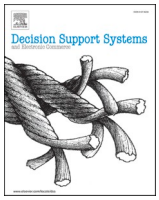
Decision Support Systems 179 (2024) 114182

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss



Designing trust-enabling blockchain systems for the inter-organizational exchange of capacity

Nick Große [a,*], Frederik Möller [b,c], Thorsten Schoormann [b,c], Michael Henke [a,d]

[a] TU Dortmund University, Germany
[b] TU Braunschweig, Germany
[c] Fraunhofer ISST, Germany
[d] Fraunhofer IML, Germany

ARTICLE INFO

Keywords:
Blockchain
Trust
Capacity exchange
Design principle
Experiment
Design science

ABSTRACT

In times of rapid and unpredictable developments, companies experience significant volatility in capacity utilization. Virtual capacity exchange platforms help to mitigate this challenge by exchanging capacities with anonymous participants in market-like peer-to-peer networks. However, its efficiency is hindered by behavioral uncertainties, including a lack of inter-organizational trust in other participants. To leverage the potential of such exchange platforms, this paper reports on a Design Science Research project aiming to derive and validate design principles for establishing trust in inter-organizational capacity exchange in two design iterations. Using blockchain technology, we instantiate six design principles into an artifact and perform experimental evaluations to investigate their effect on perceived trust. Our paper contributes to research and practice by identifying and applying prescriptive design knowledge and advancing our understanding of how to design trust-enabling inter-organizational systems. The originality lies within the empirical investigation of how and why different design principle combinations can be established through blockchain technology as one of the promising approaches for establishing trust. In doing this, we also disclose future pathways for IS and blockchain researchers and practitioners.

1. Introduction

Globalization and the ever-increasing interconnectedness make supply chains more prone to uncertainties caused by an unstable environment (e.g., pandemic crisis) and changing organizational behavior (e.g., actions of suppliers), leading to inefficiencies in capacity utilization [1]. This particularly applies to complex industrial networks, such as in the automotive industry, which needs to coordinate and align hundreds of suppliers and manufacturers [2,3]. Durugbo and Balushi [4] even found that trust is a recurring theme in supply chain crises. Blockchain is among the technologies associated with generating trust in inter-organizational transactions [5] through permanent and immutable transaction records [6]. Given its promising abilities, using blockchain and showing how it benefits inter-organizational trust at multiple levels is a key concern in design-oriented blockchain Information Systems (IS) research [7]. Some researchers even see its potential to unlock entirely trust-free digital transactions [8]. In contrast, however, various scholars have argued that there is a need for more empirical evidence about how and why blockchain as an inter-organizational information system (IOS) enables trust [9–11]. This includes advanced research in decentralized capacity exchange [12,13]. Contributing to this, we shed light on the trust-enhancing effects of blockchain technology (BCT) in virtual capacity exchange platforms.

Besides the underlying technology, our paper is informed by the lenses of transaction costs [14] and agency theory [15]. Across company boundaries, transaction costs represent the accumulation of coordination costs between suppliers and customers along the transaction lifecycle [16,17]. For example, exchanging sensitive information usually requires intensive coordination, which could be reduced through IOSs [18,19]. Electronic markets are one specific IOS type, which applies technology to enable suppliers and demanders to exchange information via digital transactions [20]. As instantiations of electronic markets, virtual capacity exchange platforms allow companies to offer excess capacity (providers) and request additional capacity (demanders).

* Corresponding author at: TU Dortmund, Leonhard-Euler-Str. 5, 44227 Dortmund, Germany.
E-mail addresses: nick.grosse@tu-dortmund.de (N. Große), frederik.moeller@tu-braunschweig.de (F. Möller), thorsten.schoormann@tu-braunschweig.de (T. Schoormann), michael.henke@tu-dortmund.de (M. Henke).

https://doi.org/10.1016/j.dss.2024.114182
Received 13 January 2023; Received in revised form 30 December 2023; Accepted 22 January 2024
Available online 23 January 2024

However, these effects are reduced by difficulties from behavioral uncertainties between platform participants. The reduction of trust among the partners leads to coordination efforts and, thus, transaction costs, which are relevant for outsourcing decisions [16]. Following Suematsu [16,p. 58], trust plays an important role due to its benefits in "*adjust* [ing] *conflicts of profits in the short term from perspectives of a long term and enable*[ing] *handling uncertainties in the relationship flexibly.*" As mechanisms to form and maintain trust between the participants on such platforms are required, we ask: *How to design an artifact that establishes trust in inter-organizational capacity exchange?*

To answer this, we propose a novel software artifact based on the blockchain. This allows us to promote transparency and immutability, and thus overcome the issues of inter-organizational trust in virtual capacity exchange platforms and transaction costs. Following Design Science Research (DSR), we (1) build an artifact that shows how and why blockchain fosters trust and (2) extract design knowledge for the class of systems [21]. Subsequently, our study is at the interplay of generating an artifact and theory [21]. To accommodate this, we derive initial design principles from the literature and expert interviews to codify knowledge about the successful design of platforms for inter-organizational capacity exchange. Then, we instantiate the design principles in a software artifact and indicate their contribution to inter-organizational trust through experiments. Our findings add theoretical-grounded knowledge based on transaction cost economics and agency theory as kernel theories on designing trust-building capacity exchange platforms. With our work, we respond to recent calls for additional empirical blockchain research [7] by providing empirical evidence for blockchain as a trust-enabling technology.

The paper is structured as follows: In Section 2, we elaborate on networks, principles of trust, and blockchain-related designs. Section 3 outlines the research method, including cycles of building and evaluating our artifact. In Section 4, we formalize findings about how and why inter-organizational trust can be established through blockchain to guide research and practice. While Section 5 discusses the implications and limitations, Section 6 concludes the paper.

2. Research background

2.1. Networks and trust

The starting point of our investigation is the *information bias* evoked by uncertainty, which can be specified as the complexity of the environmental level and opportunism caused by human-induced behavior [22]. Reducing uncertainty between the stakeholders is part of agency theory [15]. Networks can be seen as a coordination structure, such as in markets [23], and imply "*inter-personal and inter-organizational relationships, which are accumulated when people or organizations interact with each other in certain geographic locations or in social groups*" [17,p. 5]. Inside networks, participants with mutual interests can form and maintain cooperation [23], which premises trust as this is a crucial factor in reducing complexity and transaction costs [17,24]. Trust is the "*willingness to rely on an exchange partner in whom one has confidence*" [25, p. 315] and is needed as a threshold condition for inter-organizational transactions [17]. From an inter-organizational viewpoint, trust in the entire organization (systemical trust) and trust in a single entity as a subset of the organization (interpersonal trust) can be distinguished [26]. Lewiki & Bunker [27] assume that it evolves and reaches different stages, starting with calculus-based trust, over knowledge-based trust to identity-based trust. Trustworthiness can be derived from the factors of the trustee's ability, benevolence, and integrity [28]. Nielsen [29] derives six types of trust in alliances (competence-based, calculus-based, deterrence-based, affect-based, competence-based, and institution-based), from which each can take the role of an antecedent, moderation, and outcome function along the transaction process. Following Cai [17], trust can affect the entire transaction lifecycle, ranging from ex-ante transaction costs, including information and negotiation costs, to ex-post transaction costs for implementation, monitoring, and enforcement [30]. Also, trust is affected by information, shared value, and communication [31]. Riegelsberger et al. [32] propose six heuristics (stable identity, traceability, accountability, group membership, group identity, social presence, and recording outcomes) as mechanisms between the trustor and trustee. Signaling and screening [33], authority [34], or reputation [35] are cooperation designs for coping against behavioral uncertainties [36].

Prior literature on trust, as outlined above, is rich and diverse and aids in grounding our paper. Particularly, we shed light on inter-organizational trust since it contributes to reducing transaction costs. Each cooperation passes ex-ante and ex-post transaction stages, covering different kinds of uncertainties that need to be considered; this spans our problem space. Existing work also provides cooperation designs, trust models, and mechanisms to overcome the issues evoked by uncertainties in the agents' behavior; this is contributing to our solution space.

2.2. Blockchain technology

Blockchain technology (BCT) has received considerable attention for increasing trust in networks and establishing both the immutability and transparency of shared data [6,7]. As part of the distributed ledger technologies (DLT) [37], blockchain is a "*distributed database that is practically immutable by being maintained by a decentralized P2P network using a consensus mechanism, cryptography and back-referencing blocks to order and validate transactions.*" [38,p. 8]. In conjunction with electronic markets, blockchain has the ability to establish trust, reduce transaction times and transfer values, as well as provide privacy and security [39]. Once established, blockchain can lead to a trust-free system as all relevant data are technologically stored in an immutable way [8,12]. The technology consists of the triad interplay of consensus mechanisms, decentralized data storage, and cryptographic protocols [10,40,41]. On top of this, smart contracts can be implemented as "*autonomous interacting pieces of code*" [41,p. 1543].

Given the relevance of BCT, prior literature already captures design knowledge for blockchain, including digital storage and exchange of each data, ensuring traceability of the changes made to the responsible users, and ensuring accessibility for participants [42]. Characteristics to specify blockchains (e.g., accessibility, excludability) and consensus algorithms can be found in [12,43,44]. Considering an emphasis on trust through blockchain, we found several papers. Abebe et al. [45] present six design principles for a trusted data transfer in decentralized permissioned blockchains. Fan et al. [46] derive three general design principles on trust management, elaborate on how blockchain contributes to trust, and stress that this field is still emerging. Nærland et al. [42] propose four blockchain-based design principles to mitigate uncertainty and risk in decentralized systems, such as 'digitization,', 'tamper-proof storage', 'accessibility' and 'user authentication'. Utz et al. [47] propose four design principles for blockchain-based customer loyalty programs, arguing that their principles have various effects on trust (e.g., the principle 'give customers agency' provides the customer with transparency and ultimately leads to decreasing institution-based distrust). Carvalho [48] presents a blockchain-based solution for transparency and trust in loot boxes using the gaming industry as an illustration. Despite the design knowledge in previous BCT-centric literature, a call for more advanced research on blockchain can be found, too [11].

In summary, although this promising field is still emerging, insights into trust enabled by blockchain can be extracted, providing reusable knowledge for approaching our intended solution space (e.g., establishing inter-organizational trust). Grounded in the literature, we aim to improve the existing body of knowledge by investigating the effectiveness of BCT designs in the real world and responding to the calls for more empirical and theoretical-grounded research [11].

3. Research design

DSR studies craft real-world artifacts to solve problems and make the knowledge gained in these activities accessible [21]. Collecting design knowledge ensures the transferability of successful design instances and enables them to go "*far beyond a single success story*" [49,p. 180]. For this, researchers codify design knowledge in a standardized format so that "*the professionals of the discipline in question can use to design solutions*" [50,p. 20]. One way to codify this design knowledge is through *design principles*, which prescribe specific actions to design an artifact capable of achieving a specific goal [51]. Design principles require sound kernel theory to explain why and how a design works [52], which we operationalize to extract and justify meta-requirements [53]. For building an IT artifact and extracting design knowledge, we adapted the DSRM [54] and used 'Baustein' for its visualization [55] (see Fig. 1). Each of the two design iterations contains an evaluation (ex-ante and ex-post) [56] and is informed by different field accesses that aid in maturing the solution. In total, we conducted 22 interviews and collected over 1200 min of interview data across the DSR phases to support purposes, such as grounding the meta-requirements and validating the solution's usefulness.

3.1. Problem identification and solution objectives

Building upon design knowledge on trust and blockchain (see Section 2), our contribution extends the empirical foundation on how and why blockchain affects perceived inter-organizational trust. The scope of our problems space ranges from lack of information about the offerer's ability to perform a task (competence-based trust [29]), uncertainty about fair awarding of contracts (integrity [28]), and appropriate payment and evaluation (deterrence- or calculus-based trust [27,29]). Neglecting these uncertainties can result in coordination efforts and, thus, increased transaction costs. Fig. 2 illustrates an abstract view of the problem and solution space addressed in this paper.

The research problem builds upon the need to gather empirical evidence about how and why blockchain establishes trust. For example, Treiblmaier [11] calls for framing blockchain studies to clarify the actual purpose and reason for its implementation. Beck et al. [57] and Rossi et al. [7] highlight the relevance of blockchain as a trust-enabling technology and outline organizational implications as areas for design-oriented IS blockchain research. Chanson et al. [58] and Lindman et al. [59] concur with this and stress the potential of system design features enhancing trust through blockchain for research. Inspired by the examples above, as well as related literature dealing with blockchain and trust [9,10,12], we infer a demand for design-relevant knowledge on the trust-enhancing capabilities of BCT. In our case, we adapt this to the scenario of inter-organizational trust using virtual capacity exchange platforms as a case for instantiation.

Given the aforementioned problem space, the artifact is supposed to show the effectiveness of blockchain on the perceived trust in the inter-organizational exchanges of capacity. Specifically, the artifact needs to be ingrained with actionable guidance that can be made available to others and help them to design blockchain for trust-enhancing more efficiently. For this purpose, we propose design principles as codified prescriptive design knowledge [60].

3.2. Design and development

The first step is to derive *meta-requirements* (i.e., requirements for a class of artifacts [61]). In our case, we identified experts in practice as relevant informants. To entangle this practical and qualitative approach with *kernel theory*, we condensed the knowledge about trust and uncertainty in transactions to compose a guide for the interviews. We approached two sets of experts affected by capacity exchange from industrial domains. *First-order stakeholders* are those informants close to the artifact in real settings and deal directly with exchange platforms as users. *Second-order stakeholders* are platform providers with the intention of providing a negotiation platform for inter-organizational capacity exchange; working on the implementation. In turn, these groups also make the *target users* [62] of the design principles as they are supposed to help them establish trust. All interviews were semi-structured as it gives orientation but leaves room for the informants to answer flexibly and draw from their rich experiences [63]. The interview guide was designed to center around relevant themes in capacity exchange platforms. The guide's categories were derived from literature about uncertainties and trust in networks (see Section 2) and refined exploratorily during the interviews. It covers questions about the uncertainties along the transaction lifecycle of capacity, such as the outsourcing process, information and communication platforms, uncertainties during the transaction process, and dealing with uncertainties in the information exchange during outsourcing. We conducted interviews with eight first-order and three second-order stakeholders to elicit requirements for a trust-building negotiation platform for inter-organizational capacity exchange (total of 615 min, see Table 1). After eleven interviews, theoretical saturation was reached since only a few very specific and less generalizable requirements were mentioned. For data analysis, we employed the qualitative GIOIA method [64], conducting a double-sided reflection of deductive, theory-led, and inductive, practice-led approaches. As a result, we produced a category system of relevant categories and used them as anchor points to derive meta-requirements. Following [76], first-order codes are close to the actual statements, which we then aggregated and condensed to

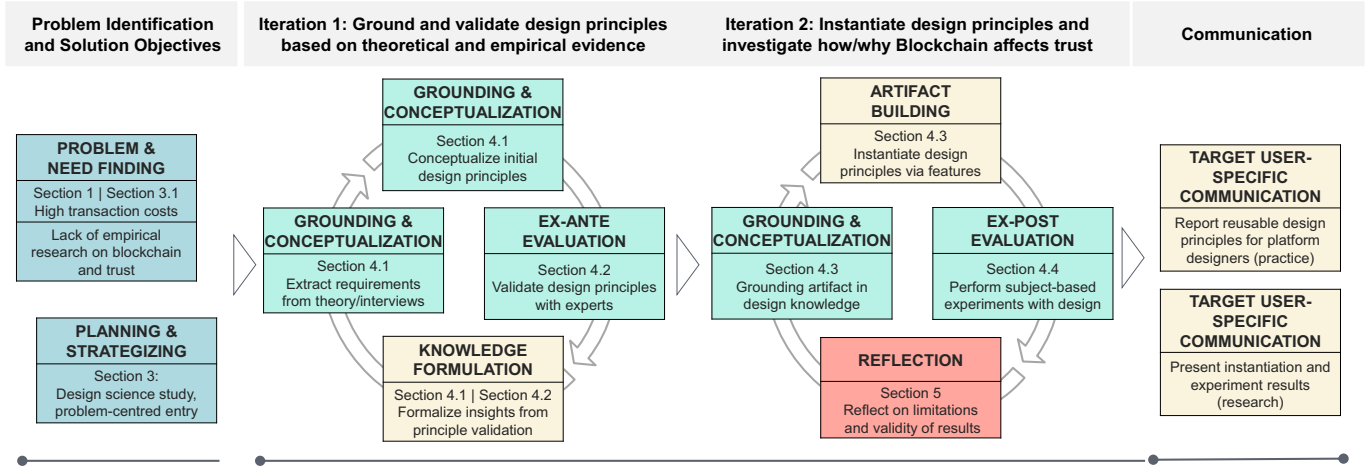


Fig. 1. Overall research design.

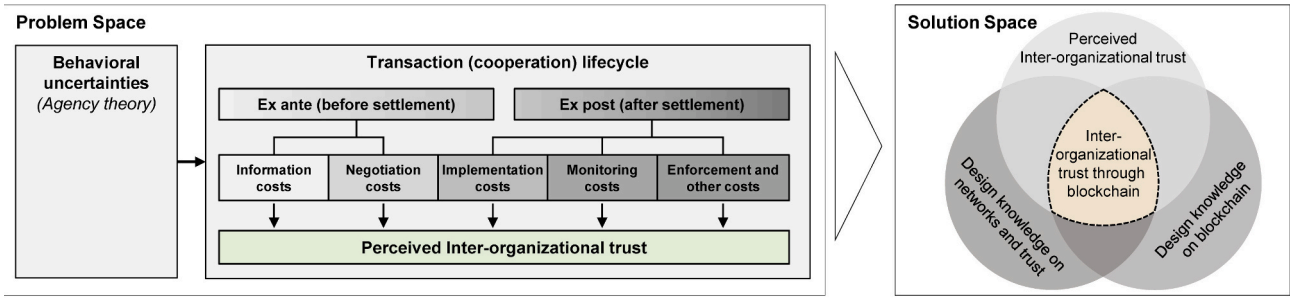


Fig. 2. Research model (illustration based on [17,19,22]).

Table 1
Interview sampling and data sources across the DSR project.

Expert code	Expert role	Purpose	Data sources	Duration
DSR phase: Define the objectives of a solution (Iteration 1)				*Σ 615* min
I1_S1	First-order stakeholder (domain experts)	Gather requirements	Literature for interview guide and theoretical categories (deductive); Transcripts for inductive refinement of categories	52 min
I2_S1				56 min
I3_S1				55 min
I7_S1				73 min
I8_S1				69 min
I9_S1				62 min
I10_S1				144 min
I11_S1				29 min
I4_S2	Second-order stakeholder (IS experts)			54 min
I5_S2				58 min
I6_S2				65 min
DSR phase: Ex-ante evaluation (Iteration 1)				*Σ 232* min
VAL_I1	Expert in trust research	Evaluate design principles	Questionnaire; Transcripts	49 min
VAL_I2				53 min
VAL_I3	Second-order stakeholder			69 min
VAL_I4	First-order stakeholder			40 min
VAL_I5 (I9_S1)				21 min
DSR phase: Ex-post evaluation (Iteration 2)				*Σ 354* min
P_1C (VAL_ I1)	Expert in trust research	Validate the how and why of perceived trust	Questionnaire; Observations; Transcripts	69 min
P_2C (I1_S1)	First-order stakeholder			50 min
P_3T (I11_S1)	First-order stakeholder			60 min
P_4T (I9_S1)	First-order stakeholder			52 min
P_5T	Second-order stakeholder			70 min
P_6C VAL_ I3)	Expert in trust research			53 min

Note: S1 / S2: First-order / Second-order stakeholder; C / T: Control / Test group;
The category system, interview guide, and questionnaires are available on request.

second-order themes and, ultimately, into *aggregated dimensions* (i.e., the transaction stages).

The appropriateness of participants in all interviews was ensured in several ways. First, as part of the contact process, we sent out general invitations for our interviews via e-mail, including the expertise and area of knowledge we requested, allowing the recipients to decide whether they were appropriate candidates. If the informant could not attend the meeting, we asked for a knowledgeable substitute. The invitation consists of common aspects for both roles. Second, during all interviews, we provided a first question in the interview dealing with the background knowledge, the participant's role in their company and their years of experience. This gave the interviewer insights about which stakeholder group the interviewee belongs to and how to navigate them through the interview appropriately. Third, by approaching technical or domain-related questions and through interim feedback given by the experts, we captured how far they can empathize with the situation. This created the basis for assigning the participants to roles.

To design a solution capable of meeting the requirements, we formulate design principles that guide building an artifact from the same class [60]. Therefore, the DSRM [54] is complemented by Möller et al. [65]'s method for design principle development. This allows us to follow a more general approach and leverage the advantages of a contextualized one.

3.3. Demonstration and evaluation

A strategy of two evaluations was adopted. First, after formulating the design principles, we performed an *ex-ante* evaluation (Iteration 1) of the design principles in terms of their form and function before they were instantiated [56,66]. We used the evaluation framework of Iivari et al. [67], which is tailored to design principles. Interviews with one first-order and one second-order stakeholder, as well as three theoretical experts knowledgeable in trust, platforms, and partially BCT, further supplemented these questionnaires (total of 232 min). Second, to show how and why a blockchain-based implementation of design principles affects the perceived inter-organizational trust, we performed an *ex-post* validation based on subject-based experiments [68] (Iteration 2). We relied on six informants, including four first-order and one second-order

Dimension	Code	Meta-requirement
Specification	MR-S1	Creation and management of tender
	MR-S2	Cross-domain management
Information	MR-I1	Search functions
	MR-I2	Identity management and verification
	MR-I3	Services to support the initiation process
Negotiation	MR-N1	Possibility for intermediate connection
	MR-N2	Heterogeneity of contracts
	MR-N3	Function for final award of the contract
Fulfilment	MR-F1	Conditions for fulfilling the payment
	MR-F2	Compliance with legal framework conditions
After-Sales	MR-A1	Serious rating
	MR-A2	Provision of decision relevant KPIs
Overlapping category	MR-O1	Transparency and completeness of collected data relevant to transaction
	MR-O2	Decentralization and Simultaneity
	MR-O3	Communication services
	MR-O4	Equality of participants
	MR-O5	Interface compatibility and standards
	MR-O6	Depictability of human interaction and role models
	MR-O7	Encryption concepts

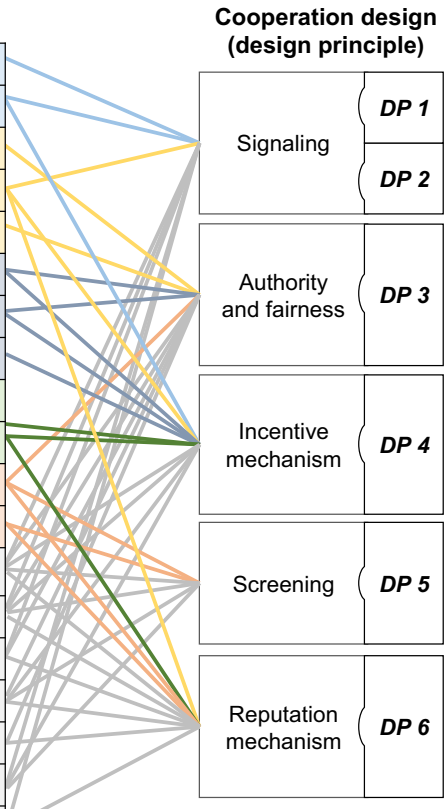


Fig. 3. Formulation and categorization of meta-requirements and design principles.

stakeholders, and two experts in trust research (total of 354 min, see Table 1).

4. Artifact description

4.1. Meta-requirements and design principles

To logically organize the meta-requirements, we drew from the transaction stages proposed by [30] as aggregated dimensions. We enriched them through the upstream specification process, in which the requested or demanded capacity is specified. This considers intra-organizational hierarchical evoked transaction costs [16] as a guiding mechanism to analyze the data [53]. We added a category with all meta-requirements that were not categorizable but overlapped. Fig. 3 shows the resulting 19 meta-requirements and how they relate to the design principles (DP). The meta-requirements are represented by codes in order to show their affiliation to an aggregate dimension.

The meta-requirements relate to one or more design principles. Coherent with our research model (see Fig. 2), we used theoretically grounded cooperation designs derived from literature as a basis for logically aligning the meta-requirements and possible solution fragments coping with trust-decreasing uncertainties along the transaction lifecycle. The design principles are based on cooperation designs or heuristics to reduce behavioral uncertainty evoked by mutual information asymmetries, such as signaling and screening [33,36], reputation [35,36], and authority [36]. Enriched by designs for trust [32], such as identity and traceability of its interactions, the design principles aim to increase trust, despite the occurrence of behavioral uncertainties between the participants in a market-like negotiation platform. Here, we focus on design knowledge of inter-organizational trust (see Section 2.1). Based on this, we formulate design principles that guide "*how to build an artifact in order to achieve a predefined design goal*" [60,p.4040]. Therefore, we use a well-accepted template structuring design principles into the implementer, the user, the aim, the context, the mechanisms, the enactors, and the rationale for why they work [62]. Ultimately, we derived six design principles (see Table 2). As part of the continuous refinement and to gather formative feedback from expert communities, the design principles and the related research design were communicated through scientific contributions [13,69]. Among the measures to prevent transaction costs is the conscious revelation of information, called signaling [33]. Information asymmetries evoked by hidden characteristics can be mitigated by signaling [36], addressed as competence-based trust [29], and the ability to act as a trustworthy anchor [28]. The first principle, **DP 1,** addresses the relevant tender information because each network participant reveals information about the requested or provided capacity. As each user or group of users must be represented by a stable identity [32], issues of signaling related to user identities need to be considered. Thus, the principle **DP 2** is about signaling of information relevant to the identity. Once cooperation is established, manipulations in terms of exploiting contractual gaps can occur, which are hidden intentions and can be overcome with authority [36]. Mechanisms are required to enforce measures in case one actor is unjustly disadvantaged. Thus, **DP 3** addresses authority and fairness. Another ex-post uncertainty is the moral hazard, encouraging actors to act opportunistically, which can be circumvented with incentive mechanisms [36]. A counter lever here lies within the calculus- and deterrence-based trust [27,29,70] to manage the short-term benefit of selfishness with the long-term consequences of broken trust. This covers benevolence as an antecedent to trust [28]. As a result, the fourth principle, **DP 4,** is dedicated to incentive mechanisms. Mechanisms in which the less informed side is willing to spend effort gathering information to ensure that the opposite side is qualified ('quality screening'

Table 2
Design principle overview.

DP	Formulation of design principles
DP 1	**Signaling of information relevant to the tender:** To allow the demander and supplier (**U**) the storage of a precise tender (**A**) during the specification stage (**C**), the platform provider or developer (**I**) has to provide functions for a customized creation of tenders and its linkage to a verified identity and reveal them in a simultaneous and distributed manner (**M/E**). This allows the reduction of uncertainties due to a vague specification and a lack of identity assignments, simultaneously revealing information to authorized participants (**R**).
DP 2	**Signaling of information relevant to the identity:** To establish trust in the identity (**A**) of each participant (**U**) during the information and initiation stage (**C**), the platform provider or developer (**I**) has to provide functions for the decentralized storage, configuration, and verification of identities (**M/E**). This allows transparency and correctness of the identity (**R**).
DP 3	**Authority and Fairness:** To maintain the authority (**A**) of the cooperation partner (**U**) before and after the negotiation and settlement stage (**C**), the platform provider or developer (**I**) has to provide functions and mechanisms for creating and decentralized storage of contracts as well as their order-relevant contents, functions for monitoring the compliance with the agreed terms and conditions for enforcing sanctions/rewards (**M/E**). This provides a transparent data basis for all participants, as well as traceability in the enforcement of countermeasures (**R**).
DP 4	**Incentive Mechanisms:** To motivate the participants (**U**) to join and maintain cooperation before and after the negotiation and settlement stage (**A**), the platform provider or developer (**I**) has to provide the value-adding benefits of each cooperation and imminent losses in case of violations, as well as demonstrate them using comprehensible and transparent data that can be observed by all participants (**M/E**). So, market participants are motivated and deterred from acting opportunistically (**R**).
DP 5	**Screening Functionality:** To ensure that the participants of the negotiation platform (**U**) can trust the deposited information (**A**) during the information and initiation phase (**C**), the platform provider or developer (**I**) has to provide functions for depositing information and for distributed and verified access, functions for checking its validity and services for searching information and contacting participants (**M/E**). This ensures that the information obtained during the information retrieval is valid and thus trustworthy (**R**).
DP 6	**Reputation Mechanism:** To achieve a retraceable reputation (**A**) for each participant (**U**), the platform provider or developer (**I**) has to provide a reputation mechanism (**M**), which allows, after the fulfillment stage (**C**) a serious rating of each identity, a decentralized collection of rating-relevant data, its transparent processing and distribution to all participants (**E**). In this way, participants have transparency over the data coining the reputation, and can trust them (**R**).

[33]) are captured by **DP 5**. Finally, reputation as an overlapping measure to reduce information asymmetry in terms of behavioral uncertainty needs to be taken into account [36], since it is related to identity and can reveal information about prior actions and the reliability of actors [35]. Following Riegelsberger et al. [32], actors on both sides (e.g., customers and providers) are encouraged to treat each other honestly to maintain their good reputations. According to Voss [35], reputation mechanisms consist of a collector, processor, and emitter of information relevant to indicating the reputation, which are considered mandatory mechanisms and enactors. Based on this, **DP 6** is dedicated to reputation mechanisms.

4.2. Ex-ante evaluation of the design principles

To evaluate the design principles before they are instantiated, we used the evaluation framework of Iivari et al. [67], which differentiates between five metrics: accessibility, importance, novelty and insightfulness, actability and guidance, and effectiveness [67]. We operationalized the evaluation through a questionnaire and defined items for each metric (see Fig. 4). For each item, we used a ranking scale from 0 (no approval) to 4 (total approval). We complemented the questionnaires by interviewing each expert. The framework's sequencing of questions is predetermined since non-compliance with one criterion leads to non-compliance with the following criteria [67]. The dual use of questionnaires and interviews enables triangulation through the mixed-method application of qualitative and quantitative data [71]. As a source of expertise, we asked one first and a second-order stakeholder. The latter one is an envisaged practitioner and implementer of the design principles. We also consulted three experts from the fields of platform economy and trust to assess the design principles from a research point of view (see Table 1), leading to a sample of five experts (n_i). The questionnaires have an average source of **2.78**, which points to an overall approval of the design principles' reusability. Given the promising results of this ex-ante validation, we concluded with Iteration 1 and proceeded to instantiate the design principles in Iteration 2.

4.3. Instantiation of the design principles

To instantiate the design principles, we de-abstracted them into *design features* [65]. At this point, the BCT and its recent design

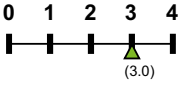
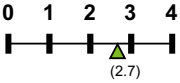
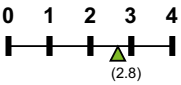
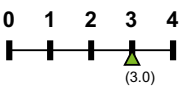
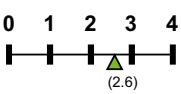
Criterion	Mean Value (MV)	Translated and paraphrased statements
Accessibility of the design principles		"The design principles are **clear** and **understandable** to me."(VAL_I4)
Importance of the design principles		"I expect that **in the future, trust** is getting **more important**." (VAL_I1)
Novelty & Insightfulness of the design principles		"They are definitely informative, also known mostly. But to **see them together** and **to have a guideline** is I think a **relevant** thing." (VAL_I5)
Actability and Guidance of the design principles		"[…] I now understand **the whole thing as a guideline**, **which I can use, but I can also decide against it**." (VAL_I5)
Effectiveness of the design principles		"[…] if there is an **outflow of customers** changing to a platform with **better service**, this will encourage existing platforms to think about the reasons." (VAL_I5)

Fig. 4. Results of the ex-ante evaluation ($n_i = 5$).

knowledge (see Section 2.2) came into play to implement trust-enhancing mechanisms technically. This is sensible because the blockchain enables systemic trust via an interplay of consensus mechanisms, decentralization, and cryptographic protocols [40], especially in distributed networks [11] and decentralized markets [39], as well as reduces transaction costs evoked by behavioral uncertainties [5]. Information asymmetries evoked by behavioral uncertainties in inter-organizational networks can be overcome through blockchain functionalities [5]. Transferred to the context of capacity exchange, transaction cost theory and agency theory can be applied to BCT to address transaction costs in make-or-buy decisions and minimize the scope of uncertainty between the contractors (e.g., principal and agent) [72]. We limit our scope to short-term cooperation in market-like networks, in which trust is a complexity-reducing factor [23,24]. In terms of *accessibility*, blockchains differ between private and public and concerning *excludability* between permissioned and permissionless [44]. Transferred to the context of sharing capacity in an open system with a multitude of participants, we refer to a permissionless public blockchain. According to Wuest & Gervais [73], this is justified because it becomes necessary to store the state. More than one writer is allowed to write in the blockchain; no trusted third party is involved, and not every writer is known in the network. Also, in permissionless public blockchains, every participant receives access and is allowed to run a node [44], which is "*a software client that participates in the network*" [74,p. xxxiv]. We use *Ethereum* as a permissionless framework [73]. To operationalize the design principles, we refer to *smart contracts* as a subset of BCT, serving as an embedded code that can be executed based on predefined conditions [41]. Following the blockchain framework from Hawlitschek et al. [10], the instantiation was carried out using three smart contracts embedded into a set-up test network based on the Ethereum framework (e.g., infrastructure layer) (see Fig. 5). Our test-net consists of a full node using the proof-of-authority consensus algorithm since it allows a near real-time transaction throughput. Participants operate via a light node. To ensure internal valid experiments and thus to avoid any bias evoked by external influences, we restricted the access to our test net on predefined light nodes, resulting in a permissioned public DLT type [44]. The smart contracts are created in Solidity using Remix IDE. In our case, they are instantiated for capacity exchange, in which a prototype of a decentralized negotiation platform for unutilized 3D printer tasks is picked up. This case consists of simplified processes illustrating trust issues resulting from behavioral uncertainties along the ex-ante and ex-post transaction stages, which are generalizable for every platform intended for the inter-organizational ex-change of tangible or intangible assets. Referring to [10], the principles aim at overcoming the trust frontier spanning the continuum of behavioral uncertainty between the agent and the behavioral layer.

The prototype (see Fig. 6) consists of a Web3 frontend application in which the smart contracts have been embedded. Usually, the intended implementer mentioned in the design principles (i.e., second-order stakeholder) deploys the smart contracts and owns these. Each envisaged participant was only navigating through the frontend application and playing through the whole transaction lifecycle without any deployment of code, in which the smart contracts were implemented beforehand by the moderator. Smart contracts are provided for handling the tender (**DP 1**), identity (**DP 2**), and reputation (**DP 6**). Authority (**DP 3**) is considered through permissions embedded in each smart contract via require statements, which prevent the execution of services from non-authorized users. Screening mechanisms (**DP 5**) are considered through reading functionalities. To show the degree of information bias between the suppliers and demanders, the participants get an insight into both roles. Referring to the reputation mechanism (**DP 6**), the possibility of mutual rating could prevent users from acting opportunistically (**DP 4**). Thus, maintaining reputation can be explained by the mechanism of deterrence-based trust [70], which occurs "[…] *when the potential costs of discontinuing the relationship or the likelihood of retributive action outweigh the short-term advantage of acting in a distrustful way.*" [70, p. 366]. The mechanisms and enactors mentioned in the six design principles facilitated the extraction of design features. Due to the beginner-friendly documentation driven by the Ethereum community, a transfer into real Ethereum code proved to be feasible.

4.4. Ex-post evaluation of the instantiated design principles

We further evaluated the design principles through subject-based experiments with the prototype operationalized in an illustrative scenario [68]; here, a *negotiation platform for 3D-printer capacity*. Subjects involved are experts in the domains of capacity planning as intended platform users. They are familiar with platform design and trust as an intended platform provider. Our experiment follows the *pretest-posttest control group design* [75] because it provides before and after comparisons to ensure the same starting point for each participant [76]. In the pretest, two user groups applied the artifact, and we collected their feedback on the design principle-specific functionalities via a questionnaire and interviews (see Table 3). In the posttest, we provided the

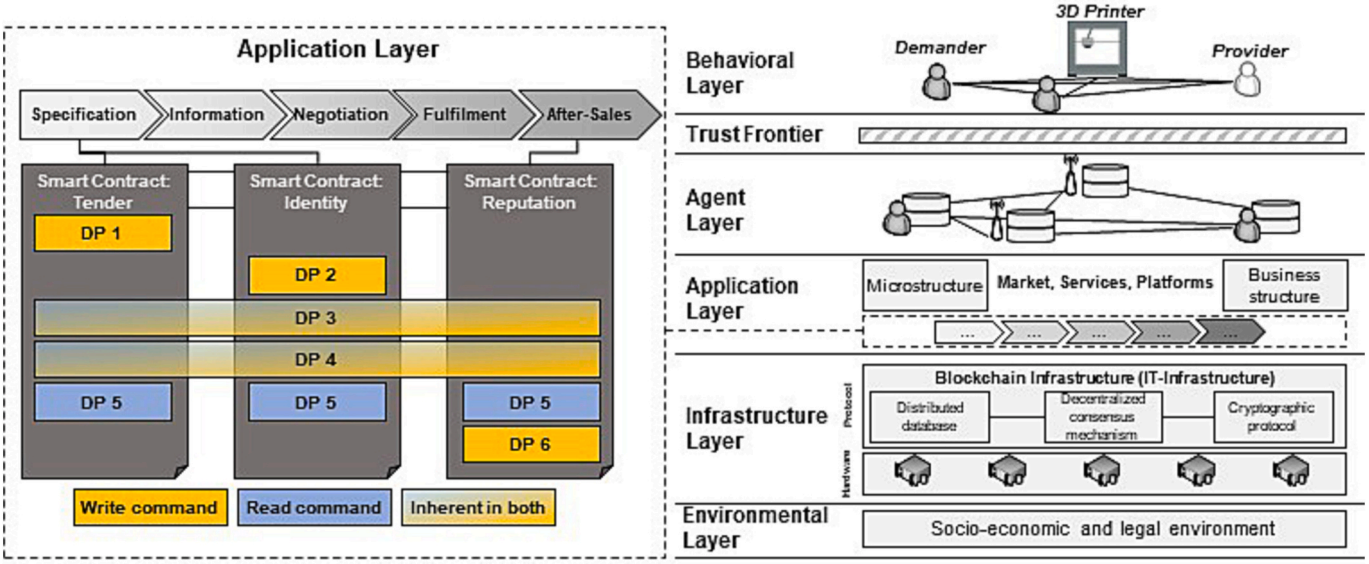


Fig. 5. Smart contracts embedded in the blockchain framework proposed by [10].

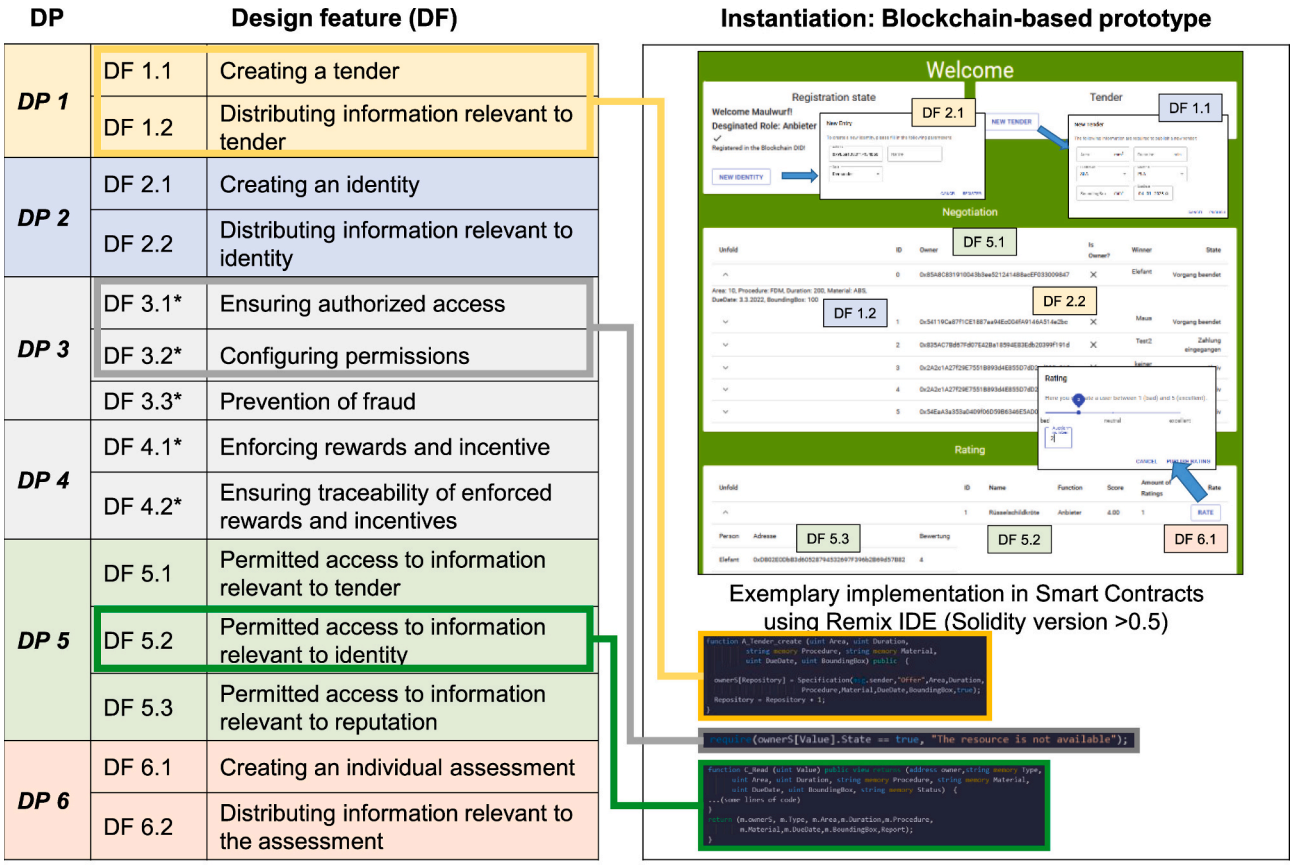


Fig. 6. Design features and their consideration in a blockchain-based instantiation using Solidity.

Table 3
Pretest-posttest control group design based on [75].

Group	n_i	Assignment	Pretest	Manipulation	Posttest
Control-Group	3	Randomized	$\mathbf{Pre_C}$	–	$\mathbf{Post_C}$
Test-Group	3	Randomized	$\mathbf{Pre_T}$	X	$\mathbf{Post_T}$

groups with two different artifacts: one the same as in the pretest and one manipulated to simulate behavior contradictory to the design principles. This enables us to assess the design principles in an experimental setting [54,66]. Compared to case studies, experiments can be used for artificial validation [56,66] as they allow conscious control over the events [77]. For each run and participant, two Ethereum accounts based on the wallet provider Metamask (supplier and agent) were prepared and provided with pre-funded Ether, allowing them to initiate transactions during the experimental procedure. The term n_i indicates the number of participants.

Due to the number of challenges concerning implementing BCT in a naturalistic environment (e.g., latency, lack of standards and regulations, or risk of attacks [11]), the evaluation was conducted in an artificial setting addressing problems with realistic reference and envisaged platform users [56,66]. To ensure rigor, we refer to the framework for blockchain-based case studies [11], which consists of the intertwined components of theory, artifact, uses cases for blockchain research, and the conducted case studies. We apply conduct experiments as they allow answering the questions of *how* and *why* (comparable to case studies) with additional control along the observation [77]. In our investigation, the theory is based on transaction costs and agency theory, emphasizing the correlations between trust and transaction costs for inter-organizational capacity exchange.

The assessment sheet consists of eight items aligned to one or more design principles. Items 1 and 2 focus on writing and reading tender-relevant information and are thus item pairs analogous to items 3 and 4 in terms of identity and items 7 and 8 for reputation. Each item pair belongs to a smart contract embedded in the demonstrator, whereas items 3 and 4 overlap and are concluded in each smart contract. Authority is considered through requirement statements in each smart contract, preventing unauthorized participants from executing transactions. Incentive mechanisms are concerned with deterrence-based trust, in which opportunistic participants are afraid of a bad reputation. Testable propositions address the fact that BCT can establish trust during ex-ante and ex-post transaction stages of inter-organizational capacity exchange under compliance with the design principles (see problem space illustrated in Fig. 2). The corresponding cause-effect relationship will be retrieved from the experiment observations. The evaluation subjects include six experts with theoretical or practical backgrounds (each interview is about 60 min; see Table 1). Each candidate passed two runs, each about 20 min (including the assessment). Time for onboarding, interim feedback, and remaining questions are scheduled. During the analysis, we distinguished between the findings from the control and test groups and differentiated in terms of observations. Perceived trust is measured using a rating scale between 0 (no approval) and 4 (high approval).

4.4.1. *Pretest observations of both groups ($Pre_C + Pre_T$)*

To ensure an equal starting point for the control and test group, the first observation of both groups (see Fig. 7) includes the full consideration of each design principle during its blockchain-based implementation, assuming no significant deviation will occur in the perceived trust. The mean value (MV) of all candidates of both groups and along all items receives an average value of **3.1**, which equals a consensus of high approval. Minimal deviations were in the assertion of the first item pair (e.g., items 1 and 2 or items 7 and 8). Item 6 shows the highest value and

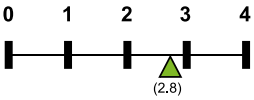
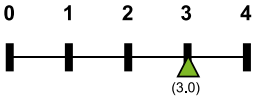
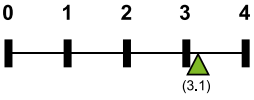
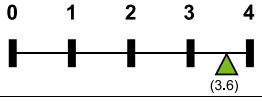
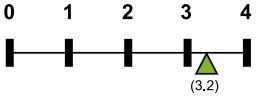
Item	DP	Mean Value	Assessment	Translated and paraphrased statements
Item 1	DP 1	2.8		"Thus I would say it is **partially applicable**. It is not worse than usual, but also not better." (P_1C)
Item 2	DP 1+5	2.8		
Item 3	DP 2	3.0		"Due to the fact that one can see the owner-key […], I would **totally agree**, yes." (P_3T)
Item 4	DP 2 + 5	3.1		
Item 5	DP 3	3.1		"[…] Yes, because of the individual steps of confirmation, everything is written down […]. Thus, **applicable** […]" (P_5T)
Item 6	DP 4	3.6		"Yes, so alone on the fact that one is not able to rate each other up […], I find that **fully applicable**. I think it is good, yes." (P_2C)
Item 7	DP 6	3.1		"Yes, I assume that. So I would say, **fully applicable**, yes." (P_2C)
Item 8	DP 6 + 5	3.3		

Fig. 7. Pretest observations (both groups: Pre_C and Pre_T; $n_i = 6$).

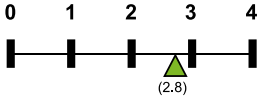
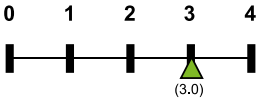
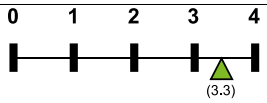
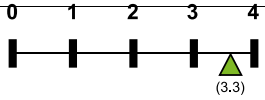
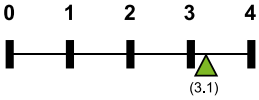
Item	DP	Mean Value	Assessment	Translated and paraphrased statements
Item 1	DP 1	3.0		"So, I would even give the first question a **consent**, simply for the reason that **it feels like you have to consent very often** […] but **in terms of counterfeit protection**, it is definitely a **positive** effect." (P_1C)
Item 2	DP 1+5	2.6		
Item 3	DP 2	3.0		"That is definitely **an approval** because I simply have this **feedback** to see which account I am logged in with, to see that **I don't do the things from a wrong account**." (P_1C)
Item 4	DP 2 + 5	3.0		
Item 5	DP 3	3.3		"That's an **approval** again because **the logic of how it's really processed cannot be seen** and that's actually this motto of smart contracts." (P_1C)
Item 6	DP 4	3.3		"No, that is completely **true**. I think that is very **discouraging** or **even impossible**." (P_2C)
Item 7	DP 6	3.3		"The same procedure as the first four […] **applicable**, yes." (P_6C)
Item 8	DP 6 + 5	3.0		

Fig. 8. Posttest observations (control group: $Post_C$; $n_i = 3$).

indicates that a blockchain-based implementation receives a high perception of trust during the ex-ante and ex-post transaction stages, revealing that in a version in which no design principle is violated, a blockchain-based implementation can successfully lead to an increase of inter-organizational trust.

4.4.2. *Posttest observations of the control group ($Post_C$)*

The posttest analysis shows the results based on the perceived trust of the control group ($n_i = 3$) (see Fig. 8). Candidates in this group run through the same scenario, wherefore only small but no significant deviations are expected. With a total mean value of **3.0** among all control group candidates and items in the second run, it can be stated that the non-manipulated version received approval. Compared with the overall mean value of the first run, which equals **2.9** for assertions from control group participants, minor improvements can be recorded. Items 4, 5, and 6 record an approval with a value of **3.3**, whereas the second item has the lowest value with **2.6** points. The perceived trust in $\mathbf{Post_T}$ can be seen as congruent to $\mathbf{Pre_C}$ and indicates a steady course.

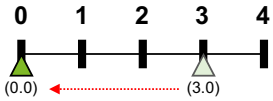
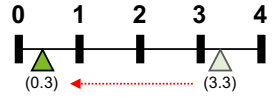
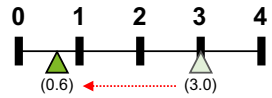
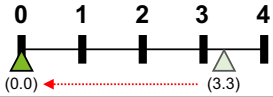
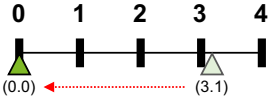
Item	DP	Mean Value	Assessment	Translated and paraphrased statements
Item 1	DP 1	0.0		"[…] **What I have specified and** what was **saved** is **not correct at all**." (P_4T)
Item 2	DP 1+5	0.0		
Item 3	DP 2	0.3		"Nevertheless my ID is recorded properly and the **wrong identity is used consequently**, therefore less applicable." (P_4T)
Item 4	DP 2 + 5	0.3		
Item 5	DP 3	0.6		"[…] I can log in, although not with my right name, **but the rest was consequent**. Thus partially applicable." (P_4T)
Item 6	DP 4	0.0		"No, that would push the whole thing more, because **I can see, what others did** and also **bid on my own**." (P_4T)
Item 7	DP 6	0.0		"No, **I can rate myself** and everything. I would not be surprised if **I type a one and the system returns a five**. […] Because it was also similar to the bid." (P_3T)
Item 8	DP 6 + 5	0.0		

Fig. 9. Pre- and Posttest observations (test group: Pre_T + $Post_T$; $n_i = 6$).

4.4.3. *Posttest observations of the test group ($Post_T$)*

Fig. 9 shows the results of the second run for the three test group candidates ($n_i = 3$). The test candidates are intentionally affected by a manipulated blockchain version in the second run. The manipulation and violations of the design principles become noticeable through (i) a wrong name and role displayed after the registration, (ii) the possibility of bidding on the own tender, (iii) an incorrect amount of the payment, and (iv) the possibility of rating the own account. The candidates notice the manipulation and give a worse assessment. With an overall mean value of **0.1** points, it can be stated that the manipulated version successfully affected the perception of the prototype in terms of establishing trust, which shows that the use of blockchain does not immediately increase trust in the system along the transaction cycle. One participant mentioned that it was at least possible to run through the whole transaction lifecycle despite the manipulated data, which is why at least items 3–5 received one or two points.

4.4.4. *Summarizing view of the ex-post validation*

Based on the evaluation of the design principles, several reflections can be formulated: First, the results indicate that the design principles affect each other. Using DP3 as an example (corresponding to item 5), reducing requirement statements in the smart contracts opens the scope of selfish interactions (e.g., self-rating corresponding to item 8), which are not prevented by the smart contracts. Require statements, which ensure the permitted execution of smart contract functions, are embedded in each of the three smart contracts and thus affect the perception of trust for all the other items and design principles. This underlines the fragile trust structure [16,27] and points to the fact that establishing trust depends on the holistic and not isolated implementation of each principle. Second, blockchain – as one implementing technology – does not immediately lead to an increase in trust. Violating or neglecting single design principles evokes new trust-affecting uncertainties instead of reducing them. The experiment results show that considering the design principles needs more attention than its actual technological implementation. Third, the demonstration and evaluation stress that a certain level of trust can be obtained even through a less resource-intensive implementation (i.e., development time, expertise, processing time). Low post-development expense is important to carry out the artifact in different instantiation scenarios. By replacing the contract address, the recent smart contracts can be changed with low effort. The decentralized infrastructure provides spatial unbound access to the test-net and thus increases its reusability and participants' range. The use of well-documented resources, such as from the Ethereum community, provides a beginner-friendly entry into the setup of a test network in Remix IDE. This enables non-technical people to modify and test the code in a local test network decoupled from real Ethereum Chains. Referring to this, our artifact and its instantiation create a basis for attaching other design principles from blockchain research even beyond trust [45–48]. Fourth, blockchain-based implementations consider different stages of the transaction lifecycle and provide a ground for empirical research on measuring the level of perceived inter-organizational trust. Inspired by [58], our research design provides decoupling points for adaption and modification through other technologies, design features, and instantiations. More variables in the experiment design are required to break down the perceived trust into its forms, levels, and antecedents (see Section 2.1). This is mandatory to derive reliable statements about the capabilities of the blockchain and the needs of the users to maintain a certain level of trust.

5. Discussion, contributions, and limitations

This paper reports on implementing a blockchain-based artifact to establish trust in inter-organizational capacity exchange, guided by six theoretically grounded and empirically validated design principles. Our solution is based on two main iterations of building and evaluation in which we (a) investigated the validity of the design principles and (b) employed a mixed-method approach of interviews and questionnaires to understand how and why the design principles affect the perceived trust. Our central results consist of (i) meta-requirements, (ii) design principles, (iii) design features of its blockchain-based implementation, and (iv) findings from an experimental design. Each of the results has implications for scholars and practitioners, which are described in the following.

5.1. Implications for research and practice

The 19 **meta-requirements** and their underlying category system inherit the knowledge derived from network and trust research (Section 2.1) and have been enriched by interviews. These requirements describe a more abstract class of goals and problems [61] and, therefore, can be employed by other scholars and practitioners to craft problem-solving artifacts. As they are rather generic, they can also be (re-)used for additional contexts and technologies. Incorporating further stakeholders (e.g., legal or public authorities as third-order or tertiary stakeholders), extending the theoretical lens, or broadening the scope of inter-organizational trust (e.g., uncertainty autonomous agents or artificial intelligence) may lead to new insights and a set of refined meta-requirements.

The knowledge obtained from our project is formalized in six **design principles** that guide the building of new solutions capable of meeting the requirements [60]. The principles are generally technology-agnostic but were instantiated via BCT. Considering our first iteration, the design principles are based on the logic of cooperative designs overcoming uncertainties. Replacing or enriching them with other trust designs may lead to new or extended principles since the alignment of the meta-requirements follows another logic. Our ex-ante validation confirms the reusability of the design principles. Embedding the design principles in further scenarios (e.g., the reflective principle development [65]) may lead to refined or new design principles.

In attempting to respond to the call for more blockchain research [11], scholars in the IS discipline gather evidence about the trust affected by blockchain-based implementations. Our work addresses specific calls for action (see Section 3), emphasizing the need for empirical, design-oriented research on trust in the blockchain. The **instantiated prototype** and **design features** serve as a contribution to blockchain research because they show how to foster perceived trust with BCT. In contrast to abstract principles, these features prescribe concrete actions for implementing artifacts.

Our design knowledge is grounded in blockchain design (see Section 2.2). While blockchain is an auspicious technology for creating trust between several actors, the proposed design principles can be challenged with design knowledge of other DLT concepts and/or technologies proposed by recent research. As an example, ‘digitization’, ‘accessibility’, ‘tamper-proof storage’, and ‘user authentification’ as design principles [42] are widely considered in our design features (see Fig. 6). The principles for a trusted data transfer [45] emphasize the infrastructure layer (see Fig. 5) and thus involve each design principle and are targeted to our intended implementer. This knowledge can be considered as refined mechanisms or, rather, enactors within the design principles (see Section 4.1). The design principles for aggregation mechanisms, feedback credibility, and thresholds for trust propagation [46] can be considered for the implementation of screening and reputation mechanisms (DP5 and DP6). The principles from [47] are conditionally considered, as our proposed demonstrator has limited freedom of action and follows a straightforward process of the transaction lifecycle. The incentive mechanisms proposed by [48] are linked to DP4 and thus provide room for exaptation. Also, smart contracts can be reused in other research and enriched by additional features.

To prevent biased influence from the authors, the formulation of the design principles refrains from mentioning the technical implementation (e.g., blockchain) to open the space for additional approaches. Blockchain came into play during the principle’s translation into design features as one possible implementation strategy. Nevertheless, to generalize our findings, practitioners are encouraged to apply them in their organizations and cases to find their individual design features.

From a methodological viewpoint, this paper presents an **experimental design** to investigate the reusability [67] and dependencies of the design principles. The experimental design is reported rather detailed and can be used as a blueprint for additional evaluations; expansions to increase the number of candidates and control variables are mandatory for proving the steady findings. The **experiment findings** stress that even the unfavorable design of smart contracts, despite implementing blockchain, decreases perceived trust. Practitioners, especially platform providers, get insights about perceived trust and blockchain. The findings indicate that blockchain can establish trust if it respects the mechanisms prescribed in the design principles, wherefore the design can be seen as internally valid [75]. Our knowledge contribution lies within a theoretical and empirical grounded explanation of how and why blockchain affects the perceived inter-organizational trust, which is limited in prior research on blockchain and trust. The proposed instantiation of a 3D printer exchange platform is only a subset of the total number of possible implementations.

5.2. Limitations

Despite a rigorous and comprehensive evaluation strategy, our study is subject to limitations. Considering internal validity, the experiments showed that insufficient consideration of one design principle leads to insufficient perceived trust. As the instantiation is based on a single case, a generalized statement in terms of induction should be treated with caution. The artificial evaluation [56] is restricted to aspects such as the conscious exclusion of environmental variables. Taking into account the claims of a naturalistic validation (e.g., the inclusion of real users, problems, and systems) [56,66], the subject-based experiment includes real users [68] (i.e., first- and second-order stakeholders). A completely naturalistic scenario can be achieved through a real public permissionless implementation (i.e., Ethereum Mainnet). However, the higher level of external influence decreases the conscious control required in an experiment. The sample size can be extended to include more users from more domains, accounting for various implementation scenarios in virtual exchange platforms. The pretest-posttest control group design [75] allowed a clearer inference about the real cause of effects, which is herein given through the change of prototype version (e.g., switch between non-manipulated and manipulated version). Despite the lack of statistical representativeness, the mixed-methods approach [71] enables collecting data from interviews and the assessment sheet and thus helps to obtain a precise perception, whose effort is hard to manage for a multitude of experts.

6. Conclusion and outlook

Facing an increasingly globalized and interconnected world, inter-organizational trust becomes a crucial aspect of successful cooperation and strong partnerships. Our research contributes to a novel empirical and theoretically grounded elicitation of design principles for establishing inter-organizational trust and reveals the extent of its perception of a blockchain-based implementation. Building upon this paper’s findings from multiple empirical and theoretical sources, we can show that a weak consideration of the design principles can lead to reduced trust, even if blockchain as an underlying technology is applied. In consequence, the implementation of BCT does not immediately result in trust. The evaluations reveal interdependencies between the design principles, making it challenging to extract the isolated cause-effect relationships of each principle. Limitations set by the univariate experiment design and the low number of stakeholders lead to the need for an extended experiment with additional control variables and participants.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used DeepL and Grammarly in order to improve the readability of the manuscript. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

CRediT authorship contribution statement

Nick Große: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Frederik Möller:** Writing – review & editing, Visualization, Conceptualization. **Thorsten Schoormann:** Writing – review & editing, Visualization, Conceptualization. **Michael Henke:** Supervision, Resources, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – GRK2193/2 – Project number 276879186.

References

[1] M. Natarajarathinam, I. Capar, A. Narayanan, Managing supply chains in times of crisis: a review of literature and insights, Int. J. Phys. Distrib. Logist. Manag. 39 (2009) 535–573, https://doi.org/10.1108/09600030910996251.
[2] D. Doran, Rethinking the supply chain: an automotive perspective, Supply Chain Manag. Int. J. 9 (2004) 102–109, https://doi.org/10.1108/13598540410517610.
[3] J. Kern, P. Wolff, The Digital Transformation of the Automotive Supply Chain - an Empirical Analysis with Evidence from Germany and China: Case Study Contribution to the OECD TIP Digital and Open Innovation Project, 2019.
[4] C.M. Durugbo, Z. Al-Balushi, Supply chain management in times of crisis: a systematic review, Manag. Rev. Quart. 73 (2022) 1179–1235, https://doi.org/10.1007/s11301-022-00272-x.
[5] C.G. Schmidt, S.M. Wagner, Blockchain and supply chain relations: a transaction cost theory perspective, J. Purch. Supply Manag. 25 (4) (2019) 100552, https://doi.org/10.1016/j.pursup.2019.100552.
[6] R. Beck, C. Mueller-Bloch, J. King, Governance in the Blockchain economy: a framework and research agenda, J. Assoc. Inf. Syst. 19 (2018) 1020–1034, https://doi.org/10.17705/1jais.00518.
[7] M. Rossi, C. Mueller-Bloch, J. Thatcher, R. Beck, Blockchain research in information systems: current trends and an inclusive future research agenda, J. Assoc. Inf. Syst. 20 (2019) 1388–1403, https://doi.org/10.17705/1jais.00571.
[8] M. Risius, K. Spohrer, A blockchain research framework, business & information, Syst. Eng. 59 (2017) 385–409.
[9] P. Mehrwald, T. Treffers, M. Titze, I.M. Welpe, Application of blockchain technology in the sharing economy: A model of trust and intermediation, in: Proceedings of the 52nd Hawaii International Conference on System Sciences, Hawaii: USA, 2019.
[10] F. Hawlitschek, B. Notheisen, T. Teubner, The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy, Electron. Commer. Res. Appl. 29 (2018) 50–63, https://doi.org/10.1016/j.elerap.2018.03.005.
[11] H. Treiblmaier, Toward more rigorous blockchain research: recommendations for writing blockchain case studies, Front. Blockchain 2 (2019), https://doi.org/10.3389/fbloc.2019.00003.
[12] B. Notheisen, Engineering Decentralized Markets: A Blockchain Approach, Dissertation,, Karlsruhe, 2019.
[13] N. Große. Design Principles for Establishing Trust in Decentralized Intercompany Capacity Exchange, Technology (DESRIST, St. Petersburg: Florida, USA, 2022.
[14] O.E. Williamson, The economics of organization: the transaction cost approach, Am. J. Sociol. 87 (1981) 548–577, https://doi.org/10.1086/227496.
[15] K.M. Eisenhardt, Agency theory: an assessment and review, Acad. Manag. Rev. 14 (1989) 57–74.
[16] C. Suematsu, Transaction Cost Management, Springer International Publishing, Cham, 2014.
[17] R. Cai, Trust and Transaction Costs in Industrial Districts. http://hdl.handle.net/10919/9948, 2004.
[18] S. Opriel, F. Möller, U. Burkhardt, B. Otto, Requirements for usage control based exchange of sensitive data in automotive supply chains, in: Proceedings of the 54th Hawaii International Conference on System Sciences, USA, Hawaii, 2021, pp. 431–440.
[19] H. Lee, M.S. Kim, K.K. Kim, Interorganizational information systems visibility and supply chain performance, Int. J. Inf. Manag. 34 (2014) 285–295, https://doi.org/10.1016/j.ijinfomgt.2013.10.003.
[20] C.P. Holland, Cooperative supply chain management: the impact of interorganizational information systems, J. Strateg. Inf. Syst. 4 (1995) 117–133, https://doi.org/10.1016/0963-8687(95)80020-Q.
[21] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, MIS Q. (2004) 75–105, https://doi.org/10.2307/25148625.
[22] O.E. Williamson, Markets and hierarchies: analysis and antitrust implications: A study in the economics of internal organization, first. Free Press paperback ed., [fourth. Dr.], The Free Press, New York, NY, 1975.
[23] W.W. Powell, Neither market nor hierarchy: network forms of organization, Res. Organ. Behav. 12 (1990) 295–336.
[24] N. Luhmann, Trust and Power, first. Auflage, John Wiley & Sons, New York, 2018.
[25] C. Moorman, G. Zaltman, R. Deshpande, Relationships between providers and users of market research: the dynamics of trust within and between organizations, J. Mark. Res. 29 (1992) 314–328.
[26] A. Zaheer, B. McEvily, V. Perrone, Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance, Organ. Sci. 9 (1998) 141–159.
[27] R.J. Lewicki, B.B. Bunker, Trust in Relationships: A Model of Development and Decline, Jossey-Bass, 1995.
[28] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Acad. Manag. Rev. 20 (1995) 709–734.
[29] B.B. Nielsen, Trust in strategic alliances: toward a co-evolutionary research model, J. Trust Res. 1 (2011) 159–176, https://doi.org/10.1080/21515581.2011.603510.
[30] J. Gebauer, A. Scharl, Between flexibility and automation: an evaluation of web technology from a business process perspective, J. Comput.-Mediat. Commun. 5 (1999), https://doi.org/10.1111/j.1083-6101.1999.tb00340.x.
[31] J. Lee, J. Kim, J.Y. Moon, What makes Internet users visit cyber stores again? Key design factors for customer loyalty, in: Proceedings of the SIGCHI conference on Human Factors in Computing Systems, 2000, pp. 305–312.
[32] J. Riegelsberger, M.A. Sasse, J.D. McCarthy, The mechanics of trust: a framework for research and design, Int. J. Human-Comp. Stud. 62 (2005) 381–422, https://doi.org/10.1016/j.ijhcs.2005.01.001.
[33] M. Spence, S. Rosen, 10, in: Signaling, Screening, and Information., in: Studies in Labor Markets, University of Chicago Press, 1981, pp. 319–358.
[34] J.L. Bradach, R.G. Eccles, Price, authority, and trust: from ideal types to plural forms, Annu. Rev. Sociol. (1989) 97–118.
[35] M. Voss, Privacy preserving online reputation systems, in: Y. Deswarte, F. Cuppens, S. Jajodia, L. Wang (Eds.), Information Security Management, Education and Privacy: IFIP 18th World Computer Congress TC11 19th International Information Security Workshops 22–27 August 2004 Toulouse, France, Firstst Ed. twentieth0fourth, Springer US, Imprint Springer, New York, NY, 2004, pp. 249–264.
[36] K. Spremann, Asymmetrische information, Z. Betriebswirt. 60 (1990) 561–586.
[37] N. Kannengießer, S. Lins, T. Dehling, A. Sunyaev, What does not fit can be made to fit! Trade-offs in distributed ledger technology designs, in: Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, pp. 7069–7078.
[38] DIN SPEC 16597, Terminology for blockchains;: Text in English, Beuth Verlag, Berlin, 2018.
[39] H. Subramanian, Decentralized blockchain-based electronic marketplaces, Commun. ACM 61 (2018) 78–84, https://doi.org/10.1145/3158333.
[40] B. Notheisen, F. Hawlitschek, C. Weinhardt, Breaking down the blockchain hype-towards a blockchain market engineering approach, in: Proceedings of the 25th European conference on Information Systems (ECIS): June 5-10, 2017, AIS eLibrary (AISeL), Guimarães, Portugal, 2017, pp. 1062–1080.
[41] F. Glaser, Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis, in: Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii: USA, 2017.
[42] K. Nærland, C. Müller-Bloch, R. Beck, S. Palmund, Blockchain to rule the waves-nascent design principles for reducing risk and uncertainty in decentralized environments, in: International Conference on Information Systems (ICIS), 2017, pp. 1–16.
[43] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, Gothenburg, Sweden, 2017, pp. 243–252.
[44] ISO/TS 23635:2022, Blockchain and distributed ledger technologies - Guidelines for governance.
[45] E. Abebe, D. Behl, C. Govindarajan, Y. Hu, D. Karunamoorthy, P. Novotny, V. Pandit, V. Ramakrishna, C. Vecchiola, Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (industry track), in: Middleware Industry 2019 - Proceedings of the 2019 20th International Middleware Conference Industrial Track, Part of Middleware 2019, 2019, https://doi.org/10.1145/3366626.3368129.
[46] X. Fan, L. Liu, R. Zhang, Q. Jing, J. Bi, Decentralized trust management: Risk analysis and trust aggregation, in: ACM Comput. Surv. 53, 1, Article 2 (February 2020), 2020.
[47] M. Utz, S. Johanning, T. Roth, T. Bruckner, J. Strüker, From ambivalence to trust: using blockchain in customer loyalty programs, Int. J. Inf. Manag. 68 (2023) 102496, https://doi.org/10.1016/j.ijinfomgt.2022.102496.
[48] A. Carvalho, Bringing transparency and trustworthiness to loot boxes with blockchain and smart contracts, Decis. Support. Syst. 144 (2021) 113508, https://doi.org/10.1016/j.dss.2021.113508.

[49] L. Chandra Kruse, S. Seidel, Tensions in design principle formulation and reuse, in: Proceedings of the 12th International Conference on Design Science Research in Information Systems and Technology, Karlsruhe: Germany, Karlsruhe, 2017, pp. 180–188.
[50] J.E. van Aken, Management research as a design science: articulating the research products of mode 2 knowledge production in management, Br. J. Manag. 16 (2005) 19–36, https://doi.org/10.1111/j.1467-8551.2005.00437.x.
[51] S. Gregor, L. Chandra Kruse, S. Seidel, The anatomy of a design principle, J. Assoc. Inf. Syst. 21 (2020) 1622–1652, https://doi.org/10.17705/1jais.00649.
[52] S. Gregor, D. Jones, The anatomy of a design theory, J. Assoc. Inf. Syst. 8 (2007) 312–335, https://doi.org/10.17705/1JAIS.00129.
[53] F. Möller, T. Schoormann, G. Strobel, M. Hansen, Unveiling the cloak: Kernel theory use in design science research, in: Proceedings of the 43rd International Conference on Information Systems, Kopenhagen: Denmark, 2022.
[54] K. Peffers, T. Tuunanen, M.A. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, J. Manag. Inf. Syst. 24 (2007) 45–77.
[55] T. Schoormann, F. Möller, L. Chandra Kruse, The beauty of messiness: a flexible tool for design principle projects, in: Proceedings of the 56th Hawaii International Conference on System Sciences, 2023, pp. 5146–5155.
[56] J. Venable, J. Pries-Heje, R. Baskerville, FEDS: a framework for evaluation in design science research, Eur. J. Inf. Syst. 25 (2016) 77–89, https://doi.org/10.1057/ejis.2014.36.
[57] R. Beck, M. Avital, M. Rossi, J.B. Thatcher, Blockchain technology in business and information systems research, business & information, Syst. Eng. 59 (2017) 381–384, https://doi.org/10.1007/s12599-017-0505-1.
[58] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, F. Wortmann, Privacy-preserving data certification in the internet of things: leveraging blockchain technology to protect sensor data, J. Assoc. Inf. Syst. 20 (2019), https://doi.org/10.17705/1jais.00567.
[59] J. Lindman, V.K. Tuunainen, M. Rossi, Opportunities and risks of Blockchain Technologies–a research agenda, in: Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii: USA, 2017.
[60] L. Chandra, S. Seidel, S. Gregor, Prescriptive knowledge in IS research: Conceptualizing design principles in terms of materiality, action, and boundary conditions, in: Proceedings of the 48th Hawaii International Conference on System Sciences, Hawaii: USA, 2015.
[61] J.G. Walls, G.R. Widmeyer, O.A. El Sawy, Building an information system design theory for vigilant EIS, Inf. Syst. Res. 3 (1992) 36–59.
[62] S. Gregor, L. Kruse, S. Seidel, Research perspectives: the anatomy of a design principle, J. Assoc. Inf. Syst. 21 (2020) 1622–1652, https://doi.org/10.17705/1jais.00649.
[63] M.D. Myers, M. Newman, The qualitative interview in IS research: examining the craft, Inf. Organ. 17 (2007) 2–26, https://doi.org/10.1016/j.infoandorg.2006.11.001.
[64] D.A. Gioia, K.G. Corley, A.L. Hamilton, Seeking qualitative rigor in inductive research, Organ. Res. Methods 16 (2013) 15–31, https://doi.org/10.1177/1094428112452151.
[65] F. Möller, T.M. Guggenberger, B. Otto, Towards a method for design principle development in information systems, in: S. Hofmann, O. Müller, M. Rossi (Eds.), Designing for Digital Transformation. Co-Creating Services with Citizens and Industry, Springer International Publishing, Cham, 2020, pp. 208–220.
[66] C. Sonnenberg, J. vom Brocke, Evaluations in the science of the artificial-reconsidering the build-evaluate pattern in design science research, in: International Conference on Design Science Research in Information Systems, Las Vegas: USA, 2012.
[67] J. Iivari, M. Rotvit Perlt Hansen, A. Haj-Bolouri, A proposal for minimum reusability evaluation of design principles, Eur. J. Inf. Syst. 30 (2021) 286–303, https://doi.org/10.1080/0960085X.2020.1793697.
[68] K. Peffers, M. Rothenberger, T. Tuunanen, R. Vaezi, Design science research evaluation, in: K. Peffers (Ed.), Design Science Research in Information Systems: 7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14–15, 2012, Proceedings, Springer, Berlin / Heidelberg, Berlin, Heidelberg, 2012, pp. 398–410.
[69] T. Schoormann, F. Möller, M. Di Maria, N. Große, Guiding Design Principle Projects: A Canvas for Young Design Science Researchers, Journal of Information Systems Education 34 (3) (2023) 307–325.
[70] D.L. Shapiro, B.H. Sheppard, L. Cheraskin, Business on a handshake, Negot. J. 8 (1992) 365–377, https://doi.org/10.1007/BF01000396.
[71] N.K. Denzin, The Research Act: A Theoretical Introduction to Sociological Methods, Routledge, 2017.
[72] H. Treiblmaier, The impact of the blockchain on the supply chain: a theory-based research framework and a call for action, Supply Chain Manag. 23 (2018) 545–559, https://doi.org/10.1108/SCM-01-2018-0029.
[73] K. Wuest, A. Gervais, Do you need a Blockchain?, in: In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) IEEE, Zug, 2018, pp. 45–54.
[74] A.M. Antonopoulos, G.A. Wood, Mastering Ethereum: Building Smart Contracts and DApps, 2018.
[75] D.T. Campbell, Factors relevant to the validity of experiments in social settings, Psychol. Bull. 54 (1957) 297–312.
[76] T. Mettler, M. Eurich, R. Winter, On the use of experiments in design science research: a proposition of an evaluation framework, Commun. Assoc. Inf. Syst. 34 (2014), https://doi.org/10.17705/1CAIS.03410.
[77] R.K. Yin, Case Study Research and Applications: Design and Methods, Sixth edition, SAGE, Los Angeles, London, New Dehli, Singapore, Washington DC, Melbourne, 2018.

Nick Große [0000-0001-8066-8796] is a postdoctoral researcher at the TU Dortmund University in Dortmund, Germany. Nick's research focuses on trust, blockchain technology, intercompany exchange of capacity, and industrial services in logistics and supply chains. During his Ph.D., he was a member of the research training group 'Adaption intelligence of factories in complex and dynamic environments' (GRK 2193).

Frederik Möller [0000-0001-6274-701X] is a junior professor at TU Braunschweig and a researcher at Fraunhofer ISST in Dortmund, Germany. Frederik's research focuses on design science research, data ecosystems, and business models. His work has been published in academic journals, such as *Business & Information Systems Engineering, Electronic Markets, Communications of AIS, Journal of Enterprise Information Management,* and *IEEE Transactions on Engineering Management*, as well as presented in leading conferences, such as *ICIS, ECIS,* and *DESRIST*.

Thorsten Schoormann [0000-0002-3831-1395] is an assistant professor (Akademischer Rat) at TU Braunschweig and a researcher at Fraunhofer ISST in Dortmund, Germany. Thorsten's research focuses on business model innovation, design science research, and digital tools that foster sustainability. His work has been published in academic journals, including the *Journal of Management Information Systems*, *European Journal of Information Systems*, *Business & Information Systems Engineering*, and *Electronic Markets*, as well as has been presented at leading conferences such as *ICIS* and *ECIS*.

Michael Henke [0000-0001-8066-8796] holds the chair for enterprise logistics (LFO) at TU Dortmund University and is a director of Fraunhofer IML in Dortmund, Germany. He is also an adjunct Professor for Supply Chain Management at the School of Business and Management at the Lappeenranta University of Technology in Finland since 2015 and assumes responsibility for the association of the initiatives Blockchain Europe and Silicon Economy Logistics Ecosystems.