

In blockchain we trust?

A critical review of blockchain in supply chains

*Rami Alkhudary**

*Xavier Brusset***

*Chitu Okoli***

* Université Paris-Panthéon-Assas, LARGEPA, Paris, France

** SKEMA Business School – Université Côte d’Azur, Paris, France

Abstract

The increasing importance of blockchain in supply chains has led to myriad papers with conflicting or imprecise results. This critical review of 118 articles first summarises the emerging literature on the role of trust in blockchain use in supply chains. Next, we identify and refine concepts that have been neglected or confused in the literature. We note the critical role of physical data verification (i.e., checking that on-chain records match the state of physical goods). We distinguish interorganisational trust in partners from trust in blockchain technology. Hence, we develop a set of propositions based on these clarifications. Specifically, physical verification of the data logged onto the blockchain increases trust, both between partners and in blockchain technology. However, as trust in blockchain technology increases, partners who already trust each other may see less need to use it. Blockchain usage increases both kinds of trust. The more trust there is, the less that data logged onto the blockchain will be physically verified. Future research may investigate the role of additional technological advances required to ensure that digital records accurately represent reality.

Keywords: blockchain, supply chain information system, trust, physical data verification, critical literature review.



Immutabilité n'est pas vérité : Une revue critique de la confiance dans la blockchain pour les chaînes d'approvisionnement

*Rami Alkhudary**

*Xavier Brusset***

*Chitu Okoli***

* Université Paris-Panthéon-Assas, LARGEPA, Paris, France

** SKEMA Business School – Université Côte d'Azur, Paris, France

Résumé

L'importance croissante de la blockchain dans les chaînes d'approvisionnement a donné lieu à une avalanche d'articles présentant des résultats contradictoires ou imprécis. Dans cette revue critique de 118 articles, nous résumons tout d'abord la littérature émergente sur le rôle de la confiance dans l'utilisation de la blockchain dans les chaînes d'approvisionnement. Ensuite, nous identifions et affinons les concepts essentiels qui ont été négligés ou confondus dans la littérature. Nous soulignons le rôle crucial de la vérification physique des données, c'est-à-dire la vérification de la correspondance entre les enregistrements sur la chaîne et l'état des biens physiques. Nous distinguons la confiance interorganisationnelle dans les partenaires de la confiance dans la technologie blockchain. Sur la base de ces clarifications, nous élaborons un ensemble de propositions. Plus précisément, la vérification physique des données enregistrées sur la blockchain renforce la confiance, tant entre les partenaires qu'envers la technologie blockchain. Cependant, alors que la confiance dans la technologie blockchain augmente son utilisation, lorsque les partenaires se font déjà confiance au départ, ils peuvent considérer qu'il est moins nécessaire d'utiliser la blockchain. L'utilisation de la blockchain renforce ces deux types de confiance. Plus la confiance est grande, moins les données enregistrées sur la blockchain seront vérifiées physiquement. Des recherches futures pourraient s'intéresser au rôle des avancées technologiques supplémentaires nécessaires pour garantir que les enregistrements numériques reflètent la réalité.

Mots-clés :

blockchain, système d'information de la chaîne d'approvisionnement, confiance, vérification des données physiques, revue critique de la littérature.



1 Introduction

Various technologies have been used to support supply chain information systems (SCISs) “*designed to provide information and information processing capability to support the strategy, operations, management analysis, and decision-making functions*” (H. Hu et al., 2023; Tarokh & Soroor, 2006).

These technologies have historically included enterprise resource planning (ERP) systems. However, their effectiveness across organisations is limited (Akkermans et al., 2003), primarily because they require multiple organisations to agree on the same vendor’s technology (Al-Sumaidae et al., 2023). Enterprise application integration (EAI) combines application capabilities to build efficient, cost-effective IT infrastructures. However, as with ERPs, EAI requires a centralised data architecture, so supply chain partners must trust the central controller for the reliability of records, which can often be rather opaque to them (Brusset, 2016; Karamchandani et al., 2020).

Blockchain has been increasingly integrated into SCISs to ensure that information recorded across all supply chain members can be shared immutably to prevent any single entity from modifying it (Beck et al., 2018). Blockchain is a distributed ledger or database of non-erasable blocks of digital records registered using a precise consensus mechanism to validate and record this information (Alkhudary et al., 2020). Several organisations have already deployed blockchain across their supply chain networks to improve service quality and ensure efficient financial and physical flows (S. E. Chang et al., 2019). The global market was estimated at approximately USD 7.23 billion in 2025, which is projected to exceed USD 8.67 billion in 2030 (Fortune Business Insights, 2026). However, many challenges exist to making blockchain adoption a reality for enterprises, including concerns about standards, regulations, common governance models, and viable ecosystems (Ehrenberg & King, 2020).

Several literature reviews have studied the use of blockchain in supply chains (BCSC) from different perspectives: general reviews of current applications, future potential, and challenges (Karakas et al., 2022; Queiroz et al., 2019; Y. Wang, Han, et al., 2019); various industrial sectors that use BCSC (Dutta et al., 2020); blockchain and trust in an interorganisational context from an international business perspective

(Murimi et al., 2023); blockchain applications in the agri-food supply chain (González-Mendes et al., 2024; Vern, Panghal, Mor, & Kamble, 2024); blockchain integration with artificial intelligence for the supply chain (Charles et al., 2023); and the benefits of collaborative shared information in contrast to barriers such as conflicts of interest (Najar et al., 2024; Wan et al., 2020). However, considerable disagreement persists about the role of trust in BCSC after analysing the BCSC literature, despite broad consensus on the relationships among blockchain use, information sharing, and performance.

Batwa and Norrman's (2021) review specifically focused on trust in BCSC and distinguished trust among supply chain partners from trust in blockchain technology, each conceptualised with distinct dimensions. Batwa and Norrman developed propositions on the relationships between these trust dimensions and information sharing enabled by blockchain. Although they highlighted contradictions in the literature, they could not resolve some important questions, such as why some studies have found that blockchain increases trust, whereas others have found that it constrains trust in supply chains. Hence, their propositions left such investigations to future research.

Despite such prior reviews, we find it disconcerting that most studies and reviews have relied on questionable assumptions about the nature of trust in BCSC, thereby leading the literature in a direction that is inconducive to the successful application of blockchain aligned with how supply chains work. Even the previously mentioned review overlooked important distinctions, such as the specific subjects of trust (e.g., users vs managers), while not sufficiently developing the consequences of trust based on physical data verification of the supply chain products. Notably, Schilke and Lumineau (2023) highlighted that interorganisational trust can reside at both the individual boundary-spanner and organisational levels, thereby underscoring the need to clarify precisely whose trust is being examined in blockchain-enabled supply chain settings.

For example, a common assumption is that data on the blockchain accurately reflect the reality of the physical activities on the ground and can be trusted (e.g., de Boissieu et al., 2021; Kayikci et al., 2020).

Despite several literature reviews on BCSC, the crucial fact that blockchain lacks a mechanism to guarantee such correspondence has been widely overlooked (Albizri & Appelbaum, 2021; Baharmand et

al., 2021; Hald & Kinra, 2019; Ozdemir et al., 2021). Moreover, much of the literature has inferred that blockchain technology somehow eliminates the continued importance of trust in supply chain partners (Bai & Sarkis, 2020; Centobelli et al., 2021). Moreover, this literature has failed to distinguish between trust among supply chain partners and trust in blockchain technology, with relatively few exceptions of reporting conflicting relationships regarding the direction of trust in the consequences or antecedents of blockchain adoption and trust in partners (Batwa & Norrman, 2021).

Given the state of the field, the research objective of this critical review is to recalibrate the direction of future research to ask more meaningful questions about trust in BCSC that properly understand its specificities. Our goal is not to conduct another general literature review summarising the rapidly developing body of literature on blockchain in the supply chain context (Karakas et al., 2022; Queiroz et al., 2019; Y. Wang, Han, et al., 2019). Rather, this critical review (as characterised in Paré et al., 2015) seeks to provide a necessary summary of the scholarly consensus in this domain, including critiquing unclear concepts and questionable relationships related to trust in BCSC. Specifically, our critical review aims to address the following research question:

How are blockchain use, trust in partners, and trust in blockchain technology related to each other in supply chain information systems, and how does physical data verification affect these relationships?

A critical review is a specific approach to literature reviewing that “*critically analyze[s] the extant literature on a broad topic to reveal weaknesses, contradictions, controversies, or inconsistencies*” (Paré et al., 2015, p. 189). Unlike an empirical study that asks and answers a research question, our critique leads to propositions that pose novel questions. We build on this critique to develop a research agenda grounded in our analysis to guide future research toward answering such questions.

Hence, we offer three main contributions beyond a general review of the role of trust in BCSC. First, we highlight the crucial role of physical data verification in BCSC. Normally, people think of blockchain for digital products (e.g., cryptocurrencies; Mattke et al., 2021), so they ignore the need to verify the mapping between the digital record and the physical world. Second, we show that two distinct forms of trust related

to BCSC (i.e., trust in partners and trust in blockchain) can have opposite theoretical effects on blockchain use. Thus, we build on the information systems literature, which distinguishes between trust in technology and interpersonal trust (Lin & Lin, 2019; Lippert & Forman, 2006; McKnight et al., 2011). Moreover, in our supply chain context, we focus on interorganisational trust (i.e., trust in supply chain partners) rather than interpersonal trust. Third, we show the importance of considering the temporal sequencing of blockchain use in relation to trust development. Whereas most of the literature argues that blockchain use increases trust, we argue that when trust is initially in place, supply chain partners may not need blockchain, thereby reducing its use.

Our critical review, which aims to contribute to theory development, is structured similarly to others (Kordzadeh & Ghasemaghaei, 2022; Steininger et al., 2022; Zhang, 2013). The remainder of this article is organised as follows. First, we examine some critical theoretical concepts that have been poorly identified or altogether neglected by the BCSC literature. Next, we develop a research agenda with new theoretical propositions based on our refined concepts. Finally, we discuss the contributions and implications of the review with some directions for future research. ly summarise the literature, and list the articles constituting our review.

2 Critical Literature Review Methodology

We applied a broad yet selective search strategy in line with the critical review genre. Unlike most literature reviews that employ a comprehensive search strategy that attempts to synthesise the entire body of literature, *“Critical reviews are either selective or representative, and they rarely involve a comprehensive search of all of the relevant literature”* (Paré et al., 2015, p. 189). We followed the four major stages of a critical review (Steininger et al., 2022): review plan, literature identification, data extraction and categorisation, and critical analysis.

2.1 Review plan

We began with a general, informal exploration of literature on BCSC. During this early stage, we observed a recurring theme: the assumption that information recorded in a blockchain is inherently

trustworthy and does not require further verification. This assumption is often taken for granted in many articles, which contrasts with our observation of managerial experience with blockchain technology. This observation led us to focus our critical review on trust in blockchain systems.

2.2 Literature identification

We searched for literature on the use of blockchain in the context of supply chains from 2008, the year that blockchain emerged (Nakamoto, 2008), to July 2024 in the Scopus and EBSCO Business Source Ultimate scholarly literature databases. They offer broad coverage of management, operations, and information systems research, thereby ensuring disciplinary relevance and journal quality. We employed the following search string on the titles, abstracts, and keywords: (blockchain OR blockchains OR “block chain” OR “block and chain” OR “distributed ledger”) AND “supply chain” AND (trust OR “data verification” OR “data validation”). We found 1,372 articles. Filtering on English-language peer-reviewed journal articles resulted in 493 articles. Figure 1 outlines the search procedure described here.

Our goal for our critical review was not to replicate previously conducted reviews of BCSC, but rather to assess and critique the theoretical trends in the most influential literature while highlighting important issues that past reviews have overlooked. We only considered peer-reviewed English-language articles from journals listed in the 2021 Academic Journal Guide (AJG) from the Chartered Association of Business Schools, an extensive list of 1,698 journals from all fields of business, including information systems and supply chain management, among others. Following this choice, we focused on business-oriented journals because we are interested in the management and human aspects of blockchain use rather than being drowned in the thousands of technical articles on the topic in fields like computer science and engineering.

We verified the appropriateness of articles by reviewing the abstracts and, as needed, the full text. We also included relevant articles from our reading and references, even if they were not on the list. In addition to the AJG list, we considered articles in the FNEGE list of management and economics journals

that were not in the AJG list. However, this approach did not yield further articles. We included all such articles from the AJG and FNEGE lists.

This step ensured that the final selection addressed the relationships among the core concepts central to our study. The methodological nature of each article, whether conceptual or empirical, was not a selection criterion at this stage. Instead, we noted the methodological approach for use in the subsequent analysis phase. We thus identified a final list of 118 articles that provided either empirical evidence (i.e., qualitative or quantitative) or conceptual arguments concerning the relationships among the core concepts. By comparison, Batwa and Norrman (2021), with a similar focus on trust in BCSC, identified and reviewed 55 articles. The reviewed articles are listed in Appendix B, along with their relationships. Figure 1 outlines the search procedure described here.

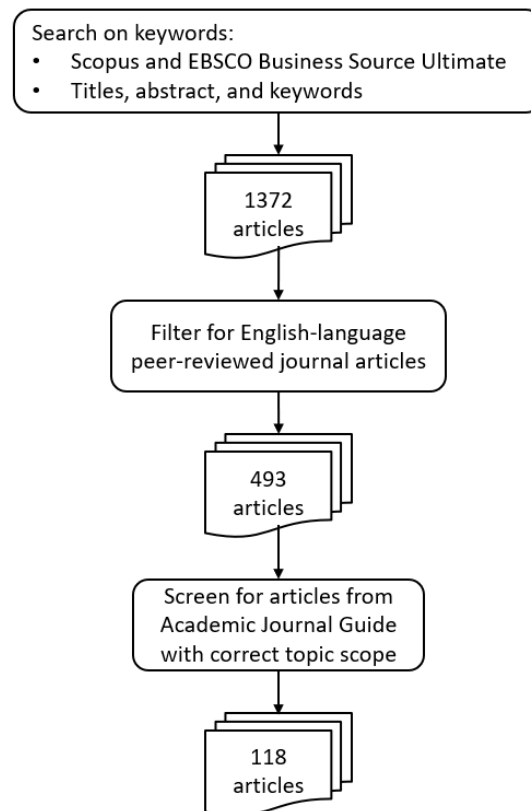


Figure 1. Literature search procedure

2.3 Data extraction and categorisation

We used the theoretical synthesis approach (Okoli, 2022) to organise the key concepts from the identified articles into theoretical concepts and their relationships using a theory extraction worksheet. These concepts were then refined based on our interaction with the literature and synthesised using a theory map and a concept matrix (see Appendix B). The use of these tools was instrumental in enhancing our understanding and ability to critique the articles under review.

We also read numerous other articles related to BCSC. We found that the most problematic relationships examined were those among blockchain use, trust, information sharing, and performance. Therefore, we focused on these theoretical concepts in the first part of this review, which summarises the existing literature. We summarise the findings from this stage of the review in Figure 6 and Appendix B.

2.4 Critical analysis

The final step, critical analysis, involved applying problematisation techniques to challenge assumptions in the literature. We used two techniques. First, we framed our inquiry in terms of contrastive research questions (Tsang & Ellsaesser, 2011) that stated the base question and explicitly highlighted the contrast that made the question non-intuitive. While we did not retain the contrastive forms of our final research question, they helped us focus our attention on what was not intuitive. For example, we focused our analysis on intermediary questions, similar to the following:

- Why is physically unverified blockchain data not a trustworthy representation of physical reality rather than being a trustworthy representation?
- Why does trust between partners decrease the likelihood of implementing blockchain rather than either increasing its likelihood or at least having no effect?
- Why should two different types of trust (i.e., trust in partners versus trust in blockchain) have opposite effects on the use of blockchain rather than having similar effects?

Second, we followed Okoli's (2021) principles for developing research agenda propositions that problematise and extend the current literature. Specifically, we summarised the relationships and findings from the existing literature (see Appendix A and Figure 6). We then applied theoretical concept synthesis

with a propositional scope (Okoli, 2022) to extract and highlight inconsistencies in the literature (presented in Section 2). Finally, we considered the consistencies and divergences in the literature to help us identify the concerns that we formulated as a research agenda. Overall, this step was essential for developing a nuanced and critical perspective on the literature we reviewed. We summarise the insights from this research agenda in Appendix A and Figure 4 and Figure 5.

3 Critical Analysis of Conceptual Tensions in the Literature

This section critically analyses three major conceptual tensions in the literature on BCSC. We draw on examples from various industries to emphasise how seemingly overlooked nuances bear implications for integrating blockchain into SCISs. As stated, we solely focus here on surfacing these problems rather than resolving them. Their theoretical elaboration is developed in the following major Section 4.

3.1 Tension 1: Blockchain use – Intentions, actual use, and publication bias

We define blockchain use as the implementation and employment of blockchain technology in supply chains. In our BCSC research context, we include both actual use and future use intentions. Nevertheless, the underlying assumption in much of the literature is that intended and actual blockchain use can be treated interchangeably. However, this assumption is flawed because intention-based findings often reflect expectations or hype rather than observed organisational behaviour.

Given the relative novelty of blockchain, most empirical studies have measured intention to use blockchain rather than actual use (notable exceptions include Dubey et al., 2020; Fosso Wamba & Guthrie, 2020; Kshetri, 2018; Pan et al., 2020; Zelbst et al., 2019). Unsurprisingly, nearly all relationships between blockchain use and performance have been positive, given the hype surrounding it (Madaan et al., 2023; Sharma, Bhatia, et al., 2023). Indeed, the assumption that intention equals implementation obscures potential publication bias and prevents the literature from accurately theorising about blockchain's realised impacts.

Unfortunately, among the few studies empirically investigating the actual use of blockchain, we are concerned that publication bias might be at play, as we could not find a single study that had surveyed or

analysed organisations where blockchain was unsuccessful. Notably, few even studied the overall cost of investing in such technology, given the expected benefit for the supply chain (Y. Chang et al., 2020; Karakas et al., 2022; Öztürk & Yildizbaşı, 2020), with Cole et al. (2019) and Rimba et al. (2020) identifying the lack of such research. Instead, qualitative studies have only investigated promising or successful cases of blockchain deployment (e.g., Rahmanzadeh et al., 2020; Y. Wang, Singgih, et al., 2019). Moreover, quantitative studies with large samples have either studied nonusers' intention to use blockchain (e.g., Wong et al., 2020; C.-S. Yang, 2019) or the sampling only targeted current users (e.g., Roeck et al., 2020) or nonusers and users together (Dubey et al., 2020) in the few existing surveys of actual blockchain users.

Concrete examples reinforce our concern. In the food industry, the Walmart mango-traceability pilot and subsequent agri-food projects have been widely publicised as successes. However, few published studies have assessed their cost–benefit trade-offs or operational failures, despite Rogerson and Parry (2020) noting that visibility gains depend on continuous manual data entry that increases costs and errors. In the pharmaceutical sector, the MediLedger blockchain has often been cited as proof of effective industry coordination. However, available accounts have emphasised technical feasibility rather than economic performance or abandoned trials (Mattke et al., 2019).

Therefore, the silence in the empirical record illustrates how positive-case reporting dominates the literature while omitting projects that stall due to high integration costs, regulatory incompatibilities, or insufficient partner engagement. This selective visibility constitutes publication bias sustained by the assumption that only successful implementations yield theoretical insight. Therefore, we offer a deeper criticism of assumptions: the literature implicitly assumes that success stories reveal mechanisms (see generally Stanley, 2005) of trust and performance, while failures are treated as anomalies rather than as data that can falsify prevailing claims about blockchain's benefits.

As we argue later, the nature of the relationship depends on whether trust is considered *before* implementing blockchain (i.e., intention to use) or *after* its adoption (i.e., actual use). Thus, our propositions explicitly clarify whether actual or intended use is meant.

3.2 Tension 2: Whom or what is trusted in information system-driven supply chains?

In supply chain management, trust refers to when an actor is unsure of what another actor will do but has good reason to be confident that the latter will act as expected, both now and in the future. A key assumption underlying much of the literature is that “trust” is a single, unified construct. However, this assumption is flawed because it collapses two fundamentally distinct relationships: trust among partners and trust in technological systems.

The literature has established that asymmetric information and opportunistic behaviour lead to a lack of trust (Babich & Tang, 2012; Beth et al., 2003; F. Chen, 2003; Narayanan & Raman, 2004), while blockchain is seen as a solution to trust problems among supply chain partners (Di Vaio & Varriale, 2020; Yong et al., 2020). However, Cole et al. (2019) challenged the link between trust and blockchain applications based on two schools of thought. One school considers blockchain to be a network of trust among supply chain partners (D. Ghode et al., 2020; Sheel & Nath, 2019; Yeoh et al., 2023), whereas the other argues that blockchain’s trustless system removes the need for trust (Centobelli et al., 2021; Economist, 2015; M. Kim et al., 2018; Powell et al., 2023; Swan, 2015). The latter view switches the focus from interorganisational trust to system or machine trust (Schmidt & Wagner, 2019). Hence, participants trust that the blockchain works, regardless of which organisations participate. Therefore, we clarify between two kinds of trust pertinent to BCSC: trust in partners (i.e., interorganisational trust (Zaheer et al., 1998) and trust in the blockchain system (i.e., trust in the machine (Risius & Spohrer, 2017)). We explicitly define these two types of trust in Sections 3.2.2 and 3.2.3 below. Batwa and Norrman (2021) made this distinction in their review of trust in BCSC. Nonetheless, we add a further distinction: the subjects of trust significantly differ between these two kinds of trust. Hence, treating trust as monolithic prevents theory from explaining opposite empirical findings while concealing the critical need to distinguish trust in partners from trust in blockchain technology. The following subsection briefly discusses various aspects of trust before focusing on the two pertinent to our analysis.

3.2.1 Who is trusting? Subjects of trust

Consistent with the literature on trust in supply chains, our analysis is at the organisational level, so we do

not examine individual users' trust in the system, which fundamentally differs from most of the literature considering individuals as the subjects of trust (Lankton et al., 2015; McKnight et al., 2011). While the unit of analysis is the organisation, trust is essentially an individual concept. Strictly speaking, organisations, as abstract entities, cannot trust anything, even though, per Schulz, Valentinov, and Pies (2024), they can be viewed as possessing unique characteristics that systematically increase their reliability and legitimacy. Therefore, we consider the aggregate trust of certain groups within an organisation to represent the organisation's trust.

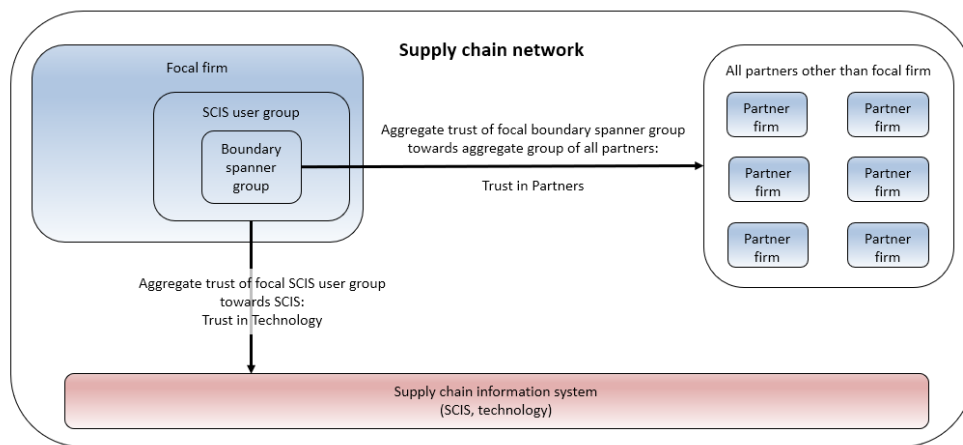


Figure 2: Trust in partners and trust in technology in a supply chain

We are interested in two primary groups. First, considering trust between organisations, we are interested in those identified by the supply chain literature as “boundary spanners”: individuals within a focal firm who directly contact counterparts in another firm, thus spanning the boundary between the two firms (Zaheer et al., 1998). Indeed, interorganisational trust can be anchored at multiple levels, from individual boundary spanners to collective organisational entities, thereby underscoring the importance of clarifying which unit is actually doing the trusting (Schilke & Lumineau, 2023). Second, considering technology in the supply chain, we focus on the collective trust of a representative group of users within an organisation. Thus, we consider collective SCIS users, which normally include boundary spanners and other users, and consider their trust towards SCISs.

The following sections elaborate on two pertinent theoretical concepts: trust in partners and trust in

technology (see the representation inspired by Zaheer et al., (1998, Figure 1) in (Zaheer et al., 1998)).

3.2.2 *Whom is being trusted? Trust in partners*

We define trust in partners as when a supply chain partner is unsure of what another partner will do but has good reason to be confident that the latter will act as expected, both now and in the future. We focus on both the dyadic trust between pairs of organisations (Gefen et al., 2008; Goo et al., 2009; Ibrahim & Ribbers, 2009; Klein & Rai, 2009) and aggregate trust that a focal organisation's collective of individuals has in all partner organisations in the supply chain. We refer to our particular focus on interorganisational trust as "trust in partners" (Z. Wang et al., 2014). However, attributing trust to an organisational entity rather than a sum of individuals often depends on the extent to which shared norms and practices shape collective perceptions of partner reliability (Schilke & Lumineau, 2023).

Indeed, trust in the present context is meaningful "*if and only if at least one party is exposed to an element of behavioural risk*" (Lyons & Mehta, 1997, p. 240), where behavioural risk is present if one party's behaviour can materially affect the other party. The fate of a supply chain lies in all partners' ability to work effectively with aligned objectives, incentives, and rules to alleviate power concerns (Allen et al., 2000). In fact, interorganisational trust often reflects organizationally embedded processes that transcend interpersonal ties (Schultz et al., 2024), thereby shaping how a collective anticipates and evaluates a partner's actions (Schilke & Lumineau, 2023). Trust stems from interlocked partners understanding that they need each other to deliver goods and services while having aligned objectives and corresponding incentives (Narayanan & Raman, 2004). In such a setting, trust springs from the choice of governance (Ghosh & Fedorowicz, 2008; Gulati & Nickerson, 2008; Robson et al., 2008) or from the level of control partners have over one another (Gallivan & Depledge, 2003).

3.2.3 *What is being trusted? Trust in technology*

The second aspect of trust is closer to our study's focus. Indeed, people also trust inanimate objects, such as computer technology and information systems (Lin & Lin, 2019; Lippert & Forman, 2006; McKnight et al., 2011). This understanding of trust comes from an information systems research perspective outside of

the supply chain management context. Nevertheless, it is particularly critical in the context of blockchain in the supply chain to counter the widespread argument that blockchain obviates the need for trust. We argue here that, rather than trust vanishing altogether, a “trustless” or “zero-trust” system (Albizri & Appelbaum, 2021; Powell et al., 2023) actually means that the object of trust shifts from the partners to the system. Therefore, blockchain does not enable “trustless” systems but rather highlights a specific type of trust: trust in technology (Lippert & Forman, 2006; McKnight et al., 2011). Hence, the partners trust that the blockchain will work as expected, regardless of which organisations participate in the supply chain (M. Kim et al., 2018).

Risius and Spohrer (2017) offered insightful observations concerning the notion of trust in blockchain. They highlighted that various blockchain technologies involve different degrees of trust in the other blockchain parties. For instance, less-trusting verification mechanisms based on cryptocurrency mining may be used for public networks, whereas alternative mechanisms based on permissions may apply within private, trusted networks (p. 387). also noted that even in low-trust networks, blockchain users must still trust technology infrastructure providers, who are people, not technology (p. 391).

McKnight et al. analysed many aspects of trust in technology. The perspective that best matches the focus of this article is what they called *“trusting belief-specific technology-functionality: the belief that the specific technology has the capability, functionality, or features to do for one what one needs to be done”* (2011, p. 7). Specifically, we define “trust in blockchain” as the composite trust of the SCIS user group in the focal firm regarding the SCIS enabled by blockchain, based on the belief that blockchain technology is capable of reliably transmitting the necessary supply chain information.

Surveys and interviews are the principal means of empirically measuring trust in blockchain technology. However, unlike trust in partners whose aggregate measurement may be dominated by a few powerful boundary spanners, the role of SCIS users is more egalitarian in the collective group for measuring an organisation’s trust in technology, as each user decides whether to use the SCIS based on trust (Hoehle et al., 2012), despite the feelings of other SCIS users or the insistence of their managers (Bhattacharjee et al., 2018). Thus, their collective trust is more accurately measured as an average.

3.3 Tension 3: The reality check – Gaps in physical data verification

One of the fundamental principles of supply chain management is the physical verification of goods recorded in the SCIS. Our term “physical data verification” is not to be confused with “data validation” (i.e., verifying that data correspond to the defined set of valid possible values consistent with the database structure). Rather, we define our term as the verification that the data correspond to the real-world reality that they are supposed to represent.

This verification can take several forms, depending on the data. For instance, an importer may have a certified third-party check imported goods for quality at the port of export. A pharmacist may check the vaccine temperature log to confirm that the cold chain was not broken since the expedition. A food inspector may check whether ground meat is indeed beef and contains no more than the expected maximum amount of fat. A manufacturer of baby talcum powder may verify the absence of asbestos in the acquired raw material.

Furthermore, the *“quality of the information shared – rather than the extent of information sharing – should be seen as the main leverage”* (Z. Wang et al., 2014). Indeed, periodic inventory checks must be conducted to ensure the accuracy of the digital records of physical goods. However, this cardinal principle is taken for granted in theoretical models. For example, on a decision-making operational level, digital twins primarily concern the representation of a complex reality through “physical-to-virtual connections” that link (i.e., twin) physical and digital assets so that the difference *“between the physical and digital entities is determined and the virtual entity is updated accordingly”* (Jones et al., 2020).

The literature commonly assumes that blockchain automatically guarantees the truth of recorded data. Nonetheless, this assumption is mistaken because immutability ensures that records cannot be changed, not that they are initially correct. For instance, in vaccine distribution, Hu et al. (2023) showed that blockchain systems must still rely on physical temperature verification through Internet of Things (IoT) sensors to maintain trust in cold-chain integrity. In the food sector, Rogerson and Parry (2020) documented that, despite blockchain-enabled traceability, verification of origin still depends on manual audits and laboratory testing of meat and dairy samples. In manufacturing and pharmaceuticals, Li et al.

(2020) and Niu et al. (2021) emphasised that sensor readings or laboratory certificates may be uploaded, but their authenticity remains untested without human or third-party inspection.

Such examples reveal that the theoretical omission of physical data verification stems from an assumption of technological sufficiency. Therefore, exposing such hidden assumptions is crucial (Steininger et al., 2022). These empirical cases reintroduce physical verification as a central concern to demonstrate that blockchain's credibility ultimately depends on continuous, costly, and fallible interactions with the physical world, which the literature has largely ignored.

Several factors impede the widespread practice of physical data verification, despite supply chain managers' awareness of its importance (Xiao et al., 2012). Physical verification requires physical access to products in partners' hands. However, when a focal firm receives goods, it is not always easy or feasible to verify their quality. Moreover, such a detailed inspection cannot verify the goods' provenance (Brun & Moretto, 2014; J. Yang et al., 2006). Therefore, thorough verification requires access to partners' factories and warehouses, which is sometimes achieved by employing third-party quality certifiers, albeit inconsistently (Yan et al., 2020).

Hence, the uncritical transfer of the "trustless" claim from digital contexts to physical supply chains blinds the literature to the unresolved problem of verifying that blockchain data genuinely reflects physical reality. We develop this and other unresolved problems in the following major section.

4 Unresolved Challenges and Theoretical Propositions

We now turn to the unresolved theoretical challenges posed by the conceptual tensions identified in Section 2, which motivate our propositions. We uncovered several key inconsistencies and puzzles regarding the relationships among the theoretical concepts of blockchain use, trust in partners, trust in blockchain technology, and physical data verification. This section first motivates our proposition development by critiquing important unresolved issues arising from our analysis. Subsequently, the next two subsections derive several propositions regarding the relationships among the theoretical concepts described in the previous section to provide resolution. These propositions mark the first steps towards answering the research question: "How do blockchain use, trust in partners, and trust in blockchain

technology influence one another, and how does physical data verification mediate these relationships within supply chain information systems?”

4.1 Unresolved issues concerning physical data verification

The literature affirms blockchain’s benefits for supply chain concerns such as visibility, traceability, and transparency (Ahmed et al., 2023; Murimi et al., 2023). However, a critical yet often-overlooked concern is the veracity of data on the blockchain. For example, Tezel et al. (2021) claimed that blockchain allows *“individuals, organisations, and machines to transact with each other over the internet without having to trust each other or use a third-party verification”* (p. 1). Moreover, *“If an organisation chooses to opt for blockchain-as-a-service (BaaS), they will not be running their Ethereum private node, meaning they are not verifying transactions and trusting a third-party machine to do so, which defies some of the purposes of blockchain implementation cases”* (p. 10).

This mistaken notion that blockchain somehow eliminates the need for third-party verification is widespread in the literature (e.g., de Boissieu et al., 2021; Kayikci et al., 2020; M. Kim et al., 2018). Nevertheless, nothing in the blockchain mechanism verifies that the true physical state of the world matches the blockchain record. Furthermore, if erroneous data are entered into a blockchain (whether accidentally or fraudulently), they are immutable and propagate throughout the supply chain. Nonetheless, the mechanisms and processes for ensuring information correctness and validity are assumed to be beyond the scope of concern for blockchain (Glaser, 2017; Hawlitschek et al., 2018, 2020), which is a major concern for BCSC. Again, this concern differs from those in blockchains for digital products and services (e.g., financial transactions), where the state of the world is digital.

We offer several examples of such oversight. The literature delegates the verification of physical reality to a “physical layer” comprising various IoT devices, including sensors and radio-frequency identification (RFID) tags (Agrawal et al., 2021; S. Hu et al., 2021; Lao et al., 2020; Saurabh & Dey, 2021). However, potential forgers can abuse the system if verification of the actual states of the world is not performed (Wasim Ahmad et al., 2021, p. 3). Thus, merely claiming that *“the blockchain facilitates the disclosure of*

information and impedes the provision of intentionally corrupted information” (Notheisen et al., 2017, p. 5) is insufficient.

Whereas some (e.g., Lu & Xu, 2017) have argued that a laboratory’s verification of a sample is enough, it does not guarantee that the rest of the batch is good or that the same sample cannot be used multiple times across batches. For example, Niu et al. (2021) did not specify how quality is to be verified beyond stating that the manufacturer does so while the retailer is not subject to verification. Monitoring and other controls involve information gathering, fact checking, and verification processes to assess the congruence between reported information and reality (Yan et al., 2020). Such verification involves processes conducted in two areas: information cross-checking in information systems and fact checking of the true state of goods (i.e., physical data verification). The latter seeks to ensure consistency between physical reality and data records, which can only be conducted offline.

Surprisingly, few studies have acknowledged the continued need for physical data verification in blockchain-based supply chains for physical products. Fortunately, some have taken this challenge quite seriously. For instance, Rogerson and Parry argued, *“Errors and fraud can enter the digital supply chain at the interface between the physical and digital”* (2020, p. 605). Thus, even after the data are reliably certified as corresponding to the blockchain record, the blockchain does not reflect any subsequent changes.

Moreover, in a Delphi study of more than 100 supply chain experts who predicted the ongoing challenges for blockchain in 2035, data verification was widely acknowledged as a problem that blockchain could not resolve (Kopyto et al., 2020). Indeed, many expert practitioners are keenly aware of the seriousness of this challenge, even though many scholars seem to overlook it.

Song et al. (2024) found that effective reliance on blockchain governance requires both data verifiability and codifiability in the blockchain; otherwise, relational and contractual governance are more important. Moreover, a few researchers have explicitly acknowledged physical data verification in their design when designing prototypes of blockchain-enabled supply chains, thereby demonstrating how blockchain, combined with IoT sensors, can reduce manual verifications without eliminating them (Albizri &

Appelbaum, 2021; Centobelli et al., 2021; J. Li et al., 2020). This demonstration starkly contrasts with the work of other researchers, who have assumed that physical data verification is unnecessary while acknowledging that the effectiveness of their automated solution would be compromised if such manual steps were required (Bader et al., 2021; Y. Chen et al., 2022; Pelé et al., 2023a; Zhu et al., 2022).

The widespread assumption that data recorded on the blockchain is more trustworthy than data recorded using other digital record technologies arises from a transfer of trust from the application of blockchain in financial services to its application in the movement of physical goods in supply chains. However, we argue that this transfer of trust is unwarranted. When considering fully electronic financial transactions, there is no meaningful difference between the actual financial status and the digital blockchain record of that status, given the confidence blockchain provides. In fact, a fundamental difference exists between a physical good and its digital record, even a blockchain record. Therefore, the physical good must be physically verified to ensure that the digital record matches it because the mere fact that the record is logged on a blockchain does not make it trustworthy. Indeed, an inaccurate record can be recorded on a blockchain, so it is not trustworthy without physical verification. Even worse, an inaccurate record on a blockchain is immutable and thus potentially more damaging than one on a conventional, mutable system.

4.2 Unresolved issues concerning trust in blockchain

We now turn to problematic assumptions with the literature's treatment of trust in blockchain. The literature predominantly associates BCSC with increased trust by arguing that blockchain use increases trust between partners (Brookbanks & Parry, 2022; Centobelli et al., 2021; Howson, 2020; Qian & Papadonikolaki, 2020; Yacoub & Castillo, 2021). However, this simplistic assumption ignores temporal sequencing and the possibility that pre-existing trust may even reduce rather than enhance the motivation to adopt blockchain. Ironically, although such arguments are premised on blockchain use *followed by* trust (Manzoor et al., 2024; Trautmann et al., 2024), most studies making this argument have surveyed supply chain members who do not use blockchain to ask them how much they trust their partners, *followed by* whether they intend to implement blockchain (e.g., Alazab et al., 2021; Chittipaka et al., 2022; Pan et al.,

2020; Reddick et al., 2019). Notably, however, a few studies have tested in the opposite direction (e.g., Queiroz et al., 2020; Queiroz & Fosso Wamba, 2019). Hence, while most arguments contend that blockchain use is first followed by subsequent trust, empirical tests find that when trust exists in the present, blockchain implementation is intended as a future result. Thus, such studies have consistently found a strong relationship between trust and blockchain.

However, we argue that such studies confuse two crucial, distinct points. First, the relationship between trust in partners and blockchain use is not symmetrical when the order of events is reversed. A difference exists between partners' trust in each other *while using blockchain* and *when they use it*, even if they already trust each other. If indeed a primary reason to implement blockchain is to help partners trust each other more, when partners already trust each other, they have less reason to implement it. Thus, we would expect trust in partners to have a negative effect rather than increasing trust or having no effect on trust. The second area of confusion is that most studies have treated "trust" as a monolithic construct, while neglecting the abundant literature that clarifies the fundamentally different types of trust. In particular, trust in supply chain partners (Gefen et al., 2008; Goo et al., 2009; Ibrahim & Ribbers, 2009; Klein & Rai, 2009) operates quite differently from trust in technology (Lin & Lin, 2019; Lippert & Forman, 2006; McKnight et al., 2011). Hence, despite the paradox of our previous point that trust in partners decreases rather than increases blockchain use, we do not believe that such a negative relationship holds for trust in blockchain as a technology. We affirm the intuitive expectation that those who trust blockchain are more likely to use it. However, this notion leads to the irony that one important type of trust related to blockchain increases its use (Brookbanks & Parry, 2022; Centobelli et al., 2021; Howson, 2020; Qian & Papadonikolaki, 2020; Yacoub & Castillo, 2021), whereas another important type of trust related to partners reduces blockchain use or may obviate it (Markus & Buijs, 2022; Tönnissen & Teuteberg, 2020). While it is not unusual for different types of trust to have different effects, it is unusual for them to have diametrically opposite effects, as the cited references indicate.

To foreground our critical stance, we challenge the prevailing assumption that physical verification merely supports trust in a one-way causal sequence. We argue that verification and trust dynamically co-evolve,

with each reinforcing or undermining the other depending on the temporal context. The next two subsections develop propositions for a research agenda that aims to address these arguments. Specifically, by “propositions” we mean the relationships between conceptual concepts or constructs, one step removed from hypotheses that express concrete, measured variables (Bacharach, 1989). Specifically, our propositions state the relationships we propose between the concepts we clarified and defined in the previous section.

As depicted in Figure 3, the primary differences from the existing literature are the crucial role of physical data verification and the distinction between two types of trust (i.e., trust in partners and trust in blockchain or technology). Since the effects of blockchain use on performance and information sharing are widely presented as positive in the literature (Vasanthraj et al., 2024; Vern, Panghal, Mor, & Kamble, 2024), our propositions do not concern these aspects. These relationships are shaded grey in Figure 3. Instead, we focus on the more questionable monolithic treatment of trust and the importance of physical data verification. In Figure 3, we depict, in blue, the concepts and relationships that are the focus of the research agenda of our critical review. Moreover, the directions and signs of the arrows depend on the temporal sequence of the concepts (e.g., if blockchain use precedes trust or if trust precedes blockchain use). Finally, we subdivide Figure 3 into Figure 4 and Figure 5 to clarify the nuanced implications of the temporal sequence.

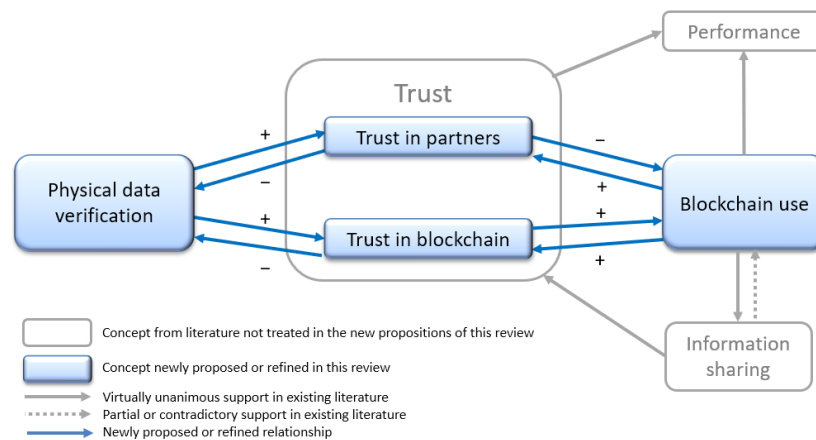


Figure 3. A refined theoretical model of blockchain and trust in supply chains

4.3 Propositions on physical data verification to trust in blockchain use

We developed theoretical propositions to offer logically grounded expectations for how physical data verification and the two kinds of trust interact with blockchain use to address the aforementioned unresolved issues. A primary interest in blockchain research is understanding the factors that may encourage a supply chain to adopt blockchain. We argue that a key factor is the extent and quality of physical data verification, which may impact both partners' trust in each other (Choi, 2019; Choi & Luo, 2019) and users' trust in blockchain technology to enhance their SCISs (Choi, Feng, et al., 2020), each of which may have various effects on their eventual use of blockchain (G. Li et al., 2021; K. Li et al., 2021). We depict these theoretical relationships in Figure 4.

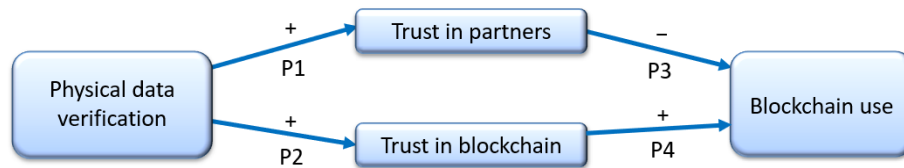


Figure 4. Theoretical relationships when physical data verification precedes blockchain use (subset of Figure 3)

As noted in Section 2.3, nothing in blockchain guarantees that a blockchain record matches physical reality (Albizri & Appelbaum, 2021). Thus, for partners to trust each other, blockchain alone is insufficient, as some physical verification is needed to reassure an organisation that its partners' records are trustworthy.

Behnke and Janssen (2020) were surprised to find that “*product and process properties (traceability data) were recorded*” in the four supply chains they studied. They found that if the conditions for traceability were met, “*trust should be provided by the blockchain technology*” (p. 8), which implies that these records provide credibility signals that reduce behavioural ambiguity. Chaudhuri et al. (2021) similarly presented several cases in which the physical verification of data recorded in the supply chain was an essential aspect of the BCSC to “[*crack*] down on poor quality or counterfeit” (p. 13). Physical inspections convey reliability and integrity by confirming that partners consistently provide verifiable and accurate data, thereby forming the basis for trust.

Nonetheless, this situation is not specific to blockchain, as physical data verification is part of information sharing required to build trust, increase performance (Zhou & Benton, 2007), and reduce transaction costs (Kwon & Suh, 2004). An organisation is more likely to expect its partners to be trustworthy if it knows that its records will be physically verified (Kafi, F. & Kafi, Majid, 2016; S. Li & Lin, 2006; J.-Z. Wu & Chien, 2008). Hence, we present the following proposition:

P1: The more data logged onto the blockchain are physically verified, the higher the trust between partners.

As indicated earlier, many blockchain advocates have argued that BCSC users no longer need to trust their partners because they can rely on blockchain as a reliable technology to protect their interests. However, such arguments are mainly based on blockchain for recording digital products without physical counterparts (e.g., digital coin wallets), which is not the case in physical product supply chains. Thus, the arguments for how data verification affects trust in partners also apply when we move from trust in partners (i.e., the aggregate trust of the boundary-spanner group) to trust in blockchain among users of the SCISs, some of whom are members of the boundary-spanner group.

The literature provides several examples of how physical data verification may enhance trust. For instance, blockchain can increase market demand for data quality, thereby improving sales forecasts (Choi & Luo, 2019). Moreover, in the food industry, blockchain enhances visibility, transaction transparency, and food safety and quality (K. Li et al., 2021), thereby preventing fraud and counterfeit products (Rogerson & Parry, 2020). Traceability is enabled by the blockchain's ability to trace every transaction and reveal the involved actors and other information (Kamble et al., 2019; Roeck et al., 2020).

Physical verification also plays a critical role for users in building confidence in the system's overall reliability. However, because blockchain technology is immutable, any error or falsification becomes permanently inscribed. Thus, regular physical verification aims to mitigate the risk of these immutable errors before they can erode trust. Indeed, physical verification enhances transparency and accountability, thereby assuring users that the blockchain remains a faithful reflection of reality. Users' trust in

blockchain would be severely damaged if they discovered that information immutably recorded on the blockchain did not correspond to physical reality (Sander et al., 2018). Hence, regular physical checks to continuously verify that the blockchain record reflects reality can increase users' trust in the blockchain system (Yan et al., 2020). Thus, we present the following proposition:

P2: The more data logged onto the blockchain are physically verified, the more users of the supply chain information system trust the blockchain.

Two main factors are likely to prompt partners to use or intend to use blockchain, regardless of physical data verification practices in a supply chain. First, partners who do not trust each other may find the idea of blockchain appealing. For example, Chen et al. (2022) showed that blockchain and smart contracts can positively influence partners' trust, while Longo et al. (2019) demonstrated that blockchain is a convenient tool for overcoming collaboration and trust issues. Hence, the proposal of a blockchain governance scheme may indicate a shortage of trust among partners (Jeanneret Medina et al., 2024).

However, blockchain's benefits are considerably less compelling in supply chains where trust among partners is already high. Three interrelated arguments support this view. First, in such situations, many existing SCISs already work well (Abiteboul et al., 1995). When partners trust each other, they typically rely on established governance mechanisms and trusted record-keeping systems (van Veen-Dirks & Verdaasdonk, 2009). For example, in the pharmaceutical, cosmetic, and food sectors, controls are enforced by regulations in most countries. Such mechanisms were established long before blockchain appeared. Thus, the additional benefit of blockchain's verifiable immutability becomes redundant in these environments.

Second, implementing blockchain is not without its costs. As Longo et al. (2019) noted, blockchain is primarily used to minimise the negative consequences of information asymmetry and to deter data counterfeiting. In high-trust settings where partners have robust mechanisms in place, the significant costs and risks associated with deploying a new technology are not justified by marginal gains in trust or performance. Consequently, these partners are less likely to invest in blockchain, as traditional systems

already provide sufficient security and transparency. Furthermore, a third disincentive to implementing blockchain when trust is high lies in its ability to protect against data manipulation by ensuring that recorded information is immutable and verifiable.

Therefore, these collective arguments suggest that when trust is high, there is less need for the additional trust-enhancing features of blockchain, so it is difficult to justify the cost of implementing such a new, complex system. In contrast, blockchain's benefits are most compelling in environments where partners lack strong pre-existing trust. Thus, we present the following proposition:

P3: The more trust exists between partners, the less likely they are to feel the need to use blockchain in their supply chain.

Naturally, if supply chain partners initially trust blockchain, they are more likely to feel comfortable using it. "Use" in this sense encompasses both a supply chain network that intends to adopt and use blockchain technology for its SCIS and its individual users (G. Li et al., 2021; W. Lu et al., 2022). At the organisational level, SCIS users include the border spanners group, which comprises senior executives who make implementation decisions and are arguably the most influential members of the SCIS user group. At the individual level, once a blockchain-based SCIS is in place, individual users decide if and how much to use it. Hence, their intention to use it versus the extent of their actual use is influenced by how much they trust the technology. Thus, we present the following proposition:

P4: The more users of the supply chain information system trust blockchain, the more they will use it.

It may seem paradoxical that this proposition holds that one kind of trust reduces blockchain use while another increases it. This tension can be resolved by recognising that trust between partners involves tight coordination and collaboration over the years, whereas trust in blockchain largely entails non-managerial blockchain users. Hence, while managers who trust their partners do not need blockchain, we argue here that SCIS users who trust blockchain may want to use it.

4.4 Propositions on blockchain use to trust in physical data verification

We now reverse the causal direction to explore how blockchain use as an initial condition can subsequently affect trust and physical data verification. Similar to the preceding propositions, the following propositions are conceptual extensions grounded in theoretical synthesis rather than empirically tested claims. They articulate relationships that are logically inferred from gaps and contradictions in prior research, as well as from the authors' professional observations. Thus, they serve as theory-generative propositions that invite future empirical validation.

Once supply chains adopt blockchain, equally pertinent to supply chain managers is how their blockchain use shapes trust and related practices (e.g., physical data verification). We argue here that blockchain use may not necessarily lead to sound supply chain practices. We depict the relevant theoretical relationships in Figure 5.

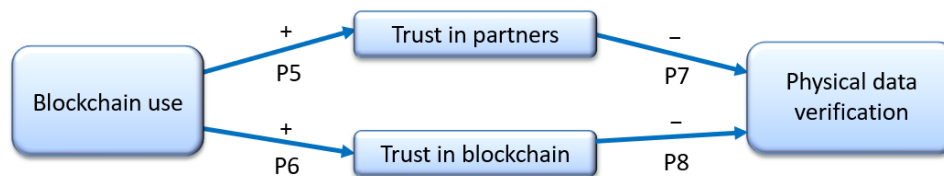


Figure 5. Theoretical relationships when blockchain use precedes physical data verification (subset of Figure 3)

Unlike propositions in which trust precedes intentions to use blockchain or its actual use, we specifically refer to the effect of actual use on trust, not merely intended use. The literature broadly concurs that BCSC increases many aspects of information sharing (e.g., Bai & Sarkis, 2020; Kshetri, 2018; Sander et al., 2018; see Appendix B for more). These aspects help partners trust each other more (Batwa & Norrman, 2021; D. Ghode et al., 2020; Sheel & Nath, 2019). Thus, we propose the following:

P5: The actual use of blockchain in the supply chain increases trust among partners.

Blockchain use improves trust in blockchain system technology for many reasons (Batwa & Norrman, 2021; Kittipanya-ngam & Tan, 2020; Notheisen et al., 2017; Yong et al., 2020). For example, blockchain systems can be fully decentralised, as each node has an identical copy of the blockchain ledger. In

addition, a strict consensus mechanism validates that each transaction is immutably registered. For instance, the MediLedger network uses zero-knowledge proof on its blockchain platform to enable pharmaceutical entities in the United States to share data while keeping their content hidden (MediLedger, 2021). In general, the longer a user has a positive experience with a specific technology, the more they use it and the more they will trust its reliability and its functionality for achieving their objectives (Hoehle et al., 2012). Thus, we present the following proposition:

P6: The actual use of blockchain in the supply chain increases the trust of users of the supply chain information system in blockchain.

Blockchain is often presented as a “trust machine” that eliminates the need for traditional trust-building measures in supply chains (H. Song et al., 2024). However, many supply chains already enjoy high levels of trust because they rely on robust governance mechanisms (Ghosh & Fedorowicz, 2008; Kittilaksanawong, 2016). These mechanisms (e.g., well-defined contracts, audits, and agreed-upon standards) are designed to prevent opportunistic behaviour. Since partners actively engage in information sharing, which both reduces behavioural uncertainty and increases mutual trust (F. Chen, 2003; Kwon & Suh, 2004), the need for an external blockchain-based trust mechanism is inherently diminished. Notably, the disadvantages of physical data verification become more pronounced when trust is high, as it is financially and operationally expensive (Choi, 2019; Niu et al., 2021), while continuously monitoring suppliers to ensure they meet quality and technical standards is costly (Gundlach & Cannon, 2010). Therefore, the additional expense of physical checks is challenging to justify in a high-trust environment. Given that these trust-building practices substitute for the need for blockchain-based verification, we propose the following:

P7: The greater the trust between partners, the less that data logged onto the blockchain are physically verified.

If SCIS users have a high level of trust in blockchain, they may naively assume little need for regular physical verification. This belief is largely rooted in the idea that information recorded on the blockchain is immutable (Longo et al., 2019; Mishra et al., 2021; Sheel & Nath, 2019). Therefore, many users erroneously assume that if data are on the blockchain, they must be true.

For instance, Longo et al. (2019) described how blockchain guarantees the integrity and origin of data by certifying it through cryptographic mechanisms. When users internalise this role, they conclude that the blockchain provides sufficient validation, so additional physical verification is redundant.

Moreover, as blockchain-based record keeping becomes more prevalent, it is normalised as the de facto source of truth. Mishra et al. (2021) emphasised that the blockchain's ability to create permanent records fosters an environment in which digital documentation is taken at face value. This normalisation leads users to rely almost exclusively on digital verification, thereby further diminishing the perceived need for physical checks.

Over time, a self-reinforcing cycle of complacency can emerge as trust in the blockchain system grows. Users become increasingly confident that the blockchain's inherent properties ensure data integrity, so they are less willing to incur the additional cost and time required for physical verification. Thus, we present the following proposition:

P8: The greater the trust of users of the supply chain information system in blockchain, the less that data logged onto the blockchain are physically verified.

These collective propositions clarify the theoretical foundations for understanding the interdependence among trust, data verification, and blockchain use. They also establish a framework for both scholars and practitioners to reassess how blockchain operates within SCISs. The next section discusses how these theoretical insights translate into broader implications for research and practice.

5 Discussion

Despite a growing body of research on blockchain use in the supply chain, the literature remains immature, marked by a shortage of empirical studies. Even existing empirical studies have often not

addressed the topic in sufficient depth. Many papers have not clearly defined or measured the studied concepts or their boundary conditions, which has led to confusion and sometimes conflicting theoretical relationships about the fundamental role of this cutting-edge technology for SCISs.

In response, this critical review endeavours to deepen understanding of the vital role of trust in the use of BCSC, in light of the turn taken by the literature. However, our critical review intends to redirect relevant future research to focus on crucial neglected issues. Therefore, this section discusses the major implications for theory and practice before concluding with directions for future research.

5.1 Theoretical contributions

We offer four major theoretical contributions that address our research question, “How do blockchain use, trust in partners, and trust in blockchain technology influence one another, and how does physical data verification mediate these relationships within supply chain information systems?” As a baseline contribution, we synthesised the current state of the rapidly growing literature on BCSC and trust and found serious concerns in its treatment of the relationships between blockchain use and trust. Our other three major contributions are as follows: (a) we emphasised the crucial role of physical data verification in blockchain use for tracking physical goods, (b) we dissected the amorphous notion of “trust” in BCSC by highlighting the different effects of the distinct concepts of trust in partners and trust in technology (specifically trust in blockchain), and (c) we demonstrated the importance of temporal sequencing of our propositions. We now elaborate on these three major contributions.

5.1.1 Role of physical data verification

Our focus on the role of physical data verification as a distinct theoretical concept has practical implications for blockchain use in supply chains and other applications where the recorded data must match physical reality. Examples of such reported uses abound, including land registries (Kayikci et al., 2020), greenhouse gas emissions certificates (Castka et al., 2020), certificates of origin or property (Danese et al., 2021; de Boissieu et al., 2021), and insurance claims (Bhawana et al., 2023). While the importance of physical data verification has been acknowledged in the blockchain literature, it has usually

been taken for granted. Although some studies have highlighted the importance of verifying physical data in a blockchain-based information system to better manage first-mile logistics (Alles & Gray, 2020; Batwa & Norrman, 2021), we are unaware of any study that has explicitly highlighted it as a theoretical concept or explained the mechanism for physically verifying data within the supply chain, including what actors should verify which types of data.

Crucially, physical data verification is not an intrinsic capability of blockchain technology but a sociotechnical and governance process that must occur before on-chain registration. Accountability for verifying data lies upstream, before its digital inscription. This distinction is essential for both practitioners and scholars, given the persistent misconception that blockchain inherently guarantees data accuracy. As reiterated, blockchain guarantees immutability, not veracity. Hence, ensuring that data accurately reflect physical reality remains an organisational and human responsibility that rests with the actor (i.e., whether an individual or an institution) who enters the data. Consequently, managers must differentiate between what the technology ensures (i.e., record integrity and traceability) and how factual accuracy is established (i.e., verification and an audit of inputs) to design physical data verification protocols accordingly.

Examples of the critical tensions in the literature vividly illustrate these implications. In food and pharmaceutical supply chains, blockchain solutions show that trust in blockchain only endures when physical verification routines remain institutionalised (H. Hu et al., 2023; Mattke et al., 2019; Rogerson & Parry, 2020). These cases substantiate our argument that physical verification is not ancillary but foundational, so ignoring its cost or failure precisely reproduces the assumptions of success and technological infallibility critiqued earlier.

However, we have shown that ignoring its importance in the context of blockchain risks inappropriately transferring certain aspects of blockchain (e.g., enhanced trust due to its immutability) from purely digital contexts to the physical supply chain, where physical verification of goods is a decisive theoretical factor. Although it is often taken for granted in supply chain theorising, it should be explicitly considered in the context of blockchain.

Furthermore, a critical implication when theorising about SCISs is that blockchain for tracking physical products fundamentally differs from blockchain for tracking digital products. The most crucial implication of this difference is that, without physical verification, the blockchain has no way to confirm that its records match any physical reality. Thus, the physical verification of data is a critical concept to include in any theoretical relationships involving trust in the context of BCSC.

The information logged on the blockchain and exchanged within the supply chain also relates to the physical flows, which require fast, dynamic physical verification of the data registered on the blockchain ledger. In most papers in our literature review, the notion of blockchain use was built on the simplistic assumption that any information logged onto the blockchain is accurate. As seen above, this assumption is true only if all members of the supply chain can be trusted to log accurate, truthful information about the physical state of the world. Since unscrupulous partners can behave opportunistically, verifying the corresponding data is mandatory if a supply chain is to prosper. Trust, whether in blockchain technology or in partners, can be built as verification occurs and grows in scope.

5.1.2 Trust in partners as distinct from trust in blockchain technology

Our second major theoretical contribution is demonstrating that trust cannot be treated generically.

Instead, trust in partners must be distinguished from trust in the blockchain system, since each has opposite theoretical effects on physical data verification and blockchain use. Batwa and Norrman (2021) similarly distinguished between “objects of trust”: trust in partners and trust in blockchain. However, they overlooked the crucial difference between the subjects of trust in each case. With trust in partners, the boundary spanners trust other boundary spanners in partner organisations, whereas, with trust in blockchain, general information system users trust the technology (e.g., operators).

This specific focus on different subjects of trust is fundamental to our propositions. The relationships between these two types of trust, physical data verification, and blockchain use are not identical, so they merit a clear distinction and careful consideration of their implications. Whereas the distinction between trust in technology and interpersonal trust is well established in the information systems literature (Lin &

Lin, 2019; Lippert & Forman, 2006; McKnight et al., 2011), it is not common to distinguish trust in partners (i.e., interorganisational trust) from trust in technology. Since trust is one of the main purported benefits of blockchain, it is essential to clarify its nature.

This distinction has crucial implications for researchers. First, because the effects of these kinds of trust on blockchain use are opposite, when trust is measured, researchers may find no effect despite strong effects, as such opposite effects may cancel each other out. Thus, we affirm the prior literature that has distinguished these two types of trust, which permits us to tease out the true effect of trust on blockchain use.

Indeed, both types of trust are similarly collective and organisational, not individual, in the supply chain context. Nevertheless, their evaluations and measurements differ somewhat in how trust across individuals is aggregated. Trust in partners is consensual, so the most influential members of the boundary group dominate any effects of the trusting relationship. By contrast, trust in technology is more egalitarian, an average collective trust of all SCIS users, since non-usage by less powerful organisational members may have significant effects on trust outcomes. Therefore, the actors and beneficiaries of trust must be accurately characterised in any scholarly discussion, while the concept of trust must be well-grounded to eliminate ambiguity and ensure coherence with the relevant literature.

5.1.3 Temporal sequencing of propositions

A third major contribution is our development of propositions about the relationships among data verification, the two types of trust in BCSC, and blockchain use. A critical aspect of our theorising lies in the attention paid to the temporal sequence of the concepts. We argue that the positive or negative nature of an effect may change depending on what comes first: trust, data verification, or blockchain use.

Specifically, physical data verification can increase trust in both partners and blockchain. However, when trust in partners or blockchain is present, the result may be less data verification. In addition, the use of blockchain can increase trust in partners. However, when trust is initially high, partners may be less likely

to use blockchain. Thus, the direction of the relationship becomes clear, depending on which is present first.

5.2 Managerial implications

This critical review, primarily addressed to academic researchers, also has important implications for managerial practice, as highlighted below.

5.2.1 Role of physical data verification

The fact that blockchain does not verify the correspondence between the digital record and the physical world has important practical implications. For example, in a logistics environment, information about customers, projects, shipments, deliveries, and handling units is logged and serves as crucial assurance that the blockchain records correspond to physical reality without blind trust (Helo & Shamsuzzoha, 2020). Since blockchain records are immutable, any blockchain system for supply chains must include a “correction” record type that allows users to correct a prior record later found to be inaccurate. “Immutability” must be strictly understood in terms of the technical features of blockchain (i.e., records cannot be deleted), not in a way that implies that inaccuracies recorded on the blockchain cannot be regularised. Unlike some other popular blockchain contexts used for purely digital products, blockchain does not obviate the crucial requirement for physical data verification. Hence, deploying blockchain without ensuring that proper fact checking is also included cannot increase trust in systems or partners (Y. Wu et al., 2021).

Indeed, managers must prioritise rigorous training and invest in robust verification technologies to trigger the benefits of BCSC. They must develop strict protocols to ensure exact correspondence between physical reality and blockchain records. Collaboration among stakeholders is also important to standardise verification processes and clearly define roles and responsibilities throughout the supply chain, thereby enhancing data quality from origin to end user. Supply chain managers must enhance physical inspection systems and integrate blockchain with tracking technologies to automate and ensure accurate data collection. Hence, developing trust protocols and conducting regular audits can reinforce stakeholder

confidence by ensuring physical verification processes are transparent. Additionally, ongoing training is crucial to ensure that all personnel understand their roles, thereby solidifying blockchain's role in enhancing the reliability and trustworthiness of SCISs.

5.2.2 Trust in partners as distinct from trust in blockchain technology

The distinction between trust in partners and trust in blockchain bears vital implications for practitioners.

First, the most significant difference between blockchain-enabled and regular SCISs is that the blockchain record is immutable, which can enhance trust in the system by preventing anyone from changing data once it is recorded (whether maliciously or in error). Nevertheless, immutability can give deliberate falsifications a false stamp of validity, thereby frustrating attempts to detect or resolve the fraud.

Second, in our theoretical model, users' trust in blockchain is distinct from boundary spanners' trust in partners, so supply chain managers may not trust their partners, while users may naively elevate trust in blockchain technology. Thus, when supply chain managers seek to increase data verification to mitigate their low trust in partners, SCIS users responsible for some of these checks may lower their guard due to naive trust in blockchain technology. Therefore, managers must distinguish between these two kinds of trust to align their strategic practices guided by interorganisational trust in partners with users' practices, prompted by their individual trust in the technology.

Third, because immutability is not absolute, managers must carefully consider whether the cost of investing in blockchain makes sense for their supply chains. Blockchain costs include hiring specialised operators or training existing ones in the necessary skills. If members largely trust each other, then blockchain may not add additional value to their supply chain. Blockchain is more beneficial for supply chains with low to moderate levels of trust, as it can help boost interorganisational and end-consumer trust (Danese et al., 2021). In this case, practitioners must consider complementing the blockchain with the means to verify that reality matches records, thereby providing the guarantees that the reported facts are indeed trustworthy (Helo & Hao, 2019).

Supply chain managers must follow a structured approach for balancing trust and verification to operationalise the distinction between the two types of trust. Physical verification must be prioritised when supply chain partners are new, geographically dispersed, or when prior performance and governance mechanisms provide limited assurance of data reliability. In contrast, when interorganisational trust is well established through proven collaboration, transparent metrics, and regulatory oversight, reliance on partner trust may suffice, with verification limited to exceptions or high-risk items. Governance of physical data verification must be explicitly assigned to an actor with both access to the physical goods and accountability for data integrity since blockchain serves as a tamper-proof repository rather than a verifier.

To align trust and data quality, managers must design governance mechanisms that link partner reputation and contractual benefits to verified data accuracy. For example, firms that consistently pass verification audits may gain preferential contract terms and reduced inspection frequency, while repeated discrepancies may trigger intensified oversight. Thus, managers can develop strategies that foster both types of trust, thereby ensuring robust physical data verification processes that align with blockchain use. Clarifying these distinctions can guide better implementation practices and address potential trust issues.

5.2.3 Temporal sequencing of propositions

Supply chain managers can consider the dynamic implications of the temporal precedence between trust, data verification, and blockchain use. For instance, starting with rigorous physical data verification can increase both trust in blockchain technology and trust in partners, which, in turn, can facilitate smoother blockchain adoption and integration. Conversely, if either type of trust is already established, there may be a tendency to rely less on data verification, which can potentially compromise the integrity of the blockchain's data. Furthermore, if blockchain is already in use, it can enhance trust in partners. However, trust in partners may reduce the perceived need for blockchain, as traditional trust mechanisms may seem sufficient. Therefore, managers must strategically navigate these nuances by implementing processes that either build trust where it is deficient or enhance data verification to improve existing trust.

5.3 Limitations and directions for future research

This critical review presents several propositions that extend the emerging literature on BCSC to explicitly consider the role of physical data verification and the differences between trust in partners and trust in blockchain technology. Nonetheless, the review has notable limitations. First, it specifically concerns the use of blockchain in the supply chains of physical goods. When the supply is digital goods or dematerialised services, the concern about physical data verification does not apply, as there are no physical goods to verify. In such a setting, our theoretical framework is, of course, irrelevant. Second, our propositions on the impact of trust on blockchain use mainly apply to a scenario before blockchain is implemented. When blockchain is already in use (e.g., when an SCIS user is newly employed to work with an existing blockchain-based system), individual trust in blockchain may have little bearing, as it would already be established within the organisation.

With these limitations in mind, the primary direction for future research is to empirically investigate the propositions outlined in the research agenda. Because BCSC is still relatively new, qualitative studies can help understand the proposed theoretical relationships in detail, especially considering the complexity of different temporal sequences. Quantitative cross-sectional snapshots can examine the direction of the proposed relationships. For example, one study can investigate how pre-existing trust affects the decision to implement blockchain, while another can examine how BCSC adoption affects subsequent trust in the supply chain. These studies can be followed up by eventual longitudinal studies that examine both directions over time.

Our review also suggests other directions for research less directly related to our propositions. Future research can consider the extra layers of technologies required for those benefits to appear in the supply chain. Blockchain networks require sensors and actuators (e.g., smart contracts, oracles, anti-tampering mechanisms, RFID scanners, motion detectors, temperature sensors, and light detectors) to directly interact with the real world (Babich & Hilary, 2020; Lao et al., 2020). These technologies also require various information system layers to ensure proper sharing and security issues (Khacef et al., 2023). Furthermore, governance and regulatory mechanisms are required to ensure that opportunistic behaviour,

indemnification, and other measures to ensure smooth operations and proper sharing of rent generated are in place. Such research must also consider the return on investment required by blockchain and other layers of technology. We suggest that the research field is wide open for major scientific contributions. We also think that information systems research can benefit from more in-depth explorations of the interactions between the aforementioned users and technologies. A high level of technical know-how is required to understand, establish, and employ such technologies and systems within a single firm or country, across the supply chain, and at varying levels of granularity for processes and acquired information. As Gregory et al. (2024) argued, the “algorithmic enforcement” of rules through blockchain-based smart contracts can facilitate cooperation among strangers and thus warrants more investigation into how such automated reciprocity can reshape traditional trust dynamics. Specifically, scalability, processing power, and information traffic models in the supply chain require further investigation. We suggest exploring the integration of emerging technologies in BCSC, such as the IoT (W. Long et al., 2021; Pelé et al., 2023b; Zhu et al., 2022), digital twins (Jones et al., 2020; Mandolla et al., 2019), and artificial intelligence (Charles et al., 2023; S. Kumar et al., 2022).

Whole new processes along supply chains must be developed if a modicum of trust in the information written on the distributed ledger is to be obtained. Algorithmic enforcement capabilities can reduce reliance on pre-existing trust by automatically executing reciprocal exchanges, which opens new possibilities for collaborating with previously unknown suppliers (Gregory et al., 2024). Operations within the supply chain can also benefit from research into the potential use of smart contract design and execution control as “cyber information services” to report on the proper execution of operations (Albizri & Appelbaum, 2021; Dolgui et al., 2020). Moreover, potential new services and business opportunities remain to be developed. Once the concepts of trust, information sharing, and blockchain use are clearly defined and the associated costs are considered, the question of how to improve supply chain performance can be addressed anew. Another insufficiently researched pertinent question concerns the financial costs and coordination effort associated with adding physical verification and blockchain deployment, and their impact on the overall performance of the supply chain and increased transaction costs (Roeck et al., 2020).

Further questions are closely related to our propositions. For instance, how can firms design blockchain implementations that effectively balance trust in partners with the need for physical data verification? What specific steps can industries with low blockchain adoption rates take to overcome barriers related to trust dynamics and verification processes? Moreover, sector-specific recommendations merit investigation. In highly regulated industries (e.g., healthcare and food), managers may face unique challenges, so future studies can examine additional considerations when implementing blockchain systems in these contexts.

5.4 Conclusion

The use of blockchain enhances trust in the technology and vice versa. As a “grand coalition” (Medlin, 1976) of partners, a supply chain exists to create value for the end customer, who trusts the quality of the final product, which increases the willingness to pay for it. This value is then distributed among the partners (Brusset et al., 2024). As blockchain use is a step toward further enhancing this value, trust in blockchain technology is irrelevant if some partners act opportunistically by falsely representing reality, thereby betraying interorganisational trust. By extension, if the research object is the use of blockchain in a physical context, then the relationship between trust in blockchain and blockchain use is tautological. The most critical relationship is between physical data verification and blockchain use. We hope these considerations can help researchers explore the role of blockchain more meaningfully in supply chains.

CRedit author statement (Only after the acceptance of the article)

Rami Alkhudary, Xavier Brusset, and Chitu Okoli: Conceptualization, Investigation, Methodology, Validation, Writing – original draft; Writing – review & editing. In addition, Xavier Brusset: Supervision; Chitu Okoli: Project Administration, Visualization.

Generative AI Disclosure

We used generative AI tools (especially ChatGPT) to help in our writing process. However, we did not use it for any part of the literature search, synthesis, or development of the propositions. We have

carefully reviewed and revised all AI-generated text and take full responsibility for the final version of the article.

References

- Abiteboul, S., Hull, R., & Vianu, V. (1995). *Foundations of databases*. Addison-Wesley.
- Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. *Computers & Industrial Engineering*, 154, 107130. <https://doi.org/10.1016/j.cie.2021.107130>
- Ahluwalia, S., Mahto, R. V., & Guerrero, M. (2020). Blockchain technology and startup financing: A transaction cost economics perspective. *Technological Forecasting and Social Change*, 151, 119854. <https://doi.org/10.1016/j.techfore.2019.119854>
- Ahmed, W., Islam, N., & Qureshi, H. N. (2023). Understanding the acceptability of block-chain technology in the supply chain; case of a developing country. *Journal of Science and Technology Policy Management*. <https://doi.org/10.1108/JSTPM-06-2022-0097>
- Akkermans, H. A., Bogerd, P., Yücesan, E., & van Wassenhove, L. N. (2003). The impact of ERP on supply chain management: Exploratory findings from a European Delphi study. *European Journal of Operational Research*, 146(2), 284–301. [https://doi.org/10.1016/S0377-2217\(02\)00550-7](https://doi.org/10.1016/S0377-2217(02)00550-7)
- Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2021). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, 24(1), 83–101. <https://doi.org/10.1007/s10586-020-03200-4>
- Albizri, A., & Appelbaum, D. (2021). Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts. *Journal of Information Systems*, 35(2), 1–16. <https://doi.org/10.2308/ISYS-19-024>
- Alkhudary, R., Brusset, X., & Fénies, P. (2020). Blockchain in general management and economics: A systematic literature review. *European Business Review*, 32(4), 765–783. <https://doi.org/10.1108/EBR-11-2019-0297>

- Allen, D. K., Colligan, D., Finnie, A., & Kern, T. (2000). Trust, power and interorganizational information systems: The case of the electronic trading community TransLease. *Information Systems Journal*, 10(1), 21–40. <https://doi.org/10.1046/j.1365-2575.2000.00078.x>
- Alles, M., & Gray, G. L. (2020). “The first mile problem”: Deriving an endogenous demand for auditing in blockchain-based business processes. *International Journal of Accounting Information Systems*, 38, 100465. <https://doi.org/10.1016/j.accinf.2020.100465>
- Al-Sumaidae, G., Alkhudary, R., Zilic, Z., & Swidan, A. (2023). Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. *Information Processing & Management*, 60(2), 103160. <https://doi.org/10.1016/j.ipm.2022.103160>
- Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. *Computers & Industrial Engineering*, 135, 582–592. <https://doi.org/10.1016/j.cie.2019.06.042>
- Babich, V., & Hilary, G. (2020). OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology. *Manufacturing & Service Operations Management*, 22(2), 223–240. <https://doi.org/10.1287/msom.2018.0752>
- Babich, V., & Tang, C. S. (2012). Managing Opportunistic Supplier Product Adulteration: Deferred Payments, Inspection, and Combined Mechanisms. *Manufacturing & Service Operations Management*, 14(2), 301–314. <https://doi.org/10.1287/msom.1110.0366>
- Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review*, 14(4), 496–515.
- Bader, L., Pennekamp, J., Matzutt, R., Hedderich, D., Kowalski, M., Lücken, V., & Wehrle, K. (2021). Blockchain-based privacy preservation for supply chains supporting lightweight multi-hop information accountability. *Information Processing & Management*, 58(3), 102529. <https://doi.org/10.1016/j.ipm.2021.102529>
- Baharmand, H., Maghsoudi, A., & Coppi, G. (2021). Exploring the application of blockchain to humanitarian supply chains: Insights from Humanitarian Supply Blockchain pilot project.

- International Journal of Operations & Production Management*, 41(9), 1522–1543.
<https://doi.org/10.1108/IJOPM-12-2020-0884>
- Bai, C., & Sarkis, J. (2020). A supply chain transparency and sustainability technology appraisal model for blockchain technology. *International Journal of Production Research*, 58(7), 2142–2162.
<https://doi.org/10.1080/00207543.2019.1708989>
- Batwa, A., & Norrman, A. (2021). Blockchain Technology and Trust in Supply Chain Management: A Literature Review and Research Agenda. *Operations and Supply Chain Management: An International Journal*, 203–220. <https://doi.org/10.31387/oscm0450297>
- Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19(10).
<https://aisel.aisnet.org/jais/vol19/iss10/1>
- Behl, A., Jayawardena, N. S., Pereira, V., & Sampat, B. (2024). Assessing retailer readiness to use blockchain technology to improve supply chain performance. *Journal of Enterprise Information Management*, 37(2), 673–697. <https://doi.org/10.1108/JEIM-07-2022-0242>
- Behnke, K., & Janssen, M. F. W. H. A. (2020). Boundary conditions for traceability in food supply chains using blockchain technology. *International Journal of Information Management*, 52, 101969.
<https://doi.org/10.1016/j.ijinfomgt.2019.05.025>
- Beth, S., Burt, D., Copacino, W., Gopal, C., Lee, H., Lynch, R., & Morris, S. (2003). Supply Chain Challenges: Building Relationships. *Harvard Business Review*, 81, 64–73, 117.
- Bhattacharjee, A., Davis, C. J., Connolly, A. J., & Hikmet, N. (2018). User response to mandatory IT use: A coping theory perspective. *European Journal of Information Systems*, 27(4), 395–414.
<https://doi.org/10.1057/s41303-017-0047-0>
- Bhawana, Kumar, S., Dohare, U., & Kaiwartya, O. (2023). FLAME: Trusted Fire Brigade Service and Insurance Claim System Using Blockchain for Enterprises. *IEEE Transactions on Industrial Informatics*, 19(6), 7517–7527. <https://doi.org/10.1109/TII.2022.3212172>

- Biswas, D., Jalali, H., Ansaripoor, A. H., & De Giovanni, P. (2022). Traceability vs. sustainability in supply chains: The implications of blockchain. *European Journal of Operational Research*, S0377221722004076. <https://doi.org/10.1016/j.ejor.2022.05.034>
- Brookbanks, M., & Parry, G. (2022). The impact of a blockchain platform on trust in established relationships: A case study of wine supply chains. *Supply Chain Management: An International Journal*, 27(7), 128–146. <https://doi.org/10.1108/SCM-05-2021-0227>
- Brun, A., & Moretto, A. (2014). Organisation and supply chain for quality control in luxury companies. *Journal of Fashion Marketing and Management*, 18(2), 206–230. <https://doi.org/10.1108/JFMM-11-2012-0070>
- Brusset, X. (2016). When manufacturers hold information back from strong suppliers. *RAIRO - Operations Research*, 50(3), 553–565. <https://doi.org/10.1051/ro/2015050>
- Brusset, X., Kinra, A., Naseraldin, H., & Alkhudary, R. (2024). Increasing willingness to pay in the food supply chain: A blockchain-oriented trust approach. *International Journal of Production Research*, 1–22. <https://doi.org/10.1080/00207543.2024.2352763>
- Cao, Y., Yi, C., Wan, G., Hu, H., Li, Q., & Wang, S. (2022). An analysis on the role of blockchain-based platforms in agricultural supply chains. *Transportation Research Part E: Logistics and Transportation Review*, 163, 102731. <https://doi.org/10.1016/j.tre.2022.102731>
- Castka, P., Searcy, C., & Mohr, J. (2020). Technology-enhanced auditing: Improving veracity and timeliness in social and environmental audits of supply chains. *Journal of Cleaner Production*, 258, 120773. <https://doi.org/10.1016/j.jclepro.2020.120773>
- Centobelli, P., Cerchione, R., Vecchio, P. D., Oropallo, E., & Secundo, G. (2021). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, 103508. <https://doi.org/10.1016/j.im.2021.103508>
- Chang, S. E., Chen, Y.-C., & Lu, M.-F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change*, 144, 1–11. <https://doi.org/10.1016/j.techfore.2019.03.015>

- Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, 58(7), 2082–2099. <https://doi.org/10.1080/00207543.2019.1651946>
- Charles, V., Emrouznejad, A., & Gherman, T. (2023). A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Annals of Operations Research*.
<https://doi.org/10.1007/s10479-023-05169-w>
- Chaudhuri, A., Bhatia, M. S., Kayikci, Y., Fernandes, K. J., & Fosso-Wamba, S. (2021). Improving social sustainability and reducing supply chain risks through blockchain implementation: Role of outcome and behavioural mechanisms. *Annals of Operations Research*.
<https://doi.org/10.1007/s10479-021-04307-6>
- Chen, F. (2003). Information Sharing and Supply Chain Coordination. In *Handbooks in Operations Research and Management Science* (Vol. 11, pp. 341–421). Elsevier.
[https://doi.org/10.1016/S0927-0507\(03\)11007-9](https://doi.org/10.1016/S0927-0507(03)11007-9)
- Chen, P.-K., He, Q.-R., & Chu, S. (2022). Influence of Blockchain and Smart Contracts on Partners' Trust, Visibility, Competitiveness, and Environmental Performance in Manufacturing Supply Chains. *Journal of Business Economics and Management*, 23(4), 754–772.
<https://doi.org/10.3846/jbem.2022.16431>
- Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Yu. (2022). Applications of Blockchain in Industry 4.0: A Review. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-022-10248-7>
- Chittipaka, V., Kumar, S., Sivarajah, U., Bowden, J. L.-H., & Baral, M. M. (2022). Blockchain Technology for Supply Chains operating in emerging markets: An empirical examination of technology-organization-environment (TOE) framework. *Annals of Operations Research*.
<https://doi.org/10.1007/s10479-022-04801-5>
- Choi, T.-M. (2019). Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains. *Transportation Research Part E: Logistics and Transportation Review*, 128, 17–29. <https://doi.org/10.1016/j.tre.2019.05.011>

- Choi, T.-M., Feng, L., & Li, R. (2020). Information disclosure structure in supply chains with rental service platforms in the blockchain technology era. *International Journal of Production Economics*, 221, 107473. <https://doi.org/10.1016/j.ijpe.2019.08.008>
- Choi, T.-M., Guo, S., & Luo, S. (2020). When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management? *Transportation Research Part E: Logistics and Transportation Review*, 135, 101860. <https://doi.org/10.1016/j.tre.2020.101860>
- Choi, T.-M., & Luo, S. (2019). Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. *Transportation Research Part E: Logistics and Transportation Review*, 131, 139–152. <https://doi.org/10.1016/j.tre.2019.09.019>
- Choi, T.-M., Wen, X., Sun, X., & Chung, S.-H. (2019). The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Transportation Research Part E: Logistics and Transportation Review*, 127, 178–191. <https://doi.org/10.1016/j.tre.2019.05.007>
- Chu, X., Wang, R., Lin, Y., & Li, Y. (2022). Building trust in online trade-in programs with a blockchain-enabled system. *Transportation Research Part E: Logistics and Transportation Review*, 164, 102833. <https://doi.org/10.1016/j.tre.2022.102833>
- Chu, X., Wang, R., Ren, L., Li, Y., & Zhang, S. (2024). Enabling joint distribution with blockchain technology in last-mile logistics. *Computers & Industrial Engineering*, 187, 109832. <https://doi.org/10.1016/j.cie.2023.109832>
- Çolak, H., & Kağrıoğlu, C. H. (2023). Predicting the Blockchain Technology Acceptance in Supply Chains with Inter-Firm Perspective: An Integrated DEMATEL and PLS-SEM Approach. *Journal of Business-to-Business Marketing*, 30(2), 125–148. <https://doi.org/10.1080/1051712X.2023.2214543>

- Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: Implications for operations and supply chain management. *Supply Chain Management: An International Journal*, 24(4), 469–483. <https://doi.org/10.1108/SCM-09-2018-0309>
- Cozzio, C., Viglia, G., Lemarie, L., & Cerutti, S. (2023). Toward an integration of blockchain technology in the food supply chain. *Journal of Business Research*, 162, 113909. <https://doi.org/10.1016/j.jbusres.2023.113909>
- Danese, P., Mocellin, R., & Romano, P. (2021). Designing blockchain systems to prevent counterfeiting in wine supply chains: A multiple-case study. *International Journal of Operations & Production Management*, 41(13), 1–33. <https://doi.org/10.1108/IJOPM-12-2019-0781>
- de Boissieu, E., Kondrateva, G., Baudier, P., & Ammi, C. (2021). The use of blockchain in the luxury industry: Supply chains and the traceability of goods. *Journal of Enterprise Information Management*, 34(5), 1318–1338. <https://doi.org/10.1108/JEIM-11-2020-0471>
- Di Vaio, A., & Varriale, L. (2020). Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *International Journal of Information Management*, 52, 102014. <https://doi.org/10.1016/j.ijinfomgt.2019.09.010>
- Dionysis, S., Chesney, T., & McAuley, D. (2022). Examining the influential factors of consumer purchase intentions for blockchain traceable coffee using the theory of planned behaviour. *British Food Journal*, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/BFJ-05-2021-0541>
- Dolgui, A., Ivanov, D., Potryasaev, S., Sokolov, B., Ivanova, M., & Werner, F. (2020). Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain. *International Journal of Production Research*, 58(7), 2184–2199. <https://doi.org/10.1080/00207543.2019.1627439>
- Du, M., Chen, Q., Xiao, J., Yang, H., & Ma, X. (2020). Supply Chain Finance Innovation Using Blockchain. *IEEE Transactions on Engineering Management*, 1–14. <https://doi.org/10.1109/TEM.2020.2971858>

- Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production Research*, 58(11), 3381–3398.
<https://doi.org/10.1080/00207543.2020.1722860>
- Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, 142, 102067. <https://doi.org/10.1016/j.tre.2020.102067>
- Economist. (2015, October 31). Blockchains—The great chain of being sure about things. *The Economist*.
<https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>
- Ehrenberg, A. J., & King, J. L. (2020). Blockchain in Context. *Information Systems Frontiers*, 22(1), 29–35. <https://doi.org/10.1007/s10796-019-09946-6>
- Elbashbishy, T. S., Ali, G. G., & El-adaway, I. H. (2022). Blockchain technology in the construction industry: Mapping current research trends using social network analysis and clustering. *Construction Management and Economics*, 40(5), 406–427.
<https://doi.org/10.1080/01446193.2022.2056216>
- Erol, I., Murat Ar, I., Peker, I., & Searcy, C. (2022). Alleviating the Impact of the Barriers to Circular Economy Adoption Through Blockchain: An Investigation Using an Integrated MCDM-based QFD With Hesitant Fuzzy Linguistic Term Sets. *Computers & Industrial Engineering*, 165, 107962. <https://doi.org/10.1016/j.cie.2022.107962>
- Farooq, U., Shahzad, K., Guan, Z., & Rauf, A. (2024). Unlocking the potential of blockchain technology in China's supply chain: A survey of industry professionals. *Journal of Entrepreneurship and Public Policy*, 13(2), 333–356. <https://doi.org/10.1108/JEPP-03-2023-0028>
- Fernandez-Vazquez, S., Rosillo, R., de la Fuente, D., & Puente, J. (2022). Blockchain in sustainable supply chain management: An application of the analytical hierarchical process (AHP) methodology. *Business Process Management Journal*. <https://doi.org/10.1108/BPMJ-11-2021-0750>

Fortune Business Insights. (2026). *Blockchain Distributed Ledger Market Size, Share | Growth 2034*.

Fortune Business Insights. <https://www.fortunebusinessinsights.com/blockchain-distributed-ledger-market-114784>

Fosso Wamba, S., & Guthrie, C. (2020). The impact of blockchain adoption on competitive performance: The mediating role of process and relational innovation. *Logistique & Management*, 28(1), 88–96. <https://doi.org/10.1080/12507970.2019.1679046>

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, 13(2), 159–190. <https://doi.org/10.1046/j.1365-2575.2003.00146.x>

Gefen, D., Wyss, S., & Lichtenstein, Y. (2008). Business Familiarity as Risk Mitigation in Software Development Outsourcing Contracts. *MIS Quarterly*, 32(3), 531–551.

Ghode, D. J., Yadav, V., Jain, R., & Soni, G. (2023). Exploring the integration of blockchain technology into supply chain: Challenges and performance. *Business Process Management Journal*, 29(1), 223–239. <https://doi.org/10.1108/BPMJ-09-2022-0421>

Ghode, D., Yadav, V., Jain, R., & Soni, G. (2020). Adoption of blockchain in supply chain: An analysis of influencing factors. *Journal of Enterprise Information Management*, 33(3), 437–456. <https://doi.org/10.1108/JEIM-07-2019-0186>

Ghosh, A., & Fedorowicz, J. (2008). The role of trust in supply chain governance. *Business Process Management Journal*, 14(4), 453–470. <https://doi.org/10.1108/14637150810888019>

Glaser, F. (2017, January 4). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS-50)*. Hawaii International Conference on System Sciences. <https://doi.org/10.24251/HICSS.2017.186>

González-Mendes, S., Alonso-Muñoz, S., García-Muiña, F. E., & González-Sánchez, R. (2024). Discovering the conceptual building blocks of blockchain technology applications in the agri-food

supply chain: A review and research agenda. *British Food Journal*, 126(13), 182–206.

<https://doi.org/10.1108/BFJ-06-2023-0517>

Goo, J., Kishore, R., Rao, H., & Nam, K. (2009). The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study. *MIS Quarterly*, 33(1), 119–145.

Gregory, R. W., Beck, R., Henfridsson, O., & Yaraghi, N. (2024). Cooperation Among Strangers: Algorithmic Enforcement of Reciprocal Exchange with Blockchain-Based Smart Contracts. *Academy of Management Review*, *Forthcoming*, amr.2023.0023.
<https://doi.org/10.5465/amr.2023.0023>

Gulati, R., & Nickerson, J. A. (2008). Interorganizational Trust, Governance Choice, and Exchange Performance. *Organization Science*, 19(5), 688–708. <https://doi.org/10.1287/orsc.1070.0345>

Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: A literature review. *International Journal of Physical Distribution & Logistics Management*, 49(9), 881–900. <https://doi.org/10.1108/IJPDLM-11-2018-0371>

Hald, K. S., & Kinra, A. (2019). How the blockchain enables and constrains supply chain performance. *International Journal of Physical Distribution & Logistics Management*, 49(4), 376–397.
<https://doi.org/10.1108/IJPDLM-02-2019-0063>

Hastig, G. M., & Sodhi, M. S. (2020). Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors. *Production and Operations Management*, 29(4), 935–954.
<https://doi.org/10.1111/poms.13147>

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, 100935.

<https://doi.org/10.1016/j.elerap.2020.100935>

Helo, P., & Hao, Y. (2019). Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering*, 136, 242–251.

<https://doi.org/10.1016/j.cie.2019.07.023>

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

<https://doi.org/10.1016/j.rcim.2019.101909>

Hoehle, H., Huff, S., & Goode, S. (2012). The Role of Continuous Trust in Information Systems Continuance. *Journal of Computer Information Systems*, 52(4), 1–9.

<https://doi.org/10.1080/08874417.2012.11645571>

Howson, P. (2020). Building trust and equity in marine conservation and fisheries supply chain management with blockchain. *Marine Policy*, 115, 103873.

<https://doi.org/10.1016/j.marpol.2020.103873>

Hu, H., Xu, J., Liu, M., & Lim, M. K. (2023). Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning. *Journal of Business Research*, 156, 113480.

<https://doi.org/10.1016/j.jbusres.2022.113480>

Hu, S., Huang, S., Huang, J., & Su, J. (2021). Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis. *Computers & Industrial Engineering*, 153, 107079.

<https://doi.org/10.1016/j.cie.2020.107079>

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, 62(3), 273–281.

<https://doi.org/10.1016/j.bushor.2019.01.002>

Ibrahim, M., & Ribbers, P. M. (2009). The impacts of competence-trust and openness-trust on interorganizational systems. *European Journal of Information Systems*, 18(3), 223–234.

<https://doi.org/10.1057/ejis.2009.17>

- Jain, G., Singh, H., Chaturvedi, K. R., & Rakesh, S. (2020). Blockchain in logistics industry: In fizz customer trust or not. *Journal of Enterprise Information Management*, 33(3), 541–558.
<https://doi.org/10.1108/JEIM-06-2018-0142>
- Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics*, 8(5), 505.
<https://doi.org/10.3390/electronics8050505>
- Jeanneret Medina, M., Baudet, C., & Lebraty, J.-F. (2024). Blockchain and agency theory in supply chain management: A question of trust. *International Journal of Information Management*, 102747.
<https://doi.org/10.1016/j.ijinfomgt.2023.102747>
- Jiang, R., Kang, Y., Liu, Y., Liang, Z., Duan, Y., Sun, Y., & Liu, J. (2022). A trust transitivity model of small and medium-sized manufacturing enterprises under blockchain-based supply chain finance. *International Journal of Production Economics*, 247, 108469.
<https://doi.org/10.1016/j.ijpe.2022.108469>
- Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52.
<https://doi.org/10.1016/j.cirpj.2020.02.002>
- Kafi, F. & Kafi, Majid. (2016). Information quality in supply chain software. In *Handbook of Research in Global Supply Chain Management* (1st edn, pp. 105–125). IGI Global.
- Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research*, 57(7), 2009–2033.
<https://doi.org/10.1080/00207543.2018.1518610>
- Karakas, S., Acar, A. Z., & Kucukaltan, B. (2022). Blockchain adoption in logistics and supply chain: A literature review and research agenda. *International Journal of Production Research*, *Forthcoming*, 1–24. <https://doi.org/10.1080/00207543.2021.2012613>

- Karamchandani, A., Srivastava, S. K., & Srivastava, R. K. (2020). Perception-based model for analyzing the impact of enterprise blockchain adoption on SCM in the Indian service industry. *International Journal of Information Management*, 52, 102019. <https://doi.org/10.1016/j.ijinfomgt.2019.10.004>
- Kayikci, Y., Subramanian, N., Dora, M., & Bhatia, M. S. (2020). Food supply chain in the era of Industry 4.0: Blockchain technology implementation opportunities and impediments from the perspective of people, process, performance, and technology. *Production Planning & Control*, 1–21. <https://doi.org/10.1080/09537287.2020.1810757>
- Khacef, K., Benbernou, S., Ouziri, M., & Younas, M. (2023). A Dynamic Sharding Model Aware Security and Scalability in Blockchain. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-023-10380-y>
- Kim, J.-S., & Shin, N. (2019). The Impact of Blockchain Technology Application on Supply Chain Partnership and Performance. *Sustainability*, 11(21), 6181. <https://doi.org/10.3390/su11216181>
- Kim, M., Hilton, B., Burks, Z., & Reyes, J. (2018). Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 335–340. <https://doi.org/10.1109/IEMCON.2018.8615007>
- Kittilaksanawong, W. (2016). Value Creation and Appropriation in Buyer-Supplier Relationship: Governance, Competition and Culture. In B. Christiansen (Ed.), *Handbook of Research on Global Supply Chain Management*: (pp. 126–136). IGI Global. <https://doi.org/10.4018/978-1-4666-9639-6>
- Kittipanya-ngam, P., & Tan, K. H. (2020). A framework for food supply chain digitalization: Lessons from Thailand. *Production Planning & Control*, 31(2–3), 158–172. <https://doi.org/10.1080/09537287.2019.1631462>
- Klein, R., & Rai, A. (2009). Interfirm Strategic Information Flows in Logistics Supply Chain Relationships. *MIS Quarterly*, 33(4), 735–762. <https://doi.org/10.2307/20650325>

- Koh, L., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – paradigms and transitions. *International Journal of Production Research*, 58(7), 2054–2062.
<https://doi.org/10.1080/00207543.2020.1736428>
- Kopyto, M., Lechler, S., von der Gracht, H. A., & Hartmann, E. (2020). Potentials of blockchain technology in supply chain management: Long-term judgments of an international expert panel. *Technological Forecasting and Social Change*, 161, 120330.
<https://doi.org/10.1016/j.techfore.2020.120330>
- Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: Review, synthesis, and future research directions. *European Journal of Information Systems*, 31(3), 388–409.
<https://doi.org/10.1080/0960085X.2021.1927212>
- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
- Kshetri, N. (2022). Blockchain systems and ethical sourcing in the mineral and metal industry: A multiple case study. *The International Journal of Logistics Management*, 33(1), 1–27.
<https://doi.org/10.1108/IJLM-02-2021-0108>
- Kumar, A., Liu, R., & Shan, Z. (2020). Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities. *Decision Sciences*, 51(1), 8–37.
<https://doi.org/10.1111/deci.12396>
- Kumar, N., Upreti, K., & Mohan, D. (2022). Blockchain Adoption for Provenance and Traceability in the Retail Food Supply Chain: A Consumer Perspective. *International Journal of E-Business Research (IJEER)*, 18(2), 1–17. <https://doi.org/10.4018/IJEER.294110>
- Kumar, S., Lim, W. M., Sivarajah, U., & Kaur, J. (2022). Artificial Intelligence and Blockchain Integration in Business: Trends from a Bibliometric-Content Analysis. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-022-10279-0>

- Kwon, I.-W. G., & Suh, T. (2004). Factors Affecting the Level of Trust and Commitment in Supply Chain Relationships. *The Journal of Supply Chain Management*, 40(2), 4–14.
<https://doi.org/10.1111/j.1745-493X.2004.tb00165.x>
- Lankton, N., McKnight, D., & Tripp, J. (2015). Technology, Humanness, and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems*, 16(10).
<https://doi.org/10.17705/1jais.00411>
- Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling. *ACM Computing Surveys*, 53(1), 1–32. <https://doi.org/10.1145/3372136>
- Li, G., Fan, Z.-P., & Wu, X.-Y. (2021). The Choice Strategy of Authentication Technology for Luxury E-Commerce Platforms in the Blockchain Era. *IEEE Transactions on Engineering Management*, 1–14. <https://doi.org/10.1109/TEM.2021.3076606>
- Li, G., Xue, J., Li, N., & Ivanov, D. (2022). Blockchain-supported business model design, supply chain resilience, and firm performance. *Transportation Research Part E: Logistics and Transportation Review*, 163, 102773. <https://doi.org/10.1016/j.tre.2022.102773>
- Li, J., Maiti, A., Springer, M., & Gray, T. (2020). Blockchain for supply chain quality management: Challenges and opportunities in context of open manufacturing and industrial internet of things. *International Journal of Computer Integrated Manufacturing*, 33(12), 1321–1355.
<https://doi.org/10.1080/0951192X.2020.1815853>
- Li, K., Lee, J.-Y., & Gharehgozli, A. (2021). Blockchain in food supply chains: A literature review and synthesis analysis of platforms, benefits and challenges. *International Journal of Production Research*, 1–20. <https://doi.org/10.1080/00207543.2021.1970849>
- Li, S., & Lin, B. (2006). Accessing information sharing and information quality in supply chain management. *Decision Support Systems*, 42(3), 1641–1656.
<https://doi.org/10.1016/j.dss.2006.02.011>

- Lin, C., & Lin, M. (2019). The determinants of using cloud supply chain adoption. *Industrial Management & Data Systems*, 119(2), 351–366. <https://doi.org/10.1108/IMDS-12-2017-0589>
- Lippert, S. K., & Forman, H. (2006). A supply chain study of technology trust and antecedents to technology internalization consequences. *International Journal of Physical Distribution & Logistics Management*, 36(4), 271–288. <https://doi.org/10.1108/09600030610672046>
- Long, W., Wu, C. H., Tsang, Y. P., & Chen, Q. (2021). An End-to-End Bidirectional Authentication System for Pallet Pooling Management Through Blockchain Internet of Things (BIoT). *Journal of Organizational and End User Computing*. <https://www.igi-global.com/article/an-end-to-end-bidirectional-authentication-system-for-pallet-pooling-management-through-blockchain-internet-of-things-biot/290349>
- Long, Y., Feng, T., Fan, Y., & Liu, L. (2023). Adopting blockchain technology to enhance green supply chain integration: The moderating role of organizational culture. *Business Strategy and the Environment*, 32(6), 3326–3343. <https://doi.org/10.1002/bse.3302>
- Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering*, 136, 57–69. <https://doi.org/10.1016/j.cie.2019.07.026>
- Lu, Q., & Xu, X. (2017). Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Software*, 34(6), 21–27. <https://doi.org/10.1109/MS.2017.4121227>
- Lu, W., Jiang, Y., Chen, Z., & Ji, X. (2022). Blockchain adoption in a supply chain system to combat counterfeiting. *Computers & Industrial Engineering*, 171, 108408. <https://doi.org/10.1016/j.cie.2022.108408>
- Luna, M., Fernandez-Vazquez, S., Tereñes Castelao, E., & Arias Fernández, Á. (2024). A blockchain-based approach to the challenges of EU's environmental policy compliance in aquaculture: From traceability to fraud prevention. *Marine Policy*, 159, 105892. <https://doi.org/10.1016/j.marpol.2023.105892>

- Lyons, B., & Mehta, J. (1997). Contracts, opportunism and trust: Self-interest and social orientation. *Cambridge Journal of Economics*, 21(2), 239–257.
<https://doi.org/10.1093/oxfordjournals.cje.a013668>
- Madaan, J., Dwivedi, A., Patil, A., & Shardeo, V. (2023). Modelling of Critical Success Factors for Blockchain Technology Adoption Readiness in the Context of Agri-Food Supply Chain. *International Journal of Industrial and Systems Engineering*, 1(1), 1.
<https://doi.org/10.1504/IJISE.2021.10037223>
- Mandolla, C., Petruzzelli, A. M., Percoco, G., & Urbinati, A. (2019). Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. *Computers in Industry*, 109, 134–152. <https://doi.org/10.1016/j.compind.2019.04.011>
- Manzoor, R., Sahay, B. S., & Singh, S. K. (2024). Examining the Factors That Facilitate or Hinder the Use of Blockchain Technology to Enhance the Resilience of Supply Chains. *IEEE Transactions on Engineering Management*, 71, 10626–10649. <https://doi.org/10.1109/TEM.2024.3358722>
- Markus, S., & Buijs, P. (2022). Beyond the hype: How blockchain affects supply chain performance. *Supply Chain Management: An International Journal*, 27(7), 177–193.
<https://doi.org/10.1108/SCM-03-2022-0109>
- Martinez, V., Zhao, M., Blujdea, C., Han, X., Neely, A., & Albores, P. (2019). Blockchain-driven customer order management. *International Journal of Operations & Production Management*, 39(6/7/8), 993–1022. <https://doi.org/10.1108/IJOPM-01-2019-0100>
- Matke, J., Maier, C., Hund, A., & Weitzel, T. (2019). How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives. *MIS Quarterly Executive*, 18(4), 245–261.
<https://doi.org/10.17705/2msqe.00019>
- Matke, J., Maier, C., Reis, L., & Weitzel, T. (2021). Bitcoin investment: A mixed methods study of investment motivations. *European Journal of Information Systems*, 30(3), 261–285.
<https://doi.org/10.1080/0960085X.2020.1787109>

- 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>
- MediLedger. (2021). *MediLedger—Blockchain solutions for Pharma companies*.
<http://www.mediledger.com>
- Medlin, S. M. (1976). Effects of grand coalition payoffs on coalition formation in three-person games. *Behavioral Science*, 21(1), 48–61. <https://doi.org/10.1002/bs.3830210107>
- Mikalef, P., Krogstie, J., Pappas, I. O., & Pavlou, P. (2020). Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities. *Information & Management*, 57(2), 103169. <https://doi.org/10.1016/j.im.2019.05.004>
- Mishra, D. P., Kukreja, R. K., & Mishra, A. S. (2021). Blockchain as a governance mechanism for tackling dark side effects in interorganizational relationships. *International Journal of Organizational Analysis*, 30(2), 340–364. <https://doi.org/10.1108/IJOA-08-2020-2362>
- Murimi, R., Bell, G., Rasheed, A. A., & Beldona, S. (2023). Blockchains: A review and research agenda for international business. *Research in International Business and Finance*, 66, 102018.
<https://doi.org/10.1016/j.ribaf.2023.102018>
- Najar, T., Ennajah, L., Aloui, A., & Wamba, S. F. (2024). Understanding the acceptance of Blockchain use in the supply chain through the Lens of the technology-organization-environment (TOE) framework. *Systèmes d'Information et Management (French Journal of Management Information Systems)*, 29(3), 7–50.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org.
<https://bitcoin.org/bitcoin.pdf>
- Narayanan, V., & Raman, A. (2004). Aligning Incentives in Supply Chains. *Harvard Business Review*, 82, 94–102, 149.
- Nath, S. D., Khayer, A., Majumder, J., & Barua, S. (2022). Factors affecting blockchain adoption in apparel supply chains: Does sustainability-oriented supplier development play a moderating role?

- Industrial Management & Data Systems*, 122(5), 1183–1214. <https://doi.org/10.1108/IMDS-07-2021-0466>
- Nayak, G., & Dhaigude, A. S. (2019). A conceptual model of sustainable supply chain management in small and medium enterprises using blockchain technology. *Cogent Economics & Finance*, 7(1). <https://doi.org/10.1080/23322039.2019.1667184>
- Niu, B., Mu, Z., Cao, B., & Gao, J. (2021). Should multinational firms implement blockchain to provide quality verification? *Transportation Research Part E: Logistics and Transportation Review*, 145, 102121. <https://doi.org/10.1016/j.tre.2020.102121>
- Nodehi, T., Zutshi, A., Grilo, A., & Rizvanovic, B. (2022). EBDF: The enterprise blockchain design framework and its application to an e-Procurement ecosystem. *Computers & Industrial Engineering*, 171, 108360. <https://doi.org/10.1016/j.cie.2022.108360>
- Notheisen, B., Cholewa, J. B., & Shanmugam, A. P. (2017). Trading Real-World Assets on Blockchain: An Application of Trust-Free Transaction Systems in the Market for Lemons. *Business & Information Systems Engineering*, 59(6), 425–440. <https://doi.org/10.1007/s12599-017-0499-8>
- Okoli, C. (2022). *Developing Theory from Literature Reviews with Theoretical Concept Synthesis: Topical, Propositional and Confirmatory Approaches* (SSRN Scholarly Paper ID 3452134). Social Science Research Network. <https://doi.org/10.2139/ssrn>.
- Ozdemir, A. I., Erol, I., Ar, I. M., Peker, I., Asgary, A., Medeni, T. D., & Medeni, I. T. (2021). The role of blockchain in reducing the impact of barriers to humanitarian supply chain management. *The International Journal of Logistics Management*, 32(2), 454–478. <https://doi.org/10.1108/IJLM-01-2020-0058>
- Öztürk, C., & Yıldızbaşı, A. (2020). Barriers to implementation of blockchain into supply chain management using an integrated multi-criteria decision-making method: A numerical example. *Soft Computing*. <https://doi.org/10.1007/s00500-020-04831-w>

- Palas, Md. J. U., & Bunduchi, R. (2020). Exploring interpretations of blockchain's value in healthcare: A multi-stakeholder approach. *Information Technology & People*, 34(2), 453–495.
<https://doi.org/10.1108/ITP-01-2019-0008>
- Pan, X., Pan, X., Song, M., Ai, B., & Ming, Y. (2020). Blockchain technology and enterprise operational capabilities: An empirical test. *International Journal of Information Management*, 52, 101946.
<https://doi.org/10.1016/j.ijinfomgt.2019.05.002>
- Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management*, 52(2), 183–199.
<https://doi.org/10.1016/j.im.2014.08.008>
- Pattanayak, S., Ramkumar, M., Goswami, M., & Rana, N. P. (2024). Blockchain technology and supply chain performance: The role of trust and relational capabilities. *International Journal of Production Economics*, 271, 109198. <https://doi.org/10.1016/j.ijpe.2024.109198>
- Pelé, P., Schulze, J., Piramuthu, S., & Zhou, W. (2023a). IoT and Blockchain Based Framework for Logistics in Food Supply Chains. *Information Systems Frontiers*, 25(5), 1743–1756.
<https://doi.org/10.1007/s10796-022-10343-9>
- Pelé, P., Schulze, J., Piramuthu, S., & Zhou, W. (2023b). IoT and Blockchain Based Framework for Logistics in Food Supply Chains. *Information Systems Frontiers*, 25(5), 1743–1756.
<https://doi.org/10.1007/s10796-022-10343-9>
- Philipp, R., Prause, G., & Gerlitz, L. (2019). Blockchain and Smart Contracts for Entrepreneurial Collaboration in Maritime Supply Chains. *Transport and Telecommunication Journal*, 20(4), 365–378. <https://doi.org/10.2478/ttj-2019-0030>
- Pournader, M., Shi, Y., Seuring, S., & Koh, S. C. L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research*, 58(7), 2063–2081. <https://doi.org/10.1080/00207543.2019.1650976>
- Powell, W., Cao, S., Foth, M., He, S., Turner-Morris, C., & Li, M. (2023). Revisiting Trust in Supply Chains: How Does Blockchain Redefine Trust? In A. Bouras, I. Khalil, & B. Aouni (Eds),

- Blockchain Driven Supply Chains and Enterprise Information Systems* (pp. 21–42). Springer International Publishing. https://doi.org/10.1007/978-3-030-96154-1_2
- Qian, X. (Alice), & Papadonikolaki, E. (2020). Shifting trust in construction supply chains through blockchain technology. *Engineering, Construction and Architectural Management*, 28(2), 584–602. <https://doi.org/10.1108/ECAM-12-2019-0676>
- Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, 46, 70–82. <https://doi.org/10.1016/j.ijinfomgt.2018.11.021>
- Queiroz, M. M., Fosso Wamba, S., De Bourmont, M., & Telles, R. (2020). Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. *International Journal of Production Research*, 1–17. <https://doi.org/10.1080/00207543.2020.1803511>
- Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Management: An International Journal*, 25(2), 241–254. <https://doi.org/10.1108/SCM-03-2018-0143>
- Rahmanzadeh, S., Pishvaei, M. S., & Rasouli, M. R. (2020). Integrated innovative product design and supply chain tactical planning within a blockchain platform. *International Journal of Production Research*, 58(7), 2242–2262. <https://doi.org/10.1080/00207543.2019.1651947>
- Rashid, A., Baber Ali, S., Rasheed, R., Amirah, N. A., & Ngah, A. H. (2023). A paradigm of blockchain and supply chain performance: A mediated model using structural equation modeling. *Kybernetes*, 52(12), 6163–6178. <https://doi.org/10.1108/K-04-2022-0543>
- Reddick, C. G., Cid, G. P., & Ganapati, S. (2019). Determinants of blockchain adoption in the public sector: An empirical examination. *Information Polity*, 24(4), 379–396. <https://doi.org/10.3233/IP-190150>

- Rejeb, A., Keogh, J. G., Simske, S. J., Stafford, T., & Treiblmaier, H. (2021). Potentials of blockchain technologies for supply chain collaboration: A conceptual framework. *The International Journal of Logistics Management*, 32(3), 973–994. <https://doi.org/10.1108/IJLM-02-2020-0098>
- Rijanto, A. (2021). Blockchain Technology Adoption in Supply Chain Finance. *Journal of Theoretical and Applied Electronic Commerce Research*, 16(7), 3078–3098. <https://doi.org/10.3390/jtaer16070168>
- Rimba, P., Tran, A. B., Weber, I., Staples, M., Ponomarev, A., & Xu, X. (2020). Quantifying the Cost of Distrust: Comparing Blockchain and Cloud Services for Business Process Execution. *Information Systems Frontiers*, 22(2), 489–507. <https://doi.org/10.1007/s10796-018-9876-1>
- Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework—What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering*, 59(6), 385–409.
- Robson, M. J., Katsikeas, C. S., & Bello, D. C. (2008). Drivers and Performance Outcomes of Trust in International Strategic Alliances: The Role of Organizational Complexity. *Organization Science*, 19(4), 647–665. <https://doi.org/10.1287/orsc.1070.0329>
- Roeck, D., Sternberg, H., & Hofmann, E. (2020). Distributed ledger technology in supply chains: A transaction cost perspective. *International Journal of Production Research*, 58(7), 2124–2141. <https://doi.org/10.1080/00207543.2019.1657247>
- Rogerson, M., & Parry, G. C. (2020). Blockchain: Case studies in food supply chain visibility. *Supply Chain Management: An International Journal*, 25(5), 601–614. <https://doi.org/10.1108/SCM-08-2019-0300>
- Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135. <https://doi.org/10.1080/00207543.2018.1533261>

- Sahoo, S., Mukherjee, A., & Halder, R. (2021). A unified blockchain-based platform for global e-waste management. *International Journal of Web Information Systems, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/IJWIS-03-2021-0024>
- Sander, F., Semeijn, J., & Mahr, D. (2018). The acceptance of blockchain technology in meat traceability and transparency. *British Food Journal, 120*(9), 2066–2079. <https://doi.org/10.1108/BFJ-07-2017-0365>
- Saurabh, S., & Dey, K. (2021). Blockchain technology adoption, architecture, and sustainable agri-food supply chains. *Journal of Cleaner Production, 284*, 124731. <https://doi.org/10.1016/j.jclepro.2020.124731>
- Schilke, O., & Lumineau, F. (2023). How Organizational is Interorganizational Trust? *Academy of Management Review, Forthcoming*, amr.2022.0040. <https://doi.org/10.5465/amr.2022.0040>
- Schmidt, C. G., & Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management, 25*(4), 100552. <https://doi.org/10.1016/j.pursup.2019.100552>
- Schultz, F. C., Valentinov, V., & Pies, I. (2024). Looking behind the Continuum: An Institutional Economics Perspective on Schilke and Lumineau’s “How Organizational Is Interorganizational Trust?” *Academy of Management Review*, amr.2024.0101. <https://doi.org/10.5465/amr.2024.0101>
- Sharma, A., Bhatia, T., Singh, R. K., & Sharma, A. (2023). Developing the framework of blockchain-enabled agri-food supply chain. *Business Process Management Journal*. <https://doi.org/10.1108/BPMJ-01-2023-0035>
- Sharma, A., Sharma, A., Singh, R. K., & Bhatia, T. (2023). Blockchain adoption in agri-food supply chain management: An empirical study of the main drivers using extended UTAUT. *Business Process Management Journal, 29*(3), 737–756. <https://doi.org/10.1108/BPMJ-10-2022-0543>
- Sheel, A., & Nath, V. (2019). Effect of blockchain technology adoption on supply chain adaptability, agility, alignment and performance. *Management Research Review, 42*(12), 1353–1374. <https://doi.org/10.1108/MRR-12-2018-0490>

- Song, H., Liu, W., Yu, K., & Han, M. (2024). Trusting the trust machine: How does blockchain-enabled governance configuration enhance financing credibility? *Technovation*, 135, 103061. <https://doi.org/10.1016/j.technovation.2024.103061>
- Song, Y., Liu, J., Zhang, W., & Li, J. (2022). Blockchain's role in e-commerce sellers' decision-making on information disclosure under competition. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-021-04276-w>
- Stanley, T. D. (2005). Beyond Publication Bias: Beyond Publication Bias. *Journal of Economic Surveys*, 19(3), 309–345. <https://doi.org/10.1111/j.0950-0804.2005.00250.x>
- Steininger, D., Mikalef, P., Pateli, A., & Guinea, A. (2022). Dynamic Capabilities in Information Systems Research: A Critical Review, Synthesis of Current Knowledge, and Recommendations for Future Research. *Journal of the Association for Information Systems*, 23(2), 447–490.
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly, 2015. https://books.google.fr/books/about/Blockchain.html?id=ygzcrQEACAAJ&redir_esc=y
- Tan, A. W. K., Zhao, Y., & Halliday, T. (2018). A Blockchain Model for Less Container Load Operations in China. *International Journal of Information Systems and Supply Chain Management*, 11(2), 39–53. <https://doi.org/10.4018/IJISSCM.2018040103>
- Tarokh, M. J., & Soroor, J. (2006). Supply Chain Management Information Systems Critical Failure Factors. *2006 IEEE International Conference on Service Operations and Logistics, and Informatics*, 425–431. <https://doi.org/10.1109/SOLI.2006.329041>
- Tezel, A., Febrero, P., Papadonikolaki, E., & Yitmen, I. (2021). Insights into Blockchain Implementation in Construction: Models for Supply Chain Management. *Journal of Management in Engineering*, 37(4), (ASCE)ME.1943-5479.0000939, 04021038. [https://doi.org/10.1061/\(ASCE\)ME.1943-5479.0000939](https://doi.org/10.1061/(ASCE)ME.1943-5479.0000939)
- Tokkozhina, U., Martins, A. L., & Ferreira, J. C. (2023). Multi-tier supply chain behavior with blockchain technology: Evidence from a frozen fish supply chain. *Operations Management Research*, 16(3), 1562–1576. <https://doi.org/10.1007/s12063-023-00377-w>

- Tönnissen, S., & Teuteberg, F. (2020). Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. *International Journal of Information Management*, 52, 101953. <https://doi.org/10.1016/j.ijinfomgt.2019.05.009>
- Trautmann, L., Hübner, T., & Lasch, R. (2024). Blockchain concept to combat drug counterfeiting by increasing supply chain visibility. *International Journal of Logistics Research and Applications*, 27(6), 959–985. <https://doi.org/10.1080/13675567.2022.2141214>
- Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, 23(6), 545–559. <https://doi.org/10.1108/SCM-01-2018-0029>
- Tsang, E. W. K., & Ellsaesser, F. (2011). How Contrastive Explanation Facilitates Theory Building. *Academy of Management Review*, 36(2), 404–419.
- van Hoek, R. (2019). Exploring blockchain implementation in the supply chain: Learning from pioneers and RFID research. *International Journal of Operations & Production Management*, 39(6/7/8), 829–859. <https://doi.org/10.1108/IJOPM-01-2019-0022>
- van Veen-Dirks, P. M. G., & Verdaasdonk, P. J. A. (2009). The dynamic relation between management control and governance structure in a supply chain context. *Supply Chain Management: An International Journal*, 14(6), 466–478. <https://doi.org/10.1108/13598540910995237>
- Vasanthraj, V., Potdar, V., Agrawal, H., & Kaur, A. (2024). Transforming milk supply chains with blockchain: Enhancing visibility and cost reduction. *Benchmarking: An International Journal*. <https://doi.org/10.1108/BIJ-10-2023-0702>
- Vern, P., Panghal, A., Mor, R. S., & Kamble, S. S. (2024). Blockchain technology in the agri-food supply chain: A systematic literature review of opportunities and challenges. *Management Review Quarterly*. <https://doi.org/10.1007/s11301-023-00390-0>
- Vern, P., Panghal, A., Mor, R. S., Kumar, V., & Sarwar, D. (2024). Unlocking the potential: Leveraging blockchain technology for agri-food supply chain performance and sustainability. *The International Journal of Logistics Management*. <https://doi.org/10.1108/IJLM-09-2023-0364>

- Wan, P. K., Huang, L., & Holtskog, H. (2020). Blockchain-Enabled Information Sharing Within a Supply Chain: A Systematic Literature Review. *IEEE Access*, 8, 49645–49656.
<https://doi.org/10.1109/ACCESS.2020.2980142>
- Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1), 62–84. <https://doi.org/10.1108/SCM-03-2018-0148>
- Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? *International Journal of Production Economics*, 211, 221–236.
<https://doi.org/10.1016/j.ijpe.2019.02.002>
- Wang, Z., Ye, F., & Tan, K. H. (2014). Effects of managerial ties and trust on supply chain information sharing and supplier opportunism. *International Journal of Production Research*, 52(23), 7046–7061. <https://doi.org/10.1080/00207543.2014.932931>
- Wasim Ahmad, R., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2021). Blockchain for aerospace and defense: Opportunities and open research challenges. *Computers & Industrial Engineering*, 151, 106982. <https://doi.org/10.1016/j.cie.2020.106982>
- Westerlund, M., Nene, S., Leminen, S., & Rajahonka, M. (2021). An Exploration of Blockchain-based Traceability in Food Supply Chains: On the Benefits of Distributed Digital Records from Farm to Fork. *Technology Innovation Management Review*, 6–18.
<https://doi.org/10.22215/timreview/1446>
- Wong, L.-W., Tan, G. W.-H., Lee, V.-H., Ooi, K.-B., & Sohal, A. (2020). Unearthing the determinants of Blockchain adoption in supply chain management. *International Journal of Production Research*, 58(7), 2100–2123. <https://doi.org/10.1080/00207543.2020.1730463>
- Wong, L.-W., Tan, G. W.-H., Ooi, K.-B., & Chan, H. K. (2024). Blockchains for SMEs: A Fit-Viability perspective moderated by organizational innovation diffusion for supply chain performance. *Transportation Research Part E: Logistics and Transportation Review*, 182, 103396.
<https://doi.org/10.1016/j.tre.2023.103396>

- Wu, J.-Z., & Chien, C.-F. (2008). Modeling strategic semiconductor assembly outsourcing decisions based on empirical settings. *OR Spectrum*, 30(3), 401–430. <https://doi.org/10.1007/s00291-007-0120-5>
- Wu, Y., Dai, H.-N., & Wang, H. (2021). Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. *IEEE Internet of Things Journal*, 8(4), 2300–2317. <https://doi.org/10.1109/JIOT.2020.3025916>
- Xiao, J. H., Cheng, Z. L., Zhang, C. W., & Xie, K. (2012). Effects of information transparency on supply chain quality management. *2012 IEEE International Conference on Industrial Engineering and Engineering Management*, 966–970. <https://doi.org/10.1109/IEEM.2012.6837884>
- Xu, D., Dai, J., Paulraj, A., & Chong, A. Y.-L. (2022). Leveraging digital and relational governance mechanisms in developing trusting supply chain relationships: The interplay between blockchain and norm of solidarity. *International Journal of Operations & Production Management*. <https://doi.org/10.1108/IJOPM-02-2022-0122>
- Xu, X., & Yang, Y. (2021). Analysis of logistics port transportation efficiency evaluation based on the block chain technology. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-021-04379-4>
- Yacoub, G., & Castillo, M. (2021). Blockchain in your grocery basket: Trust and traceability as a strategy. *Journal of Business Strategy*, *In press*. <https://doi.org/10.1108/JBS-02-2021-0032>
- Yadav, S., & Singh, S. P. (2020). Blockchain critical success factors for sustainable supply chain. *Resources, Conservation and Recycling*, 152, 104505. <https://doi.org/10.1016/j.resconrec.2019.104505>
- Yan, J., Li, X., Shi, Y., Sun, S., & Wang, H. (2020). The effect of intention analysis-based fraud detection systems in repeated supply Chain quality inspection: A context of learning and contract. *Information & Management*, 57(3), 103177. <https://doi.org/10.1016/j.im.2019.103177>

- Yang, C.-S. (2019). Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use. *Transportation Research Part E: Logistics and Transportation Review*, 131, 108–117. <https://doi.org/10.1016/j.tre.2019.09.020>
- Yang, J., Han, S., Kang, H., & Kim, J. (2006). Product data quality assurance for e-manufacturing in the automotive industry. *International Journal of Computer Integrated Manufacturing*, 19(2), 136–147. <https://doi.org/10.1080/09511920500171261>
- Yang, L., Zhang, J., & Shi, X. (2021). Can blockchain help food supply chains with platform operations during the COVID-19 outbreak? *Electronic Commerce Research and Applications*, 49, 101093. <https://doi.org/10.1016/j.elerap.2021.101093>
- Yavaprabhas, K., Pournader, M., & Seuring, S. (2023). Blockchain as the “trust-building machine” for supply chain management. *Annals of Operations Research*, 327(1), 49–88. <https://doi.org/10.1007/s10479-022-04868-0>
- Yeoh, W., Lee, A. S. H., Ng, C., Popovic, A., & Han, Y. (2023). Examining the Acceptance of Blockchain by Real Estate Buyers and Sellers. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-023-10411-8>
- Yong, B., Shen, J., Liu, X., Li, F., Chen, H., & Zhou, Q. (2020). An intelligent blockchain-based system for safe vaccine supply and supervision. *International Journal of Information Management*, 52, 102024. <https://doi.org/10.1016/j.ijinfomgt.2019.10.009>
- 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>
- Zelbst, P. J., Green, K. W., Sower, V. E., & Bond, P. L. (2019). The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. *Journal of Manufacturing Technology Management*, 31(3), 441–457. <https://doi.org/10.1108/JMTM-03-2019-0118>

Zhang, P. (2013). The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the ICT Context. *MIS Quarterly*, 37(1), 247–274.

<https://doi.org/10.25300/MISQ/2013/37.1.11>

Zhou, H., & Benton, W. C. (2007). Supply chain practice and information sharing. *Journal of Operations Management*, 25(6), 1348–1365. <https://doi.org/10.1016/j.jom.2007.01.009>

Zhu, X. N., Peko, G., Sundaram, D., & Piramuthu, S. (2022). Blockchain-Based Agile Supply Chain Framework with IoT. *Information Systems Frontiers*, 24(2), 563–578.

<https://doi.org/10.1007/s10796-021-10114-y>

Appendix A. Aggregative Synthesis of Literature on Blockchain Use and Trust in Supply Chain Information Systems

This appendix synthesises the literature findings presented in Figure 6. The figure mentions the counts of articles that have studied each relationship, whether empirically or conceptually. We did not cite every relevant article in the main text since we list them all in Appendix B along with the relevant relationships. Most of the literature reports positive relationships between the studied concepts, so we only summarise these relationships. However, we discuss relationships in more detail only when there is mixed evidence for them.

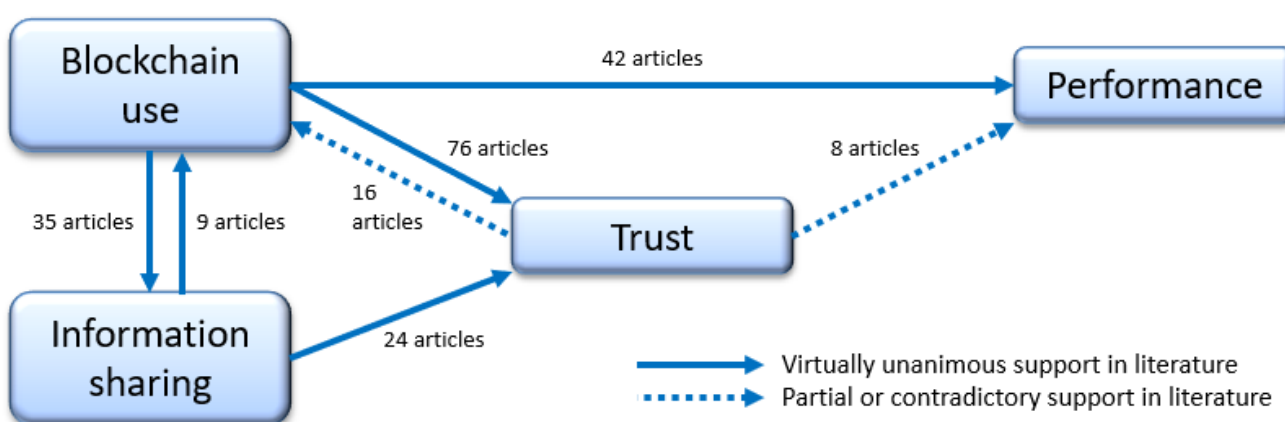


Figure 6. Relationships between blockchain use, information sharing, trust, and performance in the existing literature

Relationship between blockchain use and trust

Empirical studies investigating how blockchain affects trust have consistently found that blockchain use should enhance trust in the supply chain between an organisation and its partners. For example, blockchain enhances consumers' trust in food supply chains (Cozzio et al., 2023) and increases trust in Chinese manufacturers (Y. Long et al., 2023). However, some studies have investigated the opposite direction of causality with mixed results. While most studies have found that trust increases the use of blockchain, a few have not (see Appendix B for specific studies and the direction of their findings). For example, we found that experts in supply chain management considered trust to be an important condition for adopting blockchain (D. Ghode et al., 2020). By contrast, for other supply chain managers,

trust in partners was only moderately related to the expectation of using blockchain and depended more on attendant conditions such as social expectations or information systems know-how (Queiroz & Fosso Wamba, 2019). Moreover, this relationship was statistically significant only in the study's Indian sample; the United States sample did not exhibit a statistically significant relationship. Surprisingly, Jeanneret Medina et al. (2024), studying the actual deployment of blockchain in Switzerland, found evidence for the opposite effect: blockchain use was observed when trust between partners was low rather than when it was high. Thus, the existing evidence suggested that although blockchain should increase trust in supply chains, trust is not a prerequisite for its use.

Relationships between blockchain use, trust, and performance

The most critical objective behind using blockchain is to improve organisational performance (Fosso Wamba & Guthrie, 2020; G. Li et al., 2022; Mikalef et al., 2020). Most studies on the relationship between blockchain use and performance have discussed trust as a crucial element but have not explicitly studied it as a factor. However, a few notable exceptions stand out among studies directly examining the empirical effect of trust on performance in the context of blockchain. Indian supply chain practitioners expected that increased trust enabled by blockchain would improve firm performance (Sheel & Nath, 2019). Moreover, supply chain management experts expected that the effect of blockchain use on increasing trust and performance in supply chains depends on the presence and effectiveness of physical data verification (Kopyto et al., 2020). We revisit this and related findings below as we develop our propositions following a critique of the literature.

The bulk of the empirical literature we reviewed found that blockchain indeed led to positive performance outcomes (Behl et al., 2024; Pattanayak et al., 2024). However, this outcome was not universal. Among Chinese companies that had implemented blockchain, the relationship between blockchain implementation and turnover or the sales expense ratio was very weak or statistically nonsignificant (Pan et al., 2020). However, this result might have been a sampling artefact since only blockchain implementers were

compared. The authors also tested whether sales predicted blockchain implementation but found no significant relationship.

Relationship between blockchain use and information sharing

A global selection of supply chain experts indicated that blockchain would increase visibility of information within the supply chain (Y. Wang, Singgih, et al., 2019), as data transparency is considered critical (D. Ghode et al., 2020). Indian supply chain professionals expected that blockchain would increase their ability to trace and monitor processes (Fosso Wamba & Guthrie, 2020). Among manufacturing plant managers in the United States, blockchain use was associated with greater transparency (i.e., visibility and information sharing) across the supply chain (Zelbst et al., 2019). Among Taiwanese maritime shipping operators, those who considered digitising paperwork and tracking as useful were more likely to intend to use blockchain (C.-S. Yang, 2019). However, for supply chain managers in India and the United States with blockchain experience, transparency in blockchain was unrelated to the intention to use blockchain (Queiroz & Fosso Wamba, 2019).

For other aspects of information sharing, blockchain enables full traceability through the entire supply chain (Nayak & Dhaigude, 2019; Tönnissen & Teuteberg, 2020). However, Yang (2019) found that when BCSC systems were highly standardised, traceability was no longer considered an additional advantage of blockchain. Moreover, most of the literature did not explicitly define the type of information used in blockchains. In some cases, transaction information was paramount with no physical flow involved (O'Leary, 2017, 2018; A. Yang et al., 2019), whereas in others, information about the quality or other physical parameters of a product was given precedence (Kshetri, 2018).

Relationship between information sharing and trust

Several studies have found that efficient information sharing regarding blockchain use increased trust in the supply chain (Ahluwalia et al., 2020; Gurtu & Johny, 2019; Koh et al., 2020; Treiblmaier, 2018). Some case studies concurred (Azzi et al., 2019; Dubey et al., 2020). However, a larger survey of German and Dutch meat consumers found that the idea of having access to self-led investigation tools did not

increase the respondents' trust in origin claims, although it did strongly affect their purchase decisions (Sander et al., 2018).

Despite the broad consensus in the literature, our reading unearthed many unclear and unconvincing points, even in the empirical research, mainly due to imprecise or inconsistent definitions of related concepts. Thus, in Section 2 of the article, we critically analyse the literature by probing beneath the surface of what has been reported in existing studies.

Appendix B. Empirical and Conceptual Relationships Related to Blockchain and Trust in Supply Chains

Here, we list articles that examine the relationships between blockchain use, trust, supply chain, organisational performance, and information sharing from various perspectives. We list the articles in the following order of precedence:

1. The principal ordering is that articles that have studied the most frequent relationships (from Blockchain → Trust [on the left] to Trust → Performance [on the right]) are listed before others. Thus, articles that have studied the same relationships are grouped to make it much easier for the reader to see patterns in the literature findings.
2. Next, articles that have studied the same relationships are listed in chronological order of publication so that readers can more readily see whether findings have changed over time.

Authors	Year	Blockchain → Trust	Trust → Blockchain	Blockchain → Performance	Blockchain → Information Sharing	Information Sharing → Blockchain	Information Sharing → Trust	Trust → Performance
(D. Ghode et al., 2020)	2020	+	+			+		
(Sharma, Bhatia, et al., 2023)	2023	+		+	+		+	+
(Pattanayak et al., 2024)	2024	+		+	+		+	+
(Vern, Panghal, Mor, Kumar, et al., 2024)	2024	+		0	+		+	0
(D. J. Ghode et al., 2023)	2023	+		+	+		+	
(M. Kim et al., 2018)	2018	+		+	+		+	
(Rashid et al., 2023)	2022	+		+	+			+
(Kopyto et al., 2020)	2020	X		X	+			
(Baharmand et al., 2021)	2021	+		+	+			
(Madaan et al., 2023)	2023	+		+	+			

Authors	Year	Blockchain → Trust	Trust → Blockchain	Blockchain → Performance	Blockchain → Information Sharing	Information Sharing → Blockchain	Information Sharing → Trust	Trust → Performance
(Vasanthraj et al., 2024)	2024	+		+	+			
(Wong et al., 2024)	2024	+		0	0			
(Sheel & Nath, 2019)	2019	+		+				+
(Mishra et al., 2021)	2021	+		+				
(Longo et al., 2019)	2019	+		+				
(Hastig & Sodhi, 2020)	2020	+		+				
(Pan et al., 2020)	2020	+		+				
(de Boissieu et al., 2021)	2021	+		+				
(W. Long et al., 2021)	2021	+		+				
(X. Xu & Yang, 2021)	2021	+		+				
(Chittipaka et al., 2022)	2022	+		+				
(Y. Long et al., 2023)	2023	0			+		+	0
(Cozzio et al., 2023)	2023	0			+		+	
(H. Hu et al., 2023)	2023	+			+		+	
(Murimi et al., 2023)	2023	+			+		+	
(Luna et al., 2024)	2024	+			+		+	
(Manzoor et al., 2024)	2024	+			+		+	
(Trautmann et al., 2024)	2024	+			+		+	
(Kshetri, 2018)	2018	+			+			
(Y. Wang, Singgih, et al., 2019)	2019	+			+			
(Centobelli et al., 2021)	2021	+			+			
(Ozdemir et al., 2021)	2021	+			+			
(P.-K. Chen et al., 2022)	2022	+			+			
(González-Mendes et al., 2024)	2024	+			+			
(Vern, Panghal, Mor, & Kamble, 2024)	2024	+			+			
(Treiblmaier, 2018)	2018	+					+	
(Azzi et al., 2019)	2019	+					+	
(Gurtu & Johny, 2019)	2019	+					+	
(Dubey et al., 2020)	2020	+					+	
(Q. Lu & Xu, 2017)	2017	+						
(Notheisen et al., 2017)	2017	+						
(Tan et al., 2018)	2018	+						
(Y. Wang, Han, et al., 2019)	2018	+						
(S. E. Chang et al., 2019)	2019	+						
(Choi et al., 2019)	2019	+						
(Cole et al., 2019)	2019	+						
(Helo & Hao, 2019)	2019	+						
(Hughes et al., 2019)	2019	+						

Authors	Year	Blockchain → Trust	Trust → Blockchain	Blockchain → Performance	Blockchain → Information Sharing	Information Sharing → Blockchain	Information Sharing → Trust	Trust → Performance
(Nayak & Dhaigude, 2019)	2019	+						
(Philipp et al., 2019)	2019	+						
(Saber et al., 2019)	2019	+						
(Schmidt & Wagner, 2019)	2019	+						
(Choi, Feng, et al., 2020)	2020	+						
(Choi, Guo, et al., 2020)	2020	+						
(Du et al., 2020)	2020	+						
(Howson, 2020)	2020	+						
(Jain et al., 2020)	2020	+						
(A. Kumar et al., 2020)	2020	+						
(Pournader et al., 2020)	2020	+						
(Qian & Papadonikolaki, 2020)	2020	+						
(Roeck et al., 2020)	2020	+						
(Sahoo et al., 2021)	2021	+						
(L. Yang et al., 2021)	2021	+						
(Brookbanks & Parry, 2022)	2022	+						
(Cao et al., 2022)	2022	+						
(Chu et al., 2022)	2022	X						
(Dionysis et al., 2022)	2022	+						
(Elbashbishy et al., 2022)	2022	+						
(Erol et al., 2022)	2022	+						
(Jiang et al., 2022)	2022	+						
(Kshetri, 2022)	2022	+						
(W. Lu et al., 2022)	2022	+						
(Nodehi et al., 2022)	2022	+						
(D. Xu et al., 2022)	2022	X						
(Yavaprabhas et al., 2023)	2022	+						
(Chu et al., 2024)	2024	+						
(Rejeb et al., 2021)	2021		+	+	+		+	
(Behl et al., 2024)	2024		0	0				
(Tokkozhina et al., 2023)	2023		+		+			
(Jeanneret Medina et al., 2024)	2024		–		+			
(Queiroz & Fosso Wamba, 2019)	2019		+			0		
(Nath et al., 2022)	2022		+			+		
(Saurabh & Dey, 2021)	2021		+			+		
(Sharma, Sharma, et al., 2023)	2023		+			+		
(Rijanto, 2021)	2021		+				+	
(Queiroz et al., 2020)	2020		+					
(Yacoub & Castillo, 2021)	2021		+					

