UNDERSTANDING THE INFLUENCE BETWEEN BLOCKCHAIN TECHNOLOGY AND TRUST IN SUPPLY CHAIN MANAGEMENT: A LITERATURE REVIEW

Abbas Batwa
Lund University,
Sweden, E-mail: abbas.batwa@tlog.lth.se

Andreas Norrman
Lund University,
Sweden, E-mail: andreas.norrman@tlog.lth.se

ABSTRACT

Applying Blockchain Technology (BCT) for information sharing in the supply chains is driven by many factors, but developing trust is one of the most proposed. Trust is a multidimensional intangible concept without clear agreement of what it constitutes, and its meaning get even more confused in a supply chain management (SCM) context. The purpose of this paper is to understand how applying BCT in SCM can influence trust. In the literature, there are some findings that address trust and BCT but they are very scattered, only some related to SCM but many related to financial applications. Thus, our method used is a systematic literature review, based on a conceptual framework of trust we developed. We discovered a great gap in linking trust (and related theories) to BCT applications in SCM. This paper gave insights on the reciprocal nature of trust as well as the influence of applying BCT in SCM. In current literature, trust is highly expected as a consequence for BCT if we are considering trust in the technology. 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. Important future research agenda is to enrich the results by using empirical studies.

Keywords: Blockchain Technology, Supply Chain, Trust.

1. INTRODUCTION

Blockchain Technology (BCT) is an innovation that challenges the traditional businesses. The main BCT characteristics that brings its novelty are decentralized 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-Huumo *et al.*, 2016). Considering such characteristics, applying BCT in SCM would be driven by many factors, but trust is one of the most discussed (Wang.Y *et al*., 2019).

Trust is a multidimensional intangible concept without clear agreement of what it constitutes, and its meaning gets even more confused in a SCM context due to the difficulty of its measuring, especially in large and complex supply chains (SC) (Kshetri and Voas, 2019). Even so, many studies have proven that incorporating high level of trusted relationships can lead to a higher performance in logistics and SCM (Johnston *et al*., 2004; Li *et al*., 2007; Narasimhan and Nair, 2005). Indeed, trust is seen vital for effectively implementing collaborations, and has for example

been found to be the key reason behind the success of many Japanese automakers (Dyer and Chu, 2003). This is because the trustworthy collaboration assures that SC parties understand each other's business and assist each other in developing innovative solutions (Li *et al.*, 2007; Roy *et al*., 2004; Khan and Wisner, 2019). Moreover, some researchers like Daugherty *et al*., (2006) and Ghosh and Fedorowicz (2008) argued that trust and collaboration are essential to realize the full benefits of many SC systems such as CPFR and VMI. According to Fawcett *et al*., (2012), trust is at the heart of a collaborative innovation capability.

Trust has in different disciplines been discussed according to different types, development stages, and having different dimensions (McKnight and Chernavy, 2001; Seppänen *et al*., 2007; Whipple *et al*., 2013). In the SCM context, trust can be for example: personal, interpersonal, inter-organizational, or relating to the technology platform. The purpose of this paper is to understand how applying BCT in SCM can influence trust. In the literature, there are some findings about trust and BCT, but they are very scattered, some related to SCM and many related to financial applications (Fernández-Caramés *et al*., 2019). Some researchers argued that trust is the main driver for applying BCT (Peck, 2017). Others have introduced the concept of "digital trust" that claims to change the traditional ways of dealing with trust business. (Gaehtgens and Allan, 2017). However, in the middle of this BCT hype, there are some concerns that BCT could negatively limits trust among the SC partners due to the high level of visibility in information sharing that could harm organizational privacy especially with sensitive data (Hua *et al*., 2018; Sander *et al*., 2018). Yet, to develop a robust understanding, trust itself must be further understood and two main questions has been set for this study.

RQ1: *How is trust operationalized 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?*

The first RQ investigates how trust has been discussed in the current literature, while the second RQ will provide deeper understanding of the role of BCT related to trust in the SCM context. The next 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. Third, the findings and research propositions will be discussed. Finally a conclusion will summarize the work, its contribution and limitations, and give suggestions for future research.

2. THEORETICAL BACKGROUND

Since BCT is still a novel technology that is not yet fully discovered, we will first give a short theoretical background explaining BCT and its attributes. After that, trust will be discussed from different perspectives to unpack the concept. At last, a conceptual framework that connects between different sub-dimensions of trust with BCT and SCM will be provided and discussed.

2.1 Blockchain Technology and Supply Chain Management

The literature lacks one unified definition of the BCT but almost all researches tend to define it according to its unique characteristics (e.g. Yli-Huumo *et al.*, 2016; Iansiti and Lakhani, 2017). One of the latest definitions of BCT is proposed by Treiblmaier (2018): "*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 beside a brief of the technology itself. Accordingly, four attributes can be

constructed and defined: decentralized structure, cryptography system, consensus mechanism and smart contract (Hald and Kinara, 2019).

BCT has two main types that are permission-less (public) and permissioned (private) blockchains. In public blockchains, the digital ledger is completely decentralized, and it can be accessed by any internet user which may put sensitive information under risk of exposure. On the other hand, private blockchains allow only preselected and limited number of participants 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 the level of access provided to members (Hald and Kinara, 2019).

In the SCM context, there are many drivers for applying BCT. According to Wang.Y *et al*., (2019), there are four main drivers for applying BCT in SCM. The first and most influencing 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 supply chain disconnections and complexities that are driven from lack of real time visibility. Then, product safety, legitimacy and authenticity are the third drivers since BCT provides information with a provenance features so products can be traced to its origin. The final driver is the need for increased public safety and anti-corruption that can be provided through BCT as its consensus and immutability features works well against frauds and counterfeited products or behaviors (Wang.Y *et al*., 2019). Moreover, different applications of BCT were seen in different SCM areas. According to the same study by Wang.Y *et al*. (2019), extended visibility and products traceability is the main and most deployed application. BCT provide a temporal records of all transactions along with other related product specifications such as sender, receiver, temperature, foot print and so on. Additionally, with installed sensors and Internet of things (IOT) devices, a real time visibility can be achieved which will drive tracking and tracing applications into a next level (Wang.Y *et al*., 2019; Li *et al*., 2017).

2.2 Inter-organizational trust

There has lately been research focusing on at understanding and conceptualizing trust in SCM (e.g. Michalsi *et al*., 2018; Fawcett *et al*., 2017; Whipple *et al*.,2013; Fawcett *et al*., 2012; Kwon and Suh, 2005; Sahay, 2003). But there is still a lack of agreement of what constitutes trust, and there is no generally accepted definition.

The inter-organizational context of trust has been studied from many different disciplines and perspectives (McKnight and Chernavy, 2001; Seppänen *et al*., 2007: Whipple *et al*., 2013). The common observation is that trust, and especially inter-organizational trust, is a vague, multidimensional and complex construct to unpack as there are many different aspects of it. Every discipline also tend to view trust from its own perspective and not understanding or appreciating the view of others (McKnight and Chervany, 2001). Thus, to reduce its ambiguity, trust will now be discussed from different perspectives such as the reciprocal nature of trust, the objects, classes, temporal development and the sub-dimensions of trust.

2.2.1 Reciprocal nature of trust

One reason for the ambiguity and confusion of trust is its two-sided reciprocal nature, leading to unclear causality (Seppänen *et al*., 2005). Trust could be seen either as a cause or effect related to certain aspects (e.g. cooperation, communication, and performance). This makes it hard to define what is antecedents, dimensions or consequences of trust. Among SCM researchers we find examples where 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-organizational information sharing (Handfield, 2002; Kembro *et al*, 2017).

2.2.2 Objects of trust

A second reason is that trust could relate to different "objects of trust" (Seppänen *et al*. 2007) such as kind of relationships for example: *interpersonal* (between individuals), *organizational* (one individual to an organization), *inter-organizational* (one organization to another organization) and *inter-organizational networks* (one organization to many organizations) (Whipple *et al*.,2013). While this would represent *trust in partners*, some authors differentiate this from *trust in technology* which can further be divided into *trust in platform* and *trust in records* (Lu *et al*., 2010).

2.2.3 Classes of trust

A third reason for the ambiguity is that trust can be classified into different classes which influence each other in different ways. McKnight and Chernavy (2001) differentiates between *dispositional trust* (the trustor's general willingness to trust others), *structural institutional trust* (not to personal characteristics but to social or institutional structures in a situation, like regulations), and 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 over time develop to different trust levels (e.g. Shapiro *et al*., 1987; Lewicki and Bunker, 1995) such as: i) *deterrence-based trust*: a primary form of trust existing in initial stages of any cooperation, where one fear punishment of violating trust and will do (and assume the other to do) whatever promised as breaching trust will be costlier than keeping it, with monitoring as a must to keep it effective. ii) *calculus-based trust*: based on a calculation that compares cost and benefits of creating and sustaining a relationships vs. the cost and benefits of severing it, with professional reputation as a hostage. iii) *Knowledge based trust:* while partners continuously learn about each other's and knowledge increases, this leads to anticipation of the others actions. iv) *Identification based trust*: after repeated interactions, trust has increased to the point where parties understand shared values and goals, and internalized each other's desires and intentions. Fawcett *et al*. (2012) suggest in a similar way 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) argues that temporal dynamics on element of trust has been given less attention, and that different elements of trust might influence differently on different stages.

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

A fifth reason, and maybe the one most discussed is the multitude of different sub-dimensions used for defining, operationalizing and measuring trust. The literature shows no consensus regarding trust dimensions or measurements (Fawcett *et al*., 2017). While Seppänen *et al*. (2007) find that the number dimensions vary between none (only using trust) to five, they found more than 20 dimension in the 15 articles reviewed. The main sub-dimensions proposed were: *credibility, benevolence, goodwill, predictability, reciprocity, openness and confidence*. Fawcett *et al*. (2012; 2017) states that the dominant view in marketing management and SCM uses the 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). Credibility includes reliability and predictability signals (So and Schill, 2002). Avoidance of opportunistic behavior and making investments to improve mutual performance increases the level of trust and signals that a partner's motive are trustworthy,

creating mutual confidence.

Whipple *et al*. (2013) studied scales used for trust in SCM journals 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. Fawcett *et al*. (2012; 2017) would like to challenge if benevolence exist among companies, as managers stated that companies don't have friends but interest, firms cannot afford to work on partners based on benevolence as trust emerges over time from behavior and not benevolence (Fawcett *et al*., 2017). As the dimensions credibility and benevolence draw on interpersonal trust perspectives, Fawcett *et al* (2012; 2017) would like to nuance them into two dimensions for *constructing trust*: a *perform-to-promise capability* (related to credibility) and a *relational-commitment capability* (related to benevolence).

The discussion above was related to the trust object *"trust in partners"*, but also *"trust in technology"* could be elaborated on. Trust in technology can be interpreted as the beliefs regarding the performance of an institution rather than the individual (Lu *et al*., 2010) and corresponds to structural institutional trust. We could divide this into *trust in platform* vs. *trust in records*. Trust in platform relates to Grandison and Sloman (2000) study on trust in the context of networked and distributed computing system related to internet-based services and applications. They characterized this trust into four sub-dimensions: *provision trust* (trusts to let the trustee implement a service not requiring access to the trustor'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 trustee make decisions on its behalf, with respect to a resource or service that the trustor owns or controls), and *infrastructure trust* (trust in the infrastructure and applications). Trust in records relate the sub-dimensions *reliability of records* (how originated records and who created them) and *authenticity of records* (depending on the establishing process and how the identity of records are maintained) (Mak, 2014).

2.3 A framework for supply chain trust and BCT

The aim of the framework (**Figure 1**) is to uncover the potential reciprocal nature of trust and BCT information sharing in supply chains. While many early publications related to BCT argues for that BCT (through information sharing) increases trust between supply chain actors (buyer and supplier of a good or service), other research claims that trust is necessary for inter-organizational information sharing. Thus, the supply chain (including the buyer, the seller and their information sharing by BCT) is one main elements of our 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 actors perspective). The reciprocal nature is illustrated by bidirectional arrows, but also by having the two objects of trust. While trust in technology represents institutional trust, trust in SC partner is more related to the other classes of trust.

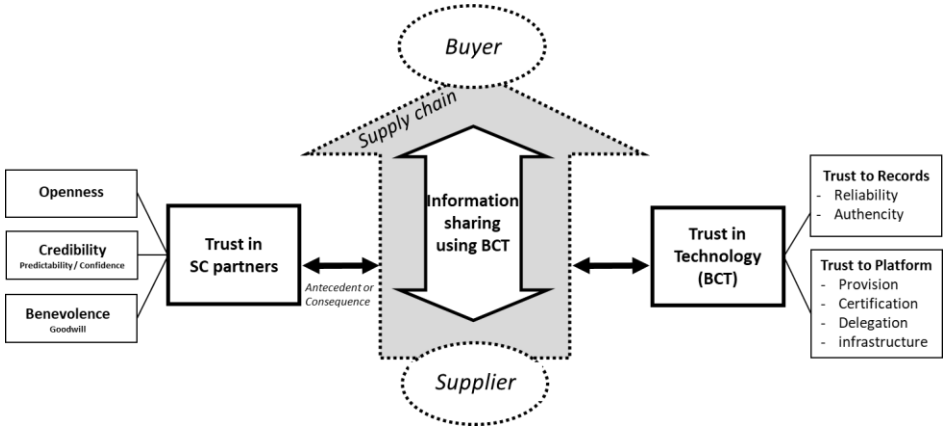

Figure 1: Framework for exploring supply chain trust and information sharing through BCT

To unpack those two trust objects, trust in partners are using the sub-dimensions credibility, benevolence, goodwill, predictability, openness and confidence. However, these sub-dimensions could be grouped into three: i) *benevolence* that includes signals of goodwill, ii) *credibility* that includes signals of predictability and confidence, and iii) openness. Trust in BCT are using sub-dimensions: *provision*, *certification*, *delegation* and *infrastructure* (for the platform) and *reliability* and *authenticity* (for the records).

3. RESARCH METHODOLOGY

To study such emerging topic as BCT, a theoretical background was developed prior to further exploration and analysis steps. In this study, a framework that links trust and BCT is established as a foundation for the research. Then, a systematic literature review (SLR) was done.

SLR has 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). However, recently there are many studies that have applied SLR successfully to emerging themes (Queiroz *et al*., 2018). In fact, SLR is an effective approach to the field development, it provides a trustworthy systematic approach for understanding issues that are not covered, and identifying ways of exploring the field, as well as generating a new research agenda 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 seen suitable to address the relation between BCT and trust in a SCM context even though it is a rapidly growing and developing topic. The following sections will explain the literature selection process and the literature analysis process.

3.1 Literature selection process

Three steps were done for the literature selection (Tranfield *et al*., 2003). The first step was to conduct an advanced search. We looked for the words "blockchain" and "trust" in the title, abstract and keywords through our University Library search engine levering numerous databases. To achieve a rigorous results, the search was limited to peer reviewed articles. The conjunction "and" is used between the words "blockchain" and "trust". Additionally, two synonyms were used for "blockchain" which are: "block chain" and "distributed ledger". The conjunction "or" was used between these synonyms. This enabled the collection of a larger sample of relevant literature (Tranfield *et al*., 2003). As a result, 629 papers was initially generated from 7 databases (Academic search complete, Business source complete, Emerald, Science direct, IEEE xplore digital library, Complementary index, and Directory of open access journals).

The second step was to narrow down the research results to only papers that discussed BCT and trust in a SCM field. Thus, we searched for "supply chain management" or "logistics" in all the abstracts of the achieved results from the first step. This resulted in 43 papers. The third step was to screen all the abstracts so that only papers discussing BCT and trust in SCM context is considered using different inclusion and exclusion criteria**.** This resulted into 28 papers that were selected for the review and analysis (20 journal articles and 8 conference papers).

3.2 Literature Analysis process

Several sub questions were generated to understand how trust is operationalized and discussed in the articles that addressed SCM and BCT. We first investigated if any theoretical connection or frameworks were used for their trust discussion, and if so, what frameworks. Second, we 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. Then, we tried to see if trust was being measured or operationalized in the literature, and if so, if the implications generated were based on empirical

studies or mainly suggestions and ideas. Finally, we looked in the literature 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 basically addresses if there is a gap in the literature between trust theories and BCT in SCM.

To further analyze the selected papers, the process proposed by Hald and Kinra (2019) was followed to develop an understanding of how BCT could impact trust in SCM. Thus, different research propositions were generated to be discussed, based on the developed conceptual framework. These propositions are falling under two main categories: propositions suggesting BCT has a positive influence and other propositions suggesting that BCT has a negative influence on trust in SCM. According to Hald and Kinra (2019), Adler and Borys (1996) and Miles and Huberman's (1994), each of the selected papers should be coded individually in order to signal the influences of BCT on trust. Specifically, words or phrases were sought indicating positive influence are for example "BCT will enable", "facilitate", "enhance", "leads to", "expected to provide" while other words such as: "blockchain constrains", "limitations", "barriers" "blockchain challenges" were sought to suggest a negative 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 in.

4. FINDINGS AND PROPOSITIONS

Several sub questions (SQ) have been tested against all the reviewed papers to reflect on how trust is operationalized and discussed in BCT and SCM literature.

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

Only 4 (14%) out of the 28 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. Fransisco and Swanson (2018) explored the adoption of blockchain technologies in supply chain traceability applications. They have used the Unified Theory of Acceptance and Use of Technology (UTAUT) as a framework for technology acceptance and the construct of information technology trust. The research concluded with blockchain implications on SC that were inspired by theory and a literature review. The third paper (Hawlitschek *et al*., 2018) used the extended blockchain framework that is based on Notheisen *et al*. (2017), which was the fourth paper. The framework is basically dealing with trust based on two point of views. The first view is the sharing economy, which includes two objects of trust: trust in peers and trust in the platform. The second point of view 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). Our observation is that frameworks or references to established research domain dealing with trust (such as psychology, social psychology, sociology, economics, and management).

SQ2: *Is trust defined?*

Only 3 out of 28 (10%) 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*". Secondly, Akram and Bross (2018) used the definition provided by Mayer et al. (1995) "*the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party".* Finally, Hawlitschek *et al*. (2018)

used the definition provided by Rousseau *et al*., (1998) "*the intention to accept vulnerability based upon positive expectations".* Although there only are 3 papers that proposed an established definition of trust, all other papers referred trust to reliability of information provided by trade partners, or the safety and security of the data managed by a central authority. Thus, BCT is repeatedly called a "trust free system" since it claims to eliminate the need for trusted third party as well as it claims to provide a single source of data without even the need to trust other peers in the SC network (e.g. Wang.Y *et al*., 2019; Akram and Bross, 2018; Notheisen *et al*., 2017). So, in general trust was discussed without using explicit and established definitions.

SQ3: *Is trust operationalized?*

In terms of operationalization, none of the reviewed papers tried to measure or operationalize trust. One reason for that could be the fact there is no single paper that is fully dedicated for conceptualizing trust using BCT in SCM. Instead, researchers discussed other topics while trust played an important role in it.

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

In total 4 out of 28 papers (14%) gave trust implications based on empirical studies, while the remaining papers just proposed ideas and suggestions, sometimes based on previous references. Indeed, some papers are case studies in itself (e.g. Chen *et al*., 2017) but trust implications are not driven from the actual case. Sander *et al*., (2018) was based on survey, Akram and Bross (2018) was based on interviews. The other 2 papers depended on modeling based on case data (Notheisen *et al*., 2017; Zaerens, 2018). Our conclusions is that claims regarding trust related to BCT and SCM are seldom based on empirical studies.

SQ5: *Are "classes of trust" or "trust development over time" or "trust levels" discussed or is trust only a general undefined term?*

Only one paper (out of 28) discussed only two classes of trust, related to the sharing economy context (Hawlitschek *et al*., 2018) and distinguished between institution-based trust (trust in for example Airbnb) and the disposition to trust (trust in hosts). None of the remaining references discussed trust development over time or trust levels. This can be due to the novelty of the topic. However, some papers mentioned trust object as different types of trust which for instance could be trust in platform or inter-organizational trust (e.g. Fransisco and Swanson, 2018; Hawlitschek *et al*., 2018; Notheisen *et al*., 2017).

From the literature, it can be concluded that trust has been used in a very vague way. Thus, the reciprocal nature of trust is explored through reflecting upon the positive or negative influence of BCT using the proposed framework. So for instance, if the BCT will enable, enhance or, in general, have positive influence on trust, then, it can be said that trust is a consequence of applying BCT in SCM context. On the contrary, if BCT will limit, constrain or will have a negative influence on trust, then trust is still needed and hence it reflects an antecedent nature with regards to applying BCT in the SCM. The research propositions are shown in **Table 1**.

Table 1: Research propositions

Index	Propositions
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.
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.
P3	Applying BCT will enhance trust in SC partners through openness in the information sharing.
P4	Applying BCT in SCM will enhance trust in SC partners through credibility.
P5	Applying BCT in SCM will enhance trust in SC partners through benevolence or goodwill.
P6	Applying BCT in SCM will constrain 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.
P7	Applying BCT in SCM will constrain 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.
P8	Applying BCT will constrain trust in SC partners by limiting the openness of information sharing.
P9	Applying BCT in SCM will constrain trust in SC partners through limiting credibility.
P10	Applying BCT in SCM will constrain trust in SC partners through limiting benevolence.

4. DISSCUSSIONS

In this chapter, each proposition will be discussed based on the findings from the literature. To strengthen the understanding, all propositions are linked to the main BCT attributes discussed by Hald and Kinara (2019) which are: the decentralized structure, cryptography system, consensus mechanism and smart contract.

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

In the literature, all the 28 (100%) reviewed papers explicitly or implicitly referred to a relationship between BCT and enabling data reliability or authenticity. In particular, all the papers have linked data authenticity with BCT features like decentralized structure, cryptography system and consensus mechanism. But data reliability is mostly linked to the smart contract features as accrued in 23 papers out of 28 (82%). This is due to the fact that data reliability is related to the data entry at first place, in which BCT cannot guarantee its reliability unless the smart contract is used and linked to the different sensors, Radio frequency identification (RFID) or IOT devices. Particularly RFID and IOT with BCT's smart contract are supposed to be highly reliable since it involves less human interference (Chen *et al*., 2017; Feng, 2017; Augusto *et al*., 2019; Figueroa *et al*., 2019; Sander *et al*., 2018). Smart contract in this situations will also help in data authentication (Dasaklis and Casino, 2019; Rejeb *et al*., 2019). Some researchers such as Hua *et al*. (2018) argued

that BCT's consensus mechanism can develop a consensus trust that helps in improving data reliability, especially in public blockchains were data are validated from all participants. Although the distinction between data reliability and authenticity seems to be clear, there still some papers (e.g. Wang.S *et al*., 2019; Rejeb *et al*., 2019) that are mixing between these two concepts.

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

With regards to trust provision, 7 out of 28 papers (25%) mentioned private BCT without differentiating between BCT's attributes. Private BCT assumes some level of trust between peers in exchange for limited decentralization and visibility capabilities, and hence trust provision is enabled as the trustor could trust the trustee to implement a service not requiring access to all the ledger's data (Figueroa *et al*., 2019; Zhang and Jacobsen, 2018; Johng *et al*., 2018). In other scenarios, BCT enabled trust provision through IOT to relieve trusted third parties from data provision duties such as proposed by Notheisen *et al*. (2017) in the case of a trust-free transaction systems in the market for used cars (lemons) where IOT devices was linked to BCT to let smart cars directly report their status to the registry system (Notheisen *et al*., 2017).

For enabling trust certification, 10 out of 28 papers (36%) referred to enabling trust certification either implicitly or explicitly through all BCT attributes in SCM context. This is in the context of visible and transparent information sharing that allows the provenance and tracking of the transactions to its origin and hence this works as a certification for the trustee (Chen *et al*., 2017; Feng, 2017; Augusto *et al*., 2019; Figueroa *et al*., 2019; Dasaklis and Casino, 2019; Rejeb *et al*., 2019; Zaerens, 2018; Akram and Bross, 2018). BCT also offers an opportunity for new entrants to showcase the virtues of their supply chain (Francisco and Swanson, 2018) also applied in 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 (82% of reviewed papers). This means BCT is highly expected to enable trust through delegation. However, this is not yet fully deployed in practice so far (Wang.Y *et al*., 2019).

All the 28 reviewed papers signaled 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 it promised. However, many of these papers has in the same context mentioned that BCT could also limit the trust in infrastructure due to many issues but scalability might be the highest concern. (Wang.Y *et al*., 2019). This will be further explained in the limiting propositions later in this section.

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

Among the studied papers, only 5 out of 28 (18%) mentioned that BCT could enhance openness in information sharing. In the case of VMI, openness in information sharing is seen 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 (Akram and Bross, 2018). Other sources simply considered openness in information sharing as a consecutive event caused by applying BCT in SCM context (Feng, 2017;Wang.S *et al*., 2019; Zaerens, 2018).

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

There are 4 out of 28 papers (14%) that discussed how BCT can enhance credibility among SC partners. Some researchers as Hua *et al*. (2018) and Sander *et al*. (2018) refers it to "natural credibility" due to the consensus mechanism, immutability (cryptography system) and peer to peer transactions (decentralized structure) that makes a tamper proof system which will stand against any

cheating or fraud attempts. Others related it to smart contract attribute in the financial transactions as it eliminates the need of a credible third party and create a peer to peer transactions (Norberg, 2019; Wang.S *et al*., 2019).

P5: *Applying BCT in SCM will enhance trust in SC partners through benevolence or goodwill*

Only one paper discussed how BCT can enhance trust through benevolence or goodwill. The main idea is that BCT attributes construct a "digital trust" that help prevent SC partners from behaving unethically or opportunistically as every transaction in a blockchain builds on every other, any unethical behavior will be readily visible to all the network (Wang.Y *et al*., 2019). This can be reflected upon as benevolence or goodwill intentions. In fact, all the remaining papers without exception has mentioned this in an implicit way but the selected paper was more explicit through mentioning "opportunistic behaviors".

P6: *Applying BCT in SCM will constrain trust in the technology through limiting trust in the records*

Not many papers have discussed that BCT would have any negative impact on trust in the technology either through reduction of data reliability or authenticity. Only one paper mentioned that BCT could be vulnerable to fraud despite its unique attributes because SC members could write a multitude of fake transactions in order to build up a credible financial history. This is directly related to the reliability definition (Verhoeven *et al*., 2018). However, if such data ever gone through the BCT's consensus mechanism, the problem could be more complicated (Verhoeven *et al*., 2018).

P7: *Applying BCT in SCM will constrain trust in the technology by limiting trust in the platform*

In the reviewed literature, there was no mentioning of a negative impact for BCT on trust certification. However, BCT was proposed as a constraint to trust provision in some cases related to public BCT. This is because the trustor could not control which data can be exposed or which SC partner is authorized to enter the network (Figueroa *et al*., 2019; Wang.Y *et al*., 2019; Johng *et al*., 2018). For trust delegation, there is a single paper that noted such occurrence. Dasaklis and Casino (2019) proposed that scaling BCT's smart contract to "one vendor many retailers" or more complex structures might end up in high monetary losses and data disclosure, as it could be difficult to manage in the VMI settings (Dasaklis and Casino, 2019).

With regards to the negative relation between BCT and trust in the infrastructure, there are 7 out of 28 reviewed papers (25%) that suggested BCT might limit trust in the infrastructure. The main discussed reason for that is scalability of the technology as it failed in many current projects (Wang.Y *et al*., 2019). This is either due to slow processing time among other related technical issues (Augusto *et al*., 2019; Verhoeven *et al*., 2018; Dasaklis and Casino, 2019; Notheisen *et al*., 2017) or due to sustainability reasons as BCT is a high energy consumption technology (Akram and Bross, 2018). From another point of view, Akram and Bross (2018) stated that BCT could limit trust in BCT infrastructure is it based on open source programming that has many concerns with regards to intellectual properties. As mentioned before, BCT is still vunerable to fraud since members could write a multitude of fake transactions (Dasaklis and Casino, 2019) and that could also limits the trust of BCT infrastructure.

P8: *Applying BCT will constrain trust in SC partners by limiting openness of information sharing*

Five of the reviewed papers (18%) mentioned that BCT will limit the openness of information sharing due to privacy concerns (Augusto *et al*., 2019; Hua *et al*., 2018). For instance, the data uploaded by the participating companies will be visible to all the other participants, which means that some of the data considered as trade secrets will also be available to others. This could be avoided by using authorizations, yet it is very limited in public BCT (Hua *et al*., 2018). An example of "trade secrets" that can be found in the SC of a large meat providers who compete on a cost base, as they are unlikely to have an interest in sharing their information about how their animals

have been farmed, slaughtered and processed (Sander *et al*., 2018). Moreover, publishing sensitive and private data in public blockchain can lead to serious legal consequences for organizations, especially after the introduction of the general data protection regulations (GDPR) (Akram and Bross, 2018).

P9/P10: *Applying BCT in SCM will constrain trust in SC partners through limiting credibility or benevolence*

Not many literatures has discussed the limiting impact of BCT on trust credibility or benevolence. Only one paper predicted that future honest behavior is impossible since there is no central authority to police or enforce honesty in a blockchain-enabled supply chain (Wang.Y *et al*., 2019). This can be reflected on both credibility and benevolence aspects and so the two proposition are discussed together in this situation. **Table 2** summarize the articles and its corresponding research propositions.

Table 2: Reviewed articles and its corresponding research propositions

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 *et al* . (2017)	x	x		x	x	x												
Feng (2017)	x	x		x	x	x	x								x			
Augusto *et al* . (2019)	x	x		x	x	x									x	x		
Figueroa *et al* . (2019)	x	x	x	x	x	x						x						
Wang.S*et al* . (2019)	x	x		x	x	x	x	x										
Kshetri and Loukoianova (2019)		x				x												
Hua *et al* . (2018)	x	x			x	x		x								x		
Anjum *et al* . (2017)		x				x												
Zaerens (2018)	x	x	x	x	x	x	x									x		
Benčić *et al* . (2019)	x	x	x		x	x												
Verhoeven *et al* . (2018)		x				x				x	x				x			
Tseng *et al* . (2018)	x	x			x	x												
Dasaklis and Casino (2019)	x	x	x	x	x	x	x							x	x			
Arumugam *et al* . (2018)	x	x			x	x												
Rejeb *et al* . (2019)	x	x		x	x	x												
Francisco and Swanson (2018)	x	x		x	x	x												
Kshetri and Voas (2019)		x				x												
Sander *et al* . (2018)	x	x			x	x		x								x		
Hawlitschek *et al* . (2018)	x	x			x	x												
Fernández-Caramés *et al* . (2019)	x	x			x	x												
Zhang and Jacobsen (2018)	x	x	x		x	x												
Notheisen *et al* . (2017)	x	x	x		x	x									x			
Westerkamp *et al* . (2019)	x	x			x	x												
Norberg (2019)		x				x		x										
Wang, Y. *et al* . (2019)	x	x			x	x			x			x			x			x
Kamble *et al* . (2018)	x	x			x	x												
Johng *et al* . (2018)	x	x	x		x	x						x						
Akram and Bross (2018)	x	x		x	x	x	x								x	x		
Total	23	28	7	10	23	28	5	4	1	1	1	3	0	1	7	5	0	1
%	82%	100%	25%	36%	82%	100%	18%	14%	4%	4%	4%	11%	0%	4%	25%	18%	0%	4%

6. CONCLUSION

The aim of this study was to understand the role of BCT related to trust in SCM. The conducted literature review helped in answering the two main research questions.

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

The study showed that none of the reviewed articles did any operationalization to measure trust in BCT and SCM context. There is no mention of trust development over time or trust levels. Yet, only one paper mentioned classes of trust. There are only very few papers that defined trust before discussing it or trying to connect trust to a previous frameworks or concepts. Few relied on established frameworks from domain (e.g. psychology, social psychology, sociology, economics, and management) were trust have been researched for a long time. Most of the implications related to trust, proposed in the literature, were driven from ideas or suggestions rather than empirical studies. In general, the reviewed papers showed that trust is usually discussed in relation to the reliability of information provided by trade partners, or the safety and security of the data managed by a central authority.

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

There is a reciprocal nature of trust, as it can be both a consequence and an antecedent of applying BCT. This reciprocal nature is reflected by the BCT's positive and negative impacts on trust in SCM. There is a sort of a consent in the literature on the positive impact for 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 is less agreement upon trust provision and trust certification. In regards to trust in SC partners, there are much fewer signals that BCT can enable credibility, benevolence or openness in information sharing. On the other hand, BCT has a constraining impact when it comes to trust the SC partners especially in the openness of the information sharing due to privacy concerns that are more common in the public BCT. Moreover, trust in the infrastructure can also be limited by applying BCT. In fact, some of the papers that proposed the enabling impact of BCT on infrastructure trust did also propose the opposite, especially when BCT is scaled up as it becomes difficult to apply and to succeed. In general, it is very difficult and complex to find a single answer on the reciprocal nature or the impacts of BCT on trust. But, based on the results of this study, trust is highly expected as a consequence for BCT if we are considering trust in the technology. While in 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.

This study contributes to the research field by clearly pointing out the lack of theoretical underpinning for the statement regarding BCT and trust and SCM given in current literature, and a gap between BCT and trust theories in the SCM context. This research however has limitations. Due to the novelty of the discussed topic, not many cases in the market have implemented BCT on a large scale and hence this research was limited to a literature review.

Understanding the interrelation between trust and BCT in SCM seems to be an area where a lot of future rigorous research is needed, and especially empirically grounded. Future research should explicitly define and operationalize how they view trust. One interesting issue would be to understand the reciprocal nature of trust related to information sharing (e.g. through BCT) in SCM. Another dimension would be if culture (related e.g. to nations or industries) influence trust related to BCT in SCM.

7. REFERENCES

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.

Adler, P.S., Borys, B., (1996). Two types of bureaucracy: enabling and coercive", *Administrative Science Quarterly*, 41 (1), 61-89.

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.

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.

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.

Daugherty, P.J. Richey, R.G., Roath, A.S., Min, S., Chen, H., Arndt, A.D., Genchev, S.E. (2006). Is collaboration paying off for firms? *Business Horizons*, 49 (1), 61-70.

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.

Figueroa, 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.

Gaehtgens, 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 [Accessed 10 July 2019).

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.

Ghosh, A. and Fedorowicz, J., (2008). The role of trust in supply chain governance. *Business Process Management Journal*, 14 (4), 453-470.

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.

Hawlitschek, F., Notheisen, B., Teubner, T., (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, 29 (1), 50-63.

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., 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Shapiro, S., (1987). The social control of impersonal trust. *American Journal of Sociology*, 93 (3), 623-658. 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.

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.

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.

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.

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).

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.