

# Blockchain Technology and Trust in Supply Chain Management: A Literature Review and Research Agenda

**Abbas Batwa**

Department of Industrial Management and Logistics, Faculty of Engineering (LTH),  
Lund University, Sweden

Email: abbas.batwa@tlog.lth.se (*Corresponding Author*)

**Andreas Norrman**

Department of Industrial Management and Logistics, Faculty of Engineering (LTH),  
Lund University, Sweden

Email: andreas.norrman@tlog.lth.se

## ABSTRACT

Applying blockchain technology for information sharing in supply chain is driven by many factors, but developing trust is one of the most proposed. However, trust is a multidimensional, intangible concept without an agreed-upon definition. Whereas some argue that trust is the main driver of blockchain technology, others have found a negative relationship. This study focuses on how applying blockchain in supply chain management can influence trust and proposes a corresponding research agenda. Trust and blockchain technology discussions are scattered throughout the literature. Thus, a systematic literature review was performed based on a conceptual trust framework. This study discovered a gap in linking trust theories to blockchain technology applications especially in supply chain management, and provided insights into trust's reciprocal nature. Current literature strongly expects trust as a consequence for blockchain adoption if considered in the technology. Simultaneously, trust in supply chain partners is strongly expected as an antecedent to blockchain because it requires openness in information sharing. Thus, propositions and agenda for future research are suggested. The research is limited to literature findings due to the immaturity and low scalability of blockchain technology adoption; however, the most reviewed articles in less than two years old, increase the results' accuracy.

**Keywords:** *blockchain technology, supply chain, trust.*

## 1. INTRODUCTION

Technology innovations—such as blockchain technology (BCT)—that challenge traditional business practices have become well-established phenomena over the past decade. The main BCT characteristics that give rise to its novelty are decentralised peer-to-peer transactions with no central party, high transparency, immutability and computational logic (Iansiti and Lakhani, 2017). BCT is argued to provide a single trusted and visible source of information which can change the nature of information sharing, especially within the supply chain management (SCM) field (Loop, 2016; Yli-Huomo *et al.*, 2016) in both strategic level and process level (Martinez *et al.*, 2019). Considering such characteristics, applying BCT in SCM is

driven by many factors, but developing trust is one of the most discussed (Y. Wang *et al.*, 2019).

Trust is a multidimensional, intangible concept without clear agreement regarding what it is made of; its meaning gets even more confused in a SCM context due to the difficulty of measuring trust, especially in large and complex supply chains (SCs) (Kshetri and Voas, 2019; Panayides and Lun, 2009). Even so, many studies have proven that incorporating a high level of trusted relationships can lead to a better performance in logistics and SCM (Johnston *et al.*, 2004; Narasimhan and Nair, 2005). Indeed, trust is considered vital for effectively implementing collaborations; for example, trust has been found to be the key reason behind the success of many Japanese automakers (Dyer and Chu, 2003) because trustworthy collaboration ensures that SC parties understand each other's business and assist each other in developing innovative solutions (Khan and Wisner, 2019; Panayides and Lun, 2009; Roy *et al.*, 2004). In short: "Trust is at the heart of collaborative innovation capabilities. Without a foundation of trust, collaborative alliances can neither be built nor sustained. But, few companies are able to leverage trust for a sustainable competitive advantage; most companies lack high levels of trustworthy collaborations" (Fawcett *et al.*, 2012).

In different disciplines, trust been discussed regarding different types, development stages and dimensions (McKnight and Chervany, 2001; Seppänen *et al.*, 2007; Whipple *et al.*, 2010). In the SCM context, trust can be personal, interpersonal, inter-organisational or relating to the technology platform. The purpose of this paper is to understand how applying BCT in SCM can influence trust and to propose a corresponding research agenda. Although there are some findings in the literature about trust and BCT, they are very scattered, with some related to SCM, and many related to financial applications (Fernández-Caramés *et al.*, 2019). In fact, studies have shown there is a strong relationship between trust and BCT (Saber *et al.*, 2019; Y. Wang *et al.*, 2019; Batwa and Norrman, 2020). Some researchers argued that trust is the main driver for applying BCT (Peck, 2017; Y. Wang *et al.*, 2019; Batwa and Norrman, 2020). Others have introduced the concept of "digital trust", which claims to change the traditional

methods of dealing with trust in business. For example, in Gaehtgens and Allan (2017), Gartner stated that “It is often said that trust takes years to build, seconds to break and forever to repair. Digital trust, on the other hand, takes instants to build, an instant to break and is continuously adaptive”. However, some researchers argued that BCT should be seen as a complement to existing infrastructures rather than a replacement and it may use inputs from existing technologies (Van Hoek, 2019).

In the middle of this BCT hype, there are some concerns that BCT could negatively limit trust among the SC partners due to the high level of visibility in information sharing that could harm organisational privacy, especially with sensitive data (Hua *et al.*, 2018; Sander *et al.*, 2018; Sternberg *et al.* 2019). Thus, the positive and negative influences that BCT has on trust in a SC context need to be further investigated. To develop a robust understanding, however, trust itself must be further understood, which this study endeavours to do with the following two main questions:

**RQ1:** *How is trust operationalised and discussed in the articles that addressed both supply chain management and blockchain technology?*

**RQ2:** *How can blockchain technology influence trust in supply chain management?*

Both research questions (RQs) serve the purpose of this study: RQ1 is a preliminary question to investigate how trust has been discussed in the current literature, whereas RQ2 will provide a deeper understanding of BCT’s role as related to trust in the SCM context. To answer the research questions, the following sections will first give a theoretical background in which further insights about BCT and trust in SCM will be given, followed by a conceptual framework that will help facilitate the analysis of the literature review.

Second, the methodology will be explained. After that, the findings and research propositions will be discussed thoroughly. Finally, a conclusion will summarise the work, describe its contributions, limitations and suggestions for future research.

## 2. THEORETICAL BACKGROUND

Blockchain is still a novel technology that is not yet fully discovered. Therefore, a short theoretical background is provided to explain BCT and its attributes. After that, trust will be discussed from different perspectives to unpack the concept. Finally, a conceptual framework that connects different sub-dimensions of trust with BCT and SCM will be discussed.

### 2.1 Blockchain Technology and Supply Chain Management

Introduced in 2008 as the concept behind the bitcoin digital currency, BCT was first proposed by an anonymous programmer using the pseudonym Satoshi Nakamoto (2008). The literature lacks one unified definition of BCT, but almost all studies tend to define BCT according to its unique characteristics (e.g. Iansiti and Lakhani, 2017; Yli-Huumo *et al.*, 2016). One of the latest definitions of BCT was proposed by Treiblmaier (2018) as “a digital, decentralized and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamperproof records”. This definition addresses several important architectural properties besides describing the technology itself. According to Hald and Kinra (2019), four attributes of BCT can be constructed and defined (Table 1).

**Table 1:** BCT attributes explained (adapted from Hald and Kinra, 2019)

BCT Attribute	Explanation
<b>Decentralised structure</b>	All parties have a copy of the same data, which is distributed across the peer-to-peer network to allow visibility to everyone at any time and any place in the network.
<b>Cryptography system</b>	This enables the tracking of chains of data and transactions over time. From a technical point of view, the header of each block contains a “hash value” that imitates the contents of the previous blocks and descends from its predecessors all the way back to the first block in the chain. Thus, new information cannot be tampered with retroactively by changing a previous entry because the whole chain will become invalid.
<b>Consensus mechanism</b>	The consensus mechanism ensures that transactions are coded into blocks according to cryptographic rules and chronological sequence to ensure the security and immutability of the transactions. The distributed consensus protocols can take several forms, such as majority, priority or minimal number of votes, to ensure data integrity.
<b>Smart contract</b>	With this optional feature, users can set up algorithms and rules that automatically trigger transactions between nodes without human interference.

The two main types of BCT are permission-less (public) blockchains and permissioned (private) blockchains. In public blockchains, the digital ledger is completely decentralised and can be accessed by any Internet user, which may put sensitive information at risk of exposure. On the other hand, private blockchains allow only a preselected and limited number of participants to be authorised to use the ledger. In a fully private blockchain, entries are monitored by a central authority which can decide

to accept new members into the network and determine their level of access (Hald and Kinra, 2019).

In the SCM context, there are many drivers for applying BCT. According to a recent literature review of 29 papers by Y. Wang *et al.* (2019), there are four main drivers for applying BCT in SCM. The first and most influential driver is to create a trust-free environment based on the reliability and security of the information stored on the blockchain. The second driver is the SC disconnections and complexities

resulting from a lack of real-time visibility. Providing product safety, legitimacy and authenticity is the third driver as BCT provides information with a provenance feature so that products can be traced to their origin. The final driver is the need for increased public safety and anticorruption, which BCT can provide through its consensus and immutability features that work well against fraud and counterfeit products or behaviours (Y. Wang *et al.*, 2019).

Moreover, different applications of BCT were seen in different SCM areas. According to the same study by Y. Wang *et al.* (2019), extended visibility and product traceability are the main and most deployed applications. BCT provides a temporal record of all transactions, along with other related product specifications, such as sender, receiver, temperature, footprint and so on. Additionally, with installed sensors and Internet of Things (IoT) devices, real-time visibility can be achieved which will drive tracking and tracing applications to the next level (Li *et al.*, 2017; Y. Wang *et al.*, 2019). Other applications of BCT in SCM could include the following:

- Digitalisation of transactions results in less manual work and paperwork, less time validating processes and peer-to-peer transactions with no need for a central party.
- Improved data security and information sharing overcome issues such as corrupted information or information asymmetry due to the consensus mechanism.
- The smart contract application ultimately can lead to fully autonomous SCs. Although this feature is not currently deployed fully, most uses are in the realm of finance and payments issuance (Y. Wang *et al.*, 2019)

## 2.2 Unpacking Inter-organisational Trust

As trust is seen as an important governance mechanism for SCM, research in recent years has focused on understanding and conceptualising trust in SCM (e.g. Fawcett *et al.*, 2012, 2017; Michalski, *et al.*, 2019; Sahay, 2003; Whipple *et al.*, 2010). However, a lack of agreement remains regarding what constitutes trust, and there is no generally accepted definition. This problem is not new: trust has been called a “conceptual confusion” (Lewis and Weigert, 1985), a “confusing potpourri” (Shapiro, 1987) and a “conceptual morass” (Carnevale and Wechsler, 1992). One of many definitions is provided by Ganesan (1994) as “trust is the willingness to rely on an exchange partner in whom one has confidence”, but many more are discussed as well, for example, in Seppänen *et al.* (2007).

The inter-organisational context of trust that characterises SCM has been studied from many different disciplines and perspectives, such as psychology, social psychology, sociology, economics and management (McKnight and Chervany, 2001; Seppänen *et al.*, 2007; Whipple *et al.*, 2010). The common observation is that trust, especially inter-organisational trust, is a vague, multi-dimensional and complex construct to unpack due to its many aspects. Every discipline also tends to view trust from its own perspective via a lens that lacks understanding of or appreciation for the views of others (McKnight and Chervany, 2001). However, saying that trust is a complex construct is a bad argument for not trying to understand it better. Thus, to reduce its ambiguity, trust will now be

discussed from different perspectives, including its reciprocal nature, objects, classes, temporal development and the sub-dimensions.

### 2.2.1 Reciprocal nature of trust

One reason for the ambiguity and confusion surrounding trust is its two-sided reciprocal nature, which leads to unclear causality (Seppänen *et al.*, 2007). Depending on the perspective, trust could be seen either as a cause or effect related to certain aspects (e.g. cooperation, communication and performance), which makes it difficult to define the antecedents, dimensions or consequences of trust. Among SCM researchers, there are examples in which information sharing is argued to be an antecedent of trust (e.g. Kwon and Suh, 2005), and others where trust is argued to be a critical antecedent for enabling inter-organisational information sharing (Handfield and Bechtel, 2002; Kembro *et al.*, 2017). In addition, Seppänen *et al.* (2007) asked for future research to test the reciprocal loops of trust.

### 2.2.2 Objects of trust

A second reason for the ambiguity, as discussed in theory, is that trust could relate to different “objects of trust” (Seppänen *et al.*, 2007), for example, kinds of relationships: interpersonal (between individuals), organisational (one individual to an organisation), inter-organisational (one organisation to another organisation) and inter-organisational networks (one organisation to many organisations) (Whipple *et al.*, 2010). Although this would represent trust in partners, some authors differentiated this from trust in technology (e.g. Lu *et al.*, 2010), which can be divided further into trust in platform and trust in records (Lu *et al.*, 2010).

### 2.2.3 Classes of trust

The third reason for the ambiguity is that trust can be categorised into different classes which influence each other in different ways. McKnight and Chervany (2001) differentiated among dispositional trust (the truster’s general willingness to trust others), structural institutional trust (not to personal characteristics but to social or institutional structures in a situation, e.g. regulations), more interpersonal trust related to trusting beliefs (a psychological willingness to accept vulnerability) and trusting intentions (a party’s readiness and willingness to rely on another party despite probable negative consequences).

### 2.2.4 Temporal development of trust

Fourthly, trust in a professional business relationship could develop over time to different trust levels (e.g. Lewicki and Bunker, 1995; Shapiro *et al.*, 1987) such as the following:

- Deterrence-based trust: This is a primary form of trust existing in the initial stages of any cooperation where one fears punishment of violating trust and will do (and assume the other to do) whatever was promised because breaching trust will be costlier than keeping it, with monitoring as a must to keep it effective.
- Calculus-based trust: Trust is based on a calculation that compares cost and benefits of creating and sustaining a relationship versus the cost and benefits of severing it, with professional reputation held hostage.

- Knowledge-based trust: Knowledge increases from partners continuously learning about each other, which leads to anticipation of the other's actions.
- Identification-based trust: After repeated interactions, trust has increased to the point where parties understand their shared values and goals, and they internalise each other's desires and intentions.

Similarly, Fawcett *et al.* (2012) suggested a maturity framework (based on time, experience and relationship intensity) of the four stages: i) limited trust, ii) transactional trust, iii) relational trust and iv) collaborative trust. Seppänen *et al.* (2007) argued that temporal dynamics on the element of trust have been given less attention and that different elements of trust might have varying influences on different stages.

### 2.2.5 Sub-dimension of trust (in partners vs. technology)

A fifth reason—possibly the most discussed both in the SC literature and in other theoretical approaches trying to unpack trust—is the multitude of different sub-dimensions that are used for defining, operationalising and measuring trust. The literature is fragmented with no consensus regarding trust dimensions or measurements (Fawcett *et al.*, 2017).

Seppänen *et al.* (2007) found that the number of dimensions vary between 0 (only using trust) and 5, they also found more than 20 dimensions in the 15 articles reviewed. After sorting them into antecedents, sub-dimensions and consequences, the main sub-dimensions proposed were credibility, benevolence, goodwill, predictability, reciprocity, openness and confidence. Fawcett *et al.* (2012, 2017) stated that the dominant view in marketing management and SCM uses the following two sub-dimensions: credibility (the confidence that each party in a relationship will perform as promised) and benevolence (the mutual expectation between two parties that each will act in the other's best interest as decisions are made). Ganesan (1994) measured inter-organisational trust in these two distinct sub-dimensions: credibility (defined as the expectations about the required expertise of the other party) and benevolence (defined as one party's beliefs that intentions and motivations of the other party will be beneficial in the face of new conditions, indicating vulnerability) (Whipple *et al.*, 2010). Credibility includes reliability and predictability signals (So and Schill, 2002). Avoidance of opportunistic behaviour and making investments to improve mutual performance increases the level of trust and signals that a partner's motives are trustworthy, creating mutual confidence.

Other examples of measures for trust, summarised by Seppänen *et al.* (2007), are, for example, trustworthiness, openness, opportunistic behaviour, risk (Doney and Cannon, 1997), expertise, friendship, willingness to serve (Plank *et al.*, 1999) and reliability (Gassenheimer and Manolis, 2001). Whipple *et al.* (2010) studied scales used for trust in SCM journals by analysing 42 empirical articles and found that for a vast majority of instances, trust was only tested as a unidimensional construct. The most-used sub-dimension they found was benevolence. Based on their study of managers, Fawcett *et al.* (2012, 2017) challenged whether benevolence even exists among companies, as managers

stated that companies don't have friends but interests, and firms cannot afford to work with partners based on benevolence because trust emerges over time from behaviour, not benevolence (Fawcett *et al.*, 2017). As the credibility and benevolence dimensions draw on interpersonal trust perspectives, Fawcett *et al.* (2012; 2017) nuanced them into two dimensions for constructing trust: a perform-to-promise capability (related to credibility) and a relational-commitment capability (related to benevolence). The relational-commitment capability is operationalised into information sharing, investment in partner capabilities, respect-based relationship and empathy.

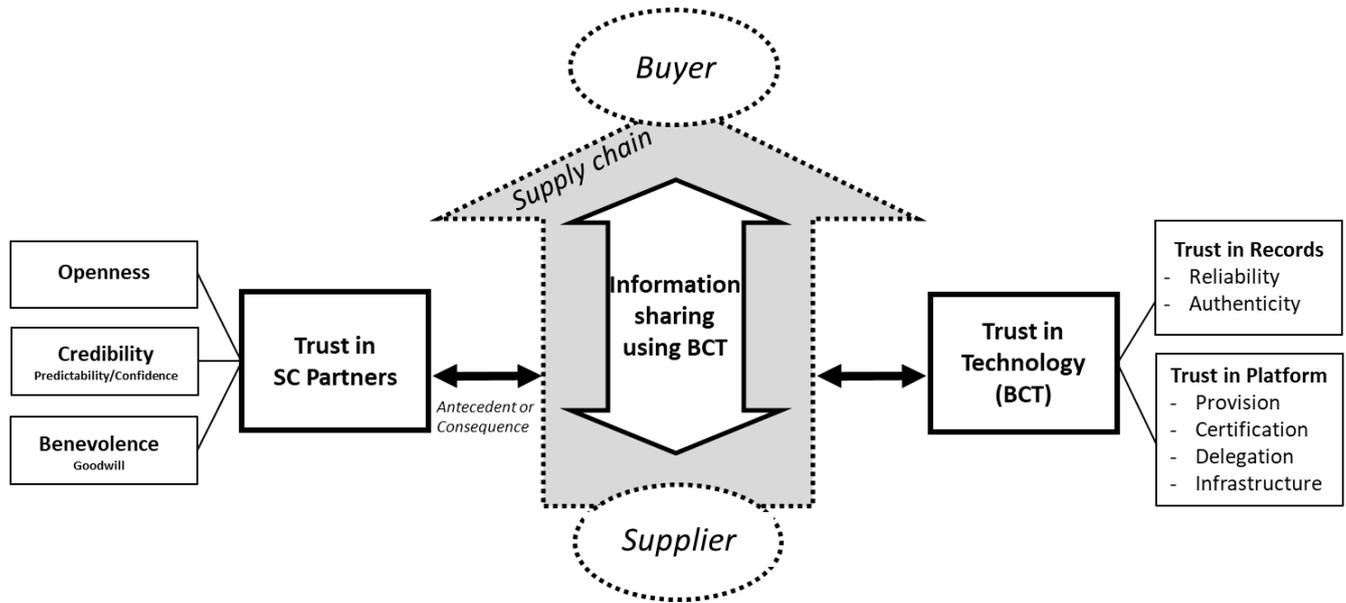
As the preceding discussion was related to the "trust in partners" trust object, the "trust in technology" trust object can also be elaborated on. Trust in technology can be interpreted as the beliefs regarding the performance of an institution or organisation rather than the individual (Lu *et al.*, 2010), and it corresponds to structural institutional trust. This trust can be divided into trust in platform versus trust in records. Trust in platform relates to Grandison and Sloman's (2000) study on trust in the context of networked and distributed computing systems related to Internet-based services and applications. They characterised this trust into the following four sub-dimensions:

- Provision trust: Trust to let the trustee implement a service without requiring access to the truster's resources.
- Certification trust: The belief that the trustees' identity is claimed based on certifications presented that should authenticate identity.
- Delegation trust: Trust to let the trustee make decisions on its behalf with respect to a resource or service that the truster owns or controls.
- Infrastructure trust: Trust in the infrastructure and applications.

Trust in records relates to the sub-dimension's reliability of records (how records originated and who created them) and authenticity of records (depends on the establishing process and how the identity of records is maintained) (Mak, 2014).

## 2.3 A Framework for Exploring Trust and BCT for Information Sharing in SCM

The aim of this framework is to uncover the potential reciprocal nature of trust and BCT information sharing in SCM. While many early publications related to BCT argued that BCT (through information sharing) increases trust between SC actors (buyer and supplier of a good or service), other research claims that trust is necessary for inter-organisational information sharing. Thus, the SC (including the buyer, the seller and their information sharing by BCT) is one of the main elements of this study's framework. The other main element is trust, which is divided between i) trust in SC partners (supplier and buyer) and ii) trust in technology (in BCT from the actors' perspective) (Mansouribakvand, 2019). The reciprocal nature is illustrated by bidirectional arrows, as well as by having the two objects of trust. While trust in technology represents institutional trust, trust in the SC partner is more related to the other classes of trust (Mansouribakvand, 2019).



**Figure 1** Framework for exploring trust and BCT for information sharing in SCM (Mansouribakvand, 2019)

Trust in partners uses the credibility, benevolence, goodwill, predictability, openness and confidence sub-dimensions. However, these sub-dimensions could be grouped into three categories: i) *benevolence*, which includes signals of goodwill; ii) *credibility*, which includes signals of predictability and confidence; and iii) *openness*. Trust in BCT uses the provision, certification, delegation and infrastructure (for the platform) and reliability and authenticity (for the records) sub-dimensions.

### 3. RESEARCH METHODOLOGY

Trust is an established concept that has been discussed for many decades (Lewis and Weigert, 1985), whereas BCT is a rapidly growing technology that is promising to change transactional trust in the SCM field. To study such emerging topics, a theoretical background was carried out prior to further exploration and analysis steps. In this study, a framework that links trust and BCT was chosen as the foundation for the research, followed by the selection of a systematic literature review (SLR).

SLR is “a referential method to organize, synthesize and identify emerging paths and opportunities, as well as understanding the relevant issues, contradictions and limitations, based on previous studies” (Queiroz *et al.*, 2018). SLRs have traditionally been applied in established fields as published papers in journals can be scarce in emerging topics and rapidly growing fields (Tranfield *et al.*, 2003). Recently, however, many studies have applied the SLR successfully to emerging themes (Queiroz *et al.*, 2018). For example, Tachizawa and Wong (2014) conducted a SLR to propose a framework for multi-tier, sustainable SCs using 39 papers, and Pereira *et al.* (2014) used a SLR of literature published between 2000 and 2013 to understand procurement and SC resilience. In fact, SLR is an effective approach to field development, provides a trustworthy systematic approach for understanding issues that are not covered, identifies ways of exploring the field and generates new research agendas for

the future. It also guarantees that no relevant research is overlooked and ensures replicability (Pereira *et al.*, 2014; Queiroz *et al.*, 2018). Thus, a SLR is suitable to address how BCT and trust are related in a SCM context, even though it is a rapidly growing and developing topic. The following sections will explain the literature selection and literature analysis processes.

#### 3.1 Literature Selection Process

Following Tranfield *et al.* (2003), three steps were used in selecting the literature. The first step was to conduct an advanced search for the words “blockchain” and “trust” in the title, abstract and keywords through the university library search engine that leverages numerous databases (e.g. Academic Search Complete, Business Source Complete, Emerald, ScienceDirect, IEEE Xplore Digital Library, Complementary Index, and Directory of Open Access Journals). To achieve rigorous results, the search was limited to peer-reviewed articles mainly journals or conference papers. The conjunction “and” was used between the words “blockchain” and “trust”. Additionally, two synonyms were used for “blockchain”—“block chain” and “distributed ledger”—with the conjunction “or” used between the synonyms. This enabled a larger sample of relevant literature to be collected (Tranfield *et al.*, 2003). As a result, 1480 papers were initially generated from 7 different databases (as listed previously). The second step was to narrow down the research results to only papers that discussed BCT and trust in a SCM field. Thus, all the abstracts of the achieved results from the first step were searched for “supply chain” or “logistics”, resulting in 135 papers. The third step was to screen all the abstracts so that only papers discussing BCT and trust in the SCM context were considered. The inclusion and exclusion criteria are given in **Table 2**. This resulted in 55 papers that were selected for the review and analysis (44 journal articles and 11 conference papers).

**Table 2:** Inclusion and exclusion criteria for the selected papers

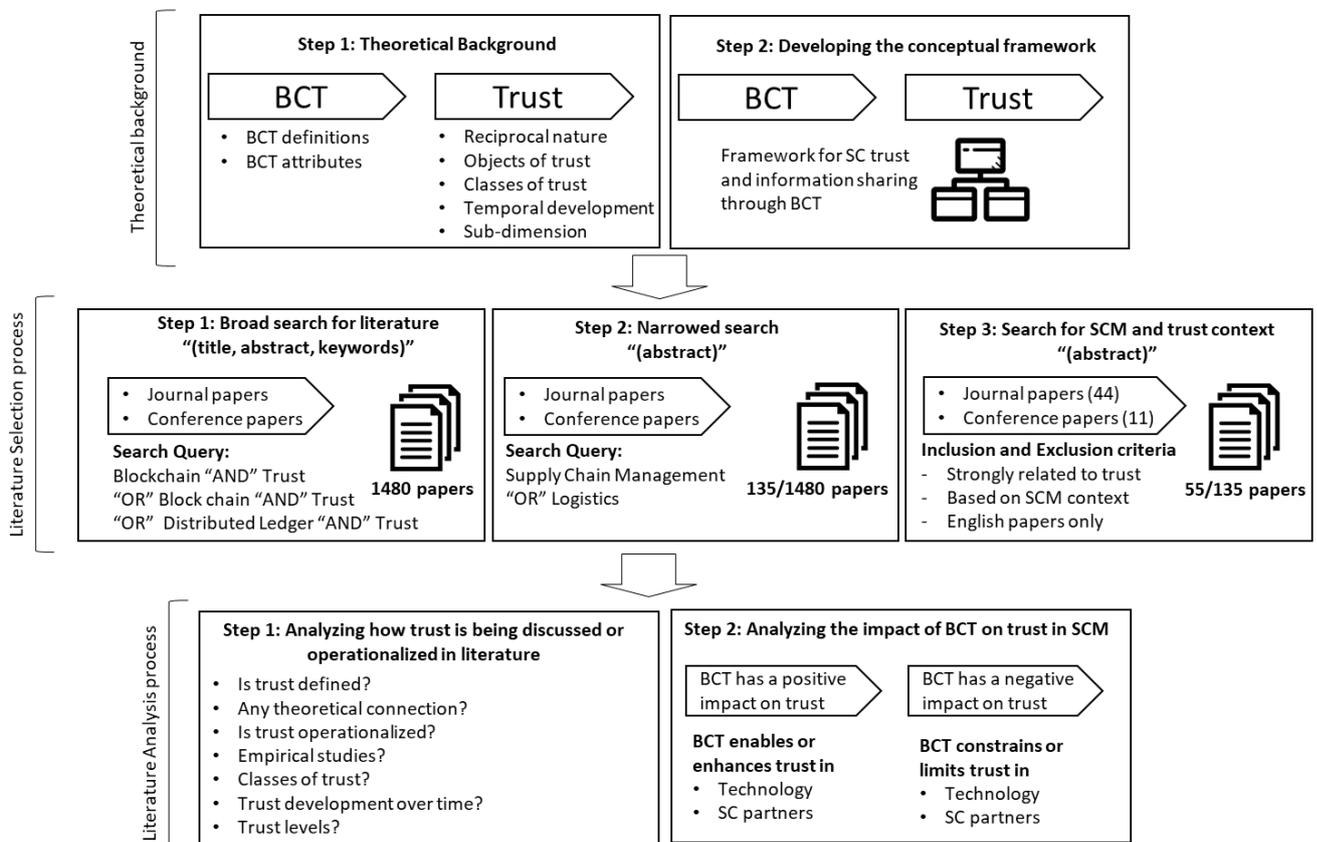
Inclusion Criteria	Exclusion Criteria
English language papers.	Papers are written in different languages.
Trust is discussed with “trust” as a topic and not as a passing word.	Trust is just a passing word without further insight into the topic of trust.
Supply chain management or logistics is the context of applying trust using BCT.	BCT is discussed to develop trust in other fields

**3.2 Literature Analysis Process**

To understand how trust is operationalised and discussed in the articles that addressed SCM and BCT, several sub-questions were generated. First, the study investigated whether any theoretical connections or frameworks were used for their trust discussion and, if so, what these frameworks were. Second, the study looked for the trust definition in each paper to have a view of which definitions are the most used in relation to BCT and SCM. Third, the study tried to determine if trust was measured or operationalised in the literature and, if so, if the implications generated were based on empirical studies or mainly suggestions and ideas. Finally, the literature was examined for different trust constructs used, if any, such as the classes of trust, trust development over time and trust levels. Answering these sub-questions should address whether there is a gap in the literature between trust theories and BCT in SCM.

To further analyse the selected papers, the process proposed by Hald and Kinra (2019) was followed to develop

an understanding of how BCT could influence trust in SCM. Thus, different research propositions were generated to be discussed based on the conceptual framework. These propositions fall under two main categories: i) propositions suggesting that BCT has a positive influence on trust in SCM, and ii) other propositions suggesting that BCT has a negative or non-positive influence on trust in SCM. According to Hald and Kinra (2019), Adler and Borys (1996) and Miles and Huberman (1994), each of the selected papers should be coded individually to signal the influences of BCT on trust. Specifically, words or phrases indicating positive influence included, for example, “BCT will enable”, “facilitate”, “enhance”, “leads to” and “expected to provide”, whereas other words and phrases, such as “blockchain constrains”, “limitations”, “barriers” and “blockchain challenges”, suggested a negative or non-positive influence on trust. However, to increase reliability, the final selected papers were read by the authors to identify the context in which positive or negative influences have occurred. The whole research design is summarised in **Figure 2**.



**Figure 2** Research design

## 4. FINDINGS AND PROPOSITIONS

This section first discusses the findings from the literature review regarding trust and BCT in the SCM context, which will contribute to answering RQ1. The section following then examines research propositions related to RQ2.

### 4.1 Literature Review Findings

Several sub-questions (SQ) have been tested against all the reviewed papers. **Table 3** shows these questions and their index numbers.

**Table 3:** Sub-questions to address literature review findings

Index	Sub-questions
SQ1	Are there any theoretical connections/frameworks used for a trust discussion?
SQ2	Is trust defined?
SQ3	Is trust operationalised?
SQ4	Are trust and its implications (in BCT and SCM) empirically researched, or are conclusions/propositions mainly ideas/suggestions?
SQ5	Are different “classes of trust” discussed, or is trust only a general, undefined term?
SQ6	Are different “trust development over time” objects discussed, or is trust only a general, undefined term?
SQ7	Are different “trust levels” discussed, or is trust only a general, undefined term?

**SQ1:** *Are there any theoretical connections/frameworks used for a trust discussion?*

Only 8 (15%) out of the 55 reviewed papers have a theoretical connection that is used for trust discussion. Zaerens (2018) discussed trust management and business-critical information sharing in a definite group of stakeholders called circle of trust. Francisco and Swanson (2018) and Wong *et al.* (2020) explored the adoption of BCTs in SC traceability applications. They both used the Unified Theory of Acceptance and Use of Technology (UTAUT) as a framework for technology acceptance and the construct of information technology trust to develop a conceptual model with researchable propositions. Hawlitschek *et al.*, (2018) used the extended blockchain framework that is based on Notheisen *et al.* (2017), The framework basically dealt with trust based on two points of view: i) from the sharing economy, which includes two objects of trust—trust in peers and trust in the platform; and ii) from BCT and discussed trust-free systems and trust-building mechanisms. Even though this paper is in the sharing economy context, it can be deployed in SCM (Hawlitschek *et al.*, 2018; Notheisen *et al.*, 2017).

Recently in late 2019 and 2020, more papers have used trust theories than before, for example: Saberi *et al.* (2019) basically examined barriers to apply BCT in SCM and trust was related to these barriers. Dubey *et al.* (2020), used a theoretical framework to study how BCT, collaboration, supply chain resilience and transparency can affect swift trust in a humanitarian logistics context. Finally, Qian and Papadonikolaki (2020) used a framework to conceptualise trust in construction SCM and differentiate between micro and macro level trusts. Different trust dimensions were mentioned such as: system-based, cognition-based and relation-based trusts. However, this paper was more specific to the construction context (Qian and Papadonikolaki, 2020). In general, our observation is that frameworks or references

to established research domains dealing with trust (e.g. psychology, social psychology, sociology, economics and management) are still seldom used for trust discussions in SCM.

**SQ2:** *Is trust defined?*

Only 6 (11%) out of 55 of the reviewed papers defined trust based on reliable sources. Zaerens (2018) used the definition of trust by Grandison and Sloman (2002): “Trust is a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context”. Hawlitschek *et al.* (2018) used the definition provided by Rousseau *et al.* (1998): “The intention to accept vulnerability based upon positive expectations” Which is similar to the one used by Wong *et al.* (2020) as well. Saberi *et al.* (2019) used an older definition of trust that is “An organisations belief that their partners will take positive actions to benefit them, and will not negatively affect them” by Anderson and Narus (1990). Other researchers such as Akram and Bross (2018), Sheel and Nath (2019), Qian and Papadonikolaki (2020) used the most common definition of trust that was provided by Mayer *et al.* (1995): “The willingness to be vulnerable to another”.

Although there are only 6 papers that proposed an established definition of trust, other papers referred to trust as a confidence provided by trade partners, or as the reliability and security of the data managed by a central authority. Thus, BCT is repeatedly called a trust-free system because it claims to eliminate the need for a trusted third party and claims to provide a single source of data without the need to trust other peers in the SC network (e.g. Akram and Bross, 2018; Notheisen *et al.*, 2017; Y. Wang *et al.*, 2019; Ghode *et al.* 2020). In general, trust was mostly discussed without using explicit and established definitions.

**SQ3: Is trust operationalised?**

In terms of operationalisation, Only 4 (7%) out of 55 of the reviewed papers have tried to operationalise or measure trust when BCT is applied in SCM, All are in 2019 and 2020. Malik *et al.* (2019) and Shahid *et al.* (2020) have tried to utilize BCT and smart contracts for making a reputation system to measure the extent a partner can be trusted. Dubey *et al.* (2020), used an empirical study to understand how swift trust in humanitarian logistics can be affected through BCT, collaboration, supply chain resilience and supply chain transparency. Qian and Papadonikolaki (2020) studied how trust is affected by the introduction of blockchain technology in construction SCM through empirical interviews and with the help of a framework based on different trust dimensions. They conclude that BCT mainly enhances trust by affecting the cognition-based trust and the system-based trust but essentially replaces relation-based trust, which means a transformation of trust from relational to technological in SCM.

Our observation is that trust is rarely operationalised in a BCT based SCM, only very few papers tried to operationalise trust. But, it is either specific to a certain context such as construction (Qian and Papadonikolaki, 2020) or humanitarian logistics (Dubey *et al.*, 2020) or it is based on a mathematical or simulation model, which is very limited (Malik *et al.*, 2019; Shahid *et al.*, 2020).

**SQ4: Are trust and its implications (in BCT and SCM) empirically researched, or are conclusions/propositions mainly ideas/suggestions?**

In total, 14 out of 55 papers (25%) gave implications based on empirical studies, whereas the remaining papers just proposed ideas and suggestions, sometimes based on previous references. Indeed, the most of the 14 papers are case studies or empirical work in themselves, but trust implications are not driven from these actual data. The most

trust related empirics are for example: Qian and Papadonikolaki (2020), Dubey *et al.* (2020), Malik *et al.*, (2019) and Shahid *et al.* (2020) which are the same papers mentioned for trust operationalisation. So, we can say that claims specified for trust and related to BCT in SCM are mostly not based on empirical studies.

**SQ5: Are different “classes of trust” discussed, or is trust only a general, undefined term?**

**SQ6: Are “trust development over time” discussed, or is trust only a general, undefined term?**

**SQ7: Are different “trust levels” discussed, or is trust only a general, undefined term?**

Only 3 papers (5%) out of 55 discussed different classes of trust such as: Hawlitschek *et al.*, (2018) who mentioned two classes of trust related to the sharing economy context, and distinguished between institution-based trust (trust in, e.g., Airbnb) and the disposition to trust (trust in hosts). Galvez *et al.* (2018) roughly mentioned different classes of trust such as: authentication trust, delegation trust, provision trust and infrastructure trust.

None of the remaining references discussed trust development over time which may be due to the novelty of the topic. However, some papers mentioned trust objects or dimensions as different types of trust which, for instance, could be trust in a platform or inter-organisational trust (e.g., Francisco and Swanson, 2018; Hawlitschek *et al.*, 2018; Notheisen *et al.*, 2017). Other papers (e.g., Qian and Papadonikolaki, 2020) have discussed different trust dimensions like system-based, cognition-based and relation-based trusts. Moreover, it is the only paper who discussed different trust levels as a micro and macro level trusts. To conclude, trust has been used in a very vague way. **Table 4** summarises all the literature review findings according to the previously discussed sub-questions.

**Table 4:** Summary of literature findings

	Reference	SQ1 Theory?	SQ2 Defined?	SQ3 Operationalise d?	SQ4 Empirics used?	SQ5 Trust classes?	SQ6 Time?	SQ7 Trust levels?
1	Chen <i>et al.</i> (2017)	No	No	No	No	No	No	No
2	Feng (2017)	No	No	No	No	No	No	No
3	Augusto <i>et al.</i> (2019)	No	No	No	No	No	No	No
4	Figueroa <i>et al.</i> (2019)	No	No	No	No	No	No	No
5	S. Wang <i>et al.</i> (2019)	No	No	No	No	No	No	No
6	Kshetri and Loukoianova (2019)	No	No	No	No	No	No	No
7	Hua <i>et al.</i> (2018)	No	No	No	No	No	No	No
8	Anjum <i>et al.</i> (2017)	No	No	No	No	No	No	No
9	Zaerens (2018)	Yes	Yes	No	Yes (Modelling)	No	No	No
10	Bencić <i>et al.</i> (2019)	No	No	No	No	No	No	No
11	Verhoeven <i>et al.</i> (2018)	No	No	No	No	No	No	No
12	Tseng <i>et al.</i> (2018)	No	No	No	No	No	No	No

	Reference	SQ1 Theory?	SQ2 Defined?	SQ3 Operationalised ?	SQ4 Empirics used?	SQ5 Trust classes?	SQ6 Time?	SQ7 Trust levels?
13	Dasaklis and Casino (2019)	No	No	No	No	No	No	No
14	Arumugam <i>et al.</i> (2018)	No	No	No	No	No	No	No
15	Rejeb <i>et al.</i> (2019)	No	No	No	No	No	No	No
16	Francisco and Swanson (2018)	Yes	No	No	No	No	No	No
17	Kshetri and Voas (2019)	No	No	No	No	No	No	No
18	Sander <i>et al.</i> (2018)	No	No	No	Yes (Survey)	No	No	No
19	Hawliitschek <i>et al.</i> (2018)	Yes	No	No	No	Yes	No	No
20	Fernández-Caramés <i>et al.</i> (2019)	No	No	No	No	No	No	No
21	Zhang and Jacobsen (2018)	No	No	No	No	No	No	No
22	Notheisen <i>et al.</i> (2017)	Yes	No	No	Yes (Modelling)	No	No	No
23	Westerkamp <i>et al.</i> (2019)	No	No	No	No	No	No	No
24	Norberg (2019)	No	No	No	No	No	No	No
25	Y. Wang <i>et al.</i> (2019)	No	No	No	No	No	No	No
26	Kamble <i>et al.</i> (2019)	No	No	No	No	No	No	No
27	Johng <i>et al.</i> (2018)	No	No	No	No	No	No	No
28	Akram and Bross (2018)	No	Yes	No	Yes (Interviews)	No	No	No
29	Saberi <i>et al.</i> (2019)	Yes	Yes	No	No	No	No	No
30	Pearson <i>et al.</i> (2019)	No	No	No	No	No	No	No
31	Longo <i>et al.</i> (2019)	No	No	No	Yes (Modelling)	No	No	No
32	Sheel and Nath (2019)	No	Yes	No	Yes (Survey)	No	No	No
33	Galvez <i>et al.</i> (2018)	No	No	No	No	Yes	No	No
34	Montecchi <i>et al.</i> (2019)	No	No	No	No	No	No	No
35	Dobler <i>et al.</i> (2019)	No	No	No	No	No	No	No
36	Sternberg <i>et al.</i> (2019)	No	No	No	Yes (Interview)	No	No	No
37	Fernando <i>et al.</i> (2019)	No	No	No	No	No	No	No
38	Malik <i>et al.</i> (2019)	No	No	Yes	Yes (Modelling)	No	No	No
39	Viriyasitavat <i>et al.</i> (2019)	No	No	No	No	No	No	No
40	Ghode <i>et al.</i> (2020)	No	No	No	Yes (Interviews)	No	No	No
41	Yong <i>et al.</i> (2020)	No	No	No	No	No	No	No
42	Batwa and Norrman (2020)	No	No	No	Yes (Interviews)	No	No	No
43	Pournader <i>et al.</i> (2020)	No	No	No	No	No	No	No
44	Shahid <i>et al.</i> (2020)	No	No	Yes	Yes (Modelling)	No	No	No
45	Rogerson and Parry (2020)	No	No	No	No	No	No	No

Reference	SQ1 Theory?	SQ2 Defined?	SQ3 Operationalised ?	SQ4 Empirics used?	SQ5 Trust classes?	SQ6 Time?	SQ7 Trust levels?
46	Wan <i>et al.</i> (2020)	No	No	No	No	No	No
47	Garrard and Fielke (2020)	No	No	No	No	No	No
48	Dubey <i>et al.</i> (2020)	Yes	No	Yes	Yes (Survey)	No	No
49	Di Vaio <i>et al.</i> (2020)	No	No	No	No	No	No
50	Behnke and Janssen (2020)	No	No	No	No	No	No
51	Howson (2020)	No	No	No	No	No	No
52	Kumar <i>et al.</i> (2020)	No	No	No	No	No	No
53	Kamble <i>et al.</i> (2020)	No	No	No	No	No	No
54	Qian and Papadonikolaki (2020)	Yes	Yes	Yes	Yes (Interviews)	No	Yes
55	Wong <i>et al.</i> (2020)	Yes	Yes	No	Yes (Survey)	No	No

### 4.2 Research propositions and discussions

Trust has a unique relationship when it comes to applying BCT in SCM. Indeed, trust has been identified as both a drive and a hurdle to the BCT adoption (Li *et al.*, 2019; Batwa and Norrman, 2020). In this section, we try to modify the previous framework to explore this reciprocal nature of trust by reflecting on the influence of BCT on SC trust (Figure 3). For instance, if the BCT enables, enhances or has a generally positive influence on trust, then it can be said that trust is a consequence of applying BCT in a SCM context. This means trust will be heavily influenced or changed after applying BCT (Qian and Papadonikolaki, 2020; Dubey *et al.*, 2020). On the other hand, if BCT limits, constrains or has a non-positive influence on trust, then trust is still required for

information sharing in SCM regardless of applying BCT (Sternberg *et al.*, 2019). This reflects an antecedent nature of trust.

Based on the above discussion, 10 different propositions have been examined through the findings from the systematic literature review. These propositions are based on the different trust objects such as trust in SC partners (which include: openness, credibility and benevolence) and Trust in technology (which includes trust in records and trust in platform). Both the positive and the negative (or non-positive) influences will be discussed separately, to understand how applying BCT influences trust in SC information sharing.

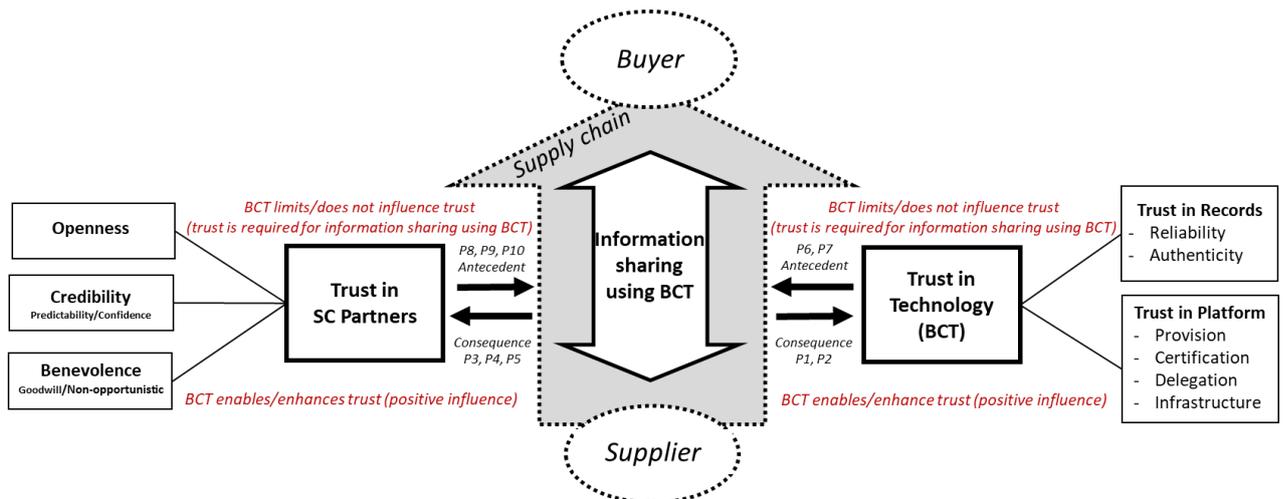


Figure 3 Modified conceptual framework

**P1:** Applying BCT in SCM will enable trust in the technology through trusting the records.

**P1a:** Applying BCT in SCM will ensure data reliability.

**P1b:** Applying BCT in SCM will ensure data authenticity.

In the literature, all 55 (100%) reviewed papers explicitly or implicitly referred to a relationship between

BCT and enabling data reliability or authenticity. In particular, all the reviewed papers (100%) linked data authenticity with BCT features such as decentralised structure, cryptography system and consensus mechanism and sometimes smart contracts. Data reliability, on the other hand, is mostly linked to the smart contract features, as accrued in 41 papers out of 55 (75%), because data reliability

is related to the initial data entry, for which BCT cannot guarantee reliability unless the smart contract is used and linked to the different sensors, radio frequency identification (RFID) or IoT devices.

In particular, RFID and IoT with BCT's smart contract are supposed to be highly reliable because they involve less human interference (Augusto *et al.*, 2019; Chen *et al.*, 2017; Feng, 2017; Figueroa *et al.*, 2019; Sander *et al.*, 2018; Sheel and Nath, 2019). Smart contract in these situations will also help in data authentication (e.g. Dasaklis and Casino, 2019; Rejeb *et al.*, 2019; Sheel and Nath, 2019). Although the distinction between data reliability and authenticity seems to be clear, some papers (e.g. Rejeb *et al.*, 2019; S. Wang *et al.*, 2019; Sternberg *et al.*, 2019) still mix these two concepts.

**P2: Applying BCT in SCM will enable trust in the technology through trusting the platform.**

*P2a: Applying BCT in SCM will enable trust provision.*

*P2b: Applying BCT in SCM will enable trust certification.*

*P2c: Applying BCT in SCM will enable trust delegation.*

*P2d: Applying BCT in SCM will enable trust in the infrastructure.*

Concerning trust provision, 21 out of 55 papers (38%) mentioned that BCT could enhance trust provision without differentiating between BCT's attributes. This is especially with private BCT. As it assumes some level of trust between peers in exchange for limited decentralisation and visibility capabilities; therefore, trust provision is enabled as the trustor could trust the trustee to implement a service not requiring access to all the ledger's data (e.g. Figueroa *et al.*, 2019; Johng *et al.*, 2018; Zhang and Jacobsen, 2018; Saberi *et al.*, 2019; Poumader *et al.*, 2020). In other scenarios, BCT enabled trust provision through IoT to relieve trusted third parties of their data provision duties, as proposed by Notheisen *et al.* (2017) in the case of a trust-free transaction system in the market for used cars (lemons).

For enabling trust certification, 27 out of 55 papers (49%) referred to enabling trust certification either implicitly or explicitly through all BCT attributes in the SCM context. This is in the context of visible and transparent information sharing that allows the provenance and tracking of the transactions to their origin; hence, this works as a certification for the trustee (e.g. Augusto *et al.*, 2019; Chen *et al.*, 2017; Feng, 2017; Figueroa *et al.*, 2019; Rejeb *et al.*, 2019; Zaerens, 2018; Montecchi *et al.*, 2019; Dobler *et al.*, 2019; Malik *et al.*, 2019; Shahid *et al.*, 2020). BCT also offers an opportunity for new entrants to showcase the virtues of their SC (Francisco and Swanson, 2018), which is also applied in vendor-managed inventory (VMI) for increasing trust between manufacturers and their vendors (Dasaklis and Casino, 2019).

In terms of enabling trust through delegation, all the papers that mentioned BCT's smart contract attribute referred to this proposition (75% of reviewed papers). This means BCT is highly expected to enable trust through delegation (e.g. Kamble *et al.*, 2020). However, this is not yet fully deployed in practice (Y. Wang *et al.*, 2019).

All the 55 reviewed papers signalled that BCT will enable trust in the infrastructure in the SCM context. In fact, there is a high expectation from the BCT itself and its

platform to work as promised. However, many of these papers have in the same context mentioned that BCT could also limit the trust in infrastructure due to many issues with scalability as the likely highest concern (Y. Wang *et al.*, 2019). Moreover, some researchers signalled that trust in infrastructure varies depending on the type of BCT whether private or public (e.g. Viriyasitavat *et al.*, 2019).

**P3: Applying BCT will enhance trust in SC partners through openness in information sharing.**

Among the studied papers, 25 (45%) out of 55 mentioned that BCT could enhance openness in information sharing. For VMI, openness in information sharing is considered important to enhance trust in BCT based on all its attributes, including smart contracts (Dasaklis and Casino, 2019). Moreover, Akram and Bross (2018) illustrated that stakeholders in logistics might prefer gaining control over private data, which can enhance trust in terms of information sharing. Other sources simply considered openness in information sharing as a consecutive event caused by applying BCT in the SCM context (Feng, 2017; S. Wang *et al.*, 2019; Zaerens, 2018; Sternberg *et al.* (2019); Fernando *et al.*, 2019; Batwa and Norrman, 2020; Dubey *et al.*, 2020; Qian and Papadonikolaki, 2020).

**P4: Applying BCT in SCM will enhance trust in SC partners through credibility.**

Out of 55 papers, 9 (16%) discussed how BCT can enhance credibility among SC partners. Some researchers, such as Hua *et al.* (2018) and Sander *et al.* (2018), referred to "natural credibility" due to the consensus mechanism, immutability (cryptography system) and peer-to-peer transactions (decentralised structure) that make a tamper-proof system which will stand against any cheating or fraud attempts. Others related credibility to the smart contract attribute in financial transactions as it eliminates the need for a credible third party and creates peer-to-peer transactions (e.g. Norberg, 2019; S. Wang *et al.*, 2019; Shahid *et al.*, 2020; Wan *et al.*, 2020; Howson, 2020).

**P5: Applying BCT in SCM will enhance trust in SC partners through benevolence, goodwill or reducing opportunistic behaviour.**

In terms of enhancing trust through benevolence, only 12 papers out of 55 (22%), have discussed it and it mostly occurred in late 2019 and 2020. The main idea is that BCT attributes construct a "digital trust" that helps prevent SC partners from behaving unethically or opportunistically. Because every transaction in a blockchain builds on every other, any unethical behaviour will be readily visible to the entire network (Y. Wang *et al.*, 2019). Moreover, some researchers such as Shahid *et al.* (2020) impose goodwill through a BCT based reputation system. This can be reflected upon as benevolence or goodwill intentions. In fact, all the remaining papers mentioned this in an implicit way, but the selected papers were more explicit by mentioning "opportunistic behaviours".

**P6:** *Applying BCT in SCM will constrain (or not influence) trust in the technology through limiting trust in the records.*

**P6a:** *Applying BCT in SCM could reduce data reliability.*

**P6b:** *Applying BCT in SCM will limit data authenticity.*

Only 2 papers have discussed that BCT would have any negative influence on trust in the technology through reduction of data authenticity. However, 7 out of 55 papers (13%) have mentioned that BCT could be vulnerable to fraud despite its unique attributes. Some researchers (e.g. Verhoeven *et al.*, 2018) refer that to the act of writing a multitude of fake transactions to build up a credible financial history. He stated that If this data ever went through the BCT's consensus mechanism, the problem could be more complicated (Verhoeven *et al.*, 2018). Other researchers (e.g. Sternberg *et al.*, 2019; Fernando *et al.*, 2019; Garrard and Fielke, 2020; Howson, 2020; Wong *et al.*, 2020) have talked about a garbage in and garbage out (GIGO) problem which is directly related to the reliability definition. Fernando *et al.* (2019) explicitly discussed that even if IoT devices were used, it cannot be blindly trusted, which means data authenticity and reliability through BCT is not fully guaranteed.

**P7:** *Applying BCT in SCM will constrain (or not influence) trust in the technology by limiting trust in the platform.*

**P7a:** *Applying BCT in SCM will limit the trust provision.*

**P7b:** *Applying BCT in SCM will limit the trust certification.*

**P7c:** *Applying BCT in SCM will limit the trust delegation.*

**P7d:** *Applying BCT in SCM will reduce trust in the infrastructure.*

In the reviewed literature, there was no mention of a negative influence for BCT on trust certification. However, BCT was proposed as a constraint to trust provision in only (11%) of the reviewed papers and mostly related to public BCT. This is because the trustor could not control which data were exposed or which SC partner was authorised to enter the network (e.g. Figueroa *et al.*, 2019; Johng *et al.*, 2018; Y. Wang *et al.*, 2019; Saberi *et al.*, 2019; Pearson *et al.*, 2019; Sternberg *et al.*, 2019).

For trust delegation, only 3 papers noted such an occurrence. Dasaklis and Casino (2019) proposed that scaling BCT's smart contract to "one vendor many retailers" or more complex structures might result in high monetary losses and data disclosure, as it could be difficult to manage in the VMI settings. Sternberg *et al.* (2019) and Saberi *et al.* (2019) signalled concerns about the governance mechanisms and how it will limit trust delegation in BCT.

Regarding the negative influence between BCT and trust in the infrastructure, 17 out of 55 papers (31%) suggested that BCT might limit trust in the infrastructure. The main reason cited for limiting trust was scalability of the technology because it had failed in many current projects (Y. Wang *et al.*, 2019; Sternberg *et al.*, 2019) due to slow processing time, among other related technical issues (e.g.

Notheisen *et al.*, 2017; Verhoeven *et al.*, 2018; Saberi *et al.*, 2019; Sternberg *et al.*, 2019), or due to sustainability issues as BCT is a high energy consumption technology (e.g. Saberi *et al.*, 2019; Sternberg *et al.*, 2019; Di Vaio *et al.*, 2020; Kumar *et al.*, 2020). From another point of view, Akram and Bross (2018) stated that BCT could limit trust in a BCT infrastructure because it is based on open source programming, which has many intellectual property concerns. As mentioned before, BCT is still vulnerable to fraud because members could write a multitude of fake transactions (Dasaklis and Casino, 2019; Ghode *et al.*, 2020; Rogerson and Parry, 2020), which could also limit the trust in the BCT infrastructure.

**P8:** *Applying BCT will constrain (or not influence) trust in SC partners by limiting the openness of information sharing.*

Fifteen of the reviewed papers (27%) mentioned that BCT will limit the openness of information sharing due to privacy concerns (e.g. Augusto *et al.*, 2019; Hua *et al.*, 2018; Sternberg *et al.*, 2019; Garrard and Fielke, 2020; Behnke and Janssen, 2020). The data uploaded by the participating companies will be visible to all other participants, which means that some of the data considered as trade secrets will also be available to others. For instance, large meat providers who compete on a cost basis are unlikely to have an interest in sharing their trade secrets regarding how their animals have been farmed, slaughtered and processed (Sander *et al.*, 2018). Although this could be avoided by using authorisations, the usage is very limited in public BCT (Hua *et al.*, 2018). Moreover, publishing sensitive and private data in a public blockchain can lead to serious legal consequences for organisations, especially after the introduction of the General Data Protection Regulation (GDPR) (Akram and Bross, 2018).

**P9:** *Applying BCT in SCM will constrain (or not influence) trust in SC partners through limiting credibility.*

**P10:** *Applying BCT in SCM will constrain (or not influence) trust in SC partners through limiting benevolence, goodwill or increasing opportunistic behaviour.*

None of the reviewed papers have discussed the limiting influence of BCT on trust credibility, and only 4 (7%) have discussed limiting influence on benevolence. Y. Wang *et al.*, 2019 predicted that future honest behaviour is impossible because there is no central authority to police or enforce honesty in a blockchain-enabled SC. Other researchers such as: Longo *et al.* (2019), Rogerson and Parry (2020), and Shahid *et al.* (2020) have shown concerns that BCT might increase opportunistic behaviours since the data could be blindly trusted. Indeed, this can be reflected on both the credibility and benevolence aspects, and hence the two propositions are discussed together in this situation. **Table 5** summarises all propositions and their references.

**Table 5** Research propositions and their references

List of articles	P1		P2				P3	P4	P5	P6		P7				P8	P9	P10
	P1a	P1b	P2a	P2b	P2c	P2d				P6a	P6b	P7a	P7b	P7c	P7d			
Chen <i>et al.</i> (2017)	x	x		x	x	x												
Feng (2017)	x	x		x	x	x	x								x			
Augusto <i>et al.</i> (2019)	x	x		x	x	x									x	x		
Figueroa <i>et al.</i> (2019)	x	x	x	x	x	x						x						
Wang,S <i>et al.</i> (2019)	x	x		x	x	x	x	x										
Kshetri and Loukoianova (2019)		x				x												
Hua <i>et al.</i> (2018)	x	x			x	x		x								x		
Anjum <i>et al.</i> (2017)		x				x												
Zaerens (2018)	x	x	x	x	x	x	x									x		
Benčić <i>et al.</i> (2019)	x	x	x		x	x												
Verhoeven <i>et al.</i> (2018)		x				x					x	x				x		
Tseng <i>et al.</i> (2018)	x	x			x	x												
Dasaklis and Casino (2019)	x	x	x	x	x	x	x							x	x			
Arumugam <i>et al.</i> (2018)	x	x			x	x												
Rejeb <i>et al.</i> (2019)	x	x		x	x	x												
Francisco and Swanson (2018)	x	x		x	x	x												
Kshetri and Voas (2019)		x				x												
Sander <i>et al.</i> (2018)	x	x			x	x		x								x		
Hawlitschek <i>et al.</i> (2018)	x	x			x	x												
Fernández-Caramés <i>et al.</i> (2019)	x	x			x	x												
Zhang and Jacobsen (2018)	x	x	x		x	x												
Notheisen <i>et al.</i> (2017)	x	x	x		x	x									x			
Westerkamp <i>et al.</i> (2019)	x	x			x	x												
Norberg (2019)		x				x		x										
Wang, Y. <i>et al.</i> (2019)	x	x			x	x			x								x	
Kamble <i>et al.</i> (2018)	x	x			x	x												
Johng <i>et al.</i> (2018)	x	x	x		x	x						x						
Akram and Bross (2018)	x	x		x	x	x	x								x	x		
Saberi <i>et al.</i> (2019)	x	x	x	x	x	x	x		x			x	x	x	x	x		
Pearson <i>et al.</i> (2019)	x	x	x	x	x	x						x				x		
Longo <i>et al.</i> (2019)	x	x	x	x	x	x	x		x	x						x	x	
Sheel and Nath (2019)	x	x	x		x	x	x		x									
Galvez <i>et al.</i> (2018)	x	x	x		x	x			x							x		
Montecchi <i>et al.</i> (2019)	x	x		x		x												
Dobler <i>et al.</i> (2019)		x		x	x	x									x	x		
Stemberg <i>et al.</i> (2019)		x	x	x	x	x	x	x	x	x		x	x	x	x	x		
Fernando <i>et al.</i> (2019)		x				x	x					x	x					
Malik <i>et al.</i> (2019)	x	x	x	x	x	x	x											
Viriyasitavat <i>et al.</i> (2019)	x	x	x		x	x			x							x		
Ghode <i>et al.</i> (2020)	x	x				x	x		x							x		
Yong <i>et al.</i> (2020)		x				x												
Batwa and Norman (2020)	x	x	x	x	x	x	x	x										
Pournader <i>et al.</i> (2020)	x	x	x	x	x	x												
Shahid <i>et al.</i> (2020)	x	x	x	x	x	x	x	x	x								x	
Rogerson and Parry (2020)		x		x	x	x	x									x	x	
Wan <i>et al.</i> (2020)	x	x				x	x	x	x									
Garrard and Fielke (2020)		x		x		x	x		x	x						x	x	
Dubey <i>et al.</i> (2020)	x	x	x	x	x	x	x											
Di Vaio <i>et al.</i> (2020)		x				x	x									x		
Behnke and Janssen (2020)	x	x				x	x										x	
Howson (2020)		x		x		x	x	x			x							
Kumar <i>et al.</i> (2020)		x	x	x	x	x	x									x	x	
Kamble <i>et al.</i> (2020)	x	x		x	x	x	x											
Qian and Papadonikolaki (2020)	x	x	x	x	x	x	x		x									
Wong <i>et al.</i> (2020)	x	x				x	x				x							
<b>Total</b>	41	55	21	27	41	55	25	9	12	7	2	6	2	3	17	15	0	4
<b>%</b>	75%	100%	38%	49%	75%	100%	45%	16%	22%	13%	4%	11%	4%	5%	31%	27%	0%	7%

## 5. CONCLUSION AND DISCUSSION

Trust is a multidimensional intangible concept that gets even more difficult to measure in complex SCs (Kshetri and Voas, 2019; Panayides and Lun, 2009). The aim of this study was to understand the role of BCT as it relates to trust in

SCM and propose a corresponding research agenda. The study follows, for example, Seppänen *et al.* (2007), and concludes that trust has a two-sided reciprocal nature that is also evident when considering BCT in SCM. In previous research, conflicting views have emerged regarding whether trust is a main driver for applying BCT (Peck, 2017), whether

BCT could create a trust-free environment (Y. Wang *et al.*, 2019) or whether BCT could negatively limit trust between SC partners (Hua *et al.*, 2018; Sander *et al.*, 2018). The conducted literature review answered the two main research questions, which will be discussed in this section followed by the research contribution and limitations. Finally, an agenda for future research is outlined.

First, to answer RQ1—*How is trust operationalised and discussed in the articles that addressed supply chain management and blockchain technology?*—seven sub-questions were generated as lenses for analysing the literature. The results were disappointing, but not altogether surprising. Only few of the reviewed articles performed operationalisation to measure trust in BCT and the SCM context. Also, there is no mention of trust development over time. Only Three papers mentioned classes of trust, but it either referred to the phrase in the sharing economy context or limited SCM context such as construction. Further, very few articles defined trust before discussing it (11%) or trying to connect trust to previous frameworks or concepts (15%). While the theory of acceptance (UTAUT) model and an extended blockchain framework were used, few studies relied on established frameworks from domains where trust has been researched for an extended period (e.g., psychology, social psychology, sociology, economics and management). In the BCT literature, most of the proposed implications related to trust were driven from ideas or suggestions rather than empirical studies. In general, the reviewed articles showed that trust is usually discussed in relation to the reliability of information provided by trade partners or in relation to the safety and security of the data managed by a central authority. Thus, our study proved a great gap in the current literature in linking BCT and trust theories in a SCM context.

Second, to answer RQ2—*How can blockchain technology influence trust in supply chain management?*—a conceptual framework was used based on trust theories to reflect on BCT in SCM. The framework was modified when reviewing the literature to uncover the relation between trust and BCT in SCM. The framework highlighted the reciprocal nature of trust, as trust can be both a consequence and an antecedent of applying BCT. This reciprocal nature is reflected by BCT’s both enhancing and constraining influences on trust in SCM. A sort of consent was found in the literature on the enhancing influence of applying BCT in SCM in terms of trusting the technology records (data authenticity and data reliability) as well as trusting in the technology platform (trust in infrastructure and trust delegation through smart contracts). However, there was less agreement on trust provision and trust certification. In terms of trust in SC partners, there are fewer signals that BCT can enable credibility, benevolence or openness in information sharing. On the other hand, BCT has a constraining influence when it comes to trust in SC partners, especially in the openness of information sharing due to privacy concerns that are more common in public blockchains. Moreover, trust in the infrastructure can also be limited by applying BCT. In fact, some of the articles that proposed the enabling influence of BCT on infrastructure’s trust also proposed the opposite, especially when BCT is scaled up; it becomes difficult to handle it.

In general, it is very difficult and complex to find a single answer on the reciprocal nature or the influences of

BCT on trust. However, based on the results of this study, trust is highly expected as a consequence for BCT if trust in the technology is under consideration. At the same time, trust is highly expected to be an antecedent for applying BCT in terms of trust in SC partners represented by openness of information sharing.

## 6. CONTRIBUTION, FUTURE RESEARCH AND LIMITATIONS

This study contributes to the research field by clearly pointing out the lack of theoretical underpinning for statements regarding BCT and trust and SCM given in the current literature. The research also extends the ongoing general discussion of trust in the operations management/SCM domain by exploring it in the context of the novel phenomenon BCT. A contribution is the clearly identified gap between BCT and trust theories in the SCM context, which could be used to develop an agenda for future research.

Practitioners would also benefit from this study to understand the relation between trust and BCT especially that trust is not an easy concept as shown in this paper. BCT merged between the freedom of the Internet and the security of cryptography to provide a new way to verify crucial information and hence establish trust. In this paper, it was shown through ten propositions that BCT might change the way SC partners trust each other and trust the technology. This could help organisations appraise precisely what BCT can provide and what change is required to gain the maximum value from investment in the technology.

In the future, a great deal of rigorous research is needed to extend our understanding of the reciprocal interrelation between trust and BCT in SCM, especially empirically grounded research, which will influence the suggested agenda for future research through three points. **First**, future research should explicitly define and operationalise their view of trust. **Secondly**, the ten propositions outlined in this study could be empirically explored and tested, for example, by qualitative case studies and later with large-scale quantitative surveys when there are enough in-the-field implementations of BCT in SCM. **Third**, the modified framework could be both challenged and further developed while also guiding future research in unpacking and understanding the complex and unclear concept of trust. Indeed, formulating theories of new phenomena starts with accumulated knowledge from previous frameworks as well as inductive and qualitative observations of practice. The framework can be used in three major ways for future studies:

### i) Support answering explanatory questions that involve “What?” and “How?”

The developed ten propositions for future research focus on what *objects of trust* (e.g., trust in persons, organisations or technology) will be enabled or constrained through different *sub-dimensions of trust* (e.g. credibility, openness, benevolence or goodwill) and by *BCT different attributes* (e.g. by the decentralised structure, the cryptography system, the consensus mechanism or smart contracts). However, more overriding future research questions could be added to those propositions, such as the following:

- What objects of trust are most important for BCT in SCM, and why?
- What sub-dimensions of trust are most important for BCT in SCM, and why?
- What is the temporal development of trust when implementing BCT in SCM?
- How can BCT support a temporal development of trust in SCM?

**ii) Guide predictive questions “e.g. can BCT eliminate the need of trust”?**

An interesting predictive question is whether BCT will replace current trust practices in SCs, or to what extent that can be possible. Or can BCT completely eliminate the need of trust? While this indeed is one of the main promises of BCT, future empirical research could analyse if this promise can be delivered, and, if so, how the dynamics between buyer-supplier relationships will look like when there is no dire need for trust? Lastly, how it will affect the performance of the SC? However, to answer these questions, trust must first be operationalised so it can be measured before and after applying BCT. This might involve breaking trust into its different dimensions.

**iii) Help formulate action-oriented research questions “e.g. which governance mechanisms, polices and standards are needed”?**

While questions focusing on explanation and prediction provide theoretical answers, design or action-oriented questions tend to be more practical. Future research in this direction could study and develop BCT solutions that reduce the levels of trust needed in SC partners and design the necessary governance mechanisms, polices and standards.

As in all research, this study has limitations. Due to the novelty of the discussed topic, few cases in the market have implemented BCT on a large scale, which limits this research to a literature review. That limitation leads to the question of whether the results are complete and representative of the current situation. However, since most of the reviewed articles were published in the past two years, the current situation are therefore represented with better accuracy.

## REFERENCES

- Adler, P.S., Borys, B., (1996). Two types of bureaucracy: enabling and coercive”, *Administrative Science Quarterly*, 41 (1), 61-89.
- Akram, A., Bross, P., (2018) Trust, privacy and transparency with block-chain technology in logistics, *proceeding the 12th Mediterranean Conference on Information Systems*, Corfu, Greece.
- Anderson, J. C., Narus, J. A., (1990). A Model of Distributor Firm and Manufacturer Firm Working Partnerships” *Journal of Marketing*, 54 (1), 42–58.
- Anjum, A., Sporny, M., Sill, A., (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing*, 4 (4), 84-90.
- Arumugam, S., Umashankar, V., Narendra, N., Badrinath, R., Mujumdar, A., Höller, J. Herranz, A., (2018) IOT enabled smart logistics using smart contracts, *Proceedings of the 2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS)*, Toronto, Canada, 1-6.
- Augusto, L., Costa R., Ferreira, J., Jardim-Gonçalves, R., (2019) An application of Ethereum smart contracts and IoT to logistics, *Proceedings of the 2019 International Young Engineers Forum (YEF-ECE)*, Costa da Caparica, Portugal, 1-7.
- Batwa, A. , Norrman, A. (2020). A Framework for Exploring Blockchain Technology in Supply Chain Management. *Operations and supply chain management*, 13 (3), 294-306.
- 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.
- Benčić, F.M., Skočir P., Žarko, I.P., (2019). DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. *IEEE Access*, 7(1), 46198-46209.
- Carnevale, D.G., Wechsler, B., (1992). Trust in the public sector: Individual and organizational determinants. *Administration & Society*, 23 (4), 471-494.
- Chen, S., Shi, R., Ren, Z., Yan, J., Shi, Y., Zhang, J., (2017) A blockchain-based supply chain quality management framework, in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, New York, USA, 172-176.
- Dasaklis T., Casino, F., (2019) Improving Vendor-managed Inventory Strategy Based on Internet of Things (IoT) Applications and Blockchain Technology, In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South), 50-55.
- 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.
- Dobler, M., Ballandies, M. , Holzwarth, V. (2019) On the Extension of Digital Ecosystems for SCM and Customs with Distributed Ledger Technologies. *2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*.
- Doney, P. M., Cannon, J. P., (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, 61 (2), 35–51.
- 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.
- Dyer, J.H. Chu, W., (2003). The role of trustworthiness in reducing transaction costs and improving performance: empirical evidence from the United States, Japan and Korea. *Organization Science*, 14 (1), 57-68.
- Fawcett, S.E., Jin, H.Y., Fawcett, A.M., Magnan, G., (2017). I know it when I see it: the nature of trust, trustworthiness signals, and strategic trust construction. *The International Journal of Logistics Management*, 28 (4), 914-938.
- Fawcett, S.E., Jones, S.L., Fawcett, A.M., (2012). Supply chain trust: The catalyst for collaborative innovation. *Business Horizons*, 55(2), 163-178.
- Feng T., (2017) A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things, *Proceedings of the International Conference on Service Systems and Service Management*, Dalian, China, 1-6.
- Fernández-Caramés, T. M., Blanco-Novoa, O., Froiz-Míguez, I., Fraga-Lamas, P., (2019). Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management. *Sensors*, 19 (10), 2394.
- Fernando, E., Meyliana , Surjandy. (2019) Success Factor of Implementation Blockchain Technology in Pharmaceutical Industry: A Literature Review. *proceedings of the 2019 6th Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE)*, Semarang, Indonesia Semarang, Indonesia.
- Figuroa, S., Añorga, J., Arrizabalaga, S., (2019). An Attribute-Based Access Control Model in RFID Systems Based on Blockchain Decentralized Applications for Healthcare Environments. *Computers*, 8 (3), 57.

- Francisco, K., Swanson, D. (2018). "The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*, 2 (1), 2-3.
- Gahtgens, F., Allan, A., (2017). Digital trust: Redefining trust for the digital era, *Gartner trend insight report*. Available at: [www.gartner.com/doc/3735817/digital-trust-redefining-trust](http://www.gartner.com/doc/3735817/digital-trust-redefining-trust) [Accessed 10 July 2019].
- Galvez, J. F., Mejuto, J. C. , Simal-Gandara, J. (2018). Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in Analytical Chemistry*, 107, 222-232.
- Ganesan, S. (1994). Determinant of long-term orientation in buyer - seller relationships. *Journal of Marketing*, 58 (2), 1–19.
- Garrard, R. , Fielke, S. (2020). Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry. *Technology in Society*, 62.
- Gassenheimer, J.B., Manolis, M., (2001). The Influence of Product Customization and Supplier Selection on Future Intentions: The Mediating Effects of Salesperson and Organizational Trust. *Journal of Managerial Issues*, 13 (4), 418-435.
- 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.
- Grandison, T., Sloman, M., (2002) Specifying and analyzing trust for internet applications, *Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government*, Lisbon, Portugal.
- Hald, K., Kinra, A., (2019). How the blockchain enables and constrains supply chain performance. *International Journal of Physical Distribution & Logistics Management*, 49 (4), 376-397.
- Handfield, R.B., Bechtel, C. (2002). The role of trust and relationship structure in improving supply chain responsiveness. *Industrial Marketing Management*, 31 (4), 367-382.
- Hawlichschek, 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 (1), 50-63.
- Howson, P. (2020). Building trust and equity in marine conservation and fisheries supply chain management with blockchain. *Marine Policy*, 115.
- Hua, J., Wang, X., Kang, M., Wang, H., Wang, F., (2018) Blockchain Based Provenance for Agricultural Products: A Distributed Platform with Duplicated and Shared Bookkeeping, *Proceeding of the 2018 IEEE Intelligent Vehicles Symposium (IV)*, Changshu, China, 97-101.
- Iansiti, M., Lakhani, K.R. (2017). The truth about blockchain. *Harvard Business Review*, 118-127.
- Johng, H., Kim, D., Hill, T. Chung, L., (2018) Using Blockchain to Enhance the Trustworthiness of Business Processes: A Goal-Oriented Approach, *Proceeding of the IEEE International Conference on Services Computing (SCC)*, San Francisco, CA, USA, 249-252.
- Johnston, D.A., McCutcheon, D.M., Stuart, F., Kerwood, H., (2004). Effects of supplier trust on performance of cooperative supplier relationships. *Journal of Operations Management*, 22(1), 23-28.
- Kamble, S. S., Gunasekaran, A. , Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International Journal of Information Management*, 52.
- 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.
- Kembro, J., Naslund, D., Olhager, J., (2017). Information sharing across multiple supply chain tiers: A Delphi study on antecedents. *International Journal of Production Economics*, 193 (1), 77-86.
- Khan, H., Wisner, J.D., (2019). Supply chain integration, learning, and agility: effects on performance. *Operations and Supply Chain Management*, 12 (1), 14-23.
- Kshetri N., Voas, J., (2019). Supply Chain Trust. *IT Professional*, 21 (2), 6-10.
- Kshetri, N., Loukoianova, E., (2019). Blockchain Adoption in Supply Chain Networks in Asia. *IT Professional*, 21 (1), 11-15.
- 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.
- Kwon, I. and Suh, T., (2005). Trust, commitment and relationships in supply chain management: a path analysis, *Supply Chain Management*, 10 (1), 26-33.
- Lewicki, R.J., Bunker, B.B. (1995). Trust in relationships: A model of development and decline. In B. B. Bunker & J. Z. Rubin (Eds.), *The Jossey-Bass management series and The Jossey-Bass conflict resolution series. Conflict, cooperation, and justice: Essays inspired by the work of Morton Deutsch*, 133-173, San Francisco, CA, USA.
- Lewis, D., Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, 63 (4), 967-985.
- Li, J., Greenwood, D., Kassem, M. (2019). Blockchain in the built environment and construction industry: a systematic review, conceptual models and practical use cases, *Automation in Construction*, 102, 288-307.
- Li, Z., Wu, H., King, B., Miled, Z. B., Wassick, J., Tazelaar, J., (2017) On the integration of event-based and transaction-based architectures for supply chains, in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops*, New York, USA, 376-382.
- 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.
- Loop, P., (2016). Blockchain: the next evolution of supply chains, *Material Handling & Logistics, Industry week*, 22-24.
- Lu, Y., Zhao, L., Wang B. (2010). From virtual community members to c2c e-commerce buyers: Trust in virtual communities and its effect on consumers' purchase intention. *Electronic Commerce Research and Applications*. 9 (4), 346–360.
- Mak, B. (2014). Authenticity, in Duranti L. and Franks P., *Encyclopedia of Archival Science*, Rowman & Littlefield, NY, USA.
- Malik, S., Dedeoglu, V., Kanhere, S. S. , Jurdak, R. (2019). TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains. *2019 IEEE International Conference on Blockchain (Blockchain)*.
- Mansouribakvand, G. (2019). *The impact of blockchain technology on trust in the supply chain*. M.S. thesis, Engineering Logistics, Lund University, Sweden.
- Martinez, V., Zhao, M., Blujdea, C., Han, X., Neely, A. and Albores, P. (2019), Blockchain-driven customer order management. *International Journal of Operations & Production Management*, 39 (1), 993-1022
- Mayer, R.C., Davis, J.H., Schoorman, F. D., (1995). An integrative model of organizational trust. *Academy of Management Review*, 20 (3), 709-734.
- McKnight, D., Chervany, N., (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, 6 (2), 35-59.
- Michalski, M., Montes, J., Narasimhan, R., (2019). Relational asymmetry, trust, and innovation in supply chain management: a non-linear approach. *International Journal of Logistics Management*, 30 (1), 303-328.
- Miles, M.B., Huberman, A.M., (1994). *Qualitative Data Analysis- An Expanded Sourcebook*, Sage, London.

- Montecchi, M., Plangger, K., Etter, M. (2019). It's real, trust me! Establishing supply chain provenance using blockchain. *Business Horizons*, 62 (3), 283-293.
- Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 2 January 2019].
- Narasimhan, R., Nair, A. (2005). The antecedent role of quality, information sharing and supply chain proximity on strategic alliance formation and performance. *International Journal of Production Economics*, 96 (3), 301-313.
- Norberg, H.C. (2019). Unblocking the Bottlenecks and Making the Global Supply Chain Transparent: How Blockchain Technology Can Update Global Trade. *The School of Public Policy Publications*, 12 (9). Available at <https://ssrn.com/abstract=3353818> [Accessed 10 July 2019].
- 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 and Information Systems Engineering*, 59 (6), 425-450.
- Panayides, P. M., Venus Lun, Y.H., (2009). The impact of trust on innovativeness and supply chain performance. *International Journal of Production Economics*, 122 (1), 35-46.
- Pearson, S., May, D., Leontidis, G., Swainson, M., Brewer, S., Bidaut, L., Frey, J. G., Parr, G., Maull, R., Zisman, A. (2019). Are Distributed Ledger Technologies the panacea for food traceability? *Global Food Security*, 20, 145-149.
- Peck, M.E., (2017). Blockchain world - Do you need a Blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectrum*, 54 (10), 38-60.
- Pereira, C.R., Christopher, M. and Lago Da Silva, A., (2014). Achieving supply chain resilience: the role of procurement. *Supply Chain Management: An International Journal*, 19 (5), 626-642.
- Plank, R. E., Reid, D. A., Pullins, E. B., (1999). Perceived trust in business-to-business sales: A new measure. *Journal of Personal Selling and Sales Management*, 19 (3), 61– 71.
- Pournader, M., Shi, Y., Seuring, S., Koh, S. C. L. (2019). Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. *International Journal of Production Research*, 58 (7), 2063-2081.
- Qian, X., Papadonikolaki, E. (2020). Shifting trust in construction supply chains through blockchain technology. *Engineering, Construction and Architectural Management*, ahead-of-print (ahead-of-print).
- Queiroz, M., Telles, R. and Bonilla, S., (2019). Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management*, ahead-of-print.
- Rejeb, A., Keogh, J.G., Treiblmaier, H., (2019). Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Internet*, 11 (7), 161-183.
- Rogerson, M., Parry, G. C. (2020). Blockchain: case studies in food supply chain visibility. *Supply Chain Management: An International Journal*, 25 (5), 601-614.
- Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C., (1998). Not so different after all: across discipline view of trust. *Academy of Management Review*. 23 (3), 393–404.
- Roy, S., Sivakumar K., Wilkinson, I.F., (2004). Innovation generation in supply chain relationships: a conceptual model and research propositions. *Journal of the Academy of Marketing Science*, 32 (1), 61-79.
- 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.
- Sahay, B.S., (2003). Understanding trust in supply chain relationships. *Industrial Management and Data Systems*, 103(8), 553-63.
- Sander, F., Semeijn, J., Mahr, D., (2018). The acceptance of blockchain technology in meat traceability and transparency. *British Food Journal*, 120 (9), 2066-2079.
- Seppänen R., Blomqvist, K., Sundqvist, S., (2007). Measuring inter-organizational trust – a critical review of the empirical research in 1990-2003. *Industrial Marketing Management*, 36, (2), 249-265.
- Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F. A., Zuair, M., Alam, M. (2020). Blockchain-Based Agri-Food Supply Chain: A Complete Solution. *IEEE Access*, 8, 69230-69243.
- Shapiro, S., (1987). The social control of impersonal trust. *American Journal of Sociology*, 93 (3), 623-658.
- 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.
- So, M.C., Schill, D. (2002). The role of trust, quality, value and risk in conducting e-business. *Industrial Management & Data Systems*, 102 (9), 503-512.
- Sternberg, H. S., Hofmann, E., Roeck, D. (2020). The Struggle is Real: Insights from a Supply Chain Blockchain Case. *Journal of Business Logistics*.
- Tachizawa, E.M. and Wong, C.W. (2014). Towards a theory of multi-tier sustainable supply chains: a systematic literature review. *Supply Chain Management: An International Journal*, 19 (5), 643-663.
- Tranfield, D., Denyer, D., Smart, P., (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14 (3), 207-222.
- 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.
- Tseng, J., Liao, Y., Chong, B., Liao, S., (2018). Governance on the Drug Supply Chain via Gcoin Blockchain. *International Journal of Environmental Research and Public Health*, 15 (6), 1055.
- 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), 829-859.
- Verhoeven, P., Sinn, F., Herden, T., (2018). Examples from Blockchain Implementations in Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology. *Logistics*, 2 (3), 20.
- Viriyasitavat, W., Anuphaptrirong, T., Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *Journal of Industrial Information Integration*, 15, 21-28.
- 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.
- Wang, S., Tang, X. Zhang, Y., Chen, J., (2019). Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts. *IEEE Access*, 7, 109439-109453.
- Wang, Y., Han, J., Beynon, D.P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management*, 24 (1), 62-84.
- Westerkamp, M., Friedhelm, V., Küpper, A., (2019) Tracing manufacturing processes using blockchain-based token compositions, *Digital Communications and Networks*.
- Whipple, J.M., Lynch, D.F., Nyaga, G.N., (2010). A buyer's perspective on collaborative versus transactional relationships. *Industrial Marketing Management*, 39 (3), 507–518.
- 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.
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., (2016). Where is current research on blockchain technology? A systematic review. *PLOS ONE*, 11 (10).
- 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.
- Zaerens, K., (2008). Concept for Controlled Business Critical Information Sharing Using Smart Contracts. *Proceeding of the 2018 2nd Cyber Security in Networking Conference (CSNet)*, Paris, France, 1-8.
- Zhang, K. and Jacobsen, H., (2018) Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. *Proceeding of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, 1337-1346.

---

**Abbas Batwa** is a PhD. Student at the Faculty of Engineering in Lund University, Sweden. He is also a teaching assistant at the department of Industrial Engineering at King Abdul-Aziz University, Saudi Arabia. Currently he is on a scholarship as a PhD. Candidate. He has a double major MSc. Degrees in Industrial Engineering from King Abdul-Aziz University and in Logistics and Supply Chain Management from Lund University. Abbas has a working background as a logistics manager in Toyota's largest spare parts warehouse in the Middle-East region. His research interests are in reverse logistics, industry 4.0 applications, and utilizing technology innovations such as Blockchain for optimizing logistics and supply chain operations.

**Andreas Norrman** is Professor in Supply chain structure and organization at Lund University, Faculty of Engineering, Sweden. He has a Ph.D. in logistics from Linköping University, Sweden. Andreas has worked as a management consultant at A.T.Kearney with supply chain management and sourcing issues. His research interests include Omni-channel warehousing, Supply chain risk management, Supply chain incentive alignment, Change management and Blockchain. He publishes in leading logistics journal and he received multiple Emerald Highly Commended Awards for his work with IJPD&LM, both as author and reviewer. At Lund University he has been awarded Excellent Teaching Practice. He is a fellow of the Royal Physiographic Society of Lund (the Academy for the Natural Sciences, Medicine and Technology), he serves since many years as Senior Associate Editor for IJPD&LM and is newly appointed Senior Editor for JBL.