Bridging the Gap: Examining the trust dimensions of smart contracts using supply chain applications

Wieland Müller[1], Michael Leyer[2,3]

[1] Rostock University, Ulmenstraße 69, 18057 Rostock, Germany
[2] Marburg University, Universitätsstraße 25, 35037 Marburg, Germany
[3] Queensland University of Technology, 4101 Brisbane, Australia

Abstract

This paper examines trust towards distributed ledger-based smart contracts in supply chain management, aiming to develop a multidimensional model of trust and provide practical insights. A quantitative survey was conducted among supply chain employees in the United States. Confirmatory factor analysis validated the proposed model, revealing five trust dimensions: dispositional trust, situational social trust, information-technology trust, interaction-informed trust, and learned data trust. These dimensions capture the complexity of trust towards smart contract-enabled supply chains, considering the interplay between social and technical factors. The findings contribute to theoretical understanding and offer practical guidance for enhancing collaboration, minimizing risks, and maximizing the benefits of trustless supply chain networks. Future research should incorporate additional influencing factors to develop a more holistic trust model for smart contracts.

Keywords

smart contracts, distributed ledger technology, dimensions of trust

1. Introduction

Trust plays a pivotal role in the conventional management of supply chains, ensuring the seamless flow of goods and services among various stakeholders. Suppliers, manufacturers, distributors, and customers rely on mutual trust to fulfil their obligations, as any breach can result in delays, disputes, and financial setbacks. However, the emergence of smart contracts and distributed ledger technology holds the potential to revolutionize supply chain operations. By eliminating the need for intermediaries or third-party authorities, these technologies encode transaction rules and conditions into self-executing smart contracts. This not only mitigates the risk of fraud and human error but also streamlines the entire process while enhancing transparency. In the context of supply chains, trust manifest itself through various aspects.

Distributed ledger based smart contracts have emerged as a promising technology that aims to enable trustless network and transaction processes within various domains. The concept of a trustless network suggests that smart contracts have the potential to eliminate the reliance on trust towards traditional network architectures (Christidis and Devetsikiotis 2016). However, contrary to the belief that technology can entirely eradicate the need for trust, it actually presents a novel approach to substitute information from alternative sources to establish trust and subsequently act upon it (Lemieux et al. 2019). Consequently, a trustless system does not imply a system devoid of trust, but rather a system where trust is redefined and placed upon verifiable and automated mechanisms. Therefore, it is crucial to develop an understanding of trust and its various facets in order to facilitate the development and successful deployment of efficient trustless systems within supply chains.

Proceedings Acronym: Proceedings of the LWDA 2023 Workshops, October 09–11, 2023, Marburg, Germany
wieland.mueller@uni-rostock.de (W. Müller); michael.leyer@wiwi.uni-marburg.de (M. Leyer)
0000-0002-2172-8725 (W. Müller); 0000-0001-9429-7770 (M. Leyer)

To explain the dimensions of trust in organisations, different studies have explored trust from various organisational perspectives (Yamagishi and Yamagishi 1994; Mayer, Davis, and Schoorman 1995; Rousseau et al. 1998), including the trust in technologies (McKnight et al. 2011; Pavlou 2003). Nonetheless, none of these models consider smart contracts or fully account for the unique characteristics of this technology. Therefore, there is a research gap that needs to be addressed by developing a multidimensional model of trust and empirically investigating its implications in the field of supply chain management.

To close this gap, we want to answer following research question: How should a model be designed to represent the dimensions of trust towards distributed ledger based smart contracts? By comprehensively studying and addressing trust dimensions, we can enhance the design, implementation, and governance of smart contract-enabled supply chains. This, in turn, fosters greater trust among participants, boosts collaboration, minimizes transactional risks, and unlocks the full potential of trustless supply chain networks to enhance global trade and commerce.

The theoretical foundation of the proposed multidimensional model of trust are the three trust layers according to Hoff and Bashir (2014) and the three layers of distributed ledger technology according to Lemieux et al. (2019). A quantitative survey for the empirical analysis was conducted in the United States of America and allowed employees from companies involved in a supply chain. To analyse our research model, we initially applied the procedure outlined by Cenfetelli and Bassellier (2009) to interpret the established formative measurement model. Subsequently, we conducted a factor analysis, utilizing the maximum likelihood method. This method was chosen for factor analysis due to its robustness and suitability for capturing the complex relationships among the observed variables and latent constructs in our research model.

The paper is organised as follows: The following section presents the fundamental background and previous research about trust towards supply chain networks and distributed ledger based smart contracts. In the third section, a multidimensional model of trust towards smart contracts is established based on theoretical literature. Section four explains the method of the study, conducting a quantitative survey, and performing statistical analyses of the empirical data. Furthermore, information about the sample and results of statistical tests are given. Section five describes the development of the model and the hypotheses for the statistical analysis. The results of these analyses are presented in the following section, followed by a critical discussion. In the conclusion, we draw the theoretical and practical implications of the study as well as its limitations and directions for future research.

2. Fundamental Background

2.1. Trust in supply chain networks

Trust is a fundamental element in the realm of supply chains due to the intricate nature of relationships among the various actors involved. The presence of trust significantly impacts the willingness of these actors to share information, mitigate risks, and pursue innovation opportunities, all of which contribute to enhancing the efficiency and effectiveness of the supply chain (Gligor and Holcomb 2013). Notably, the establishment of trust is crucial for fostering robust relationships among participants within the supply chain network, as emphasized by Halldorsson et al. (2007).

In the context of client-contractor relationships, Treiblmaier (2018) posits that complete transparency of information flow has the potential to eliminate the necessity of trust, underscoring the pivotal role of transparency in cultivating trust within supply chains. Furthermore, Treiblmaier (2018) asserts that transparency and non-repudiation of data could render personal relationships obsolete in the trust-building process. Lastly, Treiblmaier (2018) highlights the potential of technology in mitigating trust-related challenges in supply chains.

2.2. Trust towards smart contracts

Smart contracts are automated executing digital contracts that can be written by an "if-this-then-that" code of a distributed ledger network structure. Distributed ledgers utilize encryption technology to securely store and transmit information. Besides of immutability of data, a complete traceability and transparency of data are two other common characteristics of distributed ledger technologies (El Ioini and Pahl 2018). Once established, smart contracts do not require any further management (Vo, Nguyen-Thi, and Nguyen-Hoang 2021).

The automatic execution and assurance of smart contracts including automatic penalties for non-fulfilment of contracts lead to no or less need for trust for transactions in networks (Treiblmaier 2018; Grosse, Guerpinar, and Henke 2021). In addition, mutual trust is nevertheless increased due to the complete transparency of the information flow for both the client and the contractor (Wang et al. 2019). Looking at automation technologies, different levels of trust have been identified by Hoff and Bashir (2014), dispositional, situational and learned trust.

Trust towards a specific information technology plays a key role in the development of IT-related beliefs and behaviour. It is defined by the ability to perform the required functions for a given task, to provide effective assistance when needed, and to work reliably or consistently without failure (McKnight et al. 2011). Different studies highlight the potential of smart contracts to enable automation of various business processes (Zheng et al. 2020; Eggers et al. 2021; Li and Kassem 2021). Trust towards automation depends mostly on the performance, process or purpose of an automated system (Hoff and Bashir 2014).

While some works argues that the underlying distributed ledger technology enables coordination without interpersonal trust, other recognises that trust plays a crucial role in distributed ledger networks (Becker and Bodo 2020). Despite the notion that technology eliminates the requirement for trust, in reality, it provides a new approach to substituting information from other sources to establish trust towards something or someone, and to act on that trust (Lemieux et al. 2019). According to Lemieux et al. (2019) distributed ledger systems rely on three interdependent trust layers, the social, data and technical layer.

3. Models of trust dimensions and hypotheses

3.1. Model conceptualisation

In the literature, there are different models of trust that represent the construct with influencing factors. The Model of Trust by Yamagishi and Yamagishi (1994) suggests that trust is influenced by both structural and cognitive factors. Another fundamental model is the integrative model of trust by Mayer, Davis, and Schoorman (1995) which identifies ability, benevolence, and integrity as the basis of trust, along with the influence of the trustor's propensity and perceived risks. The model of trust from Rousseau et al. (1998) proposes that trust in organizations is comprised of cognitive trust and affective trust. The game-theoretic model according to Das and Teng (2001) suggests that trust in organizations is determined by rational decision-making, with individuals considering the potential benefits and risks of trusting others. Pavlou's (2003) model of trust towards technology adoption includes cognitive and affective trust and incorporates integrity as a factor representing the reliability and honesty of the technology. However, in all these models, trust is seen as a one-dimensional construct that is not subdivided into different levels. We want to close this gap by developing a model that takes into account both the automation characteristics and the characteristics of the underlying distributed ledger technology and thus reflects different dimensions of trust.

To incorporate the specific attributes of distributed ledger technology as the underlying infrastructure for smart contracts, the model has been designed to encompass various levels of this technology. According to Lemieux et al. (2019), the social trust layer of the distributed ledger technology deals with how actors interact and determine the types and sources of information needed to establish trust and take action. The data layer provides the information that actors have deemed necessary to obtain from the distributed ledger system to give them confidence to act.

Finally, the technical layer pertains to the means by which actors create, store, and retrieve tamper-resistant and non-repudiable proof of facts about their interactions (Lemieux et al. 2019). Since dispositional trust refers to a person's general attitude and is not related to the application of a specific technology, this type of trust must be considered on its own. Situational trust and learned trust can be considered from the different perspectives of the three distributed ledger layers (social, data and technical). As can be seen in Figure 1, this results in a total of seven different dimensions of trust regarding smart contract use.

Since smart contracts are essentially automation processes, we have considered different levels of trust towards automation technologies in the model. Hoff and Bashir (2014) were able to empirically establish three different layers for trust towards automation: The first is dispositional trust, which refers to a person's general inclination to trust automation, regardless of the situation or the specific system. It is used to describe long-term tendencies. The second layer is situational trust, which takes into account both the external factors and the operator's own context-dependent characteristics. The third layer is learned trust, which reflects an operator's assessments of a system based on prior experience or current interaction. Since smart contracts are characterised by the automation of contracts, this differentiated dimensions are also suitable for our model (Hoff and Bashir 2014).

Based on the different layers, we created a multidimensional model of trust with seven dimensions, visualized in Figure 1.

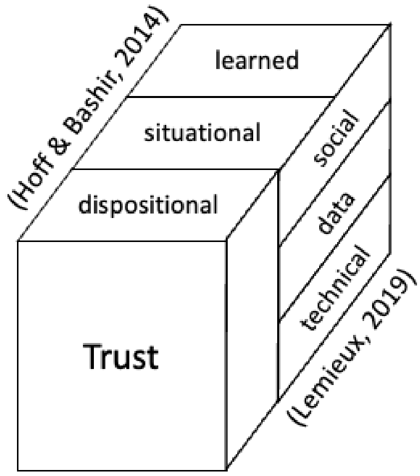

Figure 1: Dimensions of trust towards smart contracts based on Hoff and Bashir (2014) and Lemieux et al. (2019).

The seven dimensions can be defined following according Hoff and Bashir (2014) and Lemieux et al. (2019): Dispositional trust refers to an individual's general tendency to trust others over the long-term, irrespective of the context or a particular system. Situational trust in social layer relates to how social actors interact based on their trust in the external environment and the operator's internal context, such as required information amount and form. Situational trust on the data layer refers to the trust social actors have in the distributed ledger technology system's information for them to confidently act, based on the operator's internal and external context.

Situational trust on the technical layer refers to social actors' trust towards the distributed platform's internal and external characteristics for creating, storing, and exchanging information. Learned trust on the social layer is social actors' developed trust based on past experiences or current interactions, regarding how they interact with each other and required information amount or form. Learned trust on the data layer is social actors' developed trust based on past experiences or current interactions with the information provided by the system, crucial for them to confidently act. Finally, learned trust on the technical layer is the social actors' developed trust based on past experiences or current interactions at a technical level with the platform used for creating, storing, and exchanging information. This leads to the following hypotheses:

H1: Dispositional trust is an independent dimension of trust.
H2: Situational trust on the social layer is an independent dimension of trust.
H3: Situational trust on the data layer is an independent dimension of trust.
H4: Situational trust on the technical layer is an independent dimension of trust.
H5: Learned trust on the social layer is an independent dimension of trust.
H6: Learned trust on the data layer is an independent dimension of trust.
H7: Learned trust on the technical layer is an independent dimension of trust.

3.2. Model operationalisation

To test hypotheses, the model first needs to be conceptualised. For this, the following constructs are necessary: Dispositional Trust, situational trust on the three layers, learned trust on the three layers. To measure dispositional trust we use the five item scale by MacCarthy (1983). For measuring situational trust, the six item scale of Holthausen et al. (2020) was adapted and applied to each of the three distributed ledger trust layers characteristics according to Lemieux et al. (2019). Since the original scale referred partly to decision-making by automated systems, we removed two unsuitable items, resulting in a four-item scale.

For the measurement of learned trust, there is no scale in current literature that could be adopted. However, the literature shows that learned trust is based on previous experiences, similar to the trustor's propensity (Hoff and Bashir 2014). If no direct experience has been made, there is a recourse to similar situations (Gonzalez, Lerch, and Lebiere 2003). However, the propensity refers to general tendencies, the learned trust is based on learned experiences regarding an specific context (Mayer and Davis 1999). Therefore, we have adopted the propensity scale from general Mayer and Davis (1999) in a revised form. The items no longer refer to trust tendencies of general, but refer to previous experienced situations with automation technologies. In addition, we have assigned the items of the scale to the matching layers of trust towards distributed ledger technologies to differentiate between them.

4. Research Method

4.1. Questionnaire and sample

The questionnaire (found in the appendix) incorporated several measures to ensure high data quality. Initially, an attention test was administered to participants. Following that, the survey included questions on dispositional trust, which assessed general trust tendencies according to MacCarthy (1983). The subsequent section focused on the specific context of utilizing smart contracts in supply chains. Within this section, participants were queried about situational trust and adopted the scale from Holthausen et al. (2020) to the tree layer of trust towards distributed ledgers: social trust, data trust, and technical trust Lemieux et al. (2019). Moreover, learned trust was examined by an adoption from Mayer and Davis (1999) trustor's propensity items and also related to the tree layer of trust towards distributed ledgers.

The questionnaire was administered to participants via the online platform Clickworker to supply chain employees in the United States of America. The US is a suitable location for a survey on technologies in supply chain management due to the presence of many companies with key supplier relationships and the diversity of industries and supply chains in the country.

The questionnaire was answered completely by 193 persons. The minimum sample size according to (Tinsley and Kass 1979) of 5-10 cases per item is thus achieved, as is the total minimum of 100 cases for factor analysis according to Gorsuch (1990). 34.2% were women, 65.2% were men, and 0.6% were diverse. On average, participants were 36.6 years old.

4.2. Statistical analysis

By conducting a detailed assessment of the measurement model as a first part of our analysis, we can ensure that the requirements for a confirmatory factor analysis are met and that the results of the analysis are reliable and interpretable. We followed a five-step process for validating a formative measurement construct in structural equation models according to Cenfetelli and Bassellier (2009). In our study, however, we have only conducted the first four steps, as the fifth step concerns the creation of a structural equation model, which is not the focus of this study. In the first step, we looked at a possible multicollinearity among the items using the variance inflation factor (VIF), aiming for values below 5 (Henseler, Ringle, and Sinkovics 2009). Our analysis showed that none of the VIF value exceeded the limit. We also tested for a bivariate correlation between indicators and construct. Since none of the indicators exceeded the value of 0.9, it was not necessary to make adjustments here (Cenfetelli and Bassellier 2009).

The second step was to reduce the number of indicators if their weights were found not to be significant. Our results showed that all items have significant bivariate correlations with the parent construct. In the third step, we examined the presence of suppression effects. These occur when an indicator shares more variance with another indicator than with the formatively measured construct. We found that suppression effects were present for the items DT4, SS2, SD2 and ST2. These four items were eliminated. The fourth step entailed assessing the importance of individual questions for the construct to ensure that their impact was not negligible. Since all bivariate correlations between the questions and the construct were high and significant, all items could be retained for further analysis.

As a second part of the analysis, we conducted a Confirmatory factor analysis (CFA). This is used when the researcher has a pre-specified hypothesis about the underlying factor structure of the data. CFA is used to test whether the data fit the hypothesized factor structure (Graf, Nagler, and Jacobs 2005). Confirmatory factor analysis (CFA) is a statistical technique employed to assess the fit between observed data and a theoretical model. When conducting a CFA, there are several methods available, including maximum likelihood (ML), principal component analysis (PCA), and principal factor analysis (PFA). Among these methods, maximum likelihood is the most widely utilized for CFA due to its flexibility and robustness in handling various data types and model specifications. Conversely, PCA and PFA are exploratory factor analysis techniques primarily employed for uncovering the underlying structure of a dataset and are generally not employed for CFA purposes (Wood 2008). In confirmatory factor analysis (CFA), orthogonal rotation methods such as Varimax are usually used to simplify the factor structure and make it easier to interpret (Flora and Curran 2004).

The evaluation of the factor analysis reveals a very good adequacy of the sample for conducting the factor analysis, as indicated by a Kaiser-Meyer-Olkin measure of sample adequacy of 0.869 (Kaiser 1974). Furthermore, the significance value of the Bartlett's test of sphericity, which is < 0.001, indicates that the sample data are suitable for factor analysis (Bartlett 1954). The rotated sum of squared loadings shows that factor 1 accounts for the highest share of the total variance with 20.39%. The other factors shares are distributed between 3.33% and 8.38%.

5. Results

5.1. Descriptive results

Table 1 below shows the descriptive results of the items examined in the factor analysis.

Table 1
Descriptive results

Item	Minimum	Maximum	Mean	Standard deviation	Variance
DT1	1	7	3,66	1,52	2,30
DT2	1	7	4,04	1,41	1,98
DT3	1	7	4,24	1,35	1,83
DT5	1	7	3,90	1,45	2,11
SS1	1	7	4,32	1,47	2,17
SS3	1	7	4,10	1,49	2,23
SS4	1	7	4,17	1,42	2,03
SD1	1	7	4,62	1,47	2,15
SD3	1	7	4,56	1,61	2,58
SD4	1	7	4,64	1,35	1,82
ST1	1	7	4,74	1,31	1,71
ST3	1	7	4,40	1,55	2,39
ST4	1	7	4,91	1,31	1,72
LS1	1	7	4,10	1,60	2,55
LS2	1	7	4,69	1,29	1,67
LD1	1	7	4,53	1,41	2,00
LD2	1	7	4,58	1,42	2,03
LT1	2	7	5,24	1,40	1,97
LT2	1	7	4,90	1,21	1,45
DT	1	7	3,96	1,00	1,00
SS	1	7	4,20	1,19	1,43
SD	1	7	4,60	1,27	1,61
ST	1	7	4,68	1,19	1,41
LS	2	7	4,40	0,88	0,78
LD	1	7	4,55	1,19	1,42
LT	2	7	5,07	0,89	0,78

5.2. Hypotheses results

The following table 2 shows the rotated factor loadings, which indicate the strength and direction of the correlation between the variables and the factors. All values show a positive direction of the correlation. We followed the Budaev (2010) procedure for rather small sample sizes and set the minimum for interpretable loadings to higher than 0.4.

Table 2
Rotated factor matrix: Confirmatory factor analysis using maximum likelihood (loadings below 0.4 hidden if higher available).

	1	2	3	4	5	6	7
DT1		.740					
DT2		.693					
DT3		.342		.357			
DT5		.385					
SS1				.432			
SS3	.439			.471			
SS4				.772			
SD1	.770						
SD3	.699						
SD4	.772						
ST1	.697						
ST3	.689						.688
ST4	.672						
LS1					.929		
LS2						.442	
LD1			.418				
LD2			.881				
LT1					.381		
LT2						.564	

DT3 was excluded due to its cross-loadings on factors 2 and 4, according to the criteria of (Hair, 2009). Although LT1 and DT5 fell just below the threshold of 0.4, we decided to retain them. This decision was based on our assessment that the content validity of the scale was not violated (Fornell and Larcker 1981) and on the consistently positive results of all previous statistical tests. ST3 also refers to cross-loadings, but since factor 7 would represent a single dimension with a single factor, the item was retained and assigned to factor 1. Furthermore, we also refer here to the content validity of the scale according to Fornell and Larcker (1981)

H1 stated, that dispositional trust is an independent dimension of trust. This hypothesis could be confirmed, whereby only the items DT1 and DT2 can be assigned to this dimension. H2 stated, that situational trust on the social layer is an independent dimension of trust. This hypothesis could also be confirmed. All three items could be assigned to the dimension. H3 and H4 stated, that situational trust on the data layer and situational trust on the technical layer are independent dimensions of trust. This hypothesis could not be confirmed. Contrary to the assumption, however, the items of the two layers form a mutual dimension. H5 stated, that learned trust on the social layer is an independent dimension of trust. This hypothesis could not be confirmed either. However, it could be found that learned trust on social layer together with learned trust on the technical layer represent a common dimension. H7 (Learned trust on the technical layer is an independent dimension of trust.) could therefore not be confirmed either. H6 stated, that learned trust on the data layer is an independent dimension of trust. This hypothesis could be confirmed, with both of the selected items together forming the fifth trust dimension.

As can be seen in table 3, the results reveal the following dimensions with associated items regarding trust towards smart contracts:

Table 3
Dimensions of trust towards smart contracts

Dimension	Items
Dispositional trust	DT1, DT2, DT5
Situation social trust	SS1, SS2, SS4
Situational data and situational technical trust	SD1, SD3, SD4, ST1, ST3, ST4
Learned social and learned technical trust	LS1, LS2, LT1, LT2
Learned data trust	LD1, LD2

The new dimensions result from the assignment of the items to the factors. If the items correlated to different factors, the factor with the highest loading was selected. Since LT1 did not have a value above the 0.4 limit, we checked for the next highest, which is 0.381. Since the item proves to be conceptually important that it represents only one of the two items of learned trust and it is only slightly below the limit, it may be justified to keep it (Mayer 2018). Since the LD and LT load on a mutual factor with one item each, we have combined them into one common dimension. This is possible due to the similarity in content of the items and scales (Hair 2009), which all refer to learned trust, and thus facilitates interpretation of the dimensions. The factor analysis results to an updated model of trust dimensions, seen in Figure 2:

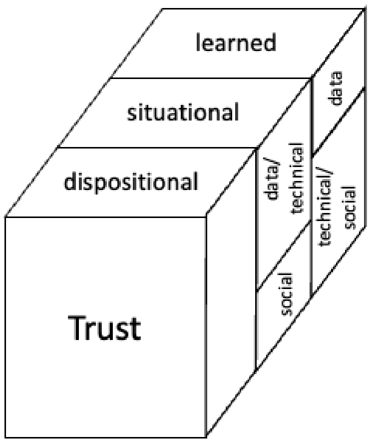

Figure 2: Dimensions of trust towards smart contracts.

6. Discussion

The findings of this study provide valuable insights into the dimensions of trust towards distributed ledger-based smart contracts within supply chain management. The theoretical foundation of the multidimensional model was based on previous literature from Lemieux et al. (2019) and Hoff and Bashir (2014). While previous models focused on one-dimensional trust constructs (Yamagishi and Yamagishi 1994; Mayer, Davis, and Schoorman 1995; Rousseau et al. 1998; Pavlou 2003; McKnight et al. 2011), this study aimed to develop a more comprehensive model that considers the specific characteristics of smart contracts and distributed ledger technology. The results of the confirmatory factor analysis (CFA) support the existence of multiple dimensions of trust towards smart contracts. The analysis revealed the presence of five distinct dimensions: dispositional trust, situational social trust, situational data and technical trust, learned social and technical trust, and learned data trust. These dimensions capture different aspects of trust in the context of smart contracts, demonstrating the complexity and multidimensionality of trust in this technology-enabled setting.

One interesting finding from the factor analysis is the mixing of theoretical dimensions in practice. Specifically, the original hypothesis that situational trust on the data layer and situational trust on the technical layer would be independent dimensions of trust was not supported. Instead, the items from these two layers formed a mutual dimension. Similarly, the hypothesis that learned trust on the social layer and learned trust on the technical layer would be independent dimensions was also not supported. These two dimensions have been merged into a single dimension. The three trust layers of Hoff and Bashir (2014) could be confirmed, while the three layers of Lemieux et al. (2019) were recognized in mixed forms.

The mixing of theoretical dimensions in practice can be attributed to the interconnectedness and interdependence of trust factors in smart contract-enabled supply chains. While theoretical models often attempt to separate trust into distinct dimensions, the practical reality is that trust is a complex construct influenced by various factors that interact and influence each other. In the context of smart contracts, the distributed ledger technology and the social interactions among actors create a dynamic environment where trust dimensions overlap and intertwine. Considering the merging of theoretical dimensions in the empirical analysis, it is essential to propose appropriate names for the new mixed dimensions based on their underlying characteristics.

The dimension combining situational trust on the data layer and situational trust on the technical layer reflects the intertwined trust towards the information provided by the distributed ledger system and the characteristics of the distributed ledger platform. This dimension can be labelled as "Information-Technology Trust" to capture the intertwined nature of trust towards the technical aspects of the system and the reliability and accuracy of the data. The dimension merging learned trust on the social layer and learned trust on the technical layer indicates the importance of past experiences and interactions in shaping trust perceptions. This dimension can be named "Interaction-Informed Trust" to highlight the role of previous interactions and learning in establishing trust towards both the social dynamics and the technical aspects of smart contract-enabled supply chains.

Understanding the influence of different dimensions on the variance provides insights into the relative importance of each dimension in explaining trust towards smart contracts. By examining the rotated sum of squared loadings, we can identify the dimensions that contribute the most to the model.

Based on the results, it can be observed that the "Information-Technology Trust" dimension (with situational trust on the data layer and situational trust on the technical layer) accounts for the highest share of the total variance, contributing 20.39%. This suggests that trust in the information provided by the distributed ledger system and the reliability of the blockchain platform plays a significant role in shaping overall trust perceptions in smart contracts. The combined "Interaction-Informed Trust" dimension (merging learned trust on the social layer and learned trust on the technical layer) also contributes a substantial amount to the variance, accounting for 11.55%. This indicates that past experiences and interactions, both social and technical, have a significant impact on establishing trust towards smart contracts. The remaining dimensions, contribute to the variance to a lesser extent. However, they still play important roles in shaping trust perceptions in specific contexts within smart contract-enabled supply chains with between 6.1% and 8.4% variance.

The transferability of the results of this study regarding trust dimensions to other industries beyond supply chain management is an important consideration. While the specific context of supply chains was examined in this research, the identified trust dimensions and their underlying concepts have the potential to be applicable to various industries.

The multidimensional model of trust developed in this study provides a framework that can be adapted and applied to other sectors. The dimensions of trust, such as dispositional trust, situational trust, and learned trust, capture fundamental aspects of trust that are relevant across different industries. The models' flexibility allows for customization and adaptation to specific industry contexts, making it transferable to diverse sectors. Also, the technological advancements and the concept of smart contracts explored in this study are not exclusive to supply chain management. Many industries are adopting distributed ledger technology and exploring the potential of smart contracts to streamline processes, enhance transparency, and reduce transactional risks. The dimensions of trust identified in this study, which encompass both technological and social aspects, can be relevant for understanding and managing trust in these industries as well.

For example, in the financial sector, where blockchain technology is being explored for applications such as digital currencies and smart contracts, the dimensions of trust identified in this study can help financial institutions build trust with customers and counterparties. By addressing the different aspects of trust, financial institutions can enhance security, reliability, and transparency, which are critical for building trust in financial transactions. Similarly, in healthcare, the use of smart contracts and distributed ledger technology has the potential to transform patient care, medical record management, and supply chain processes. Applying the trust dimensions identified in this study can help healthcare organizations establish trust in the security, accuracy, and privacy of medical data and transactions, leading to improved patient outcomes and efficiency.

7. Conclusion

7.1. Theoretical contribution

This study contributes to the theoretical understanding of trust towards distributed ledger-based smart contracts within supply chain management in several ways. Firstly, it goes beyond existing one-dimensional models by developing a multidimensional model of trust that considers the unique characteristics of smart contracts and distributed ledger technology. This multidimensional model captures the complexity and multidimensionality of trust in the context of smart contracts, highlighting the interplay between social and technical factors.

Secondly, the findings of the confirmatory factor analysis support the existence of five distinct dimensions of trust: dispositional trust, situational social trust, information-technology trust, experience-based trust, and learned data trust. This expands the understanding of trust dimensions in smart contracts and underscores the intertwined relationships among trust factors. The model and the identified dimensions contribute to the advancement of smart contract-enabled supply chains.

Furthermore, the observation of mixed theoretical dimensions in the empirical analysis suggests that trust towards smart contracts cannot be easily separated into discrete dimensions. The interplay between social dynamics, technical characteristics, and past experiences plays a crucial role in shaping trust perceptions in smart contract-enabled supply chains. This highlights the need for a holistic approach that considers not only the trust construct but also other influencing factors when examining trust towards smart contracts.

7.2. Practical contribution

The practical implications of this study have significant relevance for supply chain practitioners and decision-makers. The identified trust dimensions and their implications offer actionable insights that can be applied to enhance supply chain operations and foster trust towards smart contract-enabled networks.

Firstly, understanding the different dimensions of trust and their relative importance enables organizations to improve collaboration and mitigate transactional risks in supply chain networks. By assessing the strengths and weaknesses of each dimension, supply chain managers can identify areas that require attention and implement strategies to strengthen trust. For instance, if the dimension of learned trust on the technical layer exhibits a low level of trust among participants, efforts can be made to enhance technological literacy, provide training programs, and improve user experience.

Secondly, the findings emphasize the importance of adopting a holistic approach to trust-building in supply chains. While ensuring the reliability and security of smart contracts is crucial, attention should also be given to fostering social aspects of trust. Supply chain managers can cultivate a trust-oriented culture by promoting open communication, transparency, and collaboration among participants. Establishing strong relationships and maintaining effective communication channels can significantly contribute to building trust and facilitating the successful implementation of smart contracts.

Furthermore, the results highlight the influence of both technological and social factors on trust towards smart contracts. This implies that supply chain managers should consider not only the technical aspects of implementing smart contracts but also the social dynamics and human factors involved. Effective change management strategies, comprehensive training programs, and targeted communication initiatives can help address potential resistance to adopting smart contracts and build trust among supply chain participants.

7.3. Limitations and future research

This study has certain limitations that should be acknowledged. The sample used in the empirical analysis was limited to supply chain employees in the United States, which may restrict the generalizability of the findings to other industries and geographical regions. The data collected in this study relied on self-report measures, which are subject to potential biases such as social desirability and respondent interpretation.

Trust is a dynamic construct that can fluctuate over time due to changing circumstances and experiences. This study captured trust perceptions at a specific point in time, but it is essential to recognize that trust can evolve and be influenced by ongoing interactions, system performance, and external events. Future research should consider longitudinal studies to examine the temporal dynamics of trust towards smart contract-enabled supply chains.

To enhance the generalizability of the findings, future research should expand the study to include participants from diverse industries beyond supply chain management. Different industries may have unique characteristics and trust dynamics in the context of smart contracts. Examining trust dimensions and their relative importance across various sectors such as finance, healthcare, energy, and manufacturing would provide valuable insights and enable the development of industry-specific frameworks for trust towards smart contract-enabled environments.

Future research could explore the design and implementation of interventions aimed at fostering trust towards smart contract-enabled supply chains. These interventions could include strategies to improve transparency, establish reputation mechanisms, enhance contractual governance, and address potential trust breaches. Evaluating the effectiveness of such interventions in building and maintaining trust would provide practical guidance for supply chain practitioners and policymakers.

While this study provides valuable insights into the multidimensional nature of trust towards smart contracts, there is a need for a more holistic model that incorporates not only the trust construct but also other influencing factors. Future research should explore additional factors such as risk perception, transparency, reputation, contractual governance mechanisms, and technological characteristics (e.g., scalability, interoperability) that can influence trust towards smart contract-enabled supply chains. Developing a more comprehensive model that considers these factors would provide a deeper understanding of the complex dynamics of trust in this context.

References

[1] Bartlett, Maurice S. 1954. "A note on the multiplying factors for various χ 2 approximations." *Journal of the Royal Statistical Society. Series B (Methodological)* 16 (2):296-8.

[2] Becker, Mortiz, and Balázs Bodo. 2020. "Trust in blockchain-based systems." *Internet Policy Review* 10 (2):1-10. doi: 10.14763/2021.2.1555.

[3] Budaev, Sergey V. 2010. "Using principal components and factor analysis in animal behaviour research: caveats and guidelines." *Ethology* 116 (5):472-80. doi: 10.1111/j.1439-0310.2010.01758.x.

[4] Cenfetelli, Ronald T., and Geneviève Bassellier. 2009. "Interpretation of Formative Measurement in Information Systems Research." *MIS quarterly* 33 (4):689-707. doi: 10.2307/20650323.
[5] Christidis, Konstantinos, and Michael Devetsikiotis. 2016. "Blockchains and smart contracts for the internet of things." *IEEE Access* 4 (1):2292-303. doi: 10.1109/ACCESS.2016.2566339.
[6] Das, Tushar Kanti, and Bing-Sheng Teng. 2001. "Trust, control, and risk in strategic alliances: An integrated framework." *Organization studies* 22 (2):251-83. doi: 10.1177/0170840601222004.
[7] Eggers, Julia, Andreas Hein, Jörg Weking, Markus Böhm, and Helmut Krcmar. 2021. "Process automation on the blockchain: an exploratory case study on smart contracts." *Hawaii International Conference on System Sciences (HICSS)* 54:1-10. doi: 10.24251/HICSS.2021.681.
[8] El Ioini, Nabil, and Claus Pahl. 2018. "A review of distributed ledger technologies." *On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II*:277-88. doi: 10.1007/978-3-030-02671-4_16.
[9] Flora, D. B., and P. J. Curran. 2004. "An empirical evaluation of alternative methods of estimation for confirmatory factor analysis with ordinal data." *Psychol Methods* 9 (4):466-91. doi: 10.1037/1082-989x.9.4.466.
[10] Fornell, Claes, and David F Larcker. 1981. "Evaluating structural equation models with unobservable variables and measurement error." *Journal of marketing research* 18 (1):39-50.
[11] Gligor, David, and Mary Holcomb. 2013. "The role of personal relationships in supply chains: An exploration of buyers and suppliers of logistics services." *The International Journal of Logistics Management* 24 (3):328-55. doi: 10.1108/IJLM-07-2012-0067.
[12] Gonzalez, Cleotilde, Javier F. Lerch, and Christian Lebiere. 2003. "Instance-based learning in dynamic decision making." *Cognitive Science* 27 (4):591-635. doi: 10.1016/S0364-0213(03)00031-4.
[13] Gorsuch, Richard L. 1990. "Common factor analysis versus component analysis: Some well and little known facts." *Multivariate behavioral research* 25 (1):33-9. doi: 10.1207/s15327906mbr2501_3.
[14] Graf, Ralf Dipl.-Ing., Markus Nagler, and Arthur M. Jacobs. 2005. "Faktorenanalyse von 57 Variablen der visuellen Worterkennung." *Zeitschrift Fur Psychologie-journal of Psychology* 213 (4):205-18. doi: 10.1026/0044-3409.213.4.205.
[15] Grosse, Nick, Tan Guerpinar, and Michael Henke. 2021. "Blockchain-Enabled Trust in Intercompany Networks Applying the Agency Theory." *Blockchain and Internet of Things Conference* 3 (1):8–14. doi: 10.1145/3475992.3475994.
[16] Hair, Joseph F. 2009. *Multivariate data analysis*. 7 ed.
[17] Halldorsson, Arni, Herbert Kotzab, Juliana H Mikkola, and Tage Skjøtt-Larsen. 2007. "Complementary theories to supply chain management." *Supply Chain Management: An International Journal* 20 (6):574-86. doi: 10.1108/SCM-06-2015-0228.
[18] Henseler, Jörg, Christian M Ringle, and Rudolf R Sinkovics. 2009. "The use of partial least squares path modeling in international marketing." *New challenges to international marketing* 20 (1):277-319. doi: 10.1108/S1474-7979(2009)0000020014.
[19] Hoff, Kevin Anthony, and Masooda Bashir. 2014. "Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust." *Human Factors* 57 (3):407-34. doi: 10.1177/0018720814547570.
[20] Holthausen, Brittany E, Philipp Wintersberger, Bruce N Walker, and Andreas Riener. 2020. "Situational trust scale for automated driving (STS-AD): Development and initial validation." *International Conference on Automotive User Interfaces and Interactive Vehicular Applications* 12 (1):40-7. doi: 10.1145/3409120.3410637.
[21] Kaiser, Henry F. 1974. "An index of factorial simplicity." *Psychometrika* 39 (1):31-6. doi: 10.1007/BF02291575.
[22] Lemieux, Victoria, Darra Hofman, Danielle Batista, and Alysha Joo. 2019. "Blockchain Technology & Recordkeeping." doi: 10.13140/RG.2.2.28447.56488.

[23] Li, Jennifer, and Mohamad Kassem. 2021. "Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction." *Automation in Construction* 132:103955. doi: 10.1016/j.autcon.2021.103955.
[24] MacCarthy, Bill. 1983. "Measuring Social Life Feelings." *The British Journal of Psychiatry* 143 (2):206-7. doi: 10.1192/S0007125000117246.
[25] Mayer, Roger C, and James H Davis. 1999. "The effect of the performance appraisal system on trust for management: A field quasi-experiment." *Journal of applied psychology* 84 (1):123-36. doi: 10.1037/0021-9010.84.1.123.
[26] Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. "An Integrative Model of Organizational Trust." *The Academy of Management Review* 20 (3):709-34. doi: 10.2307/258792.
[27] Mayer, Sabrina J. 2018. "Hauptkomponentenanalyse und explorative Faktorenanalyse." In *Handbuch Methoden der Politikwissenschaft*, edited by Claudius Wagemann, Achim Goerres and Markus Siewert, 1-26. Wiesbaden: Springer Fachmedien Wiesbaden.
[28] McKnight, D Harrison, Michelle Carter, Jason Bennett Thatcher, and Paul F Clay. 2011. "Trust in a specific technology: An investigation of its components and measures." *ACM Transactions on management information systems (TMIS)* 2 (2):1-25. doi: 10.1145/1985347.1985353.
[29] Pavlou, Paul. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model." *International Journal of Electronic Commerce* 7 (3):101-34. doi: 10.1080/10864415.2003.11044275.
[30] Rousseau, Denise M, Sim B Sitkin, Ronald S Burt, and Colin Camerer. 1998. "Not so different after all: A cross-discipline view of trust." *Academy of management review* 23 (3):393-404. doi: 10.5465/amr.1998.926617.
[31] Tinsley, Howard EA, and Richard A Kass. 1979. "The latent structure of the need satisfying properties of leisure activities." *Journal of Leisure Research* 11 (4):278-91. doi: 10.1080/00222216.1979.11969406.
[32] Treiblmaier, Horst. 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):545-59. doi: 10.1108/SCM-01-2018-0029.
[33] Vo, K. T., A. T. Nguyen-Thi, and T. A. Nguyen-Hoang. 2021. "Building Sustainable Food Supply Chain Management System Based On Hyperledger Fabric Blockchain." *International Conference on Advanced Computing and Applications (ACOMP)* 15 (1):9-16. doi: 10.1109/ACOMP53746.2021.00008.
[34] Wang, Shangping, Dongyi Li, Yaling Zhang, and Juanjuan Chen. 2019. "Smart contract-based product traceability system in the supply chain scenario." *IEEE Access* 7 (1):115122-33. doi: 10.1109/ACCESS.2019.2935873.
[35] Wood, Phil. 2008. "Confirmatory Factor Analysis for Applied Research." *The American Statistician* 62 (1):91 - 2. doi: 10.1198/tas.2008.s98.
[36] Yamagishi, Toshio, and Midori Yamagishi. 1994. "Trust and commitment in the United States and Japan." *Motivation and emotion* 18 (2):129-66. doi: 10.1007/BF02249397.
[37] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. 2020. "An overview on smart contracts: Challenges, advances and platforms." *Future Generation Computer Systems* 105:475-91. doi: 10.1016/j.future.2019.12.019.

Appendix

The questionnaire, collected data, statistical tests and study results can be found online in an open-access data repository:
https://osf.io/ns2yc/?view_only=f8816609bdcb4efd924ed78e441bc8f7