How Distributed Ledger Technology Can Influence Trust Improving Data Sharing in Collaborative Networks

Ronald van den Heuvel[1], Rogier van de Wetering[1(✉)], Olaf Kruidhof[2], Rik Bos[1], and Jos Trienekens[1]

[1] Open University of the Netherlands, Valkenburgerweg 177, 6419 AT Heerlen, The Netherlands
{Ronald.vandenHeuvel,Rogier.vandeWetering,Rik.Bos,
Jos.Trienekens}@ou.nl
[2] EUROPOL, Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands
olaf.kruidhof@europol.europa.eu

Abstract. Collaborative networked organizations (CNOs) strive to achieve a common goal. Collaboration within CNOs relies on information technology (IT) and trust. Trust appears in different forms, such as relational, contractual, and competence trust that strengthens the relationships. In addition to trust, data sharing is fundamental to CNOs, as it can improve business-to-business transactions. In this paper, we show how distributed ledger technology (DLT) can increase trust and improve data sharing. We created a decision model, using a design science research (DSR) approach, that provides a mapping between DLT-characteristics and trust antecedents in order to select appropriate DLT. We use an analytic hierarchy process (AHP) approach to establish the trust antecedent ranking within the CNO for European law enforcement (ELE), Europol and its operational partners. Our research provides an evaluated model to determine the DLT-characteristics that can increase trust and data sharing in a CNO.

Keywords: Collaborative networks · Distributed ledger · Blockchain · Trust · Law enforcement

1 Introduction

Collaborative networked organizations (CNOs) are composed of organizations that want to achieve a common goal. IT is an essential component of organizational collaborations to establish the interaction [1, 2]. A recent study shows that IT facilitated face-to-face communication is the preferred way to cope with dynamic, unexpected events in a CNO (so-called CNO-dynamism) [3]. Van den Heuvel et al. [3] also found that trust plays a vital role in coping with CNO-dynamism.

Trust can be divided into various categories, such as competence, relational and contractual trust [4]. These forms of trust all have their own definitions and influencing antecedents. It would be beneficial to see how we could use IT to increase trust within

F. Ceci et al. (Eds.): *Exploring Innovation in a Digital World*, LNISO 51, pp. 62–76, 2021.
https://doi.org/10.1007/978-3-030-87842-9_6

collaborations, and not only use IT to facilitate face-to-face communication, but also to facilitate information exchange.

Blockchain is an emergent technology and can act as a distributed ledger that can establish the role of a trusted third party (TTP) in transactions between organizations [5–7]. Some researchers state that DLT has the potential to be used as a cross-organizational communication platform, or operating system, for inter-organizational communication (or collaboration) [7, 8]. As described by Pedersen et al. [5] this technology still has its limitations, for instance, with regards to scalability, capacity, latency, and privacy. Despite this, there are situations where this technology aids the transaction by providing immutability, transparency, and a single-source-of-truth [5, 9, 10].

There is abundant practitioner literature on the implementations of DLT and scientific literature on the information technology (IT) side of DLT. Research on the business implementation of DLT that is supported by empirical evidence is limited [11, 12].

We anticipate that DLT could provide CNOs with the capability not only to communicate, but also to increase data sharing and trust, and be more resilient to CNO-dynamism. Our research question is:

> ***RQ**: How does distributed ledger technology influence trust, resulting in improved data sharing within a CNO?*

We evaluated the model in an international law enforcement CNO, Europol and its operational partners, via 15 semi-structured interviews. Our results can help practitioners determine which characteristics a DLT should provide to influence specific forms of trust and set up an environment that supports trust creation. Researchers can use our results to construct new business/IT alignment models and identify requirements to research the influence of DLT on trust or even what characteristics a new DLT should have in specific conditions.

Section 2 describes the theoretical background. Section 3 describes the methodology of the research project, Sect. 4 describes the decision model. Section 5 outlines the refinement of our model as typically used in a design science approach. We conclude this paper with a discussion (Sect. 6) and a conclusion (Sect. 7).

2 Theoretical Background

2.1 Networked Organizational Context

Collaboration between organizations is a common way to set up new products or services and is becoming increasingly important in our interconnected world. CNOs comprise of multiple organizations and aim to achieve a common goal, which they could not achieve individually [13]. Two main forms are distinguished: long term strategic alliances, such as business ecosystems and virtual organization breeding environments (VBE), and goal-oriented networks, such as virtual organizations (VO) and extended enterprises [14].

Current literature shows that trust is essential for collaboration in these CNOs [3, 15, 16]. Creating trust between participating organizations in a CNO takes time. Therefore,

VBEs are commonly referred to as being able to facilitate ecosystems due to their long-term partnerships and improving the preparedness to reconfigure for new collaborations. IT is an important component within CNOs for collaboration. IT components used within a CNO are, for example, collaboration platforms, conference facilities, and forums [3].

2.2 Trust and Data Sharing

Castaldo, Premazzi, and Zerbini [17], Yang [18] show that trust is a complex, multi-faceted concept. Many dimensions of trust can be considered, for example, cognitive trust versus affective trust [19], trust between people compared to trust between organizations [20], trust between people at different levels in an organization [21], or the evolution of trust over time [22]. Castaldo et al. [17] have developed an 'architectural structure' that consists of five building pieces to structure the antecedents of trust: The different ways in which the 'conceptual nature' of trust can be perceived by; 'Subjects' (trustor and trustee), via fundamental trust antecedents, that can be influenced, expressed, and experienced by; 'Future actions' that Trustors and the trustees' experience and conduct, aligned with their trust and trustworthiness, respectively, leading to; 'Positive results' or consequences experienced by the trustor, influenced by and dependent of; The trustor's willingness to be vulnerable in a 'Risky situation,' because, "Trust is only bestowed where there is an uncertain or risky situation" [17].

The 'architectural structure' shows that trust antecedents, as part of the building pieces 'Subjects', should be influenced in order to observe 'positive results' from 'future actions' in a 'risky situation.' In our research, the CNO is considered to be the 'risky situation' where improvement should be achieved as the 'positive results' from the 'future actions' communication and data sharing.

Communication and data sharing for mutual benefit is important in business-to-business transactions [23] and is fundamental in CNOs [14]. The willingness of parties to share their data is determined by several factors, the level of trust they have in each other being a foundational one [20]. These factors are especially true in a law enforcement community [24]. An essential factor for the law enforcement community to be effective is the sharing of data, within the constraints of applicable (inter)national legal frameworks. Data sharing is defined as the transfer of data and/or information owned and held by one party to another party in order to be used by the second party, in compliance with pre-agreed rules.

2.3 Distributed Ledger Technology

The cryptocurrency Bitcoin [25] and the term blockchain seem to be inseparable but are in fact two separate things. Blockchain is a method of storing data in blocks that are linked via hash pointers [26], and bitcoin is an application of the technology for use as a digital currency. The term blockchain is often overused to depict multiple related technologies or components, such as distribution mechanisms, smart contracts, ledgers, and oracles. In the current literature, researchers are moving away from using the term 'blockchain' and are referring to distributed ledger technology (DLT).

An essential aspect of DLT is distribution, where not only the data but also the transactions are distributed, and the outcome of the transactions are compared within

the network of participants. When the participants achieve consensus on the outcome, the value is collectively committed [10, 12, 27]. Trust is a central topic in DLT research where it relates to the possibility of removing a human TTP in a transaction [10] or removing the need for a TTP by increasing transparency [5, 8, 9].

DLT is facilitating new decentralized organizational structures [28, 29] and it is not hard to envision a relationship between the CNO literature and these concepts. A move away from the use of IT only facilitating communication [3] to an 'operating system' that can be used for inter-organizational operations could be a valuable endeavor.

3 Research Methodology

We used the DSR cycle [30–32] for our methodology. Based on Van den Heuvel et al. [3], we identified a need to design an artifact to select technology suitable for improving trust and data sharing in CNOs (relevance cycle). Within the design cycle, we identified DLT a promising technology. We executed a SLR (rigor cycle) to gather a more in-depth understanding of DLT-characteristics. The output of the SLR was used to create a decision model that maps trust antecedents to DLT-characteristics. The model was evaluated by executing an AHP (formative evaluation [33]) to rank trust antecedents, thereby refining and evaluating the model by interviews (summative evaluation [33]). Our DSR approach aligns with Rossi et al. [11] to analyze the interactions between the DLT protocol and application level.

3.1 Systematic Literature Review (SLR)

The components for our SLR (based on [34]) were acquired from our research question and were: DLT, data sharing, collaborative network organizations, and trust. We used forward and backward searching on found literature. The literature had to be peer-reviewed and in the English language. Searches were executed on Academic Search Elite, Business Source Premier, E-Journals, LISTA, PsyncINFO, Psychology and Behavioral Sciences Collection, PsycARTICLES and AISeL. By reviewing the abstract, the literature was classified as relevant or not. In total 30 articles were selected from the SLR.

3.2 Decision Model Creation

We grouped the found DLT-characteristics into categories based on their functionality and construction. The trust categories and antecedents are based on the paper of Cheikhrouhou et al. [4], which is a solid basis for our research. Trust antecedents were then used to create the requirements to rationalize if the DLT-characteristics could fulfil the requirement. We logged the rationale (in terms of the initial hypothesis) behind the mappings in the decision model. The model was evaluated by two experts who were closely involved and have expertise in the areas of DLT, trust, and CNOs.

3.3 Artifact Evaluation

We evaluated the artifact by applying it to a European law enforcement (ELE) CNO, consisting of Member States, Third Parties and Europol Units. The mission and vision of Europol [35] describe a clear intention of collaboration between multiple parties, thereby fitting the CNO definition, acting as an information hub in the network. The CNO described in [4] is a vertical CNO (a CNO that includes parties with different functions in a value chain) and suggests that the exercise should be executed in a horizontal CNO (a CNO that includes parties with highly similar functions) to validate the results. ELE fits the definition of a horizontal CNO.

There were 15 participants from the ELE context. 7 member states (Croatia, Finland, Germany, Ireland, Malta, the Netherlands, Romania), 3 Third Parties (Iceland, Norway, Serbia) and 5 EUROPOL units (European Cybercrime Unit, Financial Crime Unit, Information Hub, Internet Referral Unit, Serious and Organized Crime Unit).

We selected participants according to their knowledge and involvement in data sharing and their ability to reliably represent their stakeholders' position from Member States, Third Parties, and Europol Units perspective. We provided the participants with an information package explaining our research and an interview guide to equalize their initial knowledge of DLT.

Participants work in two modes, being day-to-day operations and a taskforce. Day-to-day operation (VBE) is the sharing of data continuously between partners and where a taskforce (VO) is a dedicated group focusing on a specific investigation.

The involvement of the participants was two-fold: (1) obtain the priorities of trust antecedents for the two modes of collaboration; (2) validate the need for improvement of data sharing, the role of trust in decision-making on sharing and the usefulness of technology in this context. The first objective is achieved by an AHP exercise, the second by semi-structured interviews.

The rating exercise is based on the AHP method presented by Saaty [36]. An AHP is a multi-criteria decision method that rates factors "through pairwise comparisons and relies on the judgments of experts to derive priority scales" [36], thereby creating an ordered list of all trust antecedents for our CNO context. The list can then be used to focus on the essential characteristics within the model. The rating exercise was executed for two modes of collaboration: day-to-day operations (strategic partnership, VBE) and taskforce (goal-oriented, VO) and the three types of participants (Member States, Third Parties and Europol Units). The values were combined to provide an overview of the whole CNO and per collaboration mode. We used the consistency ratio and group consensus to validate the rating and determine the consistency. Participants used a tool provided by the researchers to execute the rating exercise.

The model was evaluated by semi-structured interviews. We presented three perspectives for evaluating the artifact: (1) validating the need and potential of data sharing improvement; (2) the role of trust in decision-making on data sharing; and (3) the possible usefulness of new technology to affect trust in the context of data sharing. Interviews were conducted during six weeks at the ELE offices. Two test interviews were executed to validate the questions. The interview length was planned to last approx. 60 min. All interviews were recorded, transcribed, and anonymized. All transcripts were validated by the resp. participant. The interviews were conducted in 2019.

4 Decision Model

4.1 Trust Categories and Antecedents

In order to affect the behavior of a trustor and/or a trustee, one or more of the determining antecedents of trust must be influenced. The work by Cheikhrouhou et al. [4] builds on Msanjila and Afsarmanesh [37] and offers a rich set of 22 trust antecedents organized into five categories that focus on a CNO. The trust categories and antecedents can be found in the horizontal dimension of Table 2.

Cheikhrouhou et al. [4] identified 'information sharing' as a trust antecedent in contractual trust, but not in the other trust categories. We wanted to see if DLT characteristics could result in improved information sharing in general. Therefore, we did not add 'information sharing' as an antecedent, which would have resulted in cyclical reasoning (improving sharing by sharing). Still, we do agree with Cheikhrouhou et al. [4] that "information sharing" is a valid trust antecedent in the category of contractual trust.

4.2 DLT-Characteristics

The SLR led to the identification of functional and constructional DLT-characteristics arranged in three categories (Table 1). The architecture category addresses the embedding of DLT into an IT landscape. The membership configuration category addresses the way in which members can participate in a distributed ledger, and data management category contains characteristics related to data processing. The names of the characteristics are implementation independent.

Table 1. DLT-characteristics.

Characteristics	Construction characteristics
Architecture	
A1: Embedding in existing ICT landscape	A1.1: Extendable, configurable solutions [38]
A2: Connectivity to non-DLT environment	A2.1: Oracle [6, 29]
A3: Processing reliability	A3.1: Distributed nodes communicating peer-to-peer [6, 25, 29, 39]
A4: Autonomous behavior	A4.1: Smart Contract/Decentralized Applications [6, 29, 39], A4.2: Integrable runtime environment types [39], A4.3: Language type [29, 39], A4.4: Code verifiability [39]
Membership configuration	
M1: Participation incentive	M1.1: Tokens (coins) [29]
M2: Identity transparency	M2.1: Authentication (2-key) [29, 39]

(*continued*)

Table 1. (*continued*)

Characteristics	Construction characteristics
M3: Identity management	M3.1: Key management [39]
Data management	
D1: Transaction integrity	D1.1: Advanced signatures [39]
D2: Data access privileges	D2.1: Various levels of restrictions to access & processing [6, 29, 39, 40]
D3: Ledger Integrity	D3.1: Cryptographic hashing of data, Chaining mechanism (blocks in chain), Hash pointers [6, 29, 39, 40]
D4: Data configuration	D4.1: Number of distributed ledgers [39]
D5: Ledger ownership	D5.1: Owner type [6, 29, 39]
D6: Data persistence	D6.1: Storage mechanism [39], D6.2: Multiple transactions per block [6, 29, 39]
D7: Data reliability	D7.1: Distributed data [6, 29, 39, 40]
D8: Data validity	D8.1: Consen-sus pro-tocol type - Byzan-tine valida-tion / D8.2:Consesus protocol type - Non-Byz-an-tine [6, 29, 39]

4.3 Interrelations Between Trust and DLT: Towards a Decision Model

The decision model is stated in Table 2 and the code explanations are below the table.

Table 2. DLT-trust decision model

DLT	Trust categories																	
	C1	C2	C3	R1	R2	R3	R4	R5	T1	T2	T3	T4	T5	N1	N3	I1	I2	I4
	Competence			Relational					Contractual					Neg		Indirect		
A1.1										X							X	
A2.1	X		X				X			X	X	X	X		–		X	
A3.1	X	X	X		X		X		X					–	–			
A4.1		X	X	X	X		X		X	X	X	X	X	–		X	X	
A4.2			X															
A4.3			X				X			X							X	
A4.4			X	X	X		X				X	X	X	–		X	X	
M1.1					X													

(*continued*)

Table 2. (*continued*)

DLT	Trust categories																	
	C1	C2	C3	R1	R2	R3	R4	R5	T1	T2	T3	T4	T5	N1	N3	I1	I2	I4
	Competence			Relational					Contractual					Neg		Indirect		
A1.1										X							X	
M2.1							X		X		X	X						
M3.1			X								X	X						
D1.1			X	X			X		X			X		–				
D2.1			X	X			X				X	X					X	X
D3.1	X		X			X					X		X			X		
D4.1	X					X				X	X	X					X	X
D5.1					X	X			X		X			–	–			
D6.1		X	X				X			X	X	X	X	–	–		X	
D6.2		X	X														X	
D7.1	X	X	X		X									–	–		X	
D8.1	X		X												–			
D8.2	X		X	X	X	X			X		X		X	–	–	X	X	

We formulated requirements based on trust antecedents that should be satisfied by a DLT-characteristic. A DLT-characteristic is expected to have a positive effect on a trust antecedent if it proves/demonstrates to be a way to realize that antecedent, improves the way the antecedent can be experienced, or enables the realization or improvement of an antecedent. Each DLT-characteristic is assessed against these requirements. An example of these assessed interrelations: The architectural characteristic of a DLT variant that offers the functionality to connect to a non-DLT environment using the construct of an oracle, enables systems/components according to agreed conditions because it allows for automated and controlled connections to provide data for the service.

When a positive effect is expected the relation is indicated by an 'X' and a negative effect is indicated by a '-.' The vertical axis shows the characteristics as mentioned in Table 1. The trust categories are identified as competence: C1 Quality; C2 Timeliness/Punctuality; C3: Reliability; relational: R1: Shared value; R2: Commitment to the relationship/relational investment; R3: Benevolent/supportive/relational flexibility; R4: Predictable behavior; R5: Friendliness/politeness; contractual: T1: Spirit of cooperation; T2: Customization/adaptation; T3: Transparency; T4: Confidentiality/Permeability; T5: Honesty; negative: N1: Dependence/asymmetric relation; N2: Opportunistic behavior; N3: Own specific asset; indirect: I1: Reputation; I2: Work standards; I3: Financial stability; I4: Qualification of employees; I5: Duration of partnership, where N2, I3, I5 were omitted because there was no mapping to the DLT characteristics.

5 Model Refinement and Evaluation

5.1 Refinement: Results of the AHP in a Horizontal CNO

The participants belong to different organizations in the CNO and therefore have different perspectives, namely: Member State, Third Party, and Europol Units. Table 3 shows the results of the AHP exercise.

Table 3. Sets of prioritized trust categories.

	Overall	Daily	Taskforce	Overall	Daily	Taskforce
Category	**Combined**			**Member States**		
Competence trust	**(1) 34.3%**	**(1) 34.9%**	**(1) 33.6%**	**(1) 28.5%**	**(1) 28.8%**	(2) 28.1%
Relational trust	(2) 23.7%	(2) 23.0%	(2) 24.4%	(2) 27.2%	(2) 26.2%	**(1) 28.2%**
Contractual trust	(3) 19.6%	(3) 18.7%	(3) 20.6%	(3) 23.0%	(3) 23.2%	(3) 22.9%
Negative trust	(4) 12.7%	(4) 12.9%	(4) 12.3%	(5) 9.6%	(5) 9.3%	(4) 10.9%
Indirect trust	(5) 9.7%	(5) 10.5%	(5) 9.0%	(4) 11.7%	(4) 12.5%	(5) 9.8%
Category	**Third Parties**			**Europol Units**		
Competence trust	(2) 26.4%	(2) 27.5%	(2a) 25.0%	**(1) 45.3%**	**(1) 45.6%**	**(1) 44.9%**
Relational trust	(4) 16.8%	(4) 16.9%	(3) 16.6%	(2) 22.2%	(2) 21.0%	(2) 23.4%
Contractual trust	(3) 20.8%	(3) 17.3%	(2b) 25.0%	(3) 13.9%	(3) 13.2%	(3) 14.6%
Negative trust	**(1) 28.3%**	**(1) 30.3%**	**(1) 26.0%**	(4) 10.3%	(4) 11.0%	(4) 9.7%
Indirect trust	(5) 7.7%	(5) 8.1%	(4) 7.3%	(5) 8.3%	(5) 9.1%	(5) 7.5%

The AHP exercise is used to refine the model to the specific horizontal CNO, operating modes, and participation styles.

The AHP shows different results in day-to-day mode, where parties share various pieces of data that require non-urgent action, and taskforce mode where a selected group of experts collaborate dedicatedly and full time (24/7) on a specific high priority case, often in the same location. Both the participants' perspectives and operation modes were grouped to provide a general overview. A tool was used to provide the trust antecedents to the participants, and in the tool the antecedents could be ranked against each other. The separate results were then combined and analyzed.

From the combined results, we can conclude that competence trust is the most crucial trust factor (34.4%), followed by relational (23.7%) and contractual trust (19.6%). These results concur with the results of Cheikhrouhou et al. [4]. Some differences are visible when looking at the different modes and groups. For day-to-day operations, the same trust categories are the most important for Member States and Europol Units. Third Parties show a deviation and rate negative trust higher (30.3%). Comparing day-to-day and taskforce modes, we see differences in Member States and Third Parties. Where Member States rate relational trust higher (28.2%) in a taskforce context, Third Parties

rate contractual trust higher (25.0%). Even so, the overall score does correspond with previous results by Cheikhrouhou et al. [4].

Another viewpoint in our AHP is the insight in the rating of trust antecedents. We can see that overall quality and reliability are ranked highest with 13.3% and 16.1% respectively, while for Third Parties the highest antecedent was dependence/asymmetric relation with 19.6%. In taskforce mode, Member States ranked quality, shared values, and reliability highest with 13%, 11.9%, and 10.3% respectively.

Table 4. Consistency and consensus ratios on trust factors.

	Combined		Member States		Third Parties		Europol Units	
Overall								
Consistency	1.7%	Strong	2.2%	Strong	7.6%	Strong	2.5%	Strong
Group consensus	64.4%	Low	85.3%	Very High	60.6%	Low	62.7%	Low
Day-to-day								
Consistency	1.6%	Strong	2.9%	Strong	6.4%	Strong	2.9%	OK
Group consensus	65.2%	Moderate	86.3%	Very High	59.0%	Low	65.0%	Moderate
Taskforce								
Consistency	2.0%	Strong	2.0%	Strong	9.9%	Strong	3.0%	Strong
Group consensus	64.1%	Low	84.7%	High	63.2%	Moderate	61.1%	Low

A consistency ratio lower than 10% indicates a strong consistency [41] of the answers per set of pairwise comparisons. Our overall consistency for combined (1.7%), Member States (2.2%), Third Parties (7,6%), and Europol Units (2.5%) is substantial. Looking more closely, the three groups shows that the Member States and Europol Units have been more consistent in their ranking within the group than third parties (Table 4).

In general, and for both modes of collaboration, the consensus between all the various participants and the consensus per group is low, except for the Member States, whose consensus is high.

5.2 Evaluation: Interviews in an ELE CNO

A total of fifty participants were invited to participate. Fifteen participants were able to take an active role in the interview; seven Member States; three Third Parties; five Europol Units. All were able to answer from their current experiences and professional positions.

Participants jointly confirmed that trust is an important component of collaboration in a CNO and also provided multiple opportunities and needs for improvement in their current way of working and IT systems (for secure messaging and large-volume data

sharing). Multiple participants used the quote "no trust, no sharing." Nevertheless, it also became clear that trust in itself is not the only issue that affects data sharing. Many practical issues were mentioned and, specifically, the need for easy-to-use tools: "Technology is too cumbersome." There are also formal obstacles in the differences between national legislation, formal data sharing agreements and their collective interpretation, and operational decision-making and procedures. Furthermore, the always present time pressure to close more cases leads to data sharing only when a clear reciprocal value is expected for the immediate case at hand: "with the workload … they just don't have the time to do it."

The most crucial recurring issue for the owner is the uncertainty whether the data will be handled in such a way that their interests will not be jeopardized, i.e., progress of an ongoing investigation or the safety of an informant. The only viable way by which this obstacle could be overcome is to have a face-to-face meeting to reach the appropriate level of trust, "I know this guy on the other side of the telephone, because we had a few meetings prior to our data exchange and I really have the impression that he is trustworthy guy, and therefore I share the data". Another sharing topic is that one of the parties should start sharing first, thus providing small portions of data to see if one gets valuable data back from the other party. A DLT could facilitate the creation of this interaction by using a smart contract and by interacting with an oracle such that data is only released when the other party also provides data. Implementing identity management and data management would not only provide transparency of the data itself but also guides proper usage, prevents abuse, and in essence, improves the sharing of that data. These DLT-characteristics could reinforce trust when it has been established.

The participants jointly confirmed that competence and relational trust are the most essential trust categories, "Because you would like to trust your recipient that he handles the data with care. …The point is to take into consideration and to make sure that you don't spoil somebody else's work." For Third Parties, negative trust is an important category, mainly due to their asymmetric relationship compared with other CNO members; as it was stated, "Different levels of membership create limitations." The participants jointly confirmed that modern technology could be useful to overcome many if not all barriers, but "it needs to be well explained how it works" to all stakeholders "in layman's terms to those who are not digi-natives." In essence, trust needs to be bestowed upon the technology. All participants stressed the importance of creating trust, initially, between persons rather than between organizations. Importance of personal trust underlines that antecedents for contractual trust are ranked as less critical.

The interview results clearly showed that there is a sound opportunity to address the trust necessary for data sharing by developing an easy-to-use, yet trusted and legally compliant, infrastructure for the law enforcement CNO, using modern technology.

6 Discussion, Limitations, and Future Research

DLT looks like a promising development to facilitate inter-organization communication as needed within a CNO [5, 7, 8]. The DLT-characteristics can be partially mapped on the CNO characteristics of Van den Heuvel et al. [16] for example, the CNO-capabilities "high amount of trust", "IT as an essential capability" and "non-hierarchical determined

control function", and thus DLT could be used to create a system for inter-organizational collaboration (an 'operating system' for collaboration) where trust is an important aspect. Our research confirms the need for trust to start data sharing in CNOs.

Due to this being a relatively new research field, dominated by technology research, implementing this technology within an IT landscape from a governance or management perspective is not yet part of the current body-of-knowledge. The interest in DLT research from a technology perspective results in a variety in DLT implementations. These DLT implementations have their own characteristics and goals and it is, therefore, necessary to choose the specific implementation based on a match between features in the DLT and requirements for the implementation itself. We think that determining the most suitable set of DLT-characteristics, matching the business needs, could help inter-organizational communication and could facilitate the complex problem of inter-organizational alignment and collaboration.

As shown in the AHP results, we concur with Cheikhrouhou et al. [4] that competence, relational, and contractual trust are the main trust factors in a horizontal CNO. Our results provided more profound insights into divisions and different styles of collaboration. The day-to-day operation could be seen as a VBE environment, whereas the taskforce mode is a VO. It seems that this difference in participation style influences the ranking of the trust factors and thus trust antecedents resulting in different needs. The DLT choice can therefore differ, or must be able to adapt to these differences. When looking at trust antecedents, we see that overall quality and reliability (competence trust) are the highest rated components. DLT can facilitate quality and reliability and facilitate data sharing between participants. While we initially foresaw the risk of cyclic reasoning as mentioned in Sect. 4.1, we discovered that well-controlled and initially limited data sharing was sometimes used as a mechanism to test if further sharing would be possible, thereby demonstrating the validity of Cheikhrouhou et al. [4] inclusion of this factor, albeit that the factor is too generic within our research.

Our model could act as a starting point for improving trust, resulting in data sharing and mutual benefits. Trust keeps being an important topic when discussing collaboration [3, 4, 16], and trust forms can be stimulated by implementing IT systems. DLT could well be a suitable solution, and our model provides a first step in influencing trust by using this technology in collaborative environments. From a practitioner perspective, our research helps to select the DLT where a specific goal needs to be achieved. If the goal of the implementation is to improve trust between parties, our model could help select a DLT that interacts with specific trust components.

Within our research, we combined DLT and CNO because we think the characteristics of these two concepts are complementary. It could be argued that any technology could be researched within a CNO context to facilitate collaboration and to cope with CNO-dynamism, however, we decided to use DLT as it seems promising for the complex collaborative context and inter-organizational communication due to its reliability emerging from its distributed nature, immutability, and transparency. We do not claim that DLT is the only solution, but it appears to be interesting to research.

We see multiple possibilities for future research. First, the mapping in our decision model between trust categories, antecedents, and DLT-characteristics is made based on requirements and evaluated by two experts. A more in-depth validation could be

executed based on empirical evidence. We do think that this method is sufficient for this paper, but additional experiments need to take place. Second, our research took place in only one CNO out of the vast number of possible configurations of CNOs, and other configurations need to be researched to strengthen the model. Even so, the resulting trust antecedents and linked DLT-characteristics provide new insights into options for trust-building in CNOs using novel technology to address CNO-dynamism. Finally, DLT research is focusing on the IT aspects, like storage, integrity, and ownership, but the usage of DLT within the IS research field is not yet part of current research. We, therefore, recommend that IS scholars should embrace this maturing technology stack as an opportunity to create operating systems for inter-organizational communication.

7 Conclusion

We researched how we could improve collaboration, specifically data sharing, between organizations by influencing trust via DLT. Our research confirmed that trust is essential for data sharing between collaborating organizations. Competence, relational, and contractual trust are the most essential trust factors within CNOs, and DLT can influence trust if the right characteristics are selected based on the type of relationship between participants and how they work together (VBE/VO). Therefore, our model provides guidance on selecting the right DLT (characteristics) to improve trust and data sharing.

References

1. Camarinha-Matos, L.M.: Collaborative networked organizations: status and trends in manufacturing. Annu. Rev. Control **33**(2), 199–208 (2009)
2. Concha, D., Espadas, J., Romero, D., Molina, A.: The e-HUB evolution: from a custom software architecture to a software-as-a-service implementation. Comput. Ind. **61**(2), 145–151 (2010)
3. van den Heuvel, R., van de Wetering, R., Bos, R., Trienekens, J.: Identification of IT-needs to cope with dynamism in collaborative networked organizations—a case study. In: Agrifoglio, R., Lamboglia, R., Mancini, D., Ricciardi, F. (eds.) Digital Business Transformation. LNISO, vol. 38, pp. 219–236. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-47355-6_15
4. Cheikhrouhou, N., Pouly, M., Madinabeitia, G.: Trust categories and their impacts on information exchange processes in vertical collaborative networked organisations. Int. J. Comput. Integr. Manuf. **26**(1–2), 87–100 (2013)
5. Pedersen, A.B., Risius, M., Beck, R.: A ten-step decision path to determine when to use blockchain technologies. MIS Q. Exec. **18**(2), 3 (2019)
6. Filipova, N.: Blockchain - an opportunity for developing new business models. Bus. Manag. Bizn. Upravlenie **2**, 75–92 (2018)
7. Beck, R.: Beyond bitcoin: the rise of blockchain world. Computer **51**(2), 54–58 (2018)
8. Guggenmos, F., Rieger, A., Wenninger, A., Fridgen, G., Lockl, J.: How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German asylum procedure. In: 53th Hawaii International Conference on System Sciences, Hawaii, Maui (2019)
9. Akram, A., Bross, P.: Trust, privacy and transparency with blockchain technology in logistics. In: 12th Mediterranean Conference on Information Systems (MCIS), Corfu, Greece (2018)

10. Hawlitschek, F., Notheisen, B., Teubner, T.: The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. **29**, 50–63 (2018)
11. Rossi, M., Mueller-Bloch, C., Thatcher, J.B., Beck, R.: Blockchain research in information systems: current trends and an inclusive future research agenda. J. Assoc. Inf. Syst. **20**(9), 1390–1405 (2019)
12. Beck, R., Avital, M., Rossi, M., Thatcher, J.B.: Blockchain technology in business and information systems research. Bus. Inf. Syst. Eng. **59**(6), 381–384 (2017). https://doi.org/10.1007/s12599-017-0505-1
13. Camarinha-Matos, L.M., Afsarmanesh, H.: Collaborative Networks: Reference Modeling. Springer Science+Business Media, LLC, New York (2008)
14. Camarinha-Matos, L.M., Afsarmanesh, H.: Taxonomy of collaborative networks forms: FInES task force on collaborative networks and socolnet - society of collaborative networks. In: Roots and Wings, European Commission (2012)
15. Msanjila, S.S., Afsarmanesh, H.: FETR: a framework to establish trust relationships among organizations in VBEs. J. Intell. Manuf. **21**(3), 251–265 (2010)
16. van den Heuvel, R., Trienekens, J., van de Wetering, R., Bos, R.: Toward CNO characteristics to support business/IT-alignment. In: Camarinha-Matos, L.M., Afsarmanesh, H., Fornasiero, R. (eds.) PRO-VE 2017. IAICT, vol. 506, pp. 455–465. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-65151-4_41
17. Castaldo, S., Premazzi, K., Zerbini, F.: The meaning(s) of trust. a content analysis on the diverse conceptualizations of trust in scholarly research on business relationships. J. Bus. Ethics **96**(4), 657–668 (2010)
18. Yang, K.-C.: Intellectual structure of trust in business and management: a co-citation analysis. Electron. Libr. **34**(3), 358–370 (2016)
19. Jarratt, D., Ceric, A.: The complexity of trust in business collaborations. Australas. Market. J. (AMJ) **23**(1), 2–12 (2015)
20. Tomkins, C.: Interdependencies, trust and information in relationships, alliances and networks. Acc. Organ. Soc. **26**(2), 161–191 (2001)
21. Fulmer, C.A., Gelfand, M.J.: At what level (and in whom) we trust: trust across multiple organizational levels. J. Manag. **38**(4), 1167–1230 (2012)
22. Jarvenpaa, S.L., Knoll, K., Leidner, D.E.: Is anybody out there? Antecedents of trust in global teams. J. Manag. Inf. Syst. **14**(4), 29–64 (1998)
23. Klein, R., Rai, A.: Inter-firm strategic information flows in supply chain logistics relationships. MIS Q. 735–762 (2009)
24. Aden, H.: Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union. West Eur. Polit. **41**(4), 981–1002 (2018)
25. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
26. Merkle, R.C.: A certified digital signature. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 218–238. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_21
27. Beck, R., Müller-Bloch, C.: Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization. In: 50th Hawaii International Conference on System Sciences, (2017)
28. Scholz, T.M., Stein, V.: The architecture of blockchain organization. In: Thirty Ninth International Conference on Information Systems, San Francisco (2018)
29. Swan, M.: Blockchain: Blueprint for a New Economy, 1st edn. O'Reilly Media Inc, Sebastopol (2015)
30. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. J. Manag. Inf. Syst. **24**(3), 45–77 (2007)
31. Bichler, M.: Design science in information systems research. Wirtschaftsinformatik **48**(2), 133–135 (2006). https://doi.org/10.1007/s11576-006-0028-8

32. Hevner, A.R.: A three cycle view of design science research. Scand. J. Inf. Syst. **19**(2), 87–92 (2007)
33. Venable, J., Pries-Heje, J., Baskerville, R.: FEDS: a framework for evaluation in design science research. Eur. J. Inf. Syst. **25**(1), 77–89 (2016)
34. Saunders, M., Lewis, P., Thornhill, A.: Research Methods for Business Students. 7th ed. Pearson Education Limited, Harlow (2016)
35. Europol: Europol Strategy 2020+. 2018. https://www.europol.europa.eu/publications-documents/europol-strategy-2020. Accessed 3 November 2019
36. Saaty, T.L.: Decision making with the analytic hierarchy process. Int. J. Serv. Sci. **1**(1), 83–98 (2008)
37. Msanjila, S.S., Afsarmanesh, H.: Trust analysis and assessment in virtual organization breeding environments. Int. J. Prod. Res. **46**(5), 1253–1295 (2008)
38. Ølnes, S., Ubacht, J., Janssen, M.: Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov. Inf. Q. **34**(3), 355–364 (2017)
39. Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
40. Conte de Leon, D., Stalick, A.Q., Jillepalli, A.A., Haney, M.A., Sheldon, F.T.: Blockchain: properties and misconceptions. Asia Pac. J. Innov. Entrep. **11**(3), 286–300 (2017)
41. Saaty, T.L., Vargas, L.G.: Decision Making with the Analytic Network Process, 2nd edn. Springer Science+Business Media, New York (2006)