Inter-organisational Capabilities and the Transformation of Trust in Blockchain-based Smart Contracts: A Framework for SME Ecosystems

Abstract

Blockchain-based smart contracts embed agreement enforcement within executable code, constraining the partner discretion that inter-organisational relationships (IORs) have traditionally coordinated through trust, communication, and relational governance. This raises a question that popular accounts tend to foreclose: whether automated enforcement makes inter-organisational trust unnecessary, or whether trust instead changes in function and object. Drawing on expert consultation with 28 blockchain specialists and 25 in-depth interviews with executives, we conduct an inductive study of how IORs transform as organisations adopt smart contracts. We develop a framework in which intensive relational exchange enables organisations to build two inter-organisational capabilities, Distributed Transparency Capability and Algorithmic Coordination Capability, through which they actualise the affordances that smart contracts offer. Through this capability development a distinctive inter-organisational trust form emerges, System-based Trust, defined as warranted reliance on coordinating infrastructure that partner organisations jointly construct. System-based Trust complements rather than replaces relational trust: it carries operational coordination and frees relational trust for strategic collaboration and exception handling, producing Hybrid Inter-organisational Relationships as the outcome of successful transformation. The framework applies to small and medium-sized enterprise ecosystems with limited numbers of trading partners; larger-scale consortia and power-asymmetric networks fall outside its scope. Our findings reposition smart contracts as occasions for capability development rather than substitutes for inter-organisational trust.

Keywords: Blockchain; smart contracts; inter-organisational relationships; inter-organisational capabilities; system-based trust; SMEs

---

1. Introduction

Information Systems research has long examined how technology supports inter-organisational relationships (IORs). Early scholarship established that inter-organisational systems (IOS) streamline transactions, reduce coordination costs, and create competitive advantage (Johnston & Vitale, 1988; Kumar & Van Dissel, 1996; Malone et al., 1987), while more recent work treats IOS as boundary objects mediating collaboration (Zhou et al., 2024) and algorithmic coordination as a distinctive governance mode (Gregory et al., 2025; Harrison et al., 2023). Across this tradition a consistent premise holds: technology supports human-directed coordination in which partners retain discretion over how they interpret and act upon shared information. Blockchain-based smart contracts unsettle this premise. By recording agreement terms in executable code that runs autonomously when encoded conditions are met, they embed enforcement within the technological architecture and constrain, rather than merely facilitate, inter-organisational coordination (Lumineau et al., 2021; Murray et al., 2021).

Smart contracts are sociotechnical arrangements whose operation depends on hardware, data, and network consensus as well as the executable rules that distinguish them from prior

IOS (Halaburda et al., 2024; Murray et al., 2021). These substrate layers are necessary for the technology to function, but we foreground the enforcement logic encoded in the rules because it is the layer at which coordination is reorganised, combining automated execution, cryptographic verification, and immutable record-keeping in ways that displace human discretion. A popular reading holds that these properties make exchange "trustless," rendering the social mechanisms of IORs unnecessary (Beck et al., 2016; Vidan & Lehdonvirta, 2019). Yet foundational IOR research shows that resolving coordination costs, information asymmetry, and partner opportunism depends on trust built through repeated interaction and relational governance (Granovetter, 1985; Poppo & Zenger, 2002; Ring & Van de Ven, 1994), and recent evidence confirms that supposedly trust-free systems are not trust-free in practice (Hawlitschek et al., 2018, 2020; Obermeier & Henkel, 2025; Völter et al., 2023). The pertinent question is therefore not whether trust survives automation but how its function and object change when enforcement moves into the coordinating architecture.

This question matters because many blockchain initiatives have not delivered their promised transformation, with prominent implementations abandoned amid scaling difficulties, vendor lock-in, and an inability to sustain ecosystem-wide participation (Jensen et al., 2019; Jovanovic et al., 2022; Lacity et al., 2025). Empirical work on blockchain and IORs remains fragmented, treating governance, consortia formation, and trust as separate phenomena without explaining how they interact and evolve as relationships mature beyond initial implementation (Chen et al., 2023; Hacker et al., 2023; Hawlitschek et al., 2020; Völter et al., 2023). What remains unresolved is the mechanism through which trust transforms when organisations embed algorithmic enforcement in their relationships, and the form those relationships take when technological and relational governance must coexist. We therefore ask: *How do inter-organisational relationships transform as organisations adopt blockchain-based smart contracts, and what enables effective relationships when algorithmic and relational governance operate together?*

To address this question, we conducted an inductive, qualitative study comprising expert consultation with 28 blockchain and smart contract specialists and 25 in-depth interviews with executives from organisations engaged with smart contracts. Following Gioia et al. (2013), our analysis traces transformation across pre-adoption and post-adoption phases and surfaces the mechanism through which organisations move from socially mediated to algorithmically governed exchange. The study examines IORs in small and medium-sized enterprise ecosystems involving limited numbers of direct trading partners, typically two to ten organisations, where direct coordination remains feasible and transformation dynamics can be observed in detail. Larger-scale consortia and power-asymmetric networks may require distinct theoretical treatment, and we position ecosystem size and power distribution as explicit boundary conditions.

The study makes three contributions. First, we specify System-based Trust (SBT) as an inter-organisational trust form: warranted reliance on coordinating infrastructure that partner organisations have jointly constructed. SBT contributes to the growing conversation on trust in technological and algorithmic systems (Dang & Li, 2026; Korsgaard et al., 2025; Obermeier & Henkel, 2025; Vanneste & Puranam, 2025) by specifying a trust form whose object is infrastructure the relying organisations jointly construct, shifting both the level of analysis, from individual users to collectives, and the basis of the warrant, from a system encountered as given to one the parties build; and by showing that this reliance complements rather than displaces relational trust. Second, we identify the two inter-

organisational capabilities through which SBT emerges, Distributed Transparency Capability and Algorithmic Coordination Capability, extending the hierarchy-of-capabilities logic (Rai et al., 2006, 2012) to algorithmically governed exchange and specifying the collective capabilities that actualising an organisational affordance presupposes (Strong et al., 2014; Volkoff & Strong, 2013, 2017). Third, we develop Hybrid Inter-organisational Relationships as the outcome of successful transformation, specifying how algorithmic and relational governance coexist through functional differentiation (Lumineau et al., 2021; Murray et al., 2021).

The paper proceeds as follows. We review research on trust and governance in IORs, on IT-enabled coordination and capabilities, and on smart contracts as a distinctive IOS. We then describe our methodology, present findings organised around the transformation process, and discuss theoretical contributions, boundary conditions, and implications for research and practice.

2. Literature Review

The study draws on three research domains: trust and governance in inter-organisational relationships, IT-enabled coordination and the development of inter-organisational capabilities, and smart contracts as a distinctive inter-organisational system. We review each to locate the theoretical problem the study addresses.

2.1 Trust and Governance in Inter-organisational Relationships

Inter-organisational relationships exist to resolve three archetypal problems of economic exchange: high coordination costs, pervasive information asymmetry, and the risk of partner opportunism (Williamson, 1996). The canonical solutions are social. Trust accumulates through repeated interaction (Granovetter, 1985), communication builds shared understanding (Gulati & Sytch, 2008), and relational governance curbs self-interest (Poppo & Zenger, 2002). Trust occupies the central position: inter-organisational trust reduces conflict and raises alliance performance (Zaheer et al., 1998), develops through cyclical negotiation, commitment, and execution in which each successful cycle reinforces expectations of cooperation (Ring & Van de Ven, 1994), and generates relational rents that neither partner could secure alone (Dyer et al., 2018). Formal and informal governance function as complements rather than substitutes in producing these outcomes (Cao & Lumineau, 2015; Poppo & Zenger, 2002).

Two features of this trust orientation matter for what follows. Inter-organisational trust operates at the collective level yet remains distinct from interpersonal trust: Zaheer et al. (1998) establish it as a collectively held orientation towards the partner firm, diffused through organisational communication, rather than the aggregate of trust between individual boundary spanners. In both forms the object of trust is the partner organisation, whose trustworthiness is judged through competence, benevolence, and integrity. Governance research treats IOS as a means of adjusting that judgement: trust and control form a dialectic in which information systems help close the gap between the trust a relationship requires and the trust it possesses (Gallivan & Depledge, 2003; Nicolaou et al., 2011).

Information Systems (IS) research has extended trust to encompass technology as a distinct object. McKnight et al. (2011) specify trust in a particular technology along functionality,

reliability, and helpfulness; Lankton et al. (2015) separate system-like from human-like trust; Schuetz et al. (2025) synthesise antecedents including transparency, reliability, and system quality; and multi-target accounts add the provider and wider network as separate objects (Söllner et al., 2016; see Appendix A for a synthesis of foundational studies). The conversation has since moved towards algorithmic and AI systems, where perceived agency becomes an explicit determinant of whether trust is directed at the technology or its designer (Killoran et al., 2024; Vanneste & Puranam, 2025), where antecedents and consequences have been catalogued across hundreds of studies (Dang & Li, 2026), and where the boundaries of trust are being reconsidered around agency and vulnerability under conditions of technological change (Korsgaard et al., 2025; Schilke et al., 2026). Closest to our setting, Obermeier and Henkel (2025) theorise trust in smart contracts as deduction-related trust, grounded in the possibility of deducing a system's future behaviour from transparent, deducible, and immutable rules; their evidence shows that deduction-related and inductive trust reinforce one another and that ostensibly trust-free systems are not trust-free in use.

These accounts share an analytical stance: an individual user evaluates a technology that an external party has provided. Even where the object is a system rather than a person, and even where its behaviour is deducible from code, trust is theorised as one party's assessment of an artefact it encounters, and Luhmann's (1979) notion of system trust similarly concerns reliance on abstract systems that actors do not themselves construct. Recent work has begun to loosen this individual-user premise: at the organisational level, a firm can cultivate trust in a provided decision-support system through an interactive capability it develops (Cui et al., 2026). Yet even there the trusted system is one the organisation encounters as given rather than one the relying parties jointly build. What remains underspecified is how trust operates when the object is coordinating infrastructure that multiple organisations jointly construct and then collectively rely upon, how such trust relates to relational trust in the partner, and how governance transforms when algorithmic enforcement is embedded in the architecture. These questions motivate our analysis.

2.2 IT-enabled Coordination and Inter-organisational Capabilities

Information Systems research has long examined how technology supports inter-organisational coordination. Early IOS scholarship established that technology streamlines transactions, reduces coordination costs, and creates competitive advantage (Johnston & Vitale, 1988; Malone et al., 1987), while Kumar and Van Dissel (1996) characterise IOS along dimensions of interdependency and warn that IT-enabled cooperation requires active nurturing to prevent degeneration into conflict.

The capabilities perspective explains how technology generates organisational value. Rai et al. (2006) establish that IT infrastructure integration enables firms to develop higher-order integration capabilities that in turn produce performance gains, demonstrating that technology features alone do not create value because organisations must build the capacity to leverage them. Saraf et al. (2007) extend this logic to interfirm relationships through cospecialised relational assets, and Grover and Kohli (2012) locate IT value co-creation in arrangements where multiple organisations invest jointly.

Affordance theory links what a technology offers to what its users must be able to do. An affordance is a potential for action that arises from the relation between a technical object and a goal-oriented actor and is a property of neither alone (Markus & Silver, 2008; Strong et al., 2014; Volkoff & Strong, 2013). The potential exists whether or not anyone acts on it, and

actualisation, the actions actors take to realise it, requires an actor with the necessary capabilities and a goal the affordance serves (Lehrer et al., 2023; Strong et al., 2014; Volkoff & Strong, 2013). In organisations those capabilities are not given: they develop as actors learn, and organisation-level outcomes follow only when many actors' actions are consistent and aligned (Strong et al., 2014). Reciprocally interdependent actors jointly realise an affordance only once they converge on a shared use of the technology's features (Leonardi, 2013). We follow this reading, in which an affordance is a durable potential distinct from the actions that realise it, in preference to accounts that tie affordances to situated practice (Bloomfield et al., 2010). The capabilities perspective draws the same line, separating an IT functionality from the interfirm capability to implement and use it with other resources in joint processes (Rai et al., 2012). Affordance and capability are therefore distinct and linked: the affordance is the potential a technology offers a set of actors, and the capability is their developed ability to actualise it. Between organisations no common hierarchy aligns those actions, so the partners must build that ability jointly.

Recent research identifies algorithmic coordination as qualitatively different from prior IT-enabled coordination. Harrison et al. (2023) show that blockchain establishes coordination on distributed-control principles, a mode beyond organisation, market, and cooperative relationship, in which interaction amongst loosely coupled organisations is mediated by the technology and intensive set-up enables subsequent economising on coordination costs. Gregory et al. (2025) theorise programmed reciprocity, cooperation sustained by coded rules, and root it in the algorithmic enforcement capability of blockchain networks, defined as the guaranteed execution of agreed rules without central authority or the possibility of human interference. This capability is a property of the network, present once a blockchain is in place. How partner organisations collectively build the capacity to leverage such a property at the inter-organisational level remains undertheorised, even as related work has begun to examine capability development in blockchain contexts at the level of the individual vendor (Du et al., 2029; Ji et al., 2024).

2.3 Smart Contracts as a Distinctive Inter-organisational System

Smart contracts are self-executing agreements whose terms are recorded in code on a blockchain, and which execute autonomously and irreversibly once encoded conditions are met (Halaburda et al., 2024; Murray et al., 2021). Their distinguishing property is automated enforcement: compliance is embedded in the architecture rather than secured through partners' discretion in interpreting and acting on shared information. This sets them apart from IOS theorised as boundary objects, which enable flexible coordination through standardisation and adaptability (Zhou et al., 2024). Halaburda et al. (2024) formalise the difference in transaction-cost terms, positioning strong smart contracts as a governance mode that forecloses ex post adaptation and so weighs the benefits of avoiding holdup against high ex ante specification costs and the loss of flexibility.

A sustained line of inquiry has examined these dynamics. Lacity (2022) frames blockchain's trajectory as a contest over the decentralisation of power; Renwick and Gleasure (2021) demonstrate that control over code is control over rules, as the values of those who write blockchain systems become inscribed in what those systems enforce; and recent work explains why enterprise blockchains often reproduce centralised governance, tracing decentralisation outcomes to platform openness and participant inclusiveness (Viguerie et al., 2026) and to the practices through which participants are empowered to govern

(Soleimanof & Neufeld, 2026). This stream establishes that governance and decentralisation are achieved rather than given, and leaves open how the relational and trust dimensions of exchange transform when organisations adopt the technology.

Empirical research on blockchain and IORs has examined governance structures (Goldsby & Hanisch, 2022), the intensive coordination consortia require before implementation (Hacker et al., 2023), blockchain's role in alliance trust (Chen et al., 2023), and coordination in public-sector settings (Roth et al., 2023), yet treats these as separate phenomena rather than theorising how they interact and evolve. The trust dimension is contested. De Filippi et al. (2020) cast blockchain as a confidence machine that substitutes technological assurance for reliance on human actors, whereas Hawlitschek et al. (2018, 2020) and Völter et al. (2023) show that traditional trust mechanisms persist and often prove ineffective rather than redundant, and Lacity et al. (2025) argue that decentralised infrastructures demand a reconceptualisation of trust that specifies its object and the conditions under which it becomes warranted. Nascent theorising has begun to respond: Danese and Romano (2025) propose blockchain system trust as trust generated by a blockchain's capacity to reduce information asymmetry, and Obermeier and Henkel (2025) ground deduction-related trust in the deducibility of code, though both treat trust as a property arising from technology design. Whether trust in infrastructure that organisations jointly construct differs from trust in technology they merely encounter, and through what mechanism such trust emerges, remains untheorised.

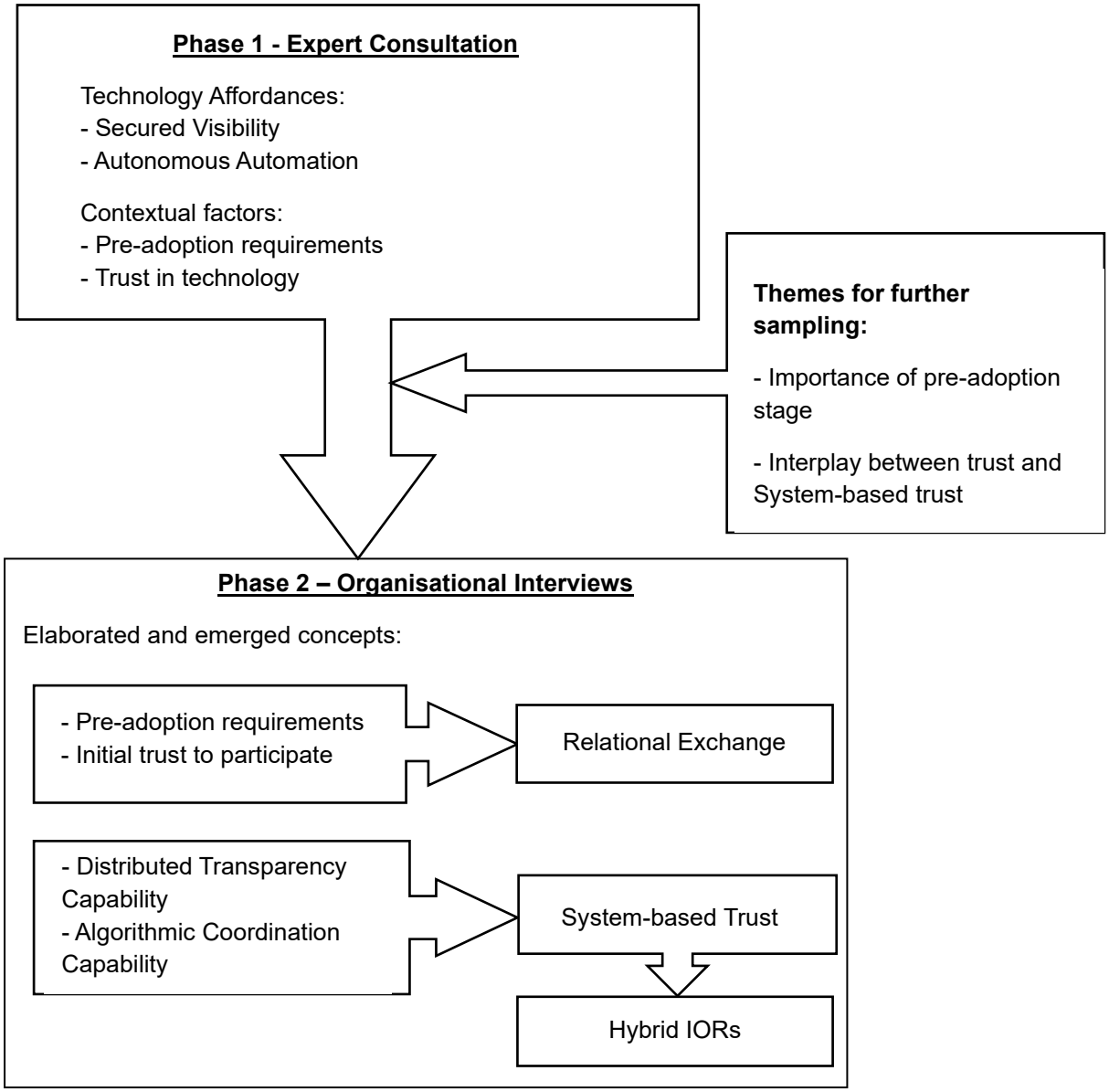
The review identifies a specific gap. IOR research shows that effective coordination depends on trust, governance, and relational maintenance, the very functions smart contracts automate. IOS and capabilities research shows how IT enables coordination and value, yet assumes human-directed processes rather than enforcement that constrains discretion. The unresolved question is the mechanism through which trust transforms when organisations embed algorithmic enforcement in their relationships, and the form those relationships take when technological and relational governance coexist. We investigate this question empirically.

3. Research Methodology

3.1 Research Design

We adopted an inductive, qualitative design to investigate how inter-organisational relationships transform through smart contract adoption, an approach suited to emergent phenomena where existing theory offers limited guidance (Eisenhardt, 1989; Gioia et al., 2013). The research comprised two sequential phases. We first consulted 28 blockchain and smart contract experts through a qualitative survey to develop a foundational understanding of the affordances smart contracts offer adopting organisations, then conducted 25 in-depth interviews with executives from organisations engaged with smart contracts to examine transformation and capability development in practice. This sequential design follows established practice in phenomenon-driven research (Monteiro et al., 2022). Figure 1 illustrates the research design.

Figure 1. Two-Phase Research Process Model



3.2 Sample and Data Collection

The first phase comprised qualitative survey responses from 28 experts. A preliminary focus group with three field experts (not included in the panel) served as a pilot and informed our purposive sampling and vetting criteria. We selected experts on five criteria: authorship of peer-reviewed work on blockchain; contributions to industry reports and white papers; presentations at international events; involvement in blockchain projects; and/or academic positions focused on blockchain. This phase surfaced the technology affordances (Secured Visibility, Autonomous Automation) and contextual factors that shaped subsequent sampling. Appendix B lists the expert informants, Appendix C presents the survey instrument, and Appendix D presents the instrument used to validate the emergent themes with experts.

The second phase comprised 25 semi-structured interviews with executives from small and medium-sized enterprises (SMEs; fewer than 250 employees under EU Recommendation

2003/361) engaged with smart contracts. We used purposive and snowball sampling to reach SMEs with direct experience, selecting on three criteria: active involvement in smart contract implementation or facilitation; decision-making authority over inter-organisational technology adoption; and willingness to discuss relationship dynamics with partners. Appendix E presents the interview guide.

To distinguish forms of engagement, we classified the 25 interviewed organisations into three categories: Users (11 cases), who have implemented smart contracts to govern their own inter-organisational relationships; User-Facilitators (5 cases), who use smart contracts in their own relationships and also develop or implement smart contract solutions for other organisations; and Facilitators (9 cases), who develop or implement smart contract solutions for client organisations but do not govern their own inter-organisational relationships through smart contracts. Facilitators contribute an observer's view of adoption across the client ecosystems they serve. This yields 16 cases with direct usage experience. Throughout the findings we mark each quotation by category and case number, for example "[User, Case 7]", and each Phase 1 survey response by expert number, for example "[Expert 7]", so readers can weigh the evidence.

Most of these SMEs are technology-oriented: 14 of the 25 are IT services or software firms, and the remainder are supply chain operators and service providers in the insurance, legal, notarial, postal, e-commerce, and consulting sectors. Their pre-existing technical capabilities may have eased adoption. Informants held senior positions, including CEO, CTO, and CIO, ensuring both strategic oversight and operational knowledge. Interviews averaged 58 minutes, ranging from 30 to 110 minutes. Users were interviewed post-implementation, enabling reflection on the full transformation from pre-adoption through post-adoption. Table 1 summarises informant characteristics, and Appendix F provides complete details.

Table 1. Summary of Organisational Interview Informants

Category	Count	Percentage
Case type		
Users	11	44%
User-Facilitators	5	20%
Facilitators	9	36%
Cases with direct usage experience	16	64%
Organisational size		
Small (< 50 employees)	11	44%
Medium (50-249 employees)	14	56%
Geographic distribution		
Europe	15	60%
North America	4	16%
Asia-Pacific	4	16%
Other	2	8%

Appendix G provides case-level detail for User and User-Facilitator cases, including industry context, smart contract application, estimated ecosystem size, and blockchain architecture where reported. Our protocol centred on relationship dynamics rather than technical implementation, and we did not systematically investigate whether each implementation ran on a public or a private network. Ten of the 16 User and User-Facilitator cases reported their

network type: seven ran on public networks and three on private or permissioned ones (Appendix G). Network type carries consequences for governance, cost, and data confidentiality, particularly for resource-constrained SMEs, and we position it as a boundary condition warranting dedicated investigation (Halaburda et al., 2024; Lacity et al., 2025).

3.3 Data Analysis

We applied the Gioia methodology (Gioia et al., 2013), maintaining the separation between informant-centric first-order codes and researcher-driven second-order themes. After repeated reading to develop familiarity, initial coding captured informants' own terms for relationship dynamics, trust mechanisms, and implementation experience, generating first-order codes in their language. We then compared codes across cases to identify higher-order themes, analytically distinguishing affordances (the potentials for action that smart contracts offer organisations seeking to coordinate exchange, drawn primarily from expert data) from inter-organisational capabilities (what partners develop collectively to actualise those potentials, drawn primarily from the interviews). The distinction emerged as we recognised that experts described what smart contracts make possible for adopting organisations in general, whereas users described what they and their partners had to become able to do together, a difference that parallels the one between a generic affordance and its case-specific actualisation (Volkoff & Strong, 2013). We then distilled second-order themes into the aggregate dimensions of our framework: Distributed Transparency Capability, Algorithmic Coordination Capability, System-based Trust, and Hybrid Inter-organisational Relationships, comparing throughout with existing literature to ground the constructs while preserving inductive integrity. We weighted evidence systematically, prioritising Users and User-Facilitators (16 cases) over Facilitator-only evidence (9 cases) for claims about lived implementation. The lead author conducted primary coding, with regular sessions amongst all authors to refine themes and resolve interpretive differences.

3.4 Research Quality

We pursued several strategies to ensure research quality (Lincoln & Guba, 1985). To address informant bias, we triangulated across stakeholder types (experts, users, facilitators); to limit recall bias, we questioned highly knowledgeable informants about recent, salient activities (Golden, 1992); and we adopted a "courtroom" style of questioning focused on what informants or their firms actually did or observed (Huber & Power, 1985; Lipton, 1977). We promised anonymity to encourage candour, and informants were motivated to report accurately by their shared interest in an unsettled question. Four limitations bound our claims. The cross-case design prioritised pattern identification over within-case depth, augmenting external validity at the cost of within-case triangulation, so we rely on informant accounts without corroborating documentary evidence or multiple respondents per organisation (Barratt et al., 2011; Eisenhardt & Graebner, 2007). Our informants represent organisations that adopted or facilitated smart contracts, so failed implementations are underrepresented; retrospective accounts may carry recall bias; and the sample's technical orientation may limit transferability to traditional SMEs. We return to these limitations in the discussion.

4. Findings

Our analysis reveals how inter-organisational relationships transform as organisations adopt blockchain-based smart contracts. We first establish the affordances smart contracts offer organisations that seek to coordinate exchange. We then trace how organisations build two inter-organisational capabilities through relational exchange that begins before adoption and continues after it, how a distinctive trust form emerges through that capability development, and how the resulting relationships settle into a hybrid configuration. Throughout, the pivotal change from pre-adoption to post-adoption is not the appearance or disappearance of relational work but the evolving role of trust.

4.1 Smart Contract Affordances

The expert survey identified two affordances that blockchain-based smart contracts provide: secured visibility and autonomous automation. Each is a potential for coordinated action that smart contracts offer organisations pursuing joint exchange; neither determines organisational outcomes.

Secured Visibility is the potential for partners to see and verify a common record of their transactions, arising from the transparency, immutability, and verifiability of the ledger. Experts emphasised that smart contracts create verifiable records accessible to all parties. As Expert 7 observed: *"Most smart contracts are built on transparent networks. It is the transaction transparency and the immutability of record keeping."* The immutability dimension recurred, with blockchain described as *"a secure, single source of truth"* [Expert 12] that enables *"sharing one single source of truth between multiple participants"* [Expert 24]. This differs from conventional systems where administrators can modify data.

Autonomous Automation is the potential for partners to have agreed terms executed without either party's intervention once encoded conditions are satisfied. As Expert 9 put it, *"Smart contracts act according to their program,"* automating *"approvals, calculations and other transacting activities that are prone to lag and error"* [Expert 12]. The affordance constrains as well as enables (Volkoff & Strong, 2013): once parties commit, neither can alter agreed terms without the other's consent. Expert 1 captured this constraining quality: *"Smart contracts limit and decrease human errors, fraud and unscheduled activity... One of the parties can't change anything without the consensus of all the parties."* Table 2 presents the data structure for these affordances.

Table 2. Smart Contract Affordances (Expert Survey)

First-order Statements	Second-order Themes	Aggregate Theme
"Most smart contracts are built on transparent networks. It is the transaction transparency and the immutability of record keeping" [Expert 7]; *"With smart contracts you know who had what, when, how long, and what they did"* [Expert 10]	Increased Transparency and Traceability of Business Processes	**Secured Visibility**
"The blockchain acts as a shared database to provide a secure, single source of truth" [Expert 12]; *"[Smart contracts help] sharing one single source of truth between multiple participants"* [Expert 24]	Increased Quality (Veracity) of Information Related to Business Processes	

First-order Statements	Second-order Themes	Aggregate Theme
"Smart contracts act according to their program" [Expert 9]; *"Smart contracts automate approvals, calculations and other transacting activities that are prone to lag and error"* [Expert 12]	Enabled Secured Autonomous Contract Execution	**Autonomous Automation**
"Smart contracts limit and decrease human errors, fraud and unscheduled activity... One of the parties can't change anything without the consensus of all the parties" [Expert 1]; *"By removing some human aspects of execution, there are fewer opportunities for bad behaviour"* [Expert 15]	Unilateral Conduct Restricted by Code	

These affordances exist as potentials for any organisations seeking to coordinate exchange through smart contracts, whether or not they act on them. Actualising them takes collective work, to which we turn next.

4.2 Relational Exchange and the Onset of Capability Development

Adoption begins with intensive relational exchange through which organisations establish the smart contract arrangement. This relational work is the setting in which the two inter-organisational capabilities first take shape, and it does not cease at go-live; it shifts in focus from establishing the system to governing and extending it. The work is most intense before adoption because the parties must build the shared foundations the technology presupposes. As one executive explained, *"The adoption of smart contracts, especially now that we are at the early stage of that, requires much more interactions and communications in order to prepare the infrastructure and the environment"* [User, Case 9]. This inverts the conventional pattern, in which intensive interaction tends to arise when disputes occur rather than at establishment.

This pre-adoption exchange does specific work that later capabilities depend on. Organisations establish shared understanding of processes and data, agreeing on *"common processes... the rules in which those processes are executed... data formats, message standards"* [Facilitator, Case 4]. They design governance for the shared infrastructure, with one facilitator stressing that *"Good governance and planning... is just the overarching necessity"* [Facilitator, Case 18]. And they develop the initial trust needed to begin: *"They definitely have to trust us to be running work, to begin with. I don't think they would hand over a large sum of money to people that they don't trust"* [User-Facilitator, Case 2]. The relational investment is heavy but front-loaded rather than perpetual: *"Still you have to set up that smart contract… you have to set up that ecosystem… you have to set up that working relationship and that as a starting point is face to face, but that's a one time thing"* [User, Case 21]. Table 3 presents the data structure for this relational exchange.

This investment is not the contract-specification cost familiar from transaction-cost accounts of strong smart contracts (Halaburda et al., 2024). What organisations build before adoption is not a fully specified set of contingencies but the collective foundations, shared interpretation, jointly defined rules, and designed governance, on which the two capabilities

rest. Where this foundation is laid, capability development proceeds; where it is truncated, the affordances remain unactualised.

Table 3. Relational Exchange during Pre-adoption Stage

First-order Statements	Second-order Themes	Aggregate Theme
"Establishing a blockchain network requires collaboration" [Facilitator, Case 4]; *"To be able to create a good smart contract, every stakeholder in the supply chain needs to be on the table"* [User, Case 7]; *"The adoption of smart contracts... requires much more interactions and communications in order to prepare the infrastructure"* [User, Case 9]	Increased collaboration and communication during set-up	**Relational Exchange (pre-adoption)**
"You have to agree in the common language" [User, Case 15]; *"To define a working smart contract, you have to ensure that both parties are in very clear agreement about the definition of terms"* [Facilitator, Case 18]; *"You need to agree on common processes... agree on the rules in which those processes are executed"* [Facilitator, Case 4]	Development of shared language and understanding	
"You need to be willing to be transparent. You need to be willing to make agreements that can be digitally facilitated" [User, Case 7]; *"They definitely have to trust us to be running work, to begin with"* [User-Facilitator, Case 2]	Increased transparency and initial trust	
"Good governance and planning. Yes, that to me is just the overarching necessity" [Facilitator, Case 18]; *"You have to think in a perspective of how to make a gradable smart contract"* [User, Case 5]	Need for ongoing governance and adaptation	

4.3 Inter-organisational Capability Development

Organisations develop two inter-organisational capabilities to actualise the affordances: Distributed Transparency Capability and Algorithmic Coordination Capability. IS research distinguishes a firm's own IT capabilities (Bharadwaj, 2000; Rai et al., 2006) from capabilities held at the level of the interfirm relationship (Rai et al., 2012). DTC and ACC are of the second kind: collective competences forged through joint participation rather than individual firm achievements. Both begin forming in the pre-adoption relational exchange described above and continue to operate as the relationship matures.

4.3.1 Distributed Transparency Capability

Distributed Transparency Capability (DTC) is the inter-organisational capacity to establish, interpret, and act upon a single immutable record that no party can unilaterally alter. Realising it requires the parties to converge on how that record is structured and read: transparency in the sense that matters here is not access to data but collective agreement on how information is recorded and interpreted. Organisations come to *"interact now based not on their own information but based on the transparent ledger and agreement that they all agreed on"* [User, Case 7], such that *"Everything is now auditable and everything is now transparent"* [Facilitator, Case 3]. Anchoring interpretation to a jointly held record lets

partners verify compliance against that record rather than reconcile and renegotiate the separate accounts that ordinarily accompany coordination. The work of converging is substantial, requiring agreement in *"the common language"* [User, Case 15] and *"structure agreement around the construct of the states"* [Facilitator, Case 23], and extending beyond data formats to shared understanding of processes, metrics, and exception handling. Table 4 presents the data structure for DTC.

Table 4. Distributed Transparency Capability

First-order Statements	Second-order Themes	Aggregate Theme
"You need to agree on common processes. You need to agree on the rules in which those processes are executed. You need to agree in data formats, message standards that you use to exchange" [Facilitator, Case 4]; *"To be able to create a good smart contract, every stakeholder in the supply chain needs to be on the table" [User, Case 7]*	Joint establishment of transparency protocols	**Distributed Transparency Capability**
"The new way of interaction it's that it's digitalised and according to the agreement of the whole supply chain, which makes it very different, because they interact now based not on their own information but based on the transparent ledger and agreement that they all agreed on" [User, Case 7]; *"Everything is now auditable and everything is now transparent"* [Facilitator, Case 3]	Collective sensemaking from shared data	
"They can connect and share what they agreed on but the connection is stronger because it's more efficient" [User, Case 7]; *"You can see exactly... You can trust them. You have that transparency and trust which is in this smart contract itself"* [User-Facilitator, Case 25]	Coordinated interpretation enabling verification	
"You have to agree in the common language" [User, Case 15]; *"It needs some structure agreement around the construct of the states. Otherwise, you're just not going to get people understanding what they're doing"* [Facilitator, Case 23]	Shared interpretive framework	

4.3.2 Algorithmic Coordination Capability

Algorithmic Coordination Capability (ACC) is the inter-organisational capacity to coordinate exchange through rules the parties define jointly and a blockchain enforces automatically. We use "algorithmic" here to denote coordination carried by these executable, automatically enforced rules, distinguishing it from the human-directed coordination of conventional IOS rather than asserting that the technology reduces to its algorithms.

ACC has two defining features. The first is joint rule definition: the rules that will execute automatically must be established collectively, requiring that *"every stakeholder in the supply chain needs to be on the table"* [User, Case 7] and that the parties make sure *"you've clearly defined how the smart contract is governed"* [Facilitator, Case 18]. The second is collective acceptance of constrained discretion: once the rules are set, organisations accept that every

transaction the contract governs executes as encoded, and that no party can intervene at the point of execution. Discretion is exercised earlier, in the joint decision about what to encode, and later only through the agreed procedure for changing the rules. Informants described being *"quite happy to work in this kind of scenario where they are both bound by a smart contract"* [User, Case 6], and recognised that this mutual binding deepens interdependence, since an *"association approach is probably best whereby you can get multiple players to agree to the smart contract, and it does make them a little bit more dependent on each other"* [User, Case 17]. Coordination then proceeds through machine-mediated execution, *"all driven by machines, the actions are done by machines"* [User, Case 21], so that recording and settlement become, in the words of one facilitator, automated such that *"the process becomes automated and reliable"* [Facilitator, Case 18]. Table 5 presents the data structure for ACC.

Table 5. Algorithmic Coordination Capability

First-order Statements	Second-order Themes	Aggregate Theme
"To be able to create a good smart contract, every stakeholder in the supply chain needs to be on the table" [User, Case 7]; *"Good governance and planning. Yes, that to me is just the overarching necessity. You have to make sure that you've clearly defined how the smart contract is governed"* [Facilitator, Case 18]	Joint rule definition	**Algorithmic Coordination Capability**
"The parties are quite happy to work in this kind of scenario where they are both bound by a smart contract" [User, Case 6]; *"If there is more transparency through the blockchain, what is done with the money, then I do believe, of course, it will strengthen... because people have more trust"* [Facilitator, Case 4]	Acceptance of constrained discretion	
"You are more connected because you share the same goal and you will interact with one smart contract... because you are bound to a smart contract" [User, Case 5]; *"An association approach is probably best whereby you can get multiple players to agree to the smart contract, and it does make them a little bit more dependent on each other"* [User, Case 17]	Shared commitment to automated coordination	
"It's all driven by machines, the actions are done by machines... There are smart contracts to guide and to define and to protect" [User, Case 21]; *"Smart contracts automate the recording of the data and the payment, so that the process becomes automated and reliable"* [Facilitator, Case 18]	Algorithmic execution	

4.3.3 From Affordances to Capabilities

Table 6 sets out how the affordances and the capabilities differ. The affordances pre-exist any particular partnership as potentials; the capabilities exist only once partners have built them together.

Table 6. Analytical Distinction: Technology Affordances and Inter-organisational Capabilities

Analytical Dimension	Technology Affordances	Inter-organisational Capabilities
Definition	Potentials for coordinated action arising from the relation between smart contract features and organisations seeking to coordinate exchange	Collective competences through which partner organisations actualise those potentials
Level of analysis	Technology in relation to adopting organisations	Inter-organisational
Source	Smart contract features in relation to organisations' coordination goals	Developed through coordinated learning
Emergence requirement	Availability of the technology to organisations with a coordination goal	Relational exchange and joint development
Theoretical grounding	Affordance theory (Markus & Silver, 2008; Strong et al., 2014; Volkoff & Strong, 2013, 2017)	Capabilities perspective (Rai et al., 2006, 2012)
Constructs in this study	Secured Visibility; Autonomous Automation	Distributed Transparency Capability; Algorithmic Coordination Capability
Relationship to System-based Trust	Necessary but insufficient	Enabling mechanism for SBT emergence

The distinction explains why adoption alone does not guarantee transformation. Secured visibility becomes coordination value only when partners build the shared, immutable record and the interpretive convergence that constitute DTC; autonomous automation becomes reliable coordination only when partners jointly define rules and collectively accept constrained discretion, which constitute ACC. Where relational exchange is truncated by time pressure, undermined by power asymmetry, or bypassed through top-down mandate, the affordances remain unactualised and capability development stalls, which helps explain documented failures in large-scale consortia (Jovanovic et al., 2022).

4.4 System-based Trust Emergence

As organisations develop DTC and ACC, a distinctive inter-organisational trust form emerges, which we term System-based Trust (SBT): warranted reliance on the shared coordinating infrastructure the partners have jointly constructed. SBT operates at the collective level and reorganises, rather than removes, the role of trust.

Adoption was frequently motivated by a perceived deficit of interpersonal trust. As one executive put it, *"Blockchain is always about third parties that want to cooperate but do not trust each other"* [Facilitator, Case 20], against a backdrop in which *"there is definitely a trust crisis right now"* [Facilitator, Case 3]. Informants often described the result in the language of trustlessness: *"I trust technology more than people"* [User, Case 1]; *"What we are creating is a trustless environment. There is no need for trust anymore because there are smart contracts to guide and to define and to protect"* [User, Case 21]. Read closely, these

accounts describe a relocation rather than an elimination of trust. The same logic surfaces in a more precise formulation: *"The thing it's not the trust between the organisations. There is no trust in the first [place], but the smart contract technology enables to exchange information or participate in a business process trusting that the system works in a way that is secured"* [User, Case 15]. Trust here attaches not to the partner but to the jointly constructed system.

What the data show, against the trustless rhetoric, is that SBT complements relational trust rather than supplanting it. One executive articulated the complementarity directly: *"If we decide to cast our agreement into a smart contract, then it's a very deep form of commitment because it's verifiable and immutable commitment that we've made between each other. That lays the groundwork for deeper levels of trust, information sharing, and reciprocity"* [User-Facilitator, Case 25]. The same informant specified the conversion: *"People that are prepared to make verifiable commitments are people that you will trust on top of those verifiable commitments. The verifiable commitments are a good platform for trusting commitments for unverifiable commitments based on trust"* [User-Facilitator, Case 25]. Reliable, verifiable commitments managed through DTC and ACC become the platform on which relational trust is redirected towards the unverifiable, strategic dimensions of the relationship. Table 7 presents the data structure for SBT.

Table 7. System-based Trust

First-order Statements	Second-order Themes	Aggregate Theme
"I trust technology more than people" [User, Case 1]; "What we are creating is a trustless environment. There is no need for trust anymore because there are smart contracts to guide and to define and to protect" [User, Case 21]; "There is no trust required, you can see that here is a system that cannot be altered even by its creators" [User-Facilitator, Case 25]	Trusting technology	**System-based Trust**
"The thing it's not the trust between the organisations. There is no trust in the first [place], but the smart contract technology enables to exchange information or participate in a business process trusting that the system works in a way that is secured" [User, Case 15]; *"The system is able to again help to generate the missing trust that you don't have with the traditional system"* [Facilitator, Case 24]	Trust in system rather than partners	
"Blockchain is always about third parties that want to cooperate but do not trust each other" [Facilitator, Case 20]; *"There's a huge distrust between people, between each other... you don't trust people anymore but you trust the systems"* [Facilitator, Case 4]	Enabling cooperation without relational trust	
"If we decide to cast our agreement into a smart contract, then it's a very deep form of commitment... That lays the groundwork for deeper levels of trust, information sharing, and reciprocity"; *"People that are prepared to make verifiable commitments are people that you will trust on top of those verifiable commitments"* [User-Facilitator, Case 25]	Platform for relational trust development	

SBT thus marks the pivotal transformation between phases. Pre-adoption coordination rests on interpersonal trust developed through relational exchange; post-adoption, that reliance is complemented by warranted reliance on the shared infrastructure, freeing relational trust for purposes that automation cannot serve.

4.5 Hybrid Inter-organisational Relationships

The emergence of SBT produces Hybrid Inter-organisational Relationships (Hybrid IORs), in which System-based Trust carries operational coordination while relational trust carries strategic collaboration. This is a transformed configuration, not a diminished one.

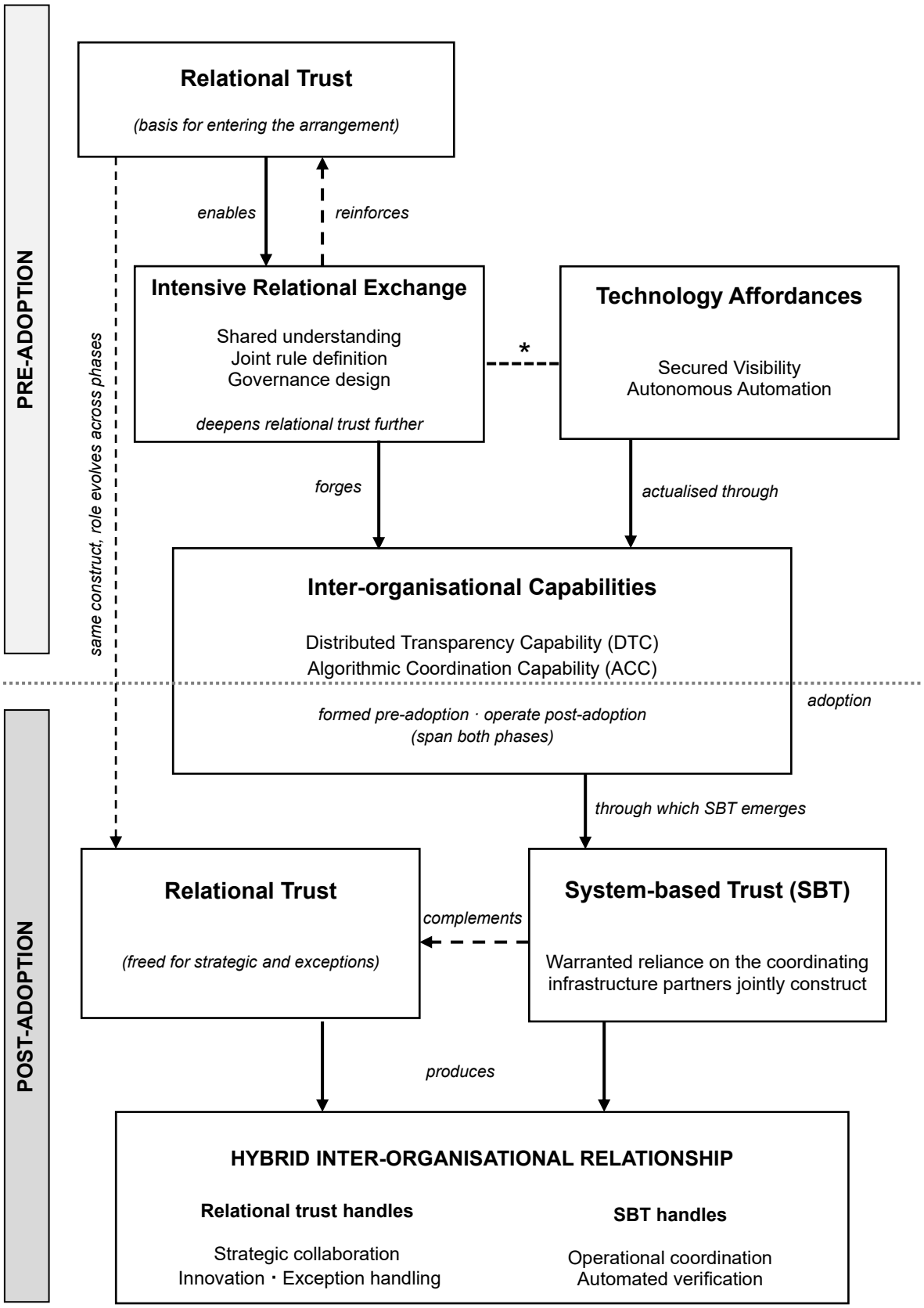
After implementation, routine exchange becomes more impersonal as automation absorbs operational contact: *"There's much more, let's say digital interaction, and not human anymore... It's turning you towardss the digital conversation or digital exchanging of information"* [User, Case 16], producing *"an increase of data, but a decrease in human communication because we're taking that out"* [User-Facilitator, Case 10]. In one healthcare application, staff *"found it very relaxing because they don't have to deal with clients or insurers face-to-face. Everything is automated"* [User, Case 6]. Automation also relieves the relationship of a defensive burden: *"If everything gets self-executing, then it's almost as if the social relationship doesn't have to bear the burden of the implied threat or the fear of this kind of opportunism or reneging. I think that's more conducive, therefore, to cooperation"* [User-Facilitator, Case 25].

The relational work does not end; it migrates to higher-value matters. Freed from process administration, *"The people that are currently doing a lot of process ending can focus on other tasks in the organizations"* [User-Facilitator, Case 10], so that the relationship can attend to strategy and innovation: automation *"saves a lot of time to talk about how to work together, and it makes it easier to just go work together"* [User-Facilitator, Case 11], becoming *"a stepping stone to communicate about innovation together"* [User-Facilitator, Case 10]. Hybrid IORs therefore exhibit a stable division of labour: System-based Trust handles transactional and operational exchange through automated verification, and relational trust handles strategic collaboration, innovation, and exception handling, which covers matters the contract does not encode and changes to the encoded rules; all three require human judgement.

4.6 Synthesis and Framework

The findings cohere into a framework in which relational exchange and capability development span both phases, while the role of trust evolves between them (Figure 2). Before adoption, intensive relational exchange builds the shared, immutable record and the jointly defined rules that constitute DTC and ACC, on the basis of interpersonal trust. Through these capabilities, System-based Trust emerges as warranted reliance on the co-constructed infrastructure. After adoption, System-based Trust carries operational coordination, relational exchange continues in transformed, strategic form, and relational trust is freed for collaboration, innovation, and exception handling. The outcome is a Hybrid IOR characterised by functional differentiation between the two trust forms.

Figure 2. Transformation of Inter-organisational Relationships in Smart Contract Settings



* *Relational exchange is partly oriented toward configuring how the affordances will be actualised; the inter-organisational capabilities are the means of that actualisation*

As System-based Trust accumulates, it lowers the relational threshold for extending the arrangement, whether by deepening the existing relationship or onboarding additional partners, so that successful transformation feeds the conditions for its own continuation.

The framework explains both success and failure. Organisations that invest adequately in pre-adoption relational exchange develop the capabilities through which SBT emerges, and reach the hybrid configuration. Organisations that do not make this investment fail to develop the capabilities, so SBT does not emerge, which helps account for documented failures in large-scale consortia (Jensen et al., 2019; Lacity et al., 2025). Initial interpersonal trust remains a precondition for entering the arrangement, linking the post-adoption configuration back to its pre-adoption foundations.

5. Discussion

This study advances understanding of inter-organisational relationships by specifying how they transform when organisations adopt blockchain-based smart contracts. Prior inter-organisational technologies support human-directed coordination while preserving partner discretion; smart contracts embed enforcement in the architecture, creating a coordination context in which organisations must build collective capacity to operate within algorithmically constrained exchange. Our framework identifies the mechanism that links adoption to outcomes as a sequence: pre-adoption relational exchange forges two inter-organisational capabilities (Distributed Transparency Capability and Algorithmic Coordination Capability); through these capabilities System-based Trust emerges as warranted reliance on co-constructed infrastructure; and the resulting functional differentiation between System-based and relational trust constitutes a Hybrid Inter-organisational Relationship. We discuss each element in turn, then the conditions of success and failure, and the boundaries within which the account holds.

5.1 Distributed Transparency Capability: Beyond Information Sharing

Distributed Transparency Capability extends inter-organisational systems scholarship, which shows how technology streamlines transactions and reduces coordination costs (Johnston & Vitale, 1988; Kumar & Van Dissel, 1996; Malone et al., 1987), by specifying the collective competence required to coordinate from an immutable shared record. Standardisation is the natural comparison, and it both facilitates and constrains coordination; jointly developed standards are themselves collective achievements built through coordinated learning. DTC's distinctiveness therefore cannot rest on collective achievement or on constraint, since standards supply both. It rests instead on the standing of the record the capability produces. Standards govern how each party records and exchanges its own data, leaving separate records to be reconciled when they diverge; an immutable ledger furnishes a single record that no party can unilaterally revise, so coordination shifts from reconciling competing accounts to verifying against one shared account. This is what lets partners confirm compliance without renewed negotiation, and it is the property that standardisation, however collective its development, does not confer.

The capability also clarifies the level at which value is created. Recent work examines capability development in blockchain contexts at the level of the individual vendor learning to deliver blockchain services (Ji et al., 2024). DTC operates at a different level: it is a competence that partner organisations hold jointly and that none possesses alone, residing

in the shared interpretive conventions and the common record rather than in any single firm's repertoire. It is also distinct from recent work that locates organisational trust in AI in an interactive capability: where Cui et al. (2026) describe a single firm developing the capacity to engage and make sense of a black-box system it does not control, DTC and ACC are inter-organisational competences, held jointly and possessed by no partner alone, for constructing the coordinating infrastructure on which the partners then rely. Strong et al. (2014) locate organisation-level actualisation in the actions of many individuals, made consistent and aligned within one organisation whose managers can intervene. Between firms no common hierarchy provides that alignment, and DTC specifies the collective competence through which partners achieve it for secured visibility: they converge, as a shared affordance requires (Leonardi, 2013), on a record they construct and interpret together. This extends Rai et al.'s (2006) hierarchy-of-capabilities logic to algorithmically governed exchange. Evidence from beyond the coordination setting reinforces this logic. Studying blockchain in global shipping, Sarker et al. (2021) find that the technology's capacity for full transactional disclosure mitigates corruption only in concert with social resources and institutional change, not through disclosure alone. The parallel holds at a different unit of analysis: transparency becomes effective through the collective work that surrounds it, which in inter-organisational coordination is the Distributed Transparency Capability rather than the visibility affordance on its own.

5.2 Algorithmic Coordination Capability: Collective Acceptance of Constrained Discretion

Algorithmic Coordination Capability speaks directly to recent theorising on algorithmic cooperation. Gregory et al. (2025) root programmed reciprocity in the algorithmic enforcement capability of blockchain networks, the guaranteed execution of agreed rules without central authority or scope for human interference. That capability is a property of the network: it is present wherever a blockchain operates, and in our framework it is a property of the technical object, a necessary condition for the autonomous automation affordance (Markus & Silver, 2008), not an organisational capability. ACC names something different and complementary: the collective competence organisations must develop to convert that network property into reliable inter-organisational coordination, through joint definition of the rules that will execute and collective acceptance that every transaction governed by those rules executes as encoded. Gregory et al. (2025) theorise cooperation amongst strangers, parties who lack prior interaction and cannot draw on human reciprocity; our SME ecosystems are not populated by strangers, and the intensive pre-adoption relational exchange we observe is precisely the work through which non-strangers establish the rules and shared understanding that the stranger model brackets. ACC thus supplies the organisational layer that sits between a network's enforcement capability and the cooperation it can sustain.

This layer determines who governs the encoded rules. Renwick and Gleasure (2021) establish that control over code is control over the rules a system enforces; ACC identifies joint rule definition as the collective practice through which partner organisations come to hold that control together rather than ceding it to whoever writes the code. The capability also recasts a claim that transaction-cost accounts already anticipate. Halaburda et al. (2024) position strong smart contracts as a governance mode whose adoption weighs the benefits of avoiding holdup against high ex ante specification costs and the loss of ex post flexibility. Our contribution is not the observation that smart contracts carry high ex ante

costs, which their analysis establishes, but the finding that these costs are substantially relational rather than purely specificational: what organisations build before adoption is shared interpretation, jointly negotiated governance, and collective acceptance of constraint, the foundations of a capability, not merely a more completely specified contract. Coordinating through automatically enforced rules is therefore an organisational achievement, and the IS tradition of identifying focused, context-specific capability sets supports treating DTC and ACC as the distinctive inter-organisational capabilities this context requires (Karimi-Alaghehband & Rivard, 2019; Pang et al., 2014; Schreieck et al., 2021), without implying they are the only capabilities adopters need.

5.3 System-based Trust: A Distinctive Inter-organisational Trust Form

Our central conceptual contribution is System-based Trust, defined as warranted reliance on shared coordinating infrastructure that partner organisations have jointly constructed through collective capability development. SBT contributes to a fast-developing conversation on trust in technological and algorithmic systems, and its distinctiveness is sharpest when positioned against the existing accounts it builds upon.

A first line of work treats technology as a trust object evaluated by an individual user. McKnight et al. (2011) specify trust in a particular technology along functionality, reliability, and helpfulness; Schuetz et al. (2025) catalogue its antecedents; and even multi-target accounts that separate the system, its provider, and the wider network retain the individual user as the trustor of an externally provided artefact (Söllner et al., 2016). The conversation has since extended to algorithmic and AI systems, where perceived agency becomes the variable that directs trust towards the technology or its designer (Vanneste & Puranam, 2025; Saffarizadeh et al., 2024), where that direction is contested because transparency may heighten rather than dampen agency perceptions and because non-sentient systems lack the capacity for the voluntary violation that "betrayal" presupposes (Killoran et al., 2024), and where antecedents and consequences have been synthesised across large empirical bodies (Dang & Li, 2026). Most recently, this conversation has begun to move beyond the individual trustor altogether – to the relational networks through which experts come to trust an AI counterpart (Hanelt et al., 2026), and to the organisational level, where a firm's trust in a decision-support system is cultivated through an interactive capability it develops rather than inferred from the system's properties (Cui et al., 2026). SBT departs from this line on two counts. The agency question does not bind, because a smart contract is deliberately non-agentic: its appeal is the foreclosure of discretion, not its exercise. And the trustor is not an individual evaluating a given artefact, nor a single firm building trust in a system provided to it, but a set of organisations relying collectively on infrastructure they themselves constructed.

A second line speaks directly to our setting. Obermeier and Henkel (2025) theorise deduction-related trust in smart contracts, grounded in the possibility of deducing a system's future behaviour from rules that are transparent, deducible, and immutable, and show empirically that deduction-related trust and inductive trust are distinct beliefs that reinforce one another, so that ostensibly trust-free systems are not trust-free in use. This finding converges with ours and strengthens it: their complementarity of deduction and induction at the level of an individual user assessing a given decentralised application parallels our complementarity of system-based and relational trust at the level of organisations governing a shared arrangement. SBT extends their insight in provenance and level. Deduction-related

trust rests on the possibility of auditing a system the trustor encounters, whose transaction core remains under a provider's control; SBT's warrant derives instead from participatory construction, because the partners themselves define the transparency conventions, automation rules, and verification mechanisms on which they then rely. The warrant is thus not the deducibility of given code but the collective capability through which the infrastructure is made transparent, rule-bound, and immutable together. Danese and Romano's (2025) blockchain system trust similarly treats trust as arising from a blockchain's capacity to reduce information asymmetry, a property of design rather than of joint construction, and SBT differs on the same axis.

A parallel body of governance research speaks directly to our setting. Hanisch et al. (2026) theorise blockchain-based inter-organisational ecosystems through a set of governance trade-offs, amongst them a tension between system reliance and actor reliance in trust and control that participants must continually reconcile, with cooperative versus competitive intent shaping how acute that tension becomes. SBT shares this object – the coexistence of system-level and actor-level reliance in blockchain ecosystems – but reframes it on three counts. First, their lens is governance design and ours is trust formation: where they ask how much control to decentralise, we specify a trust form and the conditions under which reliance on it becomes warranted. Second, their system reliance rests on the technology's codified and immutable properties, whereas System-based Trust rests on participatory provenance – partners construct the infrastructure they then rely upon. Third, and most consequentially, where they treat system and actor reliance as a trade-off to be balanced, with excessive decentralisation creating voids that demand actor-dependent checks, we find that under co-construction the relationship is not zero-sum: the capabilities partners develop convert it into the functional division of labour between system-based and relational trust that we set out below.

Positioning SBT also requires distinguishing it from older systems-theoretic notions of trust. Luhmann (1979) theorises system trust as reliance on abstract systems, such as money or expertise, that actors use but do not build; Luhmann's (1988) later distinction separates trust as an engagement with vulnerability under uncertainty, from confidence as a passive reliance on the continuity of familiar conditions, a distinction De Filippi et al. (2020) invoke to cast blockchain as a confidence machine. SBT sits across these categories rather than within any one. It carries the active, vulnerable choice that Luhmann reserves for trust, since organisations elect to enter arrangements that durably constrain their future discretion before the infrastructure's reliability is fully proven, the very dimension of vulnerability that recent work identifies as a frontier for trust theory under technological change (Korsgaard et al., 2025). It also carries the reliance on verified systemic properties that Luhmann assigns to confidence, since operational coordination proceeds through cryptographic verification rather than ongoing assessment of the partner. What separates SBT from Luhmann's system trust specifically is provenance once more: the system is not an abstract order the parties merely inhabit but infrastructure they jointly author. SBT thus specifies how trust takes form at the inter-organisational level when the coordinating system is one its users jointly author rather than one provided to them – the provenance condition that both older systems-theoretic accounts and the contemporary technology-trust literature leave open.

The consequence is that SBT complements relational trust rather than replacing it. System-level reliability handles transactional and operational exchange through automated verification, which redirects relational trust towards the unverifiable and strategic dimensions

of the relationship: collaboration, innovation, and exception handling that require human judgement. This functional differentiation reconciles the optimistic accounts that expect technology to dissolve trust requirements (Beck et al., 2016; Vidan & Lehdonvirta, 2019) with the evidence that trust requirements endure (Hawlitschek et al., 2018, 2020; Völter et al., 2023): trust neither disappears nor persists unchanged, but changes in function and object. Whether digital trust mechanisms substitute for or complement established trust has been posed as an open question spanning levels of analysis (Schilke et al., 2026); the present account locates the answer at the inter-organisational level for infrastructure the parties co-construct, where system-based and relational trust divide operational from strategic work. The sequence also explains why pre-adoption matters so much. The initial trust required to enter an arrangement is interpersonal, developed through relational exchange; once that foundation enables capability development, SBT progressively assumes the operational load, freeing relational trust for strategic work. SBT thereby provides the trust reconceptualisation that decentralised infrastructures have been argued to demand, one that specifies the object of trust and the conditions under which reliance becomes warranted (Lacity et al., 2025).

5.4 Explaining Success and Failure

The framework accounts for divergent outcomes through a single mechanism: whether organisations develop the capabilities that allow SBT to emerge. Successful transformation depends on intensive pre-adoption relational exchange through which partners establish shared understanding, common standards, and joint governance, consistent with staged accounts of consortium formation (Hacker et al., 2023) and with the observation that costly set-up interaction underwrites later economies in coordination (Harrison et al., 2023). Our contribution specifies capability development as the link between that set-up work and post-adoption outcomes, and SBT as the trust form it yields.

Failure follows when this relational work is curtailed. The TradeLens platform, developed by Maersk and IBM and discontinued in 2022, illustrates the pattern: research attributes its inability to achieve industry-wide adoption to power asymmetries that undermined collaborative governance and to the difficulty of establishing trust across competing stakeholders (Jensen et al., 2019; Jovanovic et al., 2022; Hanisch et al., 2025). Recent work clarifies why such asymmetries are decisive. Viguerie et al. (2026) show that enterprise blockchains reproduce centralised governance when platform openness and participant inclusiveness are low, with these formative conditions imprinting power asymmetries into the infrastructure and constraining subsequent governance. Viewed through our framework, top-down design by a dominant sponsor forecloses the collaborative pre-adoption processes on which DTC and ACC depend, so what emerges is compliance with a mandated system rather than warranted reliance on a co-constructed one.

Lacity et al. (2024) document the same pattern across a generation of private B2B blockchain networks that closed through an inability to attract trading partners, attributing failure to architectures built to deliver value to their founders rather than to the wider partner base. In our terms, founder-centric design pre-empts the joint rule definition on which Algorithmic Coordination Capability depends, leaving partners with a system to comply with rather than one they helped construct. Where participants are instead empowered to govern through autonomy, transparency, and communication, the conditions for capability development are present (Soleimanof & Neufeld, 2026). This pattern recurs on a far larger

canvas in Hanisch et al.'s (2026) grounded theory of 81 ecosystems, which traces recurrent breakdown to governance misalignments – most visibly the founder-led model, common amongst early enterprise networks, in which a dominant player mandates participation and thereby forecloses the collaborative governance on which warranted system-level reliance depends. Our sample, comprising organisations that reached the hybrid stage, carries a survivorship bias: those that failed to develop the requisite capabilities may have abandoned smart contracts before that stage, which the framework would predict.

5.5 Boundary Conditions

The framework holds within three boundaries. The first is ecosystem size and structure. Our evidence derives from SME ecosystems of roughly two to ten partners, where the intensive face-to-face collaboration that founds capability development remains feasible. As ecosystems grow to dozens or hundreds of partners, that collaboration becomes harder to sustain, and coordination may depend on intermediaries or phased onboarding rather than direct bilateral work. Hanisch et al. (2026) document the same dynamic across their cases: the coordination trade-off intensified with scale, and the initiatives that succeeded deliberately "started small" and were designed for smaller, less capable participants rather than only their large founders. The second is power distribution. Our cases did not include arrangements in which a dominant anchor mandated participation, which limits our ability to theorise capability development under coercion; the TradeLens and enterprise-blockchain evidence suggests that mandated participation without genuine co-creation yields compliance rather than SBT (Viguerie et al., 2026), a dynamic that warrants dedicated study. This converges with Hanisch et al.'s (2026) finding that cooperative rather than competitive intent is what lets participants rely on system-level rules: where partners are non-competing and adopt a "we need to do this together" orientation, system-level reliance becomes viable, whereas competitive postures and founder domination produce the defensive behaviour that prevents it. SBT, on our account, emerges in precisely the cooperative, broadly symmetric corner that their co-opetition boundary condition identifies as favourable. The third is technical orientation. Our informants belonged to technology-oriented SMEs whose existing capabilities likely eased adoption, so traditional SMEs may face capability-development demands the framework does not fully capture. Network architecture, public or permissioned, cuts across these boundaries. Lacity et al. (2024) argue that public decentralised networks reduce the vendor lock-in and permission dependence that contributed to the failure of first-generation private deployments, a distinction that bears directly on cost-sensitive SMEs; whether capability development proceeds differently across the two architectures is a question our data, which did not systematically record network type, cannot settle.

5.6 Future Research

These boundaries mark the most productive lines for further work. Longitudinal study would establish whether the functional differentiation between system-based and relational trust remains stable as relationships deepen, or whether the division of labour shifts over years of operation. Dedicated examination of abandoned initiatives would test the framework's failure logic, distinguishing breakdowns rooted in insufficient pre-adoption exchange from those rooted in power asymmetry or technical limits. Comparative work across ecosystem sizes and power structures would clarify whether the capability-development mechanism scales and whether mandated adoption indeed produces compliance without SBT. Quantitative operationalisation of DTC, ACC, and SBT would permit testing of the proposed relationships

and of moderators such as prior relationship history, industry, and network architecture across larger samples.

5.7 Practical Implications

For practitioners, the framework reframes smart contract adoption as capability development rather than technology procurement. The promise of automated coordination invites organisations to economise on relationship-building, yet the evidence points the other way: intensive pre-adoption collaboration is the foundation that makes subsequent automation reliable, and attempts to bypass it risk the capability deficits that underlie documented failures. Managers should therefore treat shared interpretation, jointly defined rules, and designed governance as investments to be made before go-live, not overheads to be minimised. They should also pursue functional differentiation deliberately, assigning operational coordination to system-based reliance while reserving relational effort for strategy, innovation, and exception handling. Finally, ecosystem architects should weigh size and power distribution at the design stage, since large or sponsor-dominated initiatives may need phased, genuinely collaborative onboarding to develop the collective capabilities on which warranted reliance depends.

6. Conclusion

This study asked how inter-organisational relationships transform as organisations adopt blockchain-based smart contracts, and what enables effective relationships when algorithmic and relational governance operate together. The answer reframes a technology widely cast as a substitute for trust. Smart contracts neither dissolve inter-organisational trust nor leave relationships unchanged; they relocate the work of trust. Through intensive relational exchange before adoption, organisations build two inter-organisational capabilities, Distributed Transparency Capability and Algorithmic Coordination Capability, and with them actualise the affordances that smart contracts offer. Through these capabilities a distinctive trust form emerges, System-based Trust, defined as warranted reliance on coordinating infrastructure that partners have jointly constructed. System-based Trust complements relational trust rather than displacing it: it carries operational coordination and frees relational trust for the strategic collaboration, innovation, and exception handling that human judgement still requires, producing Hybrid Inter-organisational Relationships as the outcome of successful transformation. The account holds within SME ecosystems of limited size and broadly symmetric power; larger or sponsor-dominated arrangements fall outside its scope and offer a clear agenda for further work. Its central lesson for research and practice is that smart contracts are occasions for capability development, not instruments that make inter-organisational trust unnecessary.

References

Barratt, M., Choi, T. Y., & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of Operations Management*, *29*(4), 329–342. https://doi.org/10.1016/j.jom.2010.06.002

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). *Blockchain–the gateway to trust-free cryptographic transactions*. 1–14.

Bharadwaj, A. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, *24*(1), 169–196. https://doi.org/10.2307/3250983

Bloomfield, B. P., Latham, Y., & Vurdubakis, T. (2010). Bodies, Technologies and Action Possibilities: When is an Affordance? *Sociology*, *44*(3), 415–433. https://doi.org/10.1177/0038038510362469

Cao, Z., & Lumineau, F. (2015). Revisiting the interplay between contractual and relational governance: A qualitative and meta-analytic investigation. *Journal of Operations Management*, *33*, 15–42.

Chen, R. R., Chen, K., & Ou, C. X. J. (2023). Facilitating interorganizational trust in strategic alliances by leveraging blockchain-based systems: Case studies of two eastern banks. *International Journal of Information Management*, *68*, 102521. https://doi.org/10.1016/j.ijinfomgt.2022.102521

Cui, M., Li, W., & Kamoche, K. (2026). Building Trust in Decision-Support Artificial Intelligence: A Boundary Spanning Perspective. *Information Systems Journal*, *36*(3), 435–456. https://doi.org/10.1111/isj.70015

Danese, P., & Romano, P. (2025). Blockchain Systems in Food Supply Chains: An Interpretation Through the Lens of Agency and Technology–Organization–Environment Theories. *Journal of Business Logistics*, *46*(3), e70019. https://doi.org/10.1111/jbl.70019

Dang, Q., & Li, G. (2026). Unveiling trust in AI: The interplay of antecedents, consequences, and cultural dynamics. *AI & Society*, *41*(1), 669–692. https://doi.org/10.1007/s00146-025-02477-6

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284.

Du, W. (Derek), Pan, S. L., Leidner, D. E., & Ying, W. (2019). Affordances, experimentation and actualization of FinTech: A blockchain implementation study. *The Journal of Strategic Information Systems*, *28*(1), 50–65. https://doi.org/10.1016/j.jsis.2018.10.002

Dyer, J., Singh, H., & Hesterly, W. S. (2018). The relational view revisited: A dynamic perspective on value creation and value capture. *Strategic Management Journal*, *39*(12), 3140–3162. https://doi.org/10.1002/smj.2785

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/AMR.1989.4308385

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *The Academy of Management Journal*, *50*(1), 25–32. https://doi.org/10.5465/AMJ.2007.24160888

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, *13*(2), 159–190.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Golden, B. R. (1992). The past is the past—Or is it? The use of retrospective accounts as indicators of past strategy. *Academy of Management Journal*, *35*, 848–860.

Goldsby, C., & Hanisch, M. (2022). The Boon and Bane of Blockchain: Getting the Governance Right. *California Management Review*, *64*(3), 141–168. https://doi.org/10.1177/00081256221080747

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology*, *91*, 481–510.

Gregory, R. W., Beck, R., Henfridsson, O., & Yaraghi, N. (2025). Cooperation among Strangers: Algorithmic Enforcement of Reciprocal Exchange with Blockchain-Based Smart Contracts. *Academy of Management Review*, *50*(4), 859–873. https://doi.org/10.5465/amr.2023.0023

Grover, V., & Kohli, R. (2012). Cocreating IT Value: New Capabilities and Metrics for Multifirm Environments. *MIS Quarterly*, *36*(1), 225–232. JSTOR. https://doi.org/10.2307/41410415

Gulati, R., & Sytch, M. (2008). Does familiarity breed trust? Revisiting the antecedents of trust. *Managerial and Decision Economics*, *29*, 165–195.

Hacker, J., Miscione, G., Felder, T., & Schwabe, G. (2023). Commit or not? How blockchain consortia form and develop. *California Management Review*, *65*(3), 110–131. https://doi.org/10.1177/00081256231175530

Halaburda, H., Levina, N., & Min, S. (2024). Digitization of Transaction Terms within TCE: Strong Smart Contract as a New Mode of Transaction Governance. *MIS Quarterly*, *48*(2), 825–846. https://doi.org/10.25300/MISQ/2023/17818

Hanelt, A., Wiesche, M., Benlian, A., & Hinz, O. (2026). Opening the network of trust: How domain experts in triadic relationships build trust in AI-based counterparts. *MIS Quarterly*, *50*(1), 299–326. Business Source Premier (191915797). https://doi.org/10.25300/MISQ/2025/18041

Hanisch, M., Goldsby, C., Fortin, M., & Rogerson, M. (2025). Governing Within Semirigid Limits: Navigating the Centralization–Decentralization Paradox in Blockchain-Based Platforms. *Journal of Operations Management*, *71*(7), 917–938. https://doi.org/10.1002/joom.70001

Hanisch, M., Roozen, P., & Theodosiadis, V. (2026). Success and Failure in Blockchain-Based Interorganizational Ecosystems: A Governance Perspective. *Journal of Management*, 01492063261420752. https://doi.org/10.1177/01492063261420752

Harrison, D., Munksgaard, K. B., & Prenkert, F. (2023). Coordinating Activity Interdependencies in the Contemporary Economy: The Principle of Distributed Control. *British Journal of Management*, *34*(3), 1488–1509. https://doi.org/10.1111/1467-8551.12650

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hawlitschek, F., Notheisen, B., & Teubner, T. (2020). A 2020 perspective on “The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy”. *Electronic Commerce Research and Applications*, *40*. https://doi.org/10.1016/j.elerap.2020.100935

Huber, G. P., & Power, D. J. (1985). Retrospective reports of strategic-level managers: Guidelines for increasing their accuracy. *Strategic Management Journal*, *6*, 171–180.

Jensen, T., Hedman, J., & Henningsson, S. (2019). How TradeLens Delivers Business Value With Blockchain Technology. *MIS Quarterly Executive*, *18*(4), 221–243. Business Source Premier (140328253). https://doi.org/10.17705/2msqe.00018

Ji, Y., Du, W. (Derek), & Pan, S. L. (2024). Vendor capabilities development in blockchain sourcing: A parallel play approach. *Journal of Information Technology*, *39*(2), 270–287. https://doi.org/10.1177/02683962231226399

Johnston, H. R., & Vitale, M. R. (1988). Creating competitive advantage with interorganizational information systems. *MIS Quarterly*, *12*(2), 153–165. https://doi.org/10.2307/%2520248839

Jovanovic, M., Kostić, N., Sebastian, I. M., & Sedej, T. (2022). Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens. *Technological Forecasting and Social Change*, *184*, 121981. https://doi.org/10.1016/j.techfore.2022.121981

Karimi-Alaghehband, F., & Rivard, S. (2019). Information technology outsourcing and architecture dynamic capabilities as enablers of organizational agility. *Journal of Information Technology*, *34*(2), 129–159. https://doi.org/10.1177/0268396218816271

Killoran, J., Park, A., & Kietzmann, J. (2024). Delineation of Reasoning, Intentional Disclosure, and the Potential for Harm: An Extension of Vanneste and Puranam's "Artificial Intelligence, Trust, and Perceptions of Agency". *Academy of Management Review*, amr.2024.0193. https://doi.org/10.5465/amr.2024.0193

Korsgaard, M. A., Cooper, C. D., Mayer, K. J., Poppo, L., & Zaheer, A. (2025). The Boundaries of Trust in a New Era. *Academy of Management Review*, 1–11. https://doi.org/10.5465/amr.2024.0605

Kumar, K., & Van Dissel, H. G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems. *MIS Quarterly*, 279–300.

Lacity, M. C. (2022). Blockchain: From Bitcoin to the Internet of Value and beyond. *Journal of Information Technology*, *37*(4), 326–340. https://doi.org/10.1177/02683962221086300

Lacity, M., O'Leary, D. E., & Conway, D. (2024). Developing Capabilities for B2B Commerce on Public Decentralized Networks. *MIS Quarterly Executive*, *23*(4).

Lacity, M. C., Schuetz, S. W., Kuai, L., & Steelman, Z. R. (2025). IT's a matter of trust: Literature reviews and analyses of human trust in information technology. *Journal of Information Technology*, *40*(3), 286–313. https://doi.org/10.1177/02683962231226397

Lankton, N., McKnight, D. H., & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems*, *16*(10), 880–918. https://doi.org/10.17705/1jais.00411

Lehrer, C., Constantiou, I., Matt, C., & Hess, T. (2023). How Ephemerality Features Affect User Engagement with Social Media Platforms. *MIS Quarterly*, *47*(4), 1663–1678. https://doi.org/10.25300/MISQ/2023/17085

Leonardi, P. M. (2013). When Does Technology Use Enable Network Change in Organizations? A Comparative Study of Feature Use and Shared Affordances. *MIS Quarterly*, *37*(3), 749–775.

Lipton, J. P. (1977). On the psychology of eyewitness testimony. *Journal of Applied Psychology*, *62*, 90–95.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Luhmann, N. (1979). *Trust and Power: Two Works by Niklas Luhmann. Translation of German originals Vertrauen [1968] and Macht[1975]*. John Wiley.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 94–107). Basil Blackwell. http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain Governance—A New Way of Organizing Collaborations? *Organization Science*, *32*(2), 500–521. https://doi.org/10.1287/orsc.2020.1379

Malone, T. W., Benjamin, R. I., & Yates, J. (1987). Electronic markets and electronic hierarchies. *Communications of the ACM*, *30*(6), 484–497.

Markus, M. L., & Silver, M. (2008). A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit. *Journal of the Association for Information Systems*, *9*(10), 609–632. https://doi.org/10.17705/1jais.00176

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Transactions on Management Information Systems*, *2*(2), 1–25. https://doi.org/10.1145/1985347.1985353

Monteiro, E., Constantinides, P., Scott, S., Shaikh, M., & Burton-Jones, A. (2022). Qualitative Research Methods in Information Systems: A Call for PhenomenonFocused Problematization. *MIS Quarterly*, *46*(4), i–xviii.

Murray, A., Kuban, S., Josefy, M., & Anderson, J. (2021). Contracting in the smart era: The implications of blockchain and decentralized autonomous organizations for contracting and corporate governance. *Academy of Management Perspectives*, *35*(4), 622–641. https://doi.org/doi.org/10.5465/amp.2018.0066

Nicolaou, A., Sedatole, K., & Lankton, N. (2011). Integrated Information Systems and Alliance Partner Trust. *Contemporary Accounting Research*, *28*(3), 1018–1045. https://doi.org/10.1111/j.1911-3846.2011.01077.x

Obermeier, D., & Henkel, J. (2025). Deductive Certainty? Exploring the Boundaries of Trust Formation in Smart Contracts on Blockchains. *MIS Quarterly*, *49*(4), 1513–1538.

Pang, M.-S., Lee, G., & DeLone, W. H. (2014). IT Resources, Organizational Capabilities, and Value Creation in Public-Sector Organizations: A Public-Value Management Perspective. *Journal of Information Technology*, *29*(3), 187–205. https://doi.org/10.1057/jit.2014.2

Poppo, L., & Zenger, T. R. (2002). Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal*, *23*(8), 707–725.

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities. *MIS Quarterly*, *30*(2), 225–246. JSTOR. https://doi.org/10.2307/25148729

Rai, A., Pavlou, P. A., Im, G., & Du, S. (2012). Interfirm IT Capability Profiles and Communications for Cocreating Relational Value: Evidence from the Logistics Industry. *MIS Quarterly*, *36*(1), 233–262. JSTOR. https://doi.org/10.2307/41410416

Renwick, R., & Gleasure, R. (2021). Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems. *Journal of Information Technology*, *36*(1), 16–38. https://doi.org/10.1177/0268396220944406

Ring, P. S., & Van der Ven, A. H. (1994). Developmental processes of cooperative interorganizational relationships. *Academy of Management Review*, *19*, 90–118.

Roth, T., Stohr, A., Amend, J., Fridgen, G., & Rieger, A. (2023). Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit. *International Journal of Information Management*, *68*, 102476. https://doi.org/10.1016/j.ijinfomgt.2022.102476

Saffarizadeh, K., Keil, M., & Maruping, L. (2024). Relationship Between Trust in the AI Creator and Trust in AI Systems: The Crucial Role of AI Alignment and Steerability. *Journal of Management Information Systems*, *41*(3), 645–681. https://doi.org/10.1080/07421222.2024.2376382

Saraf, N., Langdon, C. S., & Gosain, S. (2007). IS Application Capabilities and Relational Value in Interfirm Partnerships. *Information Systems Research*, *18*(3), 320–339. https://doi.org/10.1287/isre.1070.0133

Sarker, S., Henningsson, S., Jensen, T., & Hedman, J. (2021). The Use Of Blockchain As A Resource For Combating Corruption In Global Shipping: An Interpretive Case Study. *Journal of Management Information Systems*, *38*(2), 338–373. https://doi.org/10.1080/07421222.2021.1912919

Schilke, O., Bachmann, R., Blomqvist, K., Krishnan, R., & Sydow, J. (2026). Unpacking the Paradoxes of Trust in Uncertain Times. *Organization Studies*, *47*(3), 359–389. https://doi.org/10.1177/01708406261430577

Schreieck, M., Wiesche, M., & Krcmar, H. (2021). Capabilities for value co-creation and value capture in emergent platform ecosystems: A longitudinal case study of SAP's cloud platform. *Journal of Information Technology*, *36*(4), 365–390. https://doi.org/10.1177/02683962211023780

Schuetz, S., Kuai, L., Lacity, M. C., & Steelman, Z. (2025). A qualitative systematic review of trust in technology. *Journal of Information Technology*, *40*(1), 55–76. https://doi.org/10.1177/02683962241254392

Soleimanof, L., & Neufeld, D. J. (2026). Pursuit of decentralization in blockchain-based systems: An empowerment perspective. *Journal of Information Technology*, *41*(1), 37–55. https://doi.org/10.1177/02683962251389979

Söllner, M., Hoffmann, Axel, & and Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. https://doi.org/10.1057/ejis.2015.17

Strong, D., Volkoff, O., Johnson, S., Pelletier, L., Tulu, B., Bar-On, I., Trudel, J., & Garber, L. (2014). A Theory of Organization-EHR Affordance Actualization. *Journal of the Association for Information Systems*, *15*(2), 53–85. https://doi.org/10.17705/1jais.00353

Vanneste, B. S., & Puranam, P. (2025). Artificial Intelligence, Trust, and Perceptions of Agency. *Academy of Management Review*, *50*(4), 726–744. https://doi.org/10.5465/amr.2022.0041

Vidan, G., & Lehdonvirta, V. (2019). Mine the gap: Bitcoin and the maintenance of trustlessness. *New Media & Society*, *21*(1), 42–59.

Viguerie, C., Ciriello, R. F., Zavolokina, L., & Mathiassen, L. (2026). Explaining decentralisation in enterprise blockchain governance: The imprint of platform openness and participant inclusiveness. *Journal of Information Technology*, *41*(1), 56–74. https://doi.org/10.1177/02683962261422482

Volkoff, O., & Strong, D. M. (2013). Critical realism and affordances: Theorizing IT-associated organizational change processes. *MIS Quarterly, 37*(3), 819–834.

Volkoff, O., & Strong, D. M. (2017). Affordance theory and how to use it in IS research. In R. D. Galliers & M.-K. Stein (Eds.), *The Routledge companion to management information systems* (pp. 232–245). Routledge.

Völter, F., Urbach, N., & Padget, J. (2023). Trusting the trust machine: Evaluating trust signals of blockchain applications. *International Journal of Information Management*, *68*, 102429. https://doi.org/10.1016/j.ijinfomgt.2021.102429

Williamson, O. (1996). *The Mechanisms of Governance*. Oxford University Press.

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, *9*(2), 141–159. https://doi.org/10.1287/orsc.9.2.141

Zhou, J., Xu, T., Chiao, Y., & Fang, Y. (2024). Interorganizational Systems and Supply Chain Agility in Uncertain Environments: The Mediation Role of Supply Chain Collaboration. *Information Systems Research*, *35*(1), 184–202. https://doi.org/10.1287/isre.2023.1210