cost of observing or reconciling transactions does not determine who has authority to establish platform priorities, admit participants, change data-sharing arrangements, modify technical rules, or determine how benefits are distributed. These questions concern governance authority rather than record visibility.

This distinction provides the analytical core of Governance Inversion. The concept refers to a possible divergence between the distribution of technical governance and the distribution of institutional authority: a blockchain architecture may distribute validation and recordkeeping across multiple participants without producing an equivalent distribution of authority over the platform's rules.

TradeLens is particularly informative in this respect because its architecture was developed within a platform ecosystem jointly initiated by Mærsk and IBM. The literature identifies three interrelated governance domains: strategic governance concerning ownership, participation, benefits, and platform development; technology governance concerning the blockchain architecture and data arrangements; and interoperability governance concerning connections with participants' existing systems and other platforms. The case therefore demonstrates that distributed technical infrastructure does not remove the need for organizational governance above and around the ledger.

The issue was particularly consequential because the shipping industry contains powerful competing actors with limited incentives to place commercially sensitive information under arrangements perceived as favoring a direct competitor. The initial sponsor-centered governance arrangement could facilitate rapid development and decision-making, but it also created a neutrality challenge as the platform sought industry-wide participation. TradeLens subsequently introduced mechanisms intended to broaden participation and governance, demonstrating that governance itself was capable of adaptation. Nevertheless, the platform ultimately did not achieve the level of industry-wide collaboration and commercial viability required for continued operation [28].

The theoretical interpretation is therefore more specific than a simple claim of "governance failure." TradeLens illustrates how technical decentralization can coexist with organizational concentration of authority, creating a potential legitimacy problem when

participants are competitors and when the infrastructure requires broad participation to generate network value.

This is where NGT adds explanatory power beyond TCE. A reduction in monitoring or reconciliation costs does not necessarily create legitimacy. Participants may still ask whether governance arrangements are neutral, whether decision rights are fairly distributed, whether their commercially sensitive information is adequately protected, and whether they possess meaningful influence over the evolution of the platform. If these concerns remain unresolved, participants may limit participation or data sharing even when the underlying technology provides clear coordination benefits.

An STS/MLP perspective adds a further layer. TradeLens represented an attempt to establish a new socio-technical arrangement around shared digital infrastructure in an industry historically characterized by fragmented information systems and bilateral coordination. However, technical decentralization alone did not automatically transform the organizational structure through which authority was exercised. The emerging infrastructure could therefore reproduce elements of incumbent sponsor-centered coordination at the organizational level even while decentralizing aspects of digital recordkeeping.

The three perspectives consequently converge on a mechanism that is difficult to capture through any single theory:

technical decentralization $\neq$ organizational decentralization.

A network can distribute validation, recordkeeping, and access across multiple participants while a smaller group retains substantial influence over strategic priorities, membership, or rule modification. Governance Inversion therefore concerns the possibility that a technology designed to reduce dependence on centralized intermediaries can create, preserve, or relocate dependence at the governance layer.

Importantly, TradeLens should not be interpreted as proving this mechanism. Its discontinuation cannot be attributed to a single governance factor. The platform's own discontinuation announcement emphasized that full global industry collaboration had not been achieved and that the platform had not reached sufficient commercial viability. Other analyses additionally identify adoption, incentives, interoperability, and market conditions as relevant factors. TradeLens therefore provides a theoretically rich illustration of the mechanism rather than a causal test of Governance Inversion.

The Global Shipping Business Network (GSBN) provides a same-industry contrast that helps specify the boundary conditions of this mechanism. GSBN was established with an independent, not-for-profit consortium governance involving major maritime industry participants. This arrangement differs from the sponsor-led origins of TradeLens and places greater emphasis on distributing strategic authority among participating industry actors.

The comparison can again be interpreted through multiple lenses. From a TCE perspective, distributing strategic authority among multiple members can increase the upfront costs of collective decision-making and negotiation compared with concentrated sponsor control. From an NGT perspective, however, greater participation in rule-setting may strengthen perceptions of neutrality and legitimacy among organizations that are otherwise competitors. From an STS/MLP perspective, the institutional configuration surrounding the technology differs from the technical infrastructure itself, demonstrating that similar technological principles can be embedded within different organizational arrangements.

GSBN therefore identifies governance–authority distribution as a boundary condition for Governance Inversion. The relevant question is not simply whether a blockchain network is technically distributed, but whether the authority to define and modify the institutional rules of the network is distributed in a manner regarded as legitimate by participants.

At the same time, GSBN should not be interpreted as evidence that member-owned governance guarantees network survival or superior performance. Continued operation

is consistent with the proposed mechanism, but the contrast between two cases cannot establish a general causal relationship. It instead motivates comparative empirical research examining how governance–authority distribution affects participation, legitimacy, data sharing, investment, and collaboration durability across blockchain ecosystems.

3.6. Blockchain and the Failure Mode Transformation Thesis

The preceding analysis suggests that blockchain may alter not only the coordination mechanisms used in collaborative logistics, but also the form in which collaboration vulnerabilities appear. Conventional collaboration problems such as information opacity, unverifiable claims, fragmented records, and difficulties in monitoring interorganizational commitments can be partly addressed through shared records, automated verification, and rule-based execution. However, resolving one source of vulnerability does not necessarily eliminate the underlying governance problem. Instead, the problem may shift toward the rules, protocols, and governance arrangements through which collaboration is structured. This motivates the Failure-Mode Transformation thesis: blockchain adoption may transform the dominant mode of collaboration vulnerability rather than simply remove it.

This proposition follows from the interaction between increased codification and the continuing need for human and organizational adaptation. By making information more consistently recorded and selected processes more explicitly governed by shared rules, blockchain can reduce the scope for certain forms of informational opportunism and coordination ambiguity. At the same time, greater codification can create new points of vulnerability when actors adapt their behavior to the protocol, when rules become difficult to revise, or when increased observability generates additional monitoring demands. The resulting transformation is therefore conditional rather than automatic: the same mechanisms that improve coordination under one set of conditions may create new governance tensions under another.

Three mechanisms illustrate this potential transformation. First, opportunism may shift toward protocol gaming. When contractual or operational rules are encoded into smart contracts or standardized workflows, actors may have fewer opportunities to manipulate shared records directly. However, they may instead adapt their behavior to exploit gaps, thresholds, sequencing rules, or other characteristics of the protocol. The governance problem consequently moves from controlling the integrity of recorded information toward anticipating and governing strategic behavior within the rules. This does not imply that protocol gaming necessarily occurs; its relevance should depend on factors such as task complexity, incentive structures, observability, and the flexibility of the governance process.

Second, mistrust may shift toward governance rigidity. Shared records and automated rule execution can reduce the need to rely on bilateral information exchange, but they do not by themselves establish agreement about who defines, modifies, or interprets the rules. Where participants have competing interests, highly codified governance arrangements may become difficult to adapt when circumstances change. The resulting vulnerability is therefore not simply a lack of trust in information, but disagreement over the legitimacy and adaptability of the institutional rules governing that information. Architectural flexibility and the distribution of governance authority consequently become important conditions determining whether codification stabilizes or constrains collaboration.

Third, opacity may shift toward surveillance overload. Greater visibility of transactions, events, and performance indicators can improve monitoring and make deviations easier to identify. Yet more observable activity can also increase the volume and granularity of information requiring interpretation. Without appropriate governance over what is monitored, by whom, and for what purpose, increased observability may generate excessive monitoring demands, privacy concerns, or strategic responses to measurement. Thus,

transparency should not be treated as an unconditional governance benefit: its value depends on the capacity of participants to interpret information and translate it into legitimate collective action.

These mechanisms point to a broader theoretical implication. Blockchain may change the location of governance vulnerability from the absence or fragmentation of information toward the design, interpretation, and adaptation of the rules through which shared information is used. This represents a transformation of the governance problem rather than a simple transition from failure to success. Whether such transformation improves or undermines collaboration should depend on boundary conditions including task contractibility, environmental uncertainty, relational embeddedness, data provenance, architectural flexibility, and the distribution of governance authority.

The Failure-Mode Transformation thesis should therefore be understood as a theoretical proposition requiring empirical examination, rather than as an established effect of blockchain adoption. Empirical research would need to examine whether the introduction of blockchain is associated with a reduction in pre-existing vulnerabilities and, simultaneously, with the emergence or strengthening of adaptation, protocol-gaming, or governance-rigidity risks. Such evidence would help determine when blockchain changes the form of collaboration failure, when it merely reduces existing vulnerabilities, and when the newly emerging risks outweigh the original governance benefits. Section 4 formalizes this mechanism as a testable proposition and specifies candidate indicators and boundary conditions for its empirical evaluation.

Meta-Phase III: Evolution and Sustainability

3.7. Evolution: Adaptive Capacity and Institutional Change

Once collaboration becomes viable, the dominant problem shifts from stabilization toward adaptation. Partners may change, demand patterns fluctuate, regulations evolve, technologies become obsolete, and sustainability expectations become more demanding. A collaborative arrangement must therefore modify its resources, routines, governance arrangements, and strategic objectives without destroying the continuity that makes collaboration valuable.

This phase places greater emphasis on sensing environmental change, reconfiguring organizational resources, and adapting socio-technical arrangements. Nevertheless, transaction costs and relational governance remain relevant because changes generate renegotiation costs and require legitimate collective decision-making.

Blockchain can support evolutionary capacity by preserving organizational memory, standardizing selected interfaces, and enabling modular technical components. Persistent records can retain institutional knowledge across organizational and personnel changes, while modular architectures can potentially permit selected components to evolve without reconstructing the entire infrastructure.

However, institutional persistence and organizational adaptability do not necessarily evolve at the same rate.

3.8. Structural Inertia, Collaboration Durability, and Sustainability Tensions

As a collaborative blockchain infrastructure moves beyond initial implementation, its ability to support continued coordination depends not only on whether it remains operational, but also on whether its governance arrangements can adapt to changing organizational, market, and sustainability requirements. The transition from viability to evolution therefore introduces a different form of vulnerability. Mechanisms that initially stabilize collaboration by standardizing procedures, preserving shared records, and embedding agreed rules may also increase the cost or difficulty of changing those arrangements

once they become established. The evolution challenge is therefore not whether blockchain works, but whether it can work differently as conditions change.

This tension can be understood as a process of structural inertia. Once participants have aligned processes, data structures, decision rules, and interorganizational routines around a shared blockchain infrastructure, changing these arrangements may require coordinated technical and organizational adjustments across multiple actors. This creates path dependence: established rules and interfaces can become embedded in daily operations, while the costs of redesign, renegotiation, testing, and collective approval may discourage frequent modification. In this sense, persistence can become a source of rigidity. The same infrastructure that reduces uncertainty during collaboration formation and stabilization may therefore constrain adaptation when the assumptions underlying the original configuration no longer hold.

The issue is particularly important because blockchain preserves records more readily than it preserves the appropriateness of the rules used to interpret or act upon those records. A blockchain architecture may permanently preserve historical records while the interpretation, metrics, thresholds, and decision rules applied to those records change over time. Consequently, immutability should not be interpreted as a requirement that governance rules remain unchanged. Rather, the relevant question is whether the infrastructure provides legitimate and technically feasible mechanisms through which governance arrangements can be revised while preserving the integrity and continuity of the shared record. Architectural flexibility therefore becomes an important boundary condition for evolutionary governance.

From a Dynamic Capabilities perspective, this creates a potential mismatch between the need to sense and respond to changing conditions and the capacity of the collaborative infrastructure to accommodate those changes. Changes in customer requirements, regulatory expectations, environmental constraints, supply conditions, or interorganizational relationships may require new data, revised performance criteria, modified workflows, or different decision rights. If the infrastructure can be legitimately reconfigured, blockchain-based institutional memory may support adaptation by providing a persistent basis for evaluating past decisions and coordinating new ones. If reconfiguration is costly, contested, or technically constrained, however, the same institutional memory may reinforce established routines and delay necessary change. The resulting risk is not technological failure in a narrow sense, but a growing misalignment between the infrastructure and the evolving collaboration.

This mechanism also creates tensions for sustainability-oriented change. Sustainability requirements can evolve as firms face new environmental targets, social expectations, reporting requirements, or resource constraints. Such changes may require collaboration participants to modify what is measured, which thresholds trigger action, how responsibilities are allocated, or which trade-offs are considered acceptable. A governance infrastructure designed around an earlier set of objectives may therefore remain operational while becoming progressively less aligned with emerging requirements. The resulting tension is between the durability provided by institutionalized coordination and the adaptability required to accommodate changing strategic and sustainability priorities.

The theoretical implication is not that blockchain necessarily produces rigidity or undermines sustainability. Rather, persistence can have opposing effects depending on the capacity for legitimate adaptation. Stable rules and persistent records can support collaboration durability when the underlying coordination problem remains relatively stable. Under greater environmental uncertainty or changing strategic requirements, however, the benefits of persistence may be offset by adaptation costs if governance and technical arrangements cannot evolve at a sufficient pace. This provides the basis for examining, in the next subsec-

tion, how differences between organizational capability development and infrastructure reconfiguration capacity can generate Capability–Infrastructure Desynchronization.

3.9. Evolutionary Infrastructure and Capability–Infrastructure Desynchronization

Blockchain can therefore provide evolutionary infrastructure without automatically providing evolutionary governance.

Persistent records can function as institutional memory by preserving transaction histories, decisions, and documented performance. Standardized interfaces can support coordination among organizations with different systems, while modular architectures can allow selected components to evolve.

These characteristics can strengthen collaboration durability by reducing institutional amnesia and supporting continuity. Yet organizational capabilities and governance requirements may evolve faster than the infrastructure itself.

This motivates the concept of Capability–Infrastructure Desynchronization: a condition in which organizational capabilities, environmental requirements, or governance needs evolve at a different rate from the flexibility of the infrastructure supporting the collaboration.

Desynchronization can occur in two directions. Organizational and governance requirements may evolve faster than the infrastructure can be legitimately modified. Conversely, technical capabilities may evolve faster than participating organizations can absorb them, creating unused functionality, new coordination burdens, or governance arrangements that exceed organizational capacity.

The concept therefore does not imply that blockchain inevitably becomes rigid. Rather, rigidity becomes more likely to constitute a governance problem when the rate or direction of required change exceeds the architecture's capacity for legitimate reconfiguration.

Architectural flexibility consequently acts as a moderator. Upgradeable smart contracts, controlled rule-change procedures, modular architectures, explicit meta-governance mechanisms, and periodic governance review can potentially reduce desynchronization. Their relevance, however, depends on the uncertainty, contractibility, governance structure, and rate of change characterizing the collaboration.

The sustainability implications follow the same logic. The data layer may remain persistent while the metrics, interpretations, and decision rules applied to those data evolve. Such separation can preserve auditability without freezing the assumptions under which historical information was originally interpreted.

Long-term blockchain-enabled collaboration therefore requires a balance between institutional continuity and legitimate adaptability. The relevant theoretical prediction is not that persistent infrastructure inevitably becomes a constraint, but that the risk of maladaptation increases when organizational and environmental change outpaces the infrastructure's capacity for legitimate governance reconfiguration.

The three lifecycle phases therefore reveal a common pattern: blockchain can alter the location and composition of coordination problems without eliminating their underlying sources. The mechanisms identified across emergence, viability, and evolution—readiness paradox, monitoring–maladaptation tension, governance inversion, and capability–infrastructure desynchronization—provide the analytical basis for the theoretical synthesis that follows. Section 4 integrates these mechanisms across the four theoretical lenses, formulates explicit propositions, and specifies the boundary conditions and empirical requirements needed to examine them.

4. Theoretical Discussion and Empirical Agenda

4.1. Integrated Cross-Theoretical Synthesis and Propositions

The lifecycle analysis in Section 3 shows that blockchain does not affect collaborative logistics through a single mechanism or in a uniform manner. Its governance implications emerge from the interaction between technical infrastructure, transaction characteristics, relational arrangements, organizational capabilities, and the institutional context in which collaboration develops. The four theoretical perspectives adopted in this study therefore operate as complementary analytical lenses rather than sequential, stage-specific explanations. TCE explains changes in monitoring, enforcement, coordination, and adaptation costs; NGT addresses legitimacy, authority, trust, relational governance, and power; NRBV and DC explain capability development and reconfiguration over time; and STS/MLP situates these mechanisms within broader socio-technical and institutional conditions.

The integration of these perspectives is important because none of them, taken separately, captures the full mechanism proposed here. TCE can explain why shared records and automated rules may reduce verification and enforcement costs, but it does not by itself explain whether participants regard the resulting governance arrangement as legitimate. NGT addresses legitimacy and authority, but does not specify how technical codification changes the structure of transaction and adaptation costs. NRBV/DC explains organizational adaptation and capability reconfiguration, but does not explain how technical governance may redistribute decision rights among autonomous participants. STS/MLP captures the alignment between technical and institutional change, but does not by itself specify the transaction-level mechanisms through which monitoring and enforcement are transformed. Their combination therefore makes it possible to examine how a reduction in one source of coordination difficulty may simultaneously create new problems in another governance dimension.

Three cumulative lifecycle mechanisms emerge from this integration. During Emergence, blockchain may reduce some coordination and verification barriers where existing governance mechanisms are weak, while its implementation simultaneously requires collective agreement on standards, data responsibilities, governance arrangements, and participation. This produces the Readiness Paradox: the potential value of the infrastructure may increase as existing coordination becomes more fragile, while the organizational and relational conditions needed to adopt it may become weaker.

During Viability, blockchain can improve monitoring, verification, and enforcement, particularly for stable and contractible activities. However, codification can also increase the cost of dealing with exceptions, contextual decisions, and changing conditions. This produces the Monitoring–Maladaptation Trade-off, through which blockchain may redistribute rather than simply eliminate governance costs.

During Evolution, the central problem becomes the alignment between changing organizational capabilities and the infrastructure's capacity for legitimate reconfiguration. Persistent records can support institutional memory, while flexible architectures can support adaptation. However, divergence between organizational change and infrastructure change can generate Capability–Infrastructure Desynchronization.

Across these mechanisms, a cross-cutting distinction concerns the relationship between technical governance and institutional authority. Distributed records, automated validation, and programmable rules do not necessarily imply distributed authority over membership, upgrades, standards, dispute resolution, or strategic direction. The resulting divergence between the distribution of technical governance rights and the distribution of institutional decision authority is termed Governance Inversion. This is proposed as a theoretical mechanism rather than an established empirical regularity.

Together, these mechanisms suggest that blockchain-enabled governance should be evaluated through multiple dimensions rather than a single measure of technological or operational performance. They also imply that governance effects may change over the collaboration lifecycle. The following sections therefore define governance effectiveness more precisely and formulate propositions that can be empirically examined.

4.1.1. Governance Effectiveness as a Multidimensional Construct

In this framework, governance effectiveness refers to the capacity of a collaborative arrangement to coordinate participating organizations while maintaining enforceability, continuity, legitimacy, and the ability to adapt to changing conditions. It is therefore broader than transaction-cost reduction and should not be equated with logistics efficiency or sustainability performance.

Five dimensions are particularly relevant.

First, monitoring effectiveness concerns the ability to verify relevant transactions, identify discrepancies, and establish an auditable record with limited verification effort. Second, enforcement effectiveness concerns the capacity to implement agreed rules and respond to non-compliance. Third, coordination stability concerns the continuity of participation and the reliability of interorganizational coordination. Fourth, adaptability concerns the capacity to modify governance arrangements in response to technological, market, regulatory, organizational, or strategic change. Fifth, legitimacy concerns whether participants perceive the governance arrangement as sufficiently fair, representative, and acceptable to sustain participation.

These dimensions need not evolve in the same direction. An architecture may improve monitoring and enforcement while reducing adaptability, or may improve technical coordination without generating sufficient institutional legitimacy. Governance effectiveness is consequently treated as a multidimensional construct whose components may involve trade-offs.

The framework also distinguishes collaboration durability from sustainability outcomes. Collaboration durability refers to the capacity of the interorganizational arrangement to remain viable and adaptable over time. Sustainability outcomes refer instead to economic, environmental, or social consequences. The proposed causal sequence is therefore:

blockchain infrastructure → governance mechanisms → collaboration durability and adaptive capacity → ability to pursue sustainability strategies → sustainability outcomes.

Blockchain is thus not assumed to generate sustainability outcomes directly. Its potential contribution is mediated through governance conditions that allow collaborative strategies to persist and evolve.

4.1.2. Theoretical Propositions

The integrated analysis yields five propositions. They are theoretical predictions derived from the conceptual synthesis and require empirical validation.

P1—Readiness Paradox.

The potential governance value of blockchain is expected to increase as existing coordination mechanisms become weaker, while the likelihood of successful collective adoption may decrease as organizational readiness, governance capacity, and relational alignment decline.

The proposition captures the tension identified during Emergence. Blockchain may substitute for some forms of pre-existing trust and verification, but establishing the shared infrastructure requires agreement on standards, governance, data responsibilities, and participation rules. P1 should therefore be examined jointly through measures of the pre-existing coordination deficit and implementation readiness. Relevant boundary condi-

tions include digital maturity, governance capability, external institutional pressure, and relational embeddedness.

A potential counterexample would be a low-trust ecosystem that nevertheless achieves successful adoption because strong regulatory requirements, a credible neutral coordinator, or highly standardized processes compensate for limited relational readiness.

P2—Monitoring–Maladaptation Trade-off.

Blockchain-enabled codification is expected to improve monitoring and enforcement effectiveness for stable and contractible governance activities, but its contribution to overall governance effectiveness may decline as environmental uncertainty, exception frequency, and adaptation requirements increase.

The proposition combines TCE's distinction between monitoring/enforcement and maladaptation costs with NGT and STS/MLP concerns regarding contextual judgment and institutional adaptation. Blockchain should therefore provide greater governance value where rules can be specified ex ante and performance can be measured consistently. In contrast, activities characterized by ambiguity, frequent exceptions, or substantial contextual dependence may generate adaptation costs that offset monitoring gains.

Candidate indicators include verification and reconciliation time, dispute frequency, enforcement costs, exception-handling effort, and rule-change time. Architectural flexibility is an important moderator because upgradeable smart contracts, explicit exception mechanisms, and legitimate rule-change procedures may reduce the predicted maladaptation effect.

A potential counterexample would be a highly uncertain collaboration that nevertheless maintains both strong monitoring and high adaptability because its architecture and governance mechanisms support rapid and legitimate rule modification.

P3—Governance Inversion.

Greater divergence between the distribution of technical governance rights and the distribution of institutional decision authority is expected to increase the risk of legitimacy and participation problems, particularly where participating organizations are direct competitors.

Governance Inversion captures a distinction that technical decentralization alone cannot resolve. Distributed records and validation may coexist with concentrated authority over membership, upgrades, standards, strategic priorities, or dispute resolution.

TradeLens illustrates this mechanism without establishing it empirically. The platform was jointly developed by Maersk and IBM and subsequently introduced mechanisms intended to broaden participation and governance. Its discontinuation was ultimately associated with the failure to achieve sufficient global industry collaboration and commercial viability, rather than being attributable to a single governance factor [28]. The case therefore illustrates why technical functionality cannot by itself neutralize institutional power, competitive concerns, or legitimacy requirements.

Candidate indicators include concentration of decision rights, control over membership and upgrades, representation in governance bodies, perceived procedural fairness, willingness to share data, and continuity of participation. Governance–authority distribution and the competitive relationship among participants constitute important boundary conditions.

A potential counterexample would be a consortium in which technical decision rights remain concentrated, but participants nevertheless perceive the governance arrangement as legitimate and maintain sustained participation.

P4—Capability–Infrastructure Desynchronization.

The greater the divergence between the rate and direction of organizational or governance change and the infrastructure's legitimate capacity for reconfiguration, the greater the risk of maladaptation and collaboration instability.

Desynchronization can occur in either direction. When organizational requirements change faster than the infrastructure can legitimately be modified, technical or governance rigidity may emerge. Conversely, when infrastructure capabilities evolve faster than organizations can absorb or govern them, underutilization, governance complexity, or capability gaps may arise.

P4 connects NRBV/DC's emphasis on sensing, seizing, and transforming with NGT's concern for legitimate collective rule change and STS/MLP's emphasis on socio-technical alignment. Architectural flexibility is consequently a central moderator. Candidate indicators include organizational change rates, infrastructure upgrade time, frequency of governance modifications, participant onboarding time, and the extent to which governance changes can be implemented without destabilizing existing arrangements.

A potential counterexample would be a collaboration with strong meta-governance mechanisms and modular infrastructure in which substantial organizational transformation occurs without significant infrastructure misalignment.

P5—Non-Monotonic Governance Effectiveness.

Blockchain-enabled governance effectiveness may exhibit a non-monotonic relationship over the collaboration lifecycle, such that early gains in monitoring, enforcement, and coordination can be offset when adaptation, legitimacy, or governance-alignment requirements exceed the flexibility of the underlying infrastructure.

P5 is the higher-order proposition emerging from the interaction of P1–P4. An inverted-U-shaped trajectory represents one theoretically plausible form of this non-monotonic relationship, but the framework does not assume that all collaborations will follow the same functional form. The expected trajectory should depend on task contractibility, environmental uncertainty, architectural flexibility, governance–authority distribution, relational embeddedness, and data provenance.

A potential counterexample would be a collaboration in which governance effectiveness remains stable or improves monotonically despite increasing adaptation requirements, for example because modular architecture and effective meta-governance prevent adaptation costs from offsetting monitoring and coordination gains.

The present study predicts that governance gains may initially increase as blockchain reduces monitoring and enforcement burdens but may subsequently diminish when adaptation, legitimacy, or governance-alignment costs become sufficiently large. Empirical validation would therefore require longitudinal observation of the multidimensional governance-effectiveness measures defined above rather than a cross-sectional assessment of blockchain adoption.

The matrix also identifies what observations could challenge the propositions (Table 4). The framework is therefore intended to generate empirically falsifiable predictions rather than merely provide post hoc interpretations.

Table 4. Proposition and Empirical Operationalization Matrix.

Proposition	Theoretical Origin	Core Mechanism	Focal Constructs	Candidate Indicators	Key Boundary Conditions	Potential Falsification
P1 Readiness Paradox	TCE + NGT + STS/MLP	Weak existing coordination increases potential blockchain value while potentially reducing adoption readiness	Coordination deficit; organizational readiness; adoption continuity	Pre-existing governance gaps; digital maturity; implementation readiness; participation commitment	Governance maturity; external institutional pressure; relational embeddedness	Low-readiness/high-value settings repeatedly achieve adoption without compensating coordination mechanisms
P2 Monitoring–Maladaptation Trade-off	TCE + NGT + STS/MLP	Codification lowers monitoring/enforcement costs but may increase adaptation costs	Monitoring; enforcement; adaptability	Verification time; reconciliation effort; disputes; enforcement cost; exception -handling time; rule-change time	Task contractibility; uncertainty; architectural flexibility	High-uncertainty settings sustain governance gains without corresponding adaptation mechanisms

Table 4. *Cont.*

Proposition	Theoretical Origin	Core Mechanism	Focal Constructs	Candidate Indicators	Key Boundary Conditions	Potential Falsification
P3 Governance Inversion	NGT + STS/ MLP + TCE	Technical governance distribution may diverge from institutional authority	Governance–authority distribution; legitimacy; participation	Decision-right concentration; upgrade control; representation; perceived fairness; data-sharing willingness	Participant competition; governance model; institutional legitimacy	Large authority divergence occurs without legitimacy or participation deterioration
P4 Capability–Infrastructure Desynchro-nization	NRBV/ DC + STS/ MLP + NGT	Organizational change and infrastructure reconfiguration proceed at different rates	Capability evolution; infrastructure flexibility; maladaptation	Organizational change rate; upgrade time; governance-change frequency; onboarding time	Architectural modularity; meta-governance; capability maturity	Large change-rate divergence occurs without instability or maladaptation
P5 Non-Monotonic Effectiveness	P1–P4 jointly	Early monitor-ing/coordination gains may be offset by adaptation and legitimacy costs	Overall governance effectiveness	Longitudinal measures of monitoring, enforcement, stability, adaptability, and legitimacy	All preceding boundary conditions	Governance effectiveness remains monotonic or shows no systematic relationship despite changing adaptation requirements

4.1.3. Comparative Longitudinal Evidence and Case-Based Grounding

The propositions are informed by observed variation across blockchain-enabled collaborative ecosystems, but the cases are not treated as controlled tests. Their purpose is to provide comparative and longitudinal variation that helps identify mechanisms requiring further empirical examination.

Cases were selected on three criteria: sufficient publicly documented governance detail to support mechanism-level analysis rather than outcome description alone; direct relevance to horizontal collaboration among competing or formally autonomous organizations, rather than vertical buyer-supplier blockchain deployments; and, for the comparative cohort, contemporaneity with TradeLens's operating period to hold industry-wide technological and macroeconomic conditions approximately constant across cases. Case evidence was drawn from peer-reviewed case studies and analyses, official platform or organizational communications, and publicly available reporting documenting governance arrangements, participation, operational trajectories, and discontinuation or continuation decisions.

TradeLens provides the most detailed logistics illustration of Governance Inversion. The platform was technically developed and operated as a blockchain-enabled infrastructure, yet its long-term challenge involved broader industry participation, governance, and commercial viability rather than technical feasibility alone. Maersk and IBM announced its discontinuation in November 2022, citing the failure to achieve sufficient global industry collaboration and commercial viability [28]. Prior case research documents governance across strategic/off-chain, technology/on-chain, and interoperability domains and shows that governance arrangements evolved as the platform sought broader participation [28]. The case therefore illustrates the analytical distinction between technical functionality and institutional legitimacy.

GSBN provides a useful same-industry contrast. It was established as an independent, not-for-profit consortium involving participating shipping-industry actors, with governance arrangements intended to support broader industry participation [28]. The contrast does not establish that this governance form guarantees continuity. Rather, it demonstrates why governance–authority distribution should be treated as a boundary condition rather than as a technological consequence of blockchain itself.

ReLog provides an additional logistics trajectory. Its longitudinal analysis across successive pilot phases illustrates the practical difficulty of moving a blockchain collaboration from an initial proof of concept toward a functioning supply-chain application [2]. The case reinforces the distinction between technical feasibility, organizational adoption, and sustained ecosystem viability.

Broader blockchain-enabled ecosystems launched during a similar period also display divergent trajectories rather than a uniform lifecycle. In trade finance, we.trade entered insolvency proceedings in 2022, B3i ceased activities and entered insolvency in 2022, Marco Polo entered insolvency in February 2023, and Contour announced the permanent cessation of operations in November 2023 [29]. At the same time, Komgo and VAKT provide examples of platforms that continued to operate and develop their offerings. Public reporting documents Komgo's continued expansion in 2025, while VAKT reported continued use and expansion of its platform across commodity-trading processes during 2024–2025.

This divergence is analytically useful because the ecosystems differed not only in outcome but also in business model, participant composition, governance arrangements, product scope, financing structure, and market conditions. These differences make it inappropriate to attribute continuation or discontinuation to a single common cause. At the same time, the variation provides a basis for examining whether governance–authority distribution, architectural flexibility, contractibility, and organizational alignment help explain why technically similar initiatives follow different trajectories.

The cohort therefore provides comparative longitudinal motivation for P1–P5 rather than empirical validation. In particular, the divergence between continuing and discontinued ecosystems supports the need to examine governance effectiveness as a time-dependent and multidimensional construct. It does not establish that effectiveness necessarily follows an inverted-U function.

4.1.4. Boundary Conditions and Empirical Testing

The propositions imply that blockchain's governance effects are contingent rather than technologically deterministic. Six boundary conditions are particularly important.

Architectural flexibility moderates the relationship between technical codification and maladaptation. Permissioned architectures can incorporate channels, private data collections, configurable endorsement policies, and upgradeable smart contracts. Consequently, ledger-level persistence should not be equated with immutable governance. Empirical studies should distinguish the persistence of historical records from the flexibility of rules, contracts, membership, and access arrangements.

Governance–authority distribution moderates Governance Inversion. The relevant empirical question is not simply whether a ledger is distributed, but who can modify the rules governing participation, validation, access, upgrades, and strategic direction.

Environmental uncertainty affects the relative importance of monitoring versus adaptation. Stable and contractible processes should provide greater scope for codification, whereas volatile environments may require more discretion and rapid governance adjustment.

Task contractibility determines whether a governance activity can be specified sufficiently clearly for automated enforcement. Blockchain should not be expected to generate equivalent value across routine measurable transactions and context-dependent relational decisions.

Relational embeddedness influences whether technical governance complements or substitutes for existing social mechanisms. Low relational embeddedness may increase the value of credible technical commitments during formation, while excessive substitution of technical mechanisms for relational governance may weaken the social foundations of long-term collaboration.

Finally, **data quality and provenance** condition the effectiveness of blockchain-based monitoring. The relevant causal chain is:

physical event → ERP/IoT/operator input → validation and submission governance → blockchain record → persistent/auditable history.

Blockchain can preserve and make auditable a record after it has been submitted, but it does not independently establish that the original ERP entry, sensor reading, shipment status, or human-submitted event accurately represents the underlying physical transaction. Data provenance, input verification, oracle arrangements, and responsibility for erroneous submissions therefore remain part of the collaboration's institutional governance. This limits strong claims that blockchain eliminates information asymmetry or produces complete ex-post observability.

These boundary conditions also provide a basis for empirical research. P1–P4 can be examined through longitudinal case studies, comparative multiple-case research, surveys of consortium participants, interviews, or archival analysis of governance changes. P5 requires a more demanding longitudinal design in which governance effectiveness is measured repeatedly across collaboration stages. Such a design could examine whether monitoring, enforcement, coordination stability, adaptability, and legitimacy follow different trajectories and whether changes in the latter dimensions offset early gains in the former.

The fifteen diagnostic questions developed in this study can support such research, but they should be treated as theory-derived analytical prompts rather than validated measurement instruments. Their empirical validity, relative importance, and decision thresholds require future validation through longitudinal case studies, Delphi research, surveys, or action research with collaborative logistics ecosystems.

4.2. Theoretical Advancement and Cross-Theoretical Integration

The preceding analysis advances the understanding of blockchain-enabled collaborative logistics by shifting attention from the direct performance effects of blockchain toward the governance conditions through which interorganizational collaboration is formed, stabilized, and adapted. Rather than treating blockchain as a technology whose value can be assessed independently of organizational context, the framework conceptualizes it as part of the institutional infrastructure through which coordination, monitoring, authority, and adaptation are organized over time. The theoretical value of this perspective lies therefore not in assigning separate theories to separate lifecycle stages, but in using their intersection to explain how the governance consequences of shared digital infrastructure can change as collaboration develops.

The first theoretical advancement is the lifecycle-dependent view of blockchain governance. The analysis shows that the same infrastructure can address different governance problems across Emergence, Viability, and Evolution, while also creating new tensions as the dominant coordination requirements change. Blockchain-enabled verification and shared records may be valuable for reducing information asymmetries during formation and for monitoring stable transactions during viability, yet the same persistence and codification may become constraints when adaptation and institutional change become more important. Blockchain effectiveness is therefore conceptualized as conditional on the interaction between infrastructure characteristics, governance requirements, and lifecycle conditions rather than as a static property of the technology.

The second advancement is the failure mode transformation perspective. Rather than assuming that blockchain eliminates collaboration fragility, the framework explains how resolving one class of vulnerability may shift fragility toward another. Greater visibility can reduce informational opacity while increasing monitoring demands; codified rules can constrain opportunism while reducing room for contextual adaptation; and persistent records can strengthen accountability while contributing to institutional inertia. This perspective extends technology-centered accounts by treating the redistribution of governance vulnerabilities as a theoretical outcome in its own right.

The cross-theoretical synthesis further clarifies two complementary mechanisms established in Section 4.1. The TCE–NGT combination shows why reductions in monitoring and enforcement costs do not necessarily translate into legitimate or stable governance arrangements; Governance Inversion captures this conditional divergence between technical governance rights and institutionally recognized authority. The TradeLens–GSBN comparison in Section 3.5 illustrates why this distinction is relevant without implying that a particular governance structure mechanically determines outcomes. Similarly, the NRBV/DC–STS/MLP combination identifies the importance of alignment between organizational capabilities, infrastructure reconfiguration, and broader institutional change. As developed in Sections 3.7–3.9 and formalized in P4, capability–infrastructure desynchronization provides a mechanism through which an initially viable architecture may become increasingly misaligned with evolving collaboration requirements.

Taken together, these mechanisms support a conditional and potentially non-monotonic view of governance effectiveness. The propositions developed in Section 4.1 identify conditions under which initial gains in monitoring, enforcement, and coordination may be offset when adaptation, legitimacy, governance alignment, or reconfiguration requirements become more demanding. The form and magnitude of such non-monotonicity are therefore expected to depend on boundary conditions including architectural flexibility, governance–authority distribution, environmental uncertainty, task contractibility, relational embeddedness, and data provenance.

The resulting theoretical perspective is consequently not a claim that blockchain is inherently beneficial or detrimental to collaborative logistics. It is a framework for explaining when and why its governance effects may change as collaboration develops. By connecting transaction costs, relational governance, organizational capabilities, and socio-technical change within a common lifecycle structure, the framework provides a basis for examining both the governance benefits and newly emerging vulnerabilities associated with blockchain as institutional infrastructure. The propositions and diagnostic framework translate these theoretical mechanisms into empirically examinable relationships while maintaining a clear distinction between conceptual explanation and validated empirical effects.

4.3. Toward a Theory-Driven Decision Framework

The multi-theoretical lifecycle analysis generates not only theoretical propositions but also a structured diagnostic framework for assessing whether and how blockchain should be introduced into collaborative logistics. The purpose of this framework is to translate the mechanisms identified in Sections 3 and 4.1 into questions that can guide organizational assessment before and during blockchain deployment. The questions are organized according to the three lifecycle phases and are explicitly linked to the theoretical mechanisms and boundary conditions developed above.

The framework is intended as a theory-derived diagnostic scaffold rather than a validated decision instrument. It does not prescribe blockchain adoption or a particular governance model. Instead, it identifies the conditions that organizations should examine when evaluating the potential governance value, risks, and adaptability requirements of blockchain-enabled collaboration.

Emergence: Should Blockchain Be Adopted for This Collaboration?

E1—Coordination deficit and external pressure (STS/MLP + TCE).

What specific coordination, verification, or trust problem does blockchain address, and is there a credible external or collective forcing function that can support multilateral adoption, or does formation depend entirely on voluntary agreement among self-interested participants?

E2—Organizational readiness (STS/MLP).

Do potential partners possess sufficient digital maturity, governance capacity, and change-management capability to establish and maintain shared blockchain infrastructure, or could limited readiness prevent the potential governance value from being realized?

E3—Transaction characteristics (TCE).

Are the collaboration's transactions sufficiently frequent, measurable, and standardizable to justify the ex-ante costs of blockchain infrastructure, including technical integration, smart-contract design, and protocol coordination?

E4—Governance and asset specificity (TCE + NGT).

Would investment in shared blockchain infrastructure create significant relation-specific technological or governance commitments before the collaboration's viability has been established, and who would bear the resulting dependency risks?

E5—Data and institutional alignment (STS/MLP + NGT).

Do participants agree on data responsibilities, participation rules, standards, and governance authority, and are existing digital infrastructures and institutional arrangements sufficiently compatible with the proposed collaboration?

Viability: How Should Blockchain Governance Be Designed?

V1—Monitoring versus maladaptation (TCE).

For each governance activity, do the expected reductions in monitoring, verification, and enforcement costs outweigh the potential costs of rigidity and exception handling? Which activities are sufficiently routine and measurable to justify codification?

V2—Enforcement versus relational governance (NGT).

Does the collaboration primarily require rule-based enforcement, or does it depend substantially on relational mechanisms such as trust, mutual forbearance, shared identity, and collective commitment?

V3—Governance–authority alignment (NGT + STS/MLP).

Who should hold authority over membership, validation rules, standards, upgrades, access, dispute resolution, and strategic direction, and does this distribution correspond to the authority that participating organizations regard as legitimate?

V4—Hybrid governance boundary (TCE + NGT).

Which rules, transactions, and enforcement mechanisms should be automated or recorded through the technical infrastructure, and which decisions should remain subject to relational or institutional deliberation? Is the boundary between technical and relational governance explicit?

V5—Data provenance and competitive exposure (NGT + TCE).

Who is responsible for validating information before it enters the ledger, how are erroneous or conflicting inputs handled, and could the transparency created by the infrastructure expose commercially sensitive information or alter participants' willingness to share data?

Evolution: Will Blockchain Support or Constrain Long-Term Adaptation?

Ev1—Transformation capacity (NRBV/DC).

Is the collaboration expected to undergo mainly incremental change or potentially fundamental organizational or strategic transformation, and can the infrastructure be legitimately reconfigured at a corresponding rate?

Ev2—Governance and sustainability evolution (NRBV/DC + STS/MLP).

Are the collaboration's performance criteria, sustainability objectives, or measurement frameworks likely to change over time, and has the architecture separated persistent historical data from evolvable metrics, interpretations, and decision rules?

Ev3—Architectural flexibility (STS/MLP + NRBV/DC).

Can smart contracts, membership arrangements, access rights, validation rules, and other governance components be modified when collaboration requirements change, and are the procedures for making such changes technically feasible and institutionally legitimate?

Ev4—Meta-governance (NGT).

Who governs the governance infrastructure itself? Are there legitimate mechanisms and clearly assigned authority for modifying operational rules, resolving governance disputes, and responding to changes in the consortium or its institutional environment?

Ev5—Exit, reconfiguration, and desynchronization (NRBV/DC + NGT).

Does the collaboration have explicit mechanisms for participant exit, onboarding, governance transition, infrastructure migration, and potential dissolution, or could changing organizational capabilities become misaligned with an infrastructure that is difficult to reconfigure?

Taken together, these fifteen questions translate the theoretical propositions into a structured assessment logic. **E1–E5** primarily address the Readiness Paradox by examining whether the governance problem that motivates blockchain is accompanied by sufficient organizational, relational, and institutional readiness for collective implementation. **V1–V5** address the Monitoring–Maladaptation Trade-off and Governance Inversion by examining where codification creates value, where relational governance remains necessary, and whether technical governance rights are aligned with legitimate institutional authority. **Ev1–Ev5** address Capability–Infrastructure Desynchronization by examining whether the infrastructure can evolve alongside organizational capabilities, governance requirements, and changing sustainability objectives.

The framework also provides a direct bridge between the propositions and future empirical research. The questions can be operationalized into observable constructs, interview protocols, survey measures, or comparative case-study criteria. However, they should not yet be interpreted as validated measurement items or as a prescriptive scoring system. Their empirical validity, relative importance, weighting, and decision thresholds remain to be established through longitudinal case research, Delphi studies, surveys, or action research with collaborative logistics ecosystems.

4.4. Managerial and Design Implications

The theoretical synthesis suggests that blockchain deployment in collaborative logistics should be approached as a governance-design decision rather than solely as a technology-selection decision.

First, organizations should distinguish contractible governance from relational governance. Stable, measurable, and repetitive activities are more amenable to automated monitoring and rule enforcement. Activities involving contextual judgment, frequent exceptions, negotiation, or relational adaptation may require continued human and institutional discretion. The framework therefore supports selective codification rather than the assumption that all governance activities should be automated.

Second, governance authority should be designed independently of technical architecture. Distributed records or validation do not automatically produce distributed institutional authority. Consortium participants should explicitly determine who controls membership, protocol changes, smart-contract upgrades, access rules, dispute resolution, and strategic decisions. Technical decentralization should therefore be assessed separately from institutional representation and decision rights.

Third, governance evolution should be designed from the beginning. Because collaboration requirements change, architectures should include legitimate mechanisms for rule modification, smart-contract upgrades, participant onboarding and exit, and periodic gov-

ernance review. The objective is not to eliminate persistence but to distinguish persistent historical evidence from evolvable governance rules and interpretations.

Fourth, data provenance should be governed alongside ledger integrity. Organizations should specify who is responsible for submitting data, how external information is validated, how conflicting inputs are resolved, and how erroneous submissions are corrected or superseded. A tamper-evident record remains dependent on the governance process through which information enters the ledger.

These implications vary across the lifecycle. At Emergence, organizations should assess whether sufficient readiness and institutional alignment exist to establish shared infrastructure. During Viability, attention should shift toward the allocation of monitoring, enforcement, and relational governance responsibilities. During Evolution, organizations should focus on architectural flexibility, meta-governance, institutional learning, and capability–infrastructure alignment.

4.5. Limitations and Empirical Research Agenda

Several limitations delimit the scope of the framework.

First, the study is conceptual rather than empirically validated. The propositions are derived through structured theoretical synthesis and lifecycle analysis rather than tested statistically or through original longitudinal field data. The cases therefore provide illustrative and comparative evidence rather than causal validation.

Second, TradeLens is the principal detailed governance case and therefore cannot establish generality across collaborative logistics. GSBN and ReLog provide useful contrasts, while the broader cohort introduces additional variation. Nevertheless, systematic multiple-case and longitudinal research is required to determine whether the proposed mechanisms recur across ecosystems.

Third, blockchain architectures are heterogeneous. Permissioned consortium networks differ in membership models, consensus arrangements, channels, private-data mechanisms, endorsement policies, smart-contract upgradeability, and governance procedures. The propositions should therefore not be interpreted as predictions about an undifferentiated blockchain technology. Architectural flexibility is explicitly treated as a moderator because different configurations can alter the balance between persistence and adaptability.

Fourth, ledger integrity does not guarantee real-world data accuracy. Empirical research is required to determine how provenance mechanisms, oracle arrangements, validation procedures, and responsibility for external inputs affect governance effectiveness. The framework consequently avoids treating blockchain as an independent source of truth about physical events.

Fifth, collaboration durability and sustainability outcomes are conceptually distinct. The framework proposes that governance infrastructure may influence sustainability indirectly by supporting the continuity and adaptive capacity of collaboration. It does not establish a direct blockchain-to-sustainability relationship. Future studies should therefore examine the complete pathway from governance mechanisms to collaboration durability and subsequently to economic, environmental, and social outcomes.

Finally, P5 requires particular caution. The framework predicts possible non-monotonicity but does not establish a universal inverted-U functional form. Future longitudinal studies should measure governance effectiveness repeatedly across collaboration stages and examine whether early monitoring and enforcement gains are subsequently offset by adaptation, legitimacy, or governance-alignment costs. Comparative research should also test whether the trajectory varies with task contractibility, environmental uncertainty, relational embeddedness, governance–authority distribution, and architectural flexibility.

A productive empirical agenda would combine longitudinal multiple-case studies with quantitative measurement of governance effectiveness, participant surveys concerning legitimacy and willingness to continue data sharing, archival analysis of governance changes, and comparative analysis of different consortium architectures. Such research could establish whether the proposed mechanisms operate consistently, identify boundary conditions under which they weaken or disappear, and determine whether non-monotonic governance trajectories occur in practice.

The fifteen diagnostic questions developed in this study provide a starting point for such research, but their empirical validity, relative importance, and decision thresholds remain to be established. They should therefore be understood as a theoretically grounded diagnostic scaffold, not as a validated managerial instrument.

Overall, the paper's theoretical claim is deliberately bounded: blockchain can alter the institutional infrastructure through which collaborative logistics is governed, but the direction and durability of that effect depend on how technical mechanisms interact with organizational readiness, relational governance, institutional authority, environmental uncertainty, data provenance, and the capacity for legitimate change. The relevant research question is consequently not whether blockchain improves collaboration in the abstract, but under what conditions its governance mechanisms reinforce rather than constrain the capacity of collaboration to emerge, remain viable, and evolve.

5. Conclusions

This paper has conceptualized blockchain not primarily as a logistics efficiency technology, but as institutional infrastructure through which interorganizational collaboration can be coordinated, monitored, recorded, and adapted across its lifecycle. By integrating transaction cost economics, network governance theory, the natural-resource-based view with dynamic capabilities, and socio-technical systems theory with the multi-level perspective, the framework explains how the governance implications of shared digital infrastructure may change across Emergence, Viability, and Evolution.

The analysis shows that blockchain does not necessarily eliminate collaboration fragility. Rather, it may transform the location and nature of governance vulnerabilities: readiness constraints can emerge when organizations face weak relational or institutional foundations; codification can reduce monitoring and enforcement costs while creating adaptation tensions under uncertainty; and persistent infrastructure can become misaligned with evolving organizational and governance capabilities. Governance Inversion and Capability–Infrastructure Desynchronization capture two such mechanisms, while the monitoring–maladaptation trade-off links the benefits and constraints of blockchain-enabled governance across the lifecycle.

These findings are theoretical propositions rather than empirically established regularities. In particular, P1–P5 specify mechanisms and boundary conditions through which readiness, monitoring, legitimacy, authority, adaptation, and infrastructure flexibility may interact. The proposed non-monotonic relationship in governance effectiveness, including the possibility of an inverted-U pattern, should therefore be treated as a testable theoretical prediction rather than as a demonstrated trajectory. Its empirical assessment requires longitudinal and comparative research using multidimensional measures of governance effectiveness, including monitoring and enforcement effectiveness, coordination stability, adaptability, and legitimacy. Such research should also account for architectural flexibility, governance–authority distribution, environmental uncertainty, task contractibility, relational embeddedness, and data provenance.

For practice, the framework suggests that blockchain deployment should be assessed not only against immediate efficiency objectives but also against organizational readiness,

governance authority, data-submission arrangements, and the capacity to adapt rules and infrastructure as collaboration evolves. The fifteen-question diagnostic framework provides a theory-derived starting point for such assessment, while remaining subject to empirical validation.

Overall, the paper shifts the research question from whether blockchain improves collaborative logistics in general to under what conditions its governance mechanisms can support collaboration without creating new forms of rigidity, legitimacy risk, or institutional misalignment. Blockchain may provide durable shared infrastructure, but its contribution to collaborative logistics depends on how that infrastructure interacts with organizational capabilities, relational governance, institutional authority, changing environments, and the quality and provenance of the data it records.

Author Contributions: Conceptualization, Y.C.; methodology, Y.C.; validation, Y.C., M.A.E.O. and M.A.; formal analysis, Y.C.; investigation, Y.C.; resources, Y.C.; data curation, Y.C.; writing—original draft preparation, Y.C.; writing—review and editing, M.A.E.O. and M.A.; visualization, Y. Chabba.; supervision, M.A.E.O. and M.A.; project administration, M.A.E.O.; funding acquisition, Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Center for Scientific and Technical Research (CNRST), Morocco, through an excellence scholarship awarded to the first author, grant number "7 UH22022".

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: During the preparation of this manuscript, the authors disclose that AI writing assistance tools, namely OpenAI's ChatGPT (GPT-5) and Anthropic's Claude (Sonnet 4.5), were used for language editing, structural refinement and formatting purposes. The research design, implementation, data collection, analysis, and intellectual contributions remain entirely the work of the authors, who take full responsibility for the accuracy, integrity, and originality of the final manuscript content.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ERP	Enterprise Resource Planning
TMS	Transportation Management System
API	Application Programming Interface
EDI	Electronic Data Interchange
TCE	Transaction Cost Economics
TAM	Technology Acceptance Model
TOE	Technology–Organization–Environment
STS	Socio-Technical Systems
MLP	Multi-Level Perspective
NGT	Network Governance Theory
NRBV	Natural-Resource-Based View
DC	Dynamic Capabilities
VRIO	Valuable, Rare, Inimitable, and Organized
ESG	Environmental, Social and Governance
GSBN	Global Shipping Business Network

References

1. McKinnon, A. Freight Transport Deceleration: Its Possible Contribution to the Decarbonisation of Logistics. *Transp. Rev.* **2016**, *36*, 418–436. [CrossRef]
2. Sternberg, H.S.; Hofmann, E.; Roeck, D. The Struggle Is Real: Insights from a Supply Chain Blockchain Case. *J. Bus. Logist.* **2021**, *42*, 71–87. [CrossRef]
3. Cruijssen, F.; Cools, M.; Dullaert, W. Horizontal Cooperation in Logistics: Opportunities and Impediments. *Transp. Res. Part E Logist. Transp. Rev.* **2007**, *43*, 129–142. [CrossRef]
4. Leitner, R.; Meizer, F.; Prochazka, M.; Sihn, W. Structural Concepts for Horizontal Cooperation to Increase Efficiency in Logistics. *CIRP J. Manuf. Sci. Technol.* **2011**, *4*, 332–337. [CrossRef]
5. Pomponi, F.; Fratocchi, L.; Tafuri, S.R. Trust Development and Horizontal Collaboration in Logistics: A Theory Based Evolutionary Framework. *Supply Chain Manag. Int. J.* **2015**, *20*, 83–97. [CrossRef]
6. Chabba, Y.; El Oualidi, A.; Ahlaqqach, M. Optimization of Collaborative Transport and Distribution Strategies: Trends and Research Opportunities. In *Proceedings of the Communications in Computer and Information Science*; Springer Science and Business Media Deutschland GmbH: Berlin/Heidelberg, Germany, 2022; Volume 1677, pp. 425–442.
7. Schmoltzi, C.; Wallenburg, C.M. Operational Governance in Horizontal Cooperations of Logistics Service Providers: Performance Effects and the Moderating Role of Cooperation Complexity. *J. Supply Chain Manag.* **2012**, *48*, 53–74. [CrossRef]
8. Kache, F.; Seuring, S. Challenges and Opportunities of Digital Information at the Intersection of Big Data Analytics and Supply Chain Management. *Int. J. Oper. Prod. Manag.* **2017**, *37*, 10–36. [CrossRef]
9. Lumineau, F.; Wang, W.; Schilke, O. Blockchain Governance—A New Way of Organizing Collaborations? *Organ. Sci.* **2021**, *32*, 500–521. [CrossRef]
10. Cao, Z.; Lumineau, F. Revisiting the Interplay between Contractual and Relational Governance: A Qualitative and Meta-Analytic Investigation. *J. Oper. Manag.* **2015**, *33–34*, 15–42. [CrossRef]
11. Babich, V.; Hilary, G. OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know about Blockchain Technology. *Manuf. Serv. Oper. Manag.* **2020**, *22*, 223–240. [CrossRef]
12. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
13. Halaburda, H.; Levina, N.; Min, S. Digitization of Transaction Terms within TCE: Strong Smart Contract as a New Mode of Transaction Governance. *MIS Q.* **2024**, *48*, 825–846. [CrossRef]
14. Lumineau, F.; Shang, G.; Swaminathan, J.M.; Tsoukalas, G.; Wagner, S.M.; Zhao, J.L. Charting the Future of Blockchain in Operations and Supply Chain Management: Opportunities and Challenges. *J. Oper. Manag.* **2025**, *71*, 886–892. [CrossRef]
15. Schilling, L.; Pournader, M.; Seuring, S. Rethinking Blockchain and Power Dynamics in Supply Chains: A Critical Discourse Analysis. *J. Bus. Logist.* **2026**, *47*, e70047. [CrossRef]
16. Cruijssen, F.; Dullaert, W.; Fleuren, H. Horizontal Cooperation in Transport and Logistics: A Literature Review. *Transp. J.* **2007**, *46*, 22–39. [CrossRef]
17. Ramanathan, U.; Gunasekaran, A. Supply Chain Collaboration: Impact of Success in Long-Term Partnerships. *Int. J. Prod. Econ.* **2014**, *147*, 252–259. [CrossRef]
18. Williamson, O.E. Comparative Economic Organization: The Analysis of Discrete Structural Alternatives. *Adm. Sci. Q.* **1991**, *36*, 269–296. [CrossRef]
19. Williamson, O.E. *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*; Free Press: New York, NY, USA, 1985; Volume 17.
20. Jones, C.; Hesterly, W.S.; Borgatti, S.P. A General Theory of Network Governance: Exchange Conditions and Social Mechanisms. *Acad. Manag. Rev.* **1997**, *22*, 911–945. [CrossRef]
21. Provan, K.G.; Kenis, P. Modes of Network Governance: Structure, Management, and Effectiveness. *J. Public Adm. Res. Theory* **2008**, *18*, 229–252. [CrossRef]
22. Hart, S.L. A Natural-Resource-Based View of the Firm. *Acad. Manag. Rev.* **1995**, *20*, 986–1014. [CrossRef]
23. Teece, D.J. Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance. *Strateg. Manag. J.* **2007**, *28*, 1319–1350. [CrossRef]
24. Trist, E.L.; Bamforth, K.W. Some Social and Psychological Consequences of the Longwall Method of Coal-Getting. *Hum. Relat.* **1951**, *4*, 3–38. [CrossRef]
25. Geels, F.W. Technological Transitions as Evolutionary Reconfiguration Processes: A Multi-Level Perspective and a Case-Study. *Res. Policy* **2002**, *31*, 1257–1274. [CrossRef]
26. Williamson, O.E. *The Mechanisms of Governance*; Oxford University Press: New York, NY, USA, 1996.
27. Chabba, Y.; El Oualidi, M.A.; Ahlaqqach, M. From Collaborative Logistics Theory to Implementation: A Multi-Organizational Hyperledger Fabric Network for Vertical and Horizontal Collaboration. *Future Internet* **2026**, *18*, 382. [CrossRef]

28. Jovanovic, M.; Kostić, N.; Sebastian, I.M.; Sedej, T. Managing a Blockchain-Based Platform Ecosystem for Industry-Wide Adoption: The Case of TradeLens. *Technol. Forecast. Soc. Change* **2022**, *184*, 121981. [CrossRef]
29. Hanisch, M.; Roozen, P.; Theodosiadis, V. Success and Failure in Blockchain-Based Interorganizational Ecosystems: A Governance Perspective. *J. Manag.* **2026**, *OnlineFirst*. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.