Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 194, Issue 35, June/July 2023, Pages 67–91
https://doi.org/10.7250/csimq.2023-35.03

Trustworthiness Requirements in Information Systems Design: Lessons Learned from the Blockchain Community

Irina Rychkova* and Marwa Ghriba

Centre de Recherche en Informatique, University Paris 1 Panthéon-Sorbonne,
75005, 12 Place de Panthéon, Paris, France

Irina.Rychkova@univ-paris1.fr, Marwa.Ghriba@univ-paris1.fr

Abstract. In modern society, where digital security is a major preoccupation, the perception of trust is undergoing fundamental transformations. Blockchain community created a substantial body of knowledge on design and development of trustworthy information systems and digital trust. Yet, little research is focused on broader scope and other forms of trust. In this study, we review the research literature reporting on design and development of blockchain solutions and focus on trustworthiness requirements that drive these solutions. Our findings show that digital trust is not the only form of trust that the organizations seek to reenforce: trust in technology and social trust remain powerful drivers in decision making. We analyze 56 primary studies, extract and formulate a set of 21 trustworthiness requirements. While originated from blockchain literature, the formulated requirements are technology-neutral: they aim at supporting business and technology experts in translating their trust issues into specific design decisions and in rationalizing their technological choices. To bridge the gap between social and technological domains, we associate the trustworthiness requirements with three trustworthiness factors defined in the social science: ability, benevolence and integrity.

Keywords: Trust, Trustworthiness, Requirements, Blockchain, Literature review.

1 Introduction

Trust is a social construct that emerges from relationships and interactions between individuals or groups. It involves a willingness to rely on others based on perceived ability, integrity, and benevolence [1], [2] and is influenced by factors such as past experience, reputation, and social norms. Digital technologies enable novel models of social and business interactions, where trust becomes a critical design consideration for information systems. The impact of trust on system design is twofold: firstly, modern technologies act as mediators in interactions between individuals

* Corresponding author

Reference: I. Rychkova and M. Ghriba, "Trustworthiness Requirements in Information Systems Design: Lessons Learned from the Blockchain Community," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 35, pp. 67–91, 2023. Available: https://doi.org/10.7250/csimq.2023-35.03

Additional information. Author's ORCID iD: I. Rychkova – https://orcid.org/0000-0002-1100-0116. PII S225599222300194X. Received: 14 May 2023. Accepted: 28 June 2023. Available online: 31 July 2023.

and organizations, with the expectation of increasing trust between them; secondly, these technologies themselves must be trusted by users to provide them with a positive experience [3].

In the technological domain, trust is often connotated with security, reliability, and usability of digital systems or platforms. The extended ISO 27000 definition for trust [4] includes the CIA-triad (confidentiality, integrity, availability) as well as authenticity, accountability, non-repudiation, and reliability. Within this conceptualization, trust is often established through technological mechanisms, algorithms, and automated processes, and can be objectively assessed.

The gap between the social and technology-centric definitions of trust arises due to the challenges of translating the subjective, context-dependent nature of social trust into objective, measurable terms that can be addressed by technical mechanisms. To bridge this gap, it is important to recognize the multidimensional nature of trust and consider the social and cultural contexts in which technological systems are developed and used.

Three forms of trust are widely recognized in the literature: social trust, digital trust, and trust in technology. Social (or interpersonal) trust is defined as the subjective probability that an entity – a trustee – has the required capacity and willingness to perform an action that is beneficial or at least not detrimental to another entity – a trustor – in a specific context [1]. Compared to social trust, digital trust defines relationships between entities in the digital world. It is the measure of confidence that a trustor has in the trustee's ability to protect data and privacy of individuals [5]. Trust in technology is another form of trust that reflects trustor's beliefs that a specific technology has the attributes necessary to perform as expected in a given situation where negative consequences are possible [6], [7]. Social, digital, and trust towards technology are intrinsic to organizations and have important implications in organizational decision-making and technology adoption [6], [8]–[11]. They need to be explicitly addressed in the design of technological solutions.

During the past decade, the blockchain community provided a substantial contribution to the body of knowledge on the design and development of trustworthy information systems [12]–[14]. Blockchain technology fosters digital trust through reliable and efficient information sharing [15]. In the blockchain literature, trust is mainly connotated with specific technical properties such as decentralization, transparency, traceability, data integrity, etc. [11], [16]–[18]. Many of these properties are granted by the fundamental features of the blockchain technology itself [19].

While digital trust provides a foundation for secure and reliable digital interactions, it may not fully capture the complexities of social trust that arise from human relationships, emotions, and cultural factors. Moreover, different architectural and design choices, consensus mechanisms, and governance structures impact the level of trust and confidence that users have in the blockchain solutions [8]. Therefore, the broader scope and implications of trust in blockchain solution design need to be studied.

In this work, we investigate how social trust, digital trust, and trust in technology are addressed in the blockchain literature. We follow the guidelines for systematic literature review (SLR) defined by Kitchenham et al. in [20] and review primary research studies that focus on trust conceptualization, trustworthy system design, and acceptance in blockchain.

With this study, we intend to make the following contributions:

- Descriptive overview of current research in information systems engineering and blockchain that addresses trust issues and trustworthiness requirements.
- Definition and classification of trustworthiness requirements extracted from primary research studies in blockchain.
- Qualitative analysis of trustworthiness requirements.

Grounded on the lessons learned from the blockchain community, this work addresses a broader audience. First, it will help organizational stakeholders to better understand their trustworthiness requirements and to assess potential value of technological (in particular, blockchain) solutions to meet these requirements. Second, it will address technology professionals and researchers, helping them to align their design decisions with a social context. We formulate the identified trustworthiness requirements in technology-neutral language and make them reusable in different

problem and solution domains. To bridge the gap between technological and social domains, we associate the defined requirements with the three trustworthiness factors from social science: ability, benevolence, and integrity [2]. In order to effectively address the concerns of various experts involved in solution design, we identify each trustworthiness requirement with its corresponding type of trust. Additionally, we propose a mapping of these requirements on three abstraction levels: strategic, operational, and IT, to facilitate their expression in different organizational contexts. Our final intended contribution is:

- Identification of key challenges and directions for future work that would lead to improved alignment between organizational requirements and technological solutions for resolving trust issues.

The remainder of this article is organized as follows: Section 2 presents the background for this study and analyses the related works. Section 3 presents our research method. Section 4 reports on the results of this literature review with respect to the defined research questions. In Section 5, we discuss our findings and provide directions for future research. Finally, in Section 6, we conclude our article.

2 Fundamentals and Related Work

2.1 Trust and Trustworthiness

In the research literature on trust, the act of trust is often represented as a *relationship between a subject (the trustor) and an object of trust (the trustee)* [21], [22]. Outcome of trust is defined as an interaction between trustor and trustee and is characterized by the resulting experience (negative or positive). Antecedents of trust refer to the factors that influence trustor's willingness to trust and include factors related to the subject (trustor's propensity to trust), to the object (trustworthiness of the trustee) and to the environment where interaction between the subject and the object takes place (e.g., institutional trust) [2], [6], [23], [24].

In this study, we consider trustor's propensity to trust and institutional trust as invariant for a given interaction. Our primary focus is on trustworthiness factors, which are associated with the expected attributes of trustee. Trustor *perceives* the trustworthiness of a trustee by collecting information on that particular trustee. This perception can evolve based on the trust outcomes (good or bad experience) [1], [2]. Trustors expectations about trustworthiness of a trustee can be formulated as *trustworthiness requirements (TwR)*. TwR can be met by incorporating certain attributes, features, or properties by the trustee, whether a social entity or a technological solution.

Whereas researchers in social sciences study trust as relationships between social entities (individuals, groups or organizations), in information systems research, trust is considered as a socio-technical concept. It can be defined as a relationship between social entities and technological components (e.g., information systems, applications, infrastructure, etc.), in which a technological component can be either an object (trustee) or a subject (trustor) [25]. To address this complex nature of the concept, we consider three types of trust: social trust (trust between social entities), trust in technology (trust between a social entity – a trustor, and a technological component – a trustee) and digital trust (trust between social entities where technological components play the role of mediator and act "on behalf of" a trustor or a trustee).

Depending on whether the trustee is a social entity or an IT object, the trustor needs to consider different trustworthiness factors prior to engage into interaction with this trustee. Below, we provide a brief overview of social trust, trust in technology and digital trust and their trustworthiness factors. We summarize the presentation in Table 1.

Table 1. Overview of trust types

Type of Trust	Trustor (subject)	Trustee (object)	Trust antecedents (factors of trustworthiness)	Outcome
Social Trust	Org. / Individual	Org. / Individual	Ability, benevolence, integrity	Interaction / collaboration
Trust in Technology	Org. / Individual	IT object	Functionality, helpfulness, usefulness, reliability	Acceptance, use
Digital Trust	Org. / Individual	IT object	Privacy, security, transparency, traceability, control	Interaction / transaction in digital environment
	IT object	Org. / Individual		
	IT object	IT object		

Social Trust

Social trust is a precondition of collaboration. It is described by a situation in which an individual or an organization (trustor) is willing to rely on the chosen actions of another individuals (trustee). Gambetta [1] defines trust as a level of the subjective probability with which the trustor assesses that the trustee will perform a particular action. Mayer, Davis and Schoorman define trust antecedents and outcomes in their integrative model of organizational trust [2]. The authors define the trust for a trustee as "a function of the trustee's perceived ability, benevolence, and integrity and of the trustor's propensity to trust." Whereas propensity to trust is an intrinsic characteristic of a trustor, ability, integrity and benevolence are the factors of (perceived) trustworthiness that characterize a trustee and thus can be evaluated. According to [2], *ability* defines a group of skills, competencies, and characteristics that enable a trustee to have influence within some specific domain; *benevolence* defines the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive; *integrity* refers to trustee's moral quality of being sincere, honest, and her capacity and willingness to adhere to some rules/principles. Social trust is used as the basis for decision-making in diverse contexts, including enterprise strategy, governance of operations and technology [26].

Trust in Technology

Trust in technology is described by a situation in which an individual user or an organization (trustor) is willing to rely on technology (trustee) to accomplish a specific task [6]. Trust in technology reflects trustor's beliefs that a specific technology (IT object) has the attributes necessary to perform as expected in a given situation in which negative consequences are possible.

The trustworthiness factors in trust in technology include functionality, helpfulness, reliability and credibility of information [6], [7]. According to Sutcliffe [3], needs for trust in technology can be fulfilled by solutions' usability, functionality, aesthetics. He also highlights that trust can be facilitated via customizability and adaptability. In [27], [28], trustworthiness of technology is associated with (perceived) usefulness, ease of use, enjoyment and value (quality/price ratio). In [29] trustworthiness of software is associated with transparency, verifiability and compliance of the development process.

Trust in technology is an antecedent of technology acceptance and use [28], [30], [31]. To improve the acceptance, user's expectations about trustworthiness of technology need to be explicitly formulated as respective (trustworthiness) requirements and considered in technology design.

Digital Trust

Digital trust is a precondition for social and business interactions in a digital environment. In these interactions, technology (IT object) plays the role of a mediator and can impersonate a trustor or a trustee. Digital trust reflects trustor's beliefs that trustee (a social entity or an IT object) has the attributes necessary to support secured digital interactions [5]. Trustworthiness factors in digital trust include (perceived) privacy, security, transparency, traceability, and control [19], [32]. According to [3], the role of technology as a trust mediator can be also fulfilled by increasing accessibility of information, transparency of processes, communication of intent and identity.

2.2 Trustworthiness Requirements in Software and Systems Engineering

In systems engineering, trustworthiness of a particular system or component means "to be worthy of being trusted" to fulfil some specific requirements [33]. ISO/IEC 25010 Standard [34] addresses systems and software quality requirements and defines trust as a degree to which a user or other stakeholder has confidence that a product or system will behave as intended. Whereas these definitions provide some reference to the social context where the system is used, the implications of trust are not explored much further. Subjectivity, context sensitivity and emergence are characteristics of trustworthiness that make it difficult to capture and formalize in product design. Consider an example of a mobile phone: if we examine the trustworthiness factors that influence a user's decision to buy, to use for specific purposes and to rely upon this product, we discover that for different users and contexts of use these factors will not be the same. For an elderly person, the antecedents of trust will include usability and helpfulness; for people with active lifestyle they will include robustness and cost efficiency; for professionals they will include performance, resilience, data security and so on. Further, stakeholders' "needs for trust" can run into conflict with other needs and impact the requirements. For instance, using a cloud storage is attractive because of its high accessibility and low price, however this raises trust concerns related to resilience and possibility of unauthorized access to your personal or business data. Trustworthiness requirements considered in this work provide a ground for reasoning about such conflicts and their resolution.

In requirements engineering, a requirement is defined as *a statement which identifies an operational, functional or design characteristic or constraint of the product or process, which is unambiguous, testable or measurable, and necessary for the product or process to be accepted by consumers or internal quality assurance guidelines* [35]. A set of explicit, clearly stated requirements facilitates communication between stakeholders: it justifies technological and design decisions and provides a basis for solution validation. When expressed in natural language, the statement of requirement should include a subject (e.g., system, software, etc.), an active verb and other elements necessary to specify the requirement. The guidelines for writing requirements are specified by ISO/IEC standard [35].

In software engineering and systems engineering, two types of requirements are widely used during the product design: functional requirements (FRs) define a function of a system or its component; non-functional requirements (NFRs) define the properties and specify the criteria according to which the system's functioning can be judged or evaluated. In other terms, FRs define *what* the system has to do, while NFRs define *how* it should do it. Whereas FRs and NFRs focus on measurable product quality, phenomena related to people and social context where the product is developed, deployed and used require not less attention in RE. In [36] a taxonomy of 'soft' requirements is introduced. Soft requirements are a linguistic concept that addresses a wide range of phenomena related to people, organizations and society: values, attitudes, motivations, emotions. SR are extending NFR/soft goals and can be refined by FR/hard goals and met by some properties of a (software) solution. However they also address social concepts, including trust, that do not always require technological solution. Compared to FR and NFR, SR may be implicit, with their influences subtle and difficult to anticipate at design time [36]. Trust is associated in SR with the aspects of the social system where a technological system is used – its context. Context of use SR influence user requirements (FR and other SR) as well as product qualities (FR and NFR).

In this work, we focus on trustworthiness requirements (TwR) that can be associated with FR and NFR contributing to trust between the entities (e.g., a user and a software product) in a given socio-technical system (see Figure 1). We define trustworthiness requirement as *a statement made by a trustor about the expected trustworthiness of a trustee. This statement has to clearly express an operational, functional, design or other characteristic, which, according to trustor's believes, positively impacts trustworthiness of this trustee and interaction between the two.* The nature of trustor, trustee, relationship between them as well as trustworthiness factors can vary depending on the type of trust (see Table 1). Similar to SR from [36], TwR for a given product can be emergent and can vary depending on characteristics of a trustor (e.g., her propensity to trust, perception of risk) and the context where the interaction with the product will take place; if explicitly defined, TwR can change (extend) the set of product requirements (see TwR' in Figure 1).

Whereas trustworthiness is considered as an important factor of product satisfaction [34] and recognized as an antecedent of adoption, little research explicitly addresses trust and trustworthiness as a part of system requirements. In [37] the role of trustworthiness in the software development lifecycle is examined. Trustworthiness requirements are derived from user trust concerns and include usability, availability, reliability, transparency. Once users' trust concerns are elicited during a requirement engineering process, they are translated into trustworthiness requirements and mapped onto specific features / properties of the (prospective) technological solutions.

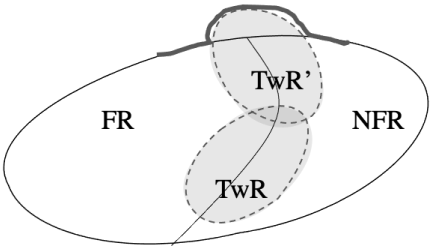


Figure 1. Trustworthiness requirements (TwR) compared to FR and NFR. If explicitly defined, TwR can change (extend) the set of product requirements (see TwR')

2.3 Trust and Trustworthiness in Blockchain

In practice, digital trust solutions consist in implementing a set of control mechanisms, which intend to modify the feasible set of alternatives (undesirable scenarios) that can be realized within a trustor-trustee interaction in a digital environment. Paraphrasing Gambetta [1], digital trust can be seen as "a device for coping with the freedom of others", which increases the probability that the other party will not (be given an opportunity to) act in a harmful way. Blockchain technology enforces digital trust by providing a set of such control mechanisms as intrinsic features.

Blockchain technology has emerged as a potential solution to cope with mistrust in traditional (centralized) institutions and online intermediaries in general [8]. Blockchain can be defined as a distributed database that allows its users to transact in a public and pseudonymous setup without the reliance on an intermediary or central authority [38]. According to [39], trust is the most influential factor driving interest in the blockchain. In blockchain, trust is not placed into the (social) entities participating in an interaction, but into specific properties of the technology. Belotti et. Al. [19] point out, "Whenever trust cannot be laid on a set of network nodes, it is better to have confidence in a protocol (i.e., a set of rules) ... that punishes or makes unfeasible any violation and thus guarantees the correct functioning of a system". Decentralized architecture, use of cryptography, distributed consensus protocols and smart contracts are fundamental features of blockchain that enable immutability, integrity, auditability and transparency of transactions. These properties are recurrently associated with digital trust in the literature [11], [16]–[18].

However, with a sheer use of blockchain, trust is not granted. While blockchain platforms support digital trust building between parties they do not remove the requirements for social (inter-personal) trust in organizations [8], [40]. Moreover, alleviating some social factors of trustworthiness, blockchain introduces their digital counterparts. For instance, independence from a central authority comes at the cost of privacy; distributed consensus and trustful transactions come at the cost of performance and interoperability etc. Depending on the industry sector and the use case, privacy, security, scalability, interoperability, performance are considered the main challenges and strongly impact blockchain adoption and trust in blockchain technology [19], [41], [42]. To meet these challenges, the blockchain technology trustworthiness has to be examined against the trustworthiness requirements in each particular use case.

2.4 Related Works

Trustworthiness of blockchain solutions is widely discussed in the related secondary studies. In [42], the authors evaluate the potential of blockchain against traditional databases in four domain

areas, including required trust assumptions, context requirements, performance characteristics and required consensus mechanisms. The literature review in [43] examines how trustworthiness of data provider ("the oracle") is addressed by blockchain solutions. In [44], the authors evaluate blockchain solutions and discuss requirements and considerations related to trust for identity management in healthcare domain. The literature review in [10] examines the barriers to blockchain adoption and highlights the issues related to high computing power requirements and implementation costs. In [45], the overview of trust-free sharing services in the financial sector is presented. Authors highlight security aspects as main trustworthiness factors. The work in [46] identifies key factors and non-functional requirements related to adoption of blockchain solutions in construction industry 4.0. These factors include information trustworthiness, transparency, traceability, and immutability. In [41], security, privacy, latency and computational cost are also identified as the main technical challenges of blockchain, however only privacy is explicitly related to trustworthiness of blockchain.

Whereas many studies discuss technical challenges in blockchain and their impact on the blockchain adoption, only a few relate these challenges with trust (social trust or trust in technology). In [47] the role and the multi-perspective view on trust in the context of the sharing economy and blockchain technology is examined. The authors identify trust in peers, trust in platform and trust in other targets (including products) and put forward the social antecedents of trust (ability, integrity, benevolence). In [48], a goal-oriented approach for business process reengineering is discussed. Here trustworthiness concerns are explicitly represented as (soft) goals and mapped to the relevant trust-enhancing features of blockchain, supporting business process reengineering.

In this work, we capture the issues and requirements expressed in the blockchain literature (FR, NFR, process requirements, etc.) that are associated with trust and trustworthiness and formulate them as non-blockchain-agnostic TwR. These requirements are intended to serve as a knowledge base and to facilitate the mapping between *trust issues* expressed by both technical and non-technical stakeholders in organizations and *trust-enabling features* of solutions, rationalizing technological and design choices.

3 Research Method

The research method used in this study follows the guidelines for systematic literature review (SLR) from [20]. The methodology consists of the following steps that will be further explained in this section: definition of the research questions, definition of the search strategy, primary source selection, data extraction, analysis and synthesis.

3.1 Research Questions

This study aims to examine the existing research on design, development and acceptance of blockchain solutions and to provide a comprehensive overview of the organizational requirements related to social trust, digital trust and trust in technology that drive these solutions. We formulate the following research questions for this study:

RQ1: What are the contributions of primary studies?
RQ 2: How trust is defined in primary studies?
RQ 3: What are the trustworthiness requirements used by primary studies?
RQ 4: What types of trust are addressed by the identified requirements?
RQ 5: At what abstraction levels the trustworthiness requirements are defined?

3.2 Search Strategy and Selection Process

The flow diagram adopted from PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [49] presents an overview of the source selection process in Figure 2.

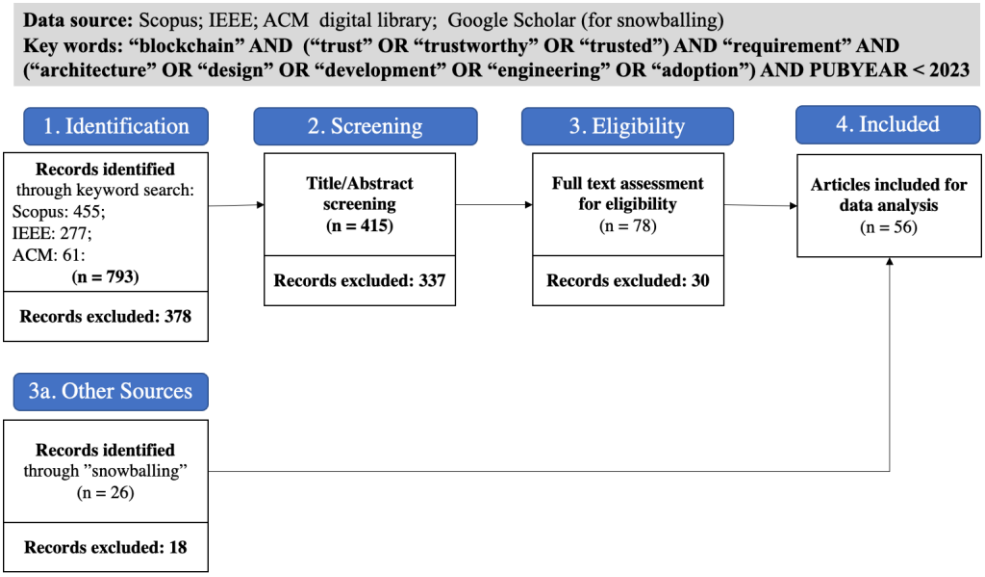


Figure 2. PRISMA flow diagram for selection process

1: Identification. To identify the initial set of records, we selected the following databases: Scopus, ACM digital library, IEEE.

Using the PICOC criteria [20], we define the search terms forming the following search string: *"blockchain" AND ("trust" OR "trustworthy" OR "trusted") AND "requirement" AND ("architecture" OR "design" OR "development" OR "engineering" OR "adoption")*.

We limit the publication year (PUBYEAR < 2023) to obtain a consistent set of publications that will not be affected by more recent apparitions. We conducted an automated search in the selected databases and identified 793 records in total. After removing duplicates and non-primary sources (e.g., proceedings, books etc.) we kept 415 records for screening.

2: Screening Relevant Publications. We screened titles and abstracts of identified records and eliminated publications based on the following exclusion criteria:

EC1: A study is unavailable for retrieval
EC2: A study is not a peer-reviewed publication
EC3: A study is not primary research
EC4: A study does not focus on requirements
EC5: Issues or requirements motivating the solution are not related to trust or trustworthiness.

We kept 78 records for the full text assessment.

3: Eligibility Assessment. We examined the full text of the preselected publications for eligibility based on the exclusion criteria EC3-EC5. The full text assessment was executed by the two authors independently; the results were compared and the conflicts were resolved. 48 records were kept for the final data set.

4: Snowballing and Final Data Set. We conducted backward and forward citation analysis of the eligible publications from the previous step (a so-called "snowballing" technique) using other databases (e.g., Google scholar) and identified a set of 26 records which was reinjected into the process. These records were screened and assessed for eligibility following the steps above. 18 records have been eliminated.

The selection process resulted in a final data set of 56 articles ([7], [11], [16]–[18], [30], [40], [49]–[97]). The overview of the selected studies is presented in Table 2. In our further analysis, we use consecutive enumeration of the studies: S1-S56.

Table 2. Overview of the selected studies

ID	Year	Biblio REF	Application Domain	Empirical	Theoretical	Artifact	Methodological	Research Outcome / Artifact Produced	Definition of Trust:	Abstraction Level:	Type of Trust:
S1	2022	[49]	Vehicular Networking	*		*		model algorithm	TECH	T, S	D, S, TT
S2	2022	[50]	Healthcare	*	*			proposal evidence principles	TECH	S, OP, T	S, TT
S3	2022	[51]	Education	*		*	*	approach prototype	IM	OP, T	S, TT
S4	2022	[52]	SCM	*		*	*	approach architecture	IM	OP, T	D
S5	2022	[53]	EAI	*			*	approach	IM	OP, T	S
S6	2022	[54]	Healthcare, IoT	*		*		architecture	IM	T	D
S7	2022	[55]	SCM	*	*	*		architecture, framework	IM	OP, S	D
S8	2022	[40]	SCM	*	*			evidence / proposal	SOC	ST, T	S, TT
S9	2022	[56]	Electronic Voting	*	*			evidence / proposal	IM	ST, T	S, TT
S10	2022	[57]	IoT			*		protocol, algorithm	IM	T	D
S11	2022	[58]	Other	*		*		framework	IM	T	D
S12	2021	[59]	AI	*	*	*		system model	IM	OP, T	TT
S13	2021	[60]	Healthcare	*		*	*	approach prototype	IM	S	S, D
S14	2021	[11]	Banking	*	*			other	IM	OP, S	TT
S15	2021	[61]	Education	*	*	*		architecture prototype model framework	IM	S, OP, T	D, TT, S
S16	2021	[62]	Healthcare	*	*			other	IM	OP, T, S	D, S, TT
S17	2021	[63]	Healthcare Industry 4.0	*	*	*		framework architecture system	SOC	S	S, TT, D
S18	2021	[64]	dApps BPM		*			framework model	SOC	S, OP, T	S, D, TT
S19	2021	[65]	SCM	*	*		*	approach conceptual model	IM	S, OP, T	S, D, TT
S20	2021	[66]	BPM	*		*	*	approach prototype	SOC	S, OP, T	S, D, TT
S21	2021	[67]	SCM IoT	*		*	*	model algorithm	IM	OP, T	TT, D, S
S22	2021	[68]	SCM IoT		*			framework model	IM	S, OP, T	D, S
S23	2021	[69]	Vehicular Networking	*		*		framework, architecture	IM	T	D
S24	2021	[70]	Other	*		*		architecture	IM	T	D
S25	2021	[71]	IoT		*			framework	IM	T	D
S26	2020	[18]	Healthcare	*	*			evidence principles	SOC	S, OP, T	S, D
S27	2020	[72]	EA		*			other		OP	S, D, TT
S28	2020	[16]	Other	*				evidence	TECH	OP, T	S, D, TT

Table 2 continued

ID	Year	Biblio REF	Application Domain	Empirical	Theoretical	Artifact	Methodological	Research Outcome / Artifact Produced	Definition of Trust:	Abstraction Level:	Type of Trust:
S29	2020	[73]	Banking	*		*		proposal architecture	TECH	T	D
S30	2020	[74]	Education	*		*		architecture	TECH	OP, T	D
S31	2020	[75]	Vehicular Networking	*	*	*		architecture concept	TECH	T	TT, D
S32	2020	[76]	BPM	*	*			evidence taxonomy	SOC	S, OP, T	S, D, TT
S33	2020	[77]	BPM	*			*	evidence method	SOC	S, OP, T	S, D, TT
S34	2020	[7]	MIS		*		*	model	SOC	S, OP, T	TT
S35	2020	[17]	Edge Computing	*		*		architecture	IM	T	D
S36	2020	[78]	Other	*		*		architecture evidence technology blueprint	IM	S, OP, T	TT, D
S37	2020	[79]	Healthcare		*			model	IM	S, OP, T	D
S38	2020	[80]	BPM	*		*	*	framework tool process	IM	S, OP	S, D
S39	2020	[81]	Healthcare EA	*		*	*	architecture proposal approach	IM	T, OP	S, D
S40	2020	[82]	BPM	*			*	evidence approach	TECH	S,OP, T	S, D
S41	2020	[30]	Other		*			framework	IM	OP	S, TT
S42	2019	[83]	SCM	*	*			other	TECH	OP	TT
S43	2019	[84]	Other	*	*			framework principles	TECH	S, OP, T	D
S44	2019	[85]	Healthcare	*		*		proposal protocol	IM	OP, T	S, D
S45	2019	[86]	Electronic Voting	*				proposal	IM	S	S
S46	2019	[87]	Healthcare	*				proposal	IM	OP, T	S, D, TT
S47	2019	[88]	IoT Industry 4.0	*	*			framework	SOC	S, OP, T	S, TT, D
S48	2019	[89]	BPM	*			*	approach proposal	IM	S, OP, T	S, D
S49	2019	[90]	BPM	*	*			model	SOC	OP, T	S, D, TT
S50	2019	[91]	Cloud	*	*			framework proposal	TECH	T	D
S51	2018	[92]	BPM	*				proposal	TECH	OP	S, D
S52	2018	[93]	Healthcare	*				proposal	TECH	T	D
S53	2018	[94]	BPM MAS	*		*		architecture proposal	IM	OP, T	S, D
S54	2018	[95]	SCM	*	*	*		protocol model	IM	T	D
S55	2018	[96]	BPM Industry 4.0	*	*			proposal framework	IM	T	D
S56	2017	[97]	Other	*		*		tool	TECH	T	D

3.3 Data Extraction, Analysis and Synthesis

Table 3 defines the data items that have been systematically extracted from the selected sources. Each data item is defined in connection with one of the research questions. Year of publication and Application domain provide a descriptive information about our data set and are not explored any further in this study. Overview of the extracted data is presented in Table 2. The results of our data analysis are presented in the next section.

Table 3. Data extraction Form

Data Item	**Value**	**RQ**
Year of publication	NUM	--
Application Domain	Text	--
Quantitative analysis:		
Contribution type	{Empirical, Artifact, Theoretical, Methodological, Dataset, Survey, Opinion}	RQ1
Research outcome	Text	RQ1
Qualitative analysis:		
Trust: definition	{IM, SOC, TECH}; IM = implicit; SOC = social; TECH = technical	RQ2
Trust Issue(s)	Text	RQ3-5
Trustworthiness Requirement(s)	Text	RQ3-5
Type of trust addressed	{S, D, TT}; S = Social, D = Digital, TT = trust in technology	RQ4
Level of abstraction	{S, OP, T}; S = Strategic, OP = Operational, T = Technical	RQ5

For the analysis of contributions, we used the guidelines of Wobbrock [98] to code the contribution types and research outcomes. For the qualitative analysis of trustworthiness requirements, first, we examined which underlying theories of trust are used in the studies and to which definition of trust (social or technology-centric) the studies adhere. Next, we extracted text evidences of trust issues and trustworthiness requirements. Further, the extracted data was coded by the authors following both semantic and latent approaches [99].

We defined the codes for our trustworthiness requirements based on the trustworthiness properties specified by the related secondary studies (Table 4). The codes most frequently used in these studies are: *Security, Privacy, Data integrity, Confidentiality, Availability, Reliability, Accountability*. Other codes used are: *Decentralization, Costs/resource efficiency, Traceability, Immutability, Transparency, Resilience, Authenticity*.

Table 4. Related literature used to define the codes for trustworthiness requirements

Article	Method	Articles analyzed
Alamri, B. et al., 2022	SLR	24
Ali, O. et al., 2020	SLR	87
Caldarelli, G., Ellul, J., 2021	SLR	49
Casino, F. et al., 2019	SLR	314
Durneva, P. et al., 2020	SLR	70
Hawlitschek, F. et al., 2018	SLR	62
Konstantinidis, I. et al., 2018	SLR	44
Pietrzak, P., 2021	SLR	34
Ross, R., et al., 2016	Technical Report	n/a
Standard ISO/IEC TR 27000, 2018.	Standard	n/a
Teisserenc, B., Samad, S., 2021	LR + Interviews	n/a
Wang, Y. et al., 2019	SLR	29

During the analysis, the set of codes was refined and new codes have been added. For instance, considering that Security is closely associated with other categories (e.g., Confidentiality, Integrity,

Availability, Authentication) in the literature, we removed it from our code list. Conversely, other categories recurrently used in the primary sources (e.g., Compliance, Interoperability, Auditability) have been added to the code list.

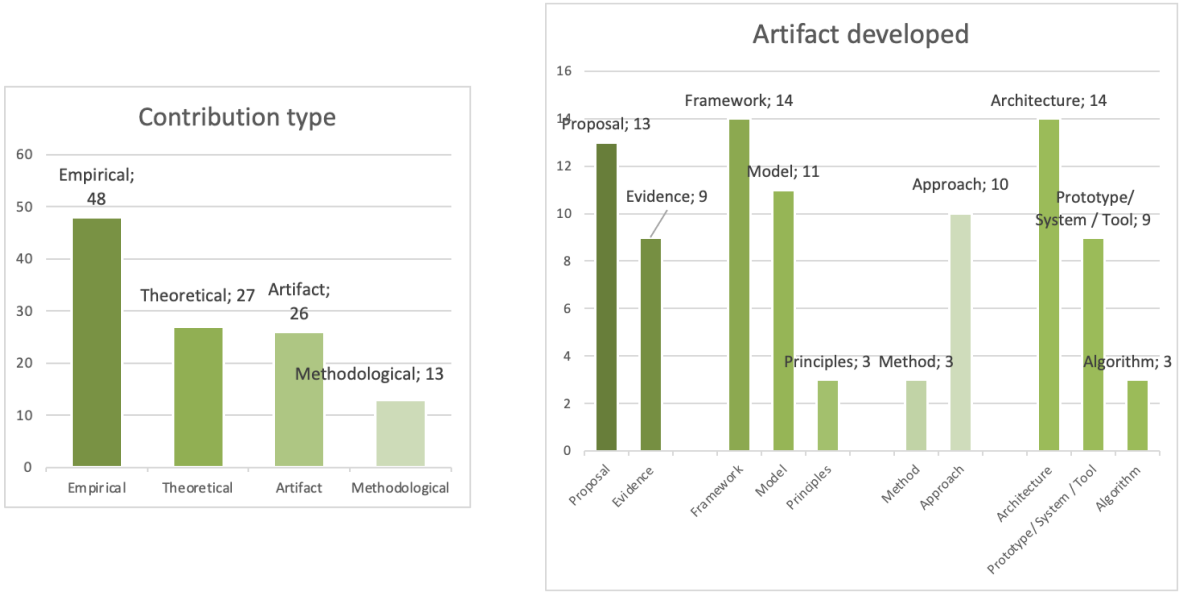
The evidences of requirements have been extracted and analytically mapped on the identified codes and categories, including type of trust and abstraction level (available in Table 2).

4 Results

4.1 What are the Contributions of Primary Studies? (RQ1)

In this review, we examine 56 primary research studies that address trust issues and requirements by designing and developing technological solutions. We apply the classification of Wobbrock [98] to analyze the general forms this new knowledge takes. This classification defines seven research contribution types: empirical, methodological, theoretical, artifact, survey and opinion.

We coded each research study with the contribution type and the type of research outcome that was produced (Table 2). The majority of studies reports on multiple contributions and outcomes. The summary is presented in Figure 3.



(a) (b)

Figure 3. (a) Distribution of the research contributions by type. (b) Distribution of the developed artifacts.

Empirical research contributions refer to findings based on observation and data gathering. The created knowledge is embedded in *new evidences and proposals* [98]. 48 out of 56 (86%) examined studies make empirical research contributions providing evidences on trustworthiness requirements, issues and solutions.

Theoretical contributions aim at improving the existing understanding or the existing way of reasoning about things. They provide *new definitions, concepts, models, principles, or frameworks* grounded on analytical thinking and reasoning [98]. Theoretical contributions are made by 27 out of 56 (48%) examined studies.

Methodological contributions aim at improving the existing practice by defining novel ways to "carry out our work". They influence how we design, develop, analyse or run systems or processes and result in new knowledge in a form of *approaches, methods, metrics, techniques* etc. Methodological contributions are identified in 13 studies (23%). Proposed methods and approaches are mostly grounded on observations (experience, empirical data).

Artifact contributions result from design and development activities. Here new knowledge is manifested by *working prototypes, architectures, tools, processes, algorithms* that demonstrate new concepts, or enable new explorations in the future [98]. Artifacts are developed in 26 examined studies (46%) including 9 working prototypes, tools or systems and 14 architectures. Other artifacts include process, protocols, algorithms.

Survey research contributions create knew knowledge by synthesizing the previous work and identifying trends and open issues. Survey contributions are also referred to as "secondary research". Following the selected research protocol [20], secondary research papers have been eliminated during the selection process (see Section 3.2.).

Dataset contributions support the research community providing common ground for testing, analysis and evaluation of other contributions. *Opinion* contributions propose the arguments and seek not only to inform but to persuade the reader. These contribution types were not identified in the examined set of studies.

4.2 How Trust is Defined in Primary Studies? (RQ2)

In addressing trust in the text, the examined primary research is divided as follows: studies that provide an explicit definition of trust grounded on social sciences, studies that provide technology-centric heuristics on trust, and studies that do not provide an explicit definition of trust. Figure 4 illustrates the distribution of studies.

We found 10 articles (18%) that define trust as a social concept and recognize the role of the social context in their technical solution design (S17, S18, S20, S26, S32, S33, S34, S47, S49, S8). In 13 articles (23%), trust is presented not as a "cause" but as an "effect" of a technological solution. For instance, a solution is considered *trusted* if it exhibits some specific properties such as decentralization, transparency, traceability, data integrity, etc. (S1, S2, S28, S29, S30, S31, S40, S42, S43, S50, S51, S52, S56). The remaining studies (59%) refer to trust and trustworthiness without defining it explicitly. Our findings show little consensus in understanding trust and its social dimension in the blockchain community. This lack of theoretical foundation impacts the way the trust issues and the trustworthiness requirements are expressed in the studies.

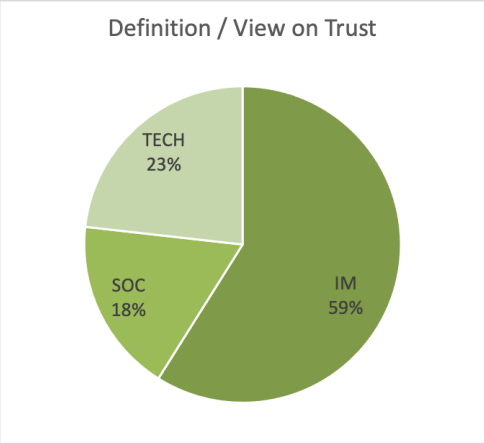


Figure. 4. Definition of trust in the primary studies: TECH – technology-centric view; SOC – social view; IM – no explicit definition of trust

4.3 What are the Trustworthiness Requirements Used by Primary Studies? (RQ3)

We extracted evidences referring to trustworthiness requirements from 56 articles and identified 21 requirements recurrently expressed in these studies – TwR. Text related to the same requirement from different sources was generalized and reformulated to comply with the ISO recommendations from [35]. In the requirement statements we use the terms "trustor" and "trustee" to identify the corresponding party in an interaction as defined in Section 2.1. The term "process" refers to an interaction between trustor

and trustee or to a service that trustee provides for trustor (depending on the context). The term "system" refers to a technological solution implementing, supporting or mediating the "process". We present the summary of requirements in Tables 5–7. Here RID – requirement identifier; Requirement – requirement name; Type of trust – indicates the type(s) of trust this requirement refers to (S – social, D – digital, TT – trust in technology); EA domain refers to the level of abstraction where requirement can be formulated (S – strategic, OP – operational, T – technical).

Trust issues often emerge in the social domain, are grounded on (subjective) beliefs of the organizational stakeholders and conditioned by culture, politics, personality etc. Whereas trustworthiness factors defined by social science (e.g., ability benevolence, integrity) are suitable to describe and reason about users' trust issues they are not providing enough details to guide technological solutions. Conversely, trustworthiness factors defined in technological domain (i.e., blockchain) provide a blueprint for technological solutions. Nevertheless, they are hard to trace back to the social context where the trust issues emerge on the first place and in which these solutions will be exploited. To bridge the gap between social and technological domains, we relate the extracted TwR to perceived trustworthiness factors defined by Mayer at al [2]: ability, benevolence and integrity.

Ability refers to a group of skills, competencies, and characteristics that enable a party to have influence within some specific domain [2]. We identified 7 trustworthiness requirements that refer to trustee's ability to fulfil a specific task or to ensure this task to be fulfilled in a specific way (Table 5). These requirements include:

Table 5. Trustworthiness requirements: Ability

RID	Requirement	Type of trust	EA domain	Articles
TwR1	Competence	S	OP, T	S17, S47, S49
TwR2	Automation	TT, D	OP, T, (S)	S21, S16, S19, S27, S28, S34, S55
TwR3	Decentralization	S, D, (TT)	S, OP, T	S3, S21, S12, S15, S18, S19, S20, S29, S32, S36, S48, S51, S53, S54, S55, S9, S23, S25
TwR4	Interoperability	S, D, TT	OP, T	S14, S15, S31, S36, S44, S46, S48, S55, S56
TwR5	Performance	S, TT	OP, T	S12, S18, S31, S32, S33, S34, S47, S49
5.1	*Efficiency/ Robustness*	TT, S, D	T, OP	S1, S21, S22, S12, S14, S15, S16, S17, S18, S19, S27, S28, S29, S31, S32, S33, S34, S47, S52, S55, S56, S8, S11
5.2	*Cost effect.*	TT	S, OP, T	S21, S14, S15, S16, S19, S27, S28, S8
TwR6	Resilience	S, TT, (D)	OP, T, (S)	S1, S6, S12, S17, S18, S27, S33
TwR7	Availability	S, TT, (D)	S, OP, T	S15, S16, S17, S18, S20, S32, S33, S49, S56, S17

TwR1 – Competence: Trustor must be able to assess trustee's ability/competence/skills/expertise to deliver a service or to perform a (part of) entrusted process with respect to some predefined level of quality. This requirement specifies relationships between social entities (individuals or organizations) and is related to social trust.

TwR2 – Automation of data processing: Trustee must minimize physical and maximize digital processing of data. Trustee fulfils this requirement by automating their processes and/or implementing dedicated services. This requirement is grounded on an assumption that the automated process reduces (human) errors, transaction time, transaction cost. This requirement determines technology acceptance and digital interactions in the examined studies; it is related to digital trust and trust in technology.

TwR3 – Decentralization: Control over process activities and data must not be delegated to a third party or to one specific party involved in the process itself. The system (trustee) has to support distributed coordination and control over transactions. This requirement is closely related to *Disintermediation*: trustor - trustee interaction must not rely on any intermediary for process coordination or control. This requirement is associated with social and digital trust in the literature. Only few studies mentioned decentralization in connection with technology acceptance or trust in technology.

TwR4 – Interoperability: Trustee must demonstrate a capability to work with trustor despite organizational, technological, cultural or other differences. This requirement is associated with all three types of trust in the studies. For digital trust and trust in technology, it can be expressed as follows: System (trustee) must be able to integrate without undue delay / work with various heterogeneous components (physical or technological). Various kinds of available data resources should be integrated.

TwR5 – Performance: While providing a service / executing an entrusted task, trustee (an organization, individual or a technological solution) must ensure an efficient distribution of resources, with respect of defined timeframe and budget. These resources may include physical, human, technological resources. In S47 performance is defined as a perception of an automated system's capability for supporting user's goals. While some sources associate performance with *efficiency and robustness* (related to social trust and trust in technology), other put forward *cost effectiveness* (related to trust in technology).

TwR6 – Resilience: Trustee has to guarantee the process execution in case of failure of one of components. Trustor must be able to recover the data and to transmit it into other system.

TwR7 – Availability: All resources (human, physical, hardware/software, information) needed for process/activity execution has to be available. This requirement has to be fulfilled by a trustee (an organization, an individual, or a mediating infrastructure). According to the literature, resilience and availability mostly determine social trust and trust in technology.

Benevolence is the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive [2]. We identified 7 trustworthiness requirements that refer to trustee's ability to guarantee (or to trustor's capacity to control) that trustee's actions will cause trustor no harm (Table 6).

Table 6. Trustworthiness requirements: Benevolence

RID	Requirement	Type of trust	EA domain	Articles
TwR8	Authentication (entity)	D, S, (TT)	S, OP, T	S1, S4, S21, S22, S17, S31, S35, S36, S37, S44, S45, S47, S48, S9, S10, S23, S25
TwR9	Authentication (data)	D, S, (TT)	S, OP, T	S1, S21, S22, S30, S31, S35, S36, S47
TwR10	Confidentiality	S, D, TT	S, OP, T	S6, S18, S19, S20, S27, S33, S38, S43, S44, S46, S47, S49
TwR11	Authorization	D (S, TT)	S, OP, T	S1, S4, S15, S17, S47
TwR12	Accountability	S, D	S, OP, T	S1, S17, S43, S47, S11
TwR13	Privacy	S, D, (TT)	S, OP, T	S1, S7, S12, S17, S26, S27, S36, S44, S49, S52, S54, S9, S10
TwR14	Usability	S, TT	S, OP, T	S12, S47, S14

TwR8 – Authentication (entity): Trustor must be able to verify the identity of trustee.

TwR9 – Authentication (data): Trustor must be able to determine the correctness and reliability of reported data (e.g., messages, events). This requirement is also referred to as data authenticity, data accuracy, data reliability in the studies. Both data and entity authentication are mainly associated with digital trust.

TwR10 – Confidentiality: Trustor's sensitive information (including identity) must not be disclosed to unauthorized parties; the executed activity is only visible to authorized resources/entities. This requirement is associated with all types of trust in the literature.

TwR11 – Authorization: Trustor must be able to determine whether trustee has the appropriate permissions (i.e., is authorized) to perform a specific action or access a specific resource. This requirement is mainly associated with digital trust and is related to TwR12.

TwR12 – Accountability: Trustee is held responsible for her actions and cannot deny them. In case of malicious activity/information, an authorized authority has to ensure accountability by tracing the identity of a source of malicious activity/information.

TwR13 – Privacy: Trustor's identity information must not be disclosed. Trustor must have the power to make decisions concerning collection, use and disclosure of personal information by trustee. This requirement is associated with social and digital trust.

TwR14 – Usability: The system (trustee) must be intuitive, easy to use, requiring minimum specific training or skills from trustor. The system must be adapted for specific needs (e.g., age, handicap). This requirement determines trust in technology and associated with acceptance/adoption.

Integrity is the moral quality of being sincere, honest, and consistent in one's behavior; capacity and willingness to adhere to some rules/principles [2]. Table 7 presents requirements that refer to trustee's ability to guarantee (or to trustor's capacity to control) that trustee's actions comply with predefined rules, norms or agreements.

Table 7. Trustworthiness requirements: Integrity

RID	Requirement	Type of trust	EA domain	Articles
TwR15	Integrity (process)	S, D, TT	(S), OP, T	S5, S18, S20, S27, S32, S33, S39, S40, S45, S47, S48, S49, S53
TwR16	Integrity (data)	D, S, (TT)	T, OP, (S)	S1, S6, S21, S15, S16, S17, S19, S28, S29, S30, S39, S40, S45, S47, S48, S50, S52, S54, S56, S8, S24, S25
TwR17	Non-repudiation	D, S	OP, T	S1, S4, S15, S16, S20, S28, S32, S33
TwR18	Compliance	S, D, TT	S, OP, (T)	S22, S14, S17, S18, S26, S27, S40, S42, S8, S17
TwR19	Auditability	S, D, (TT)	S, OP, T	S3, S4, S21, S22, S13, S16, S18, S27, S28, S40, S42, S46
TwR20	Transparency	S, D, TT	S, OP, T	S2, S3, S22, S14, S15, S16, S17, S18, S19, S28, S32, S33, S40, S42, S43, S46, S47, S53, S55, S8, S9, S11, S17
TwR21	Traceability	D, S, (TT)	OP, T, (S)	S21, S22, S12, S14, S16, S28, S38, S53, S8, S11, S25

TwR15 – Integrity (process): Trustee must ensure correct and timely execution of activities, with respect of contract agreements or process specifications. This requirement is associated with all three types of trust: it can determine trustworthiness of both social and digital interactions as well as trust into technology (an IT object).

TwR16 – Integrity (data): Trustee must ensure the overall accuracy, completeness, and consistency of data over its entire life-cycle. This includes data protection from unauthorized modification or alteration.

TwR17 – Non-repudiation: Trustee must ensure that any activity, once performed, cannot be denied. All the information artefacts should be written in a permanent, tamper-proof way. TwR16–17 are primarily associated with digital trust.

TwR18 – Compliance: Trustee has to act according to predefined rules, agreements or regulations (e.g., GDPR for data protection). Primarily associated with social trust, this requirement also determines digital trust and trust in technology. It is related to auditability, transparency and traceability requirements.

TwR19 – Auditability: Trustor must be able to validate the trustee's compliance with predefined rules (e.g., by executing the audit, by examining the execution traces, by supervising the trustee's process at run time etc.).

TwR20 – Transparency: Trustee's process (e.g., workflow) must be transparent and explicitly documented. Trustee must provide an accessible and non-repudiable audit trail showing use, change and viewing of the data.

TwR21 – Traceability: Trustor has to access any or all information related to provenance of a physical or information object accurately and trace it upward (to its source). This requirement is mainly associated with digital trust.

4.4 What Types of Trust are Addressed by the Identified Requirements? (RQ4)

In Table 5–7, each TwR is associated with one or several types of trust. Using Table 1, these requirements can be re-formulated for the relevant type of trust, by replacing "trustor" and "trustee" qualifiers by the corresponding types of entities involved in an interaction (e.g., individual, organization, IT object). For instance, in social trust, the compliance requirement (TwR18) can be expressed as follows: A company *(= trustee)* must obtain explicit consent from individuals *(= trustor)* before collecting or processing their data. For trust in technology: An information system *(= trustee)* must provide the means for users *(= trustor)* to express their consent and must not collect and/or use their personal data without their explicit consent. For digital trust: A blockchain-based system *(= trustee)* has to ensure that no personal data is collected and/or used by the network from the connected individuals or devices *(= trustor)* without their explicit consent.

Our analysis shows that, in spite of growing importance of digital trust, social trust and trust to technology remain important drivers in organizational decision making. The TwR identified in this study not only drive the design and development of trust-enabling technological solutions but also determine relationships between individuals and organizations. They reflect the needs for all three types of trust in organizations.

4.5 At What Abstraction Levels the Trustworthiness Requirements are Defined? (RQ5)

Trust concerns can be expressed by stakeholders at different abstraction levels, characterized by their scope (e.g., organization, activity, application) and/or vocabulary used. In this study, we map the identified TwR onto three abstraction levels consistent with the discipline of enterprise architecture [100], [101]: strategic, operational and IT level. To support the solution design, each trust concern should be addressed by TwR formulated at adequate abstraction level.

The strategic level addresses the organizational vision and strategic objectives. For instance, for the trust issue from (S22): *"In the gem industry, provenance of origin is critically important for environmental, social, and regulatory reasons."* the corresponding traceability requirement (TwR21) will be formulated as follows: Buyer *(= trustor)* has to access any or all information related to provenance of a gemstone accurately and trace it upward (to its source).

The operational level defines how these strategic objectives are to be met through the business processes and operations. Consider the following issue from (S28): *"the title registry is vulnerable to modification, essentially, the title records could be manipulated by malicious parties".* The corresponding integrity requirement (TwR16) will be formulated as follows: The title registry provider (= *trustee*) must ensure the overall accuracy, completeness, and consistency of data over its entire life-cycle. This includes data protection from unauthorized modification or alteration.

The technological level focuses on the IT resources necessary for the digitalization of these operations and processes. Examples of TwR expressed at technical abstraction level include: *"architectures must also guarantee the integrity and the confidentiality of data while remaining resilient to distributed attacks."*(S6); *"citizens should not have privacy concerns about the information systems. These trust issues and privacy concerns can be solved by using decentralized identity and zero-knowledge proof-based mechanisms."* (S12).

5 Discussion

Figure 5 summarizes the scope and the contributions of this work and presents the directions of the future research. The selected 56 primary studies constitute the input for this work (I).

First, we provided a descriptive overview of the collected primary studies and analyzed the nature of their research contributions (C1). Our analysis shows that 86% of the examined research is grounded on empirical data and contributes to the domain with new evidences and proposals.

Models, frameworks, and new concepts are developed in 48% of the examined publications. Working prototypes are presented in 46% while methods and approaches for design are addressed by 23% of studies. This encourages further research on new design approaches based on explicit analysis of TwR.

During our data extraction, we focused on the trust issues and trust-related requirements expressed in these primary studies. Following the ISO guidelines, we formulated a set of 21 TwR consistent with the related works (C2). While originated from blockchain literature, the TwR are formulated in a technology-neutral language and do not advocate blockchain or any other specific technological solution.

To bridge the gap between social and technological domains, we associated the identified TwR with the three trustworthiness factors defined in the social science: ability, benevolence and integrity (C3).

Our literature analysis shown that trust issues can be expressed by stakeholders at different organizational levels, varying in scope and technical details. We discussed how TwR can be mapped on three abstraction levels consistent with enterprise architecture (strategic, operational and IT) (C4).

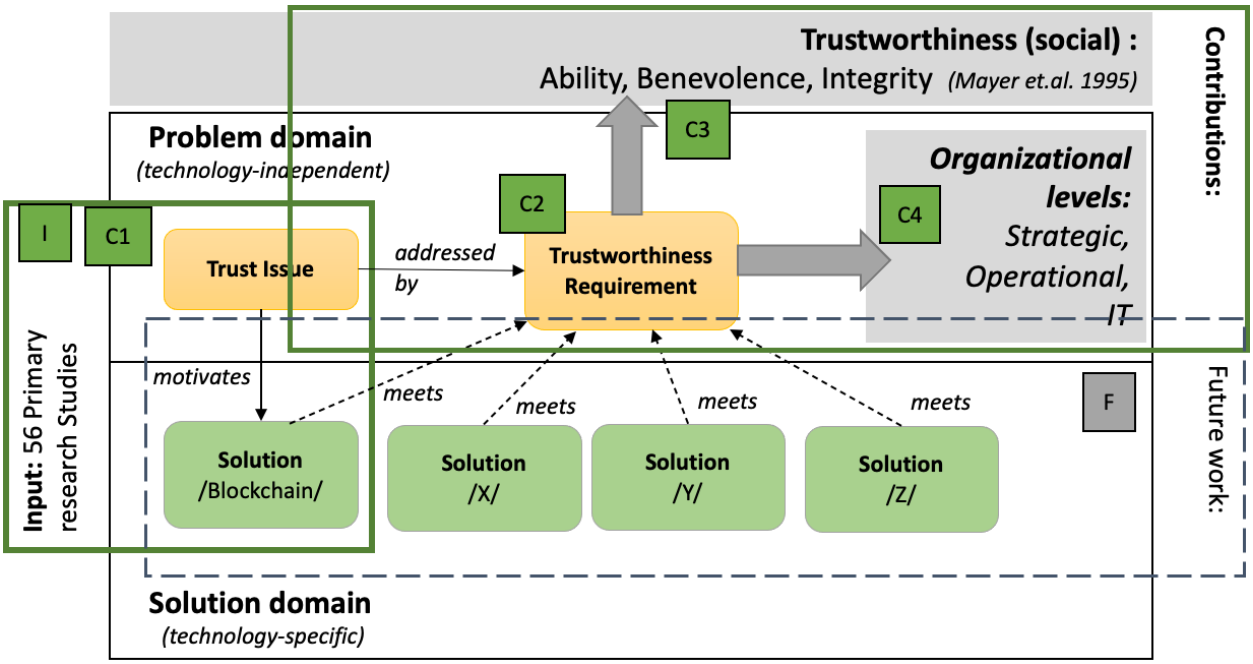


Figure 5. Overview of the contributions and the future work

While being strongly presented in the literature, digital trust is not the only form of trust that the organizations seek to reenforce: trust in technology and social trust remain powerful drivers in decision making. Specified in the problem domain and technology-neutral, trustworthiness requirements presented in this work are not bound to blockchain technological solutions and can be used to drive alternative design decisions and technological choices. We plan to elaborate on this topic in the future (F).

5.1 Trust as a Value vs. Trust as a Requirement

To enhance the trustworthiness of systems, a significant investment is needed in the requirements, architecture, design, and development of systems, alongside a fundamental shift in organizational culture [102]. The degree of trustworthiness achievable in complex systems today depends on our ability to integrate both social and technical perspectives of trust.

An important number of articles examined in this study addresses trust from the solution provider perspective (some examples include [11], [16], [71], [72], [77], [80], [91]): here trust is

considered as *a value* created for an end-user by a given technological solution (e.g., blockchain-based system), whereas the user's *need for trust* or trust concerns are taken for granted and rarely elicited. As a result, many research studies report on technology acceptance issues [11], [70], [71], [77].

To ensure better fit between trust-enabling solutions and organizational needs, deeper understanding of trust concerns and explicit analysis of TwR is needed. The advantage of system design based on explicit TwR is twofold:

1. For organizations and end-users: Translating subjective (and often implicit) *trust issues* into and explicit *trustworthiness requirements*, an organization develops better visibility and understanding of potential threats, risks and priorities. It can clearly express its needs and ensure better strategic alignment of its prospective (trust-enabling) solutions.
2. For solution providers: Shifting from *design of value-creating features* to *meeting specific trustworthiness requirements*, technology providers and solution developers can ensure better acceptance for their (trust-enabling) solutions.

5.2 Threats to Validity and Directions for the Future Work

This study follows a systematic literature review approach [20] to ensure accuracy and eliminate bias, nevertheless the following limitations can be listed:

This study examines primary research focused on design of blockchain-based solutions. This threatens completeness of our presented requirements taxonomy. More general analysis of trust issues can bring new insights and extend this taxonomy.

This SLR reveals very little agreement on trust definition in blockchain community. Whereas both social and technology-centric definitions of trust are in use, the majority of studies do not provide an explicit definition of trust. This discrepancy in trust definition represented a challenge during data extraction, analysis and coding. The authors often had to rely on their experience and interpretation, what presents a threat to the internal validity of this study.

Among identified TwR, confidentiality, integrity, availability, authentication and non-repudiation are properties commonly associated with information security. Detailed analysis of relation between trustworthiness and security and between security and trust will be addressed in our future work.

This study presents our preliminary findings on how TwR can be expressed at different abstraction levels (strategic, operational, IT). In our future work we plan to elaborate on this important topic by formalizing TwR for different enterprise architecture levels.

This work presents a list of generic TwR. Healthcare, supply chain management, banking, IoT are examples of domains addressed by the articles analyzed in this study. Domain-specific taxonomies of trust issues and their corresponding TwR may be of particular interest for practitioners from these domains. The work presented in [103] addresses TwR in supply chain management. Other domains need to be addressed by researchers in the future.

6 Conclusion

In this work, we followed the SLR guidelines defined by Kitchenham et al [20] and reviewed 56 primary research studies in ISE and blockchain that focus on trust conceptualization, trustworthy system design and development. We analyzed the trust issues presented in the literature and formulated a set of 21 TwR following the ISO guidelines. Our goal is to provide support for business and technical experts who seek to identify and articulate the scope of a problem related to trust, and to lay out the arguments that will guide design decisions and technical choices.

Generalizability and completeness of the defined set of TwR is out of the scope for this study and will be addressed in the future.

References

[1] D. Gambetta, "Can we trust?," *Trust Mak. Break. coopeative relations*, vol. 13, pp. 213–237, 1990. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.5695&rep=rep1&type=pdf%5Cnhttp://www.loa.istc.cnr.it/mostro/files/gambetta-conclusion_on_trust.pdf

[2] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model Of Organizational Trust," *Acad. Manag. Rev.*, vol. 20, no. 3, pp. 709–734, 1995. Available: https://doi.org/10.5465/amr.1995.9508080335

[3] A. Sutcliffe, "Trust: From cognition to conceptual models and design," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 4001 LNCS, pp. 3–17. Available: https://doi.org/10.1007/11767138_1

[4] I. S. Iso/iec, "Information Technology – Security Techniques – Information Security Management Systems, Standard ISO/IEC TR 27000," vol. 2018.

[5] P. Pietrzak and J. Takala, "Digital trust – a systematic literature review," *Forum Sci. OeconomiaSep*, vol. 9, no. 3, p. 30, 2021.

[6] D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," *ACM Trans. Manag. Inf. Syst.*, vol. 2, no. 2, 2011. Available: https://doi.org/10.1145/1985347.1985353

[7] S. M. Meeßen, M. T. Thielsch, and G. Hertel, "Trust in Management Information Systems (MIS): A Theoretical Model," *Zeitschrift fur Arbeits- und Organ.*, vol. 64, no. 1, pp. 6–16, 2020. Available: https://doi.org/10.1026/0932-4089/a000306

[8] P. De Filippi, M. Mannan, and W. Reijers, "Blockchain as a confidence machine: The problem of trust & challenges of governance," *Technol. Soc.*, vol. 62, p. 10128, 2020. Available: https://doi.org/10.1016/j.techsoc.2020.101284

[9] M. Alshamsi, M. Al-Emran, and K. Shaalan, "A Systematic Review on Blockchain Adoption," *Appl. Sci.*, vol. 12, no. 9, p. 9, 2022. Available: https://doi.org/10.3390/app12094245

[10] P. Durneva, K. Cousins, and M. Chen, "The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review," in *Journal of Medical Internet Research*, vol. 22, no. 7, e18619: Med. Internet Res. 22, 2020. Available: https://doi.org/10.2196/18619

[11] T. Saheb and F. H. Mamaghani, "Exploring the barriers and organizational values of blockchain adoption in the banking industry," *J. High Technol. Manag. Res.*, vol. 32, no. 2, p. 100417, 2021. Available: https://doi.org/10.1016/j.hitech.2021.100417

[12] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Comput. Sci.*, vol. 123, pp. 116–121, 2018. Available: https://doi.org/10.1016/j.procs.2018.01.019

[13] M. Swan, *Blockchain: Blueprint for a New Economy. Gravenstein Highway North*. Inc: O'Reilly Media, 2015.

[14] D. D. H. Shin, "Blockchain: The emerging technology of digital trust," *Telemat. Informatics*, vol. 45, p. 101278, 2019. Available: https://doi.org/10.1016/j.tele.2019.101278

[15] K. D. Werbach, "Trust, But Verify: Why the Blockchain Needs the Law," *Ssrn*, vol. 33, no. 2, pp. 487–550, 2016. Available: https://doi.org/10.2139/ssrn.2844409

[16] A. Kaushik, "New technology interventions including blockchain technology in land record and registry management in India," *ACM Int. Conf. Proceeding Ser.*, pp. 143–151, 2020. Available: https://doi.org/10.1145/3428502.3428521

[17] Z. Chen, A. Xu, H. Wen, Y. Zhang, and X. Xu, "Aviation Terminal Data Security Architecture Based on Blockchain," *J. Phys. Conf. Ser.*, vol. 1575, no. 1, 2020. Available: https://doi.org/10.1088/1742-6596/1575/1/012062

[18] P. Ruotsalainen and B. Blobel, "Health information systems in the digital health ecosystem—problems and solutions for ethics, trust and privacy," *Int. J. Environ. Res. Public Health*, vol. 17, no. 9, 2020. Available: https://doi.org/10.3390/ijerph17093006

[19] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A Vademecum on Blockchain Technologies: When, Which, and How," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019. Available: https://doi.org/10.1109/COMST.2019.2928178

[20] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," EBSE 2007-01, Technical Report, 2007.

[21] L. G. Zucker, “Production of trust: Institutional sources of economic structure, 1840-1920,” in *Research in Organizational Behavior*, vol. 8, JAI Press, 1986, pp. 53–111.

[22] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not so different after all: A cross-discipline view of trust,” *Acad. Manag. Rev.*, vol. 23, no. 3, pp. 393–404, 1998. Available: https://doi.org/10.5465/amr.1998.926617

[23] A. Giddens, *The consequences of modernity*, vol. 28, no. 3. 1990.

[24] A. Beldad, M. De Jong, and M. Steehouder, “How shall i trust the faceless and the intangible? A literature review on the antecedents of online trust,” *Comput. Human Behav.*, vol. 26, no. 5, pp. 857–869, 2010. Available: https://doi.org/10.1016/j.chb.2010.03.013

[25] P. S. T. Sumpf, *System Trust. Researching the Architecture of Trust in Systems*, Springer, Berlin, Heidelberg, 2019. Available: https://doi.org/10.1007/978-3-658-25628-9

[26] J. H. Cho, K. Chan, and S. Adali, “A Survey on Trust Modeling,” *ACM Comput. Surv.*, vol. 48, no. 2, p. 2, 2015. Available: https://doi.org/10.1145/2815595

[27] D. J. Kim, D. L. Ferrin, and H. R. Rao, “A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents,” *Decis. Support Syst.*, vol. 44, no. 2, pp. 544–564, 2008. Available: https://doi.org/10.1016/j.dss.2007.07.001

[28] P. A. Pavlou, “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model,” *Int. J. Electron. Commer.*, vol. 7, no. 3, pp. 101–134, 2003. Available: https://doi.org/10.1080/10864415.2003.11044275

[29] J. C. B. R P, K. Singi, V. Kaulgud, K. K. Phokela, and S. Podder, “Framework for Trustworthy Software Development,” in *2019 34th IEEE/ACM International Conference on Automated Software Engineering Workshop (ASEW)*, Nov. 2019, pp. 45–48. Available: https://doi.org/10.1109/ASEW.2019.00027

[30] J. V. Chen, D. C. Yen, and T. M. Rajkumar, “The determinants of cloud computing adoption behavior: Implications for information technology investment decisions,” *Int. J. Account. Inf. Syst.*, vol. 13, no. 1, pp. 1–17, 2012.

[31] T. Zhou, Y. Lu, and B. Wang, “Integrating TTF and UTAUT to explain mobile banking user adoption,” *Comput. Human Behav.*, vol. 26, no. 4, pp. 760–767, 2010. Available: https://doi.org/10.1016/j.chb.2010.01.013

[32] J. Mattila and T. Seppälä, “Digital Trust, Platforms, and Policy,” *ETLA Br., Res. Inst. Finnish Econ.*, vol. 7, p. 42, 2016. Available: https://doi.org/10.13140/RG.2.1.1565.1928

[33] P. Neumann, “Principled Assuredly Trustworthy Composable Architectures, CDRL A001 Final Report, SRI International, Menlo Park, CA, December 28,” vol. 2004.

[34] ISO/IEC, “ISO/IEC 25010:2011 – Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models,” vol. 2017, 2011.

[35] ISO/IEC 12207:2008, “Systems and software engineering – Software life cycle processes,” *Int. Stand. ISO/IEC 12207*, vol. 8, p. 138, 2008.

[36] A. Sutcliffe, P. Sawyer, and N. Bencomo, “The Implications of ‘Soft’ Requirements,” in *2022 IEEE 30th International Requirements Engineering Conference (RE)*, Aug. 2022, pp. 178–188. Available: https://doi.org/10.1109/RE54965.2022.00022

[37] N. G. Mohammadi, *Trustworthy cyber-physical systems: A systematic framework towards design and evaluation of trust and trustworthiness*. Wiesbaden: Springer Fachmedien Wiesbaden, 2019. Available: https://doi.org/10.1007/978-3-658-27488-7

[38] F. Glaser, “Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2017-Janua, pp. 1543–1552, 2017. Available: https://doi.org/10.24251/HICSS.2017.186

[39] Y. Wang, J. H. Han, and P. Beynon-Davies, “Understanding blockchain technology for future supply chains: a systematic literature review and research agenda,” *Supply Chain Manag.*, vol. 24, no. 1, pp. 62–84, 2019. Available: https://doi.org/10.1108/SCM-03-2018-0148

[40] M. Brookbanks and G. Parry, “The impact of a blockchain platform on trust in established relationships: a case study of wine supply chains,” *Supply Chain Manag.*, vol. 27, no. 7, pp. 128–146, Dec. 2022. Available: https://doi.org/10.1108/SCM-05-2021-0227

[41] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, “Blockchain for

business applications: A systematic literature review," in *Lecture Notes in Business Information Processing*, vol. 320, 2018, pp. 384–399. Available: https://doi.org/10.1007/978-3-319-93931-5_28

[42] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Informatics*, vol. 36, no. 36, pp. 55–81, 2019. Available: https://doi.org/10.1016/j.tele.2018.11.006

[43] G. Caldarelli and J. Ellul, "Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review," *Appl. Sci.*, vol. 11, no. 4, p. 1842, Feb. 2021. Available: https://doi.org/10.3390/app11041842

[44] B. Alamri, K. Crowley, and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," *IEEE Access*, vol. 10, pp. 59612–59629, 2022. Available: https://doi.org/10.1109/ACCESS.2022.3180367

[45] O. Ali, M. Ally, Clutterbuck, and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: A systematic literature review," *Int. J. Inf. Manage.*, vol. 54, 2020. Available: https://doi.org/10.1016/j.ijinfomgt.2020.102199

[46] B. Teisserenc and S. Sepasgozar, "Project data categorization, adoption factors, and non-functional requirements for blockchain based digital twins in the construction industry 4.0," *Buildings*, vol. 11, no. 12, p. 12, 2021. Available: https://doi.org/10.3390/buildings11120626

[47] F. Hawlitschek, B. Notheisen, and T. Teubner, "A 2020 perspective on 'The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,'" *Electron. Commer. Res. Appl.*, vol. 40, pp. 50–63, 2020. Available: https://doi.org/10.1016/j.elerap.2020.100935

[48] H. Johng, D. Kim, G. Park, J. E. Hong, T. Hill, and L. Chung, "Enhancing business processes with trustworthiness using blockchain: A goal-oriented approach," *Proc. ACM Symp. Appl. Comput.*, pp. 61–68, 2020. Available: https://doi.org/10.1145/3341105.3374022

[49] M. J. Page *et al.*, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *Med. Flum.*, vol. 57, no. 4, pp. 444–465, 2021. Available: https://doi.org/10.21860/medflum2021_264903

[50] N. Nousias, G. Tsakalidis, G. Michoulis, S. Petridou, and K. Vergidis, "A process-aware approach for blockchain-based verification of academic qualifications," *Simul. Model. Pract. Theory*, vol. 121, p. 10264, 2022. Available: https://doi.org/10.1016/j.simpat.2022.102642

[51] E. Marangone, C. Di Ciccio, and I. Weber, "Fine-Grained Data Access Control for Collaborative Process Execution on Blockchain," in *Lecture Notes in Business Information Processing*, vol. 459 LNBIP, 2022, pp. 51–67. Available: https://doi.org/10.1007/978-3-031-16168-1_4

[52] F. Parahyba *et al.*, "On the Need to Use Smart Contracts in Enterprise Application Integration," in *CIbSE 2022 - XXV Ibero-American Conference on Software Engineering*, pp. 203–217, 2022. Available: https://doi.org/10.5753/cibse.2022.20973

[53] O. Debauche *et al.*, "RAMi: A New Real-Time Internet of Medical Things Architecture for Elderly Patient Monitoring," *Inf.*, vol. 13, no. 9, p. 423, 2022. Available: https://doi.org/10.3390/info13090423

[54] Y. Liu, Z. Zhou, Y. Yang, and Y. Ma, "Verifying the Smart Contracts of the Port Supply Chain System Based on Probabilistic Model Checking," *Systems*, vol. 10, no. 1, p. 19, 2022. Available: https://doi.org/10.3390/systems10010019

[55] C. Killer, B. Rodrigues, E. J. Scheid, M. F. Franco, and B. Stiller, "Blockchain-Based Voting Considered Harmful?" *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 3603–3618, 2022. Available: https://doi.org/10.1109/TNSM.2022.3181028

[56] J. Ye, X. Kang, Y. C. Liang, and S. Sun, "A Trust-Centric Privacy-Preserving Blockchain for Dynamic Spectrum Management in IoT Networks," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13263–13278, 2022. Available: https://doi.org/10.1109/JIOT.2022.3142989

[57] C. Liu *et al.*, "Extending On-Chain Trust to Off-Chain - Trustworthy Blockchain Data Collection Using Trusted Execution Environment (TEE)," *IEEE Trans. Comput.*, vol. 71, no. 12, pp. 3268–3280, 2022. Available: https://doi.org/10.1109/TC.2022.3148379

[58] E. Karaarslan and D. Aydın, "An artificial intelligence-based decision support and resource management system for COVID-19 pandemic," in *Data Science for COVID-19 Volume 1: Computational Perspectives*, 2021, pp. 25–49. Available: https://doi.org/10.1016/B978-0-12-824536-1.00029-0

[59] I. El Kassmi and Z. Jarir, "Blockchain-oriented Inter-organizational Collaboration between Healthcare Providers to Handle the COVID-19 Process," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 12, pp. 762–780, 2021. Available: https://doi.org/10.14569/IJACSA.2021.0121294

[60] J. Xiao, Y. Jiao, Y. Li, and Z. Jiang, “Towards a trusted and unified consortium-blockchain-based data sharing infrastructure for open learning—tolfob architecture and implementation,” *Sustain.*, vol. 13, no. 24, p. 14069, 2021. Available: https://doi.org/10.3390/su132414069

[61] R. G. Shukla, A. Agarwal, and V. Shekhar, “Leveraging Blockchain Technology for Indian Healthcare system: An assessment using value-focused thinking approach,” *J. High Technol. Manag. Res.*, vol. 32, no. 2, p. 100415, 2021. Available: https://doi.org/10.1016/j.hitech.2021.100415

[62] A. Hasselgren, J. A. H. Rensaa, K. Kralevska, D. Gligoroski, and A. Faxvaag, “Blockchain for increased trust in virtual health care: Proof-of-concept study,” *J. Med. Internet Res.*, vol. 23, no. 7, 2021. Available: https://doi.org/10.2196/28496

[63] M. Müller, N. Ostern, S. R. Garzon, and A. Küpper, “Engineering Trust-Aware Decentralized Applications with Distributed Ledgers,” in *Trust Models for Next-Generation Blockchain Ecosystems. EAI/Springer Innovations in Communication and Computing*, 2021, pp. 1–35. Available: https://doi.org/10.1007/978-3-030-75107-4_1

[64] D. Ivanov and P. Pashkov, “A blockchain-based approach to providing technically expressed trust in the supply chains of the fashion industry,” *J. Phys. Conf. Ser.*, vol. 2032, no. 1, 2021. Available: https://doi.org/10.1088/1742-6596/2032/1/012086

[65] M. Muller, N. Ostern, D. Koljada, K. Grunert, M. Rosemann, and A. Kupper, “Trust Mining: Analyzing Trust in Collaborative Business Processes,” *IEEE Access*, vol. 9, pp. 65044–65065, 2021. Available: https://doi.org/10.1109/ACCESS.2021.3075568

[66] M. S. Al-Rakhami and M. Al-Mashari, “A blockchain-based trust model for the internet of things supply chain management,” *Sensors*, vol. 21, no. 5, pp. 1–15, 2021. Available: https://doi.org/10.3390/s21051759

[67] A. Albizri and D. Appelbaum, “Trust but verify: The oracle paradox of blockchain smart contracts,” *J. Inf. Syst.*, vol. 35, no. 2, pp. 1–16, 2021. Available: https://doi.org/10.2308/ISYS-19-024

[68] A. Sarker, S. Byun, W. Fan, and S.-Y. Chang, “Blockchain-based root of trust management in security credential management system for vehicular communications,” in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, Mar. 2021, pp. 223–231. Available: https://doi.org/10.1145/3412841.3441905

[69] G. Wang and M. Nixon, “InterTrust: Towards an Efficient Blockchain Interoperability Architecture with Trusted Services,” in *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*, 2021, pp. 150–159. Available: https://doi.org/10.1109/Blockchain53845.2021.00029

[70] S. Suhail, R. Hussain, R. Jurdak, and C. S. Hong, “Trustworthy Digital Twins in the Industrial Internet of Things With Blockchain,” *IEEE Internet Comput.*, vol. 26, no. 3, pp. 58–67, 2022. Available: https://doi.org/10.1109/MIC.2021.3059320

[71] J. Holbrook, “Architecting Your Enterprise Blockchain,” in *Architecting Enterprise Blockchain Solutions*, Wiley, 2020, pp. 69–115. Available: https://doi.org/10.1002/9781119557722.ch3

[72] X. Qing, L. Feng, and X. Zilong, “Research and Design of the Mutual Aid Tokenized Economy Structure Based on Blockchain Technology: Taking Time Bank as an Example,” *ACM Int. Conf. Proceeding Ser.*, pp. 158–162, 2020. Available: https://doi.org/10.1145/3397056.3397086

[73] B. M. Nguyen, T. C. Dao, and B. L. Do, “Towards a blockchain-based certificate authentication system in Vietnam,” *PeerJ Comput. Sci.*, vol. 2020, no. 3, 2020. Available: https://doi.org/10.7717/peerj-cs.266

[74] H. Sateesh and P. Zavarsky, “State-of-The-Art VANET Trust Models: Challenges and Recommendations,” *11th Annu. IEEE Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2020*, pp. 757–764, 2020. Available: https://doi.org/10.1109/IEMCON51383.2020.9284953

[75] M. Müller et al., “Silver Bullet for All Trust Issues? Blockchain-Based Trust Patterns for Collaborative Business Processes,” in *Business Process Management: Blockchain and Robotic Process Automation Forum. BPM 2020. Lecture Notes in Business Information Processing.* Springer, vol. 393, 2020, pp. 3–18. Available: https://doi.org/10.1007/978-3-030-58779-6_1

[76] M. Müller, S. R. Garzon, M. Rosemann, and A. Kupper, “Towards Trust-Aware Collaborative Business Processes: An Approach to Identify Uncertainty,” *IEEE Internet Comput.*, vol. 24, no. 6, pp. 17–25, 2020. Available: https://doi.org/10.1109/MIC.2020.3023180

[77] N. Gaur, “Blockchain challenges in adoption,” *Manag. Financ.*, vol. 46, no. 6, pp. 849–858, 2020. Available: https://doi.org/10.1108/MF-07-2019-0328

[78] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, “Design of a Secure Medical Data Sharing Scheme Based

on Blockchain," in *Journal of Medical Systems*, vol. 44, article 52, 2020. Available: https://doi.org/10.1007/s10916-019-1468-1

[79] K. Osei-Tutu, S. Hasavari, and Y. T. Song, "Blockchain-based Enterprise Architecture for Comprehensive Healthcare Information Exchange (HIE) Data Management," in *Proceedings – 2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020*, 2020, pp. 767–775. Available: https://doi.org/10.1109/CSCI51800.2020.00145

[80] P. H. Alves *et al.*, "Exploring blockchain technology to improve multi-party relationship in business process management systems," in *ICEIS 2020 – Proceedings of the 22nd International Conference on Enterprise Information Systems*, 2020, vol. 2, pp. 817–825. Available: https://doi.org/10.5220/0009565108170825

[81] K. GUPTA and A. SAM, "Blockchain in Operations Management," *Int. J. Sci. Res. Publ.*, vol. 9, no. 11, p. p9551, 2019. Available: https://doi.org/10.29322/IJSRP.9.11.2019.p9551

[82] D. E. Marcial and M. . Launer, "Towards the measurement of Digital Trust in the workplace: A proposed framework," *International Journal of Scientific Engineering and Science*, vol. 3, no. 12, pp. 1–7, 2019. Available: https://doi.org/10.5281/ZENODO.3595295

[83] G. Dong, J. Bai, Y. Chen, P. Zhang, J. Fan, and F. Li, "Anonymous cross-domain authentication scheme for medical PKI system," *ACM TURC'19: Proceedings of the ACM Turing Celebration Conference*, pp. 1–7, 2019. Available: https://doi.org/10.1145/3321408.3321574

[84] D. Seftyanto, A. Amiruddin, and A. R. Hakim, "Design of blockchain-based electronic election system using hyperledger: Case of indonesia," in *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2019*, 2019, pp. 228–233. Available: https://doi.org/10.1109/ICITISEE48480.2019.9003768

[85] D. Parry, "From fax to blockchain: Sharing health information democratically and safely," *Stud. Health Technol. Inform.*, vol. 264, pp. 1747–1748, 2019. Available: https://doi.org/10.3233/SHTI190628

[86] M. Harlamova and M. Kirikova, "Towards the trust handling framework for industry 4.0," *Frontiers in Artificial Intelligence and Applications*, vol. 315, pp. 49–64, 2019. Available: https://doi.org/10.3233/978-1-61499-941-6-49

[87] M. Autili, F. Gallo, P. Inverardi, C. Pompilio, and M. Tivoli, "Introducing trust in service-oriented distributed systems through blockchain," *Proc. – 2019 IEEE 30th Int. Symp. Softw. Reliab. Eng. Work. ISSREW 2019*, pp. 149–154, 2019. Available: https://doi.org/10.1109/ISSREW.2019.00065

[88] M. Rosemann, "Trust-Aware Process Design," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11675 LNCS, pp. 305–321. Available: https://doi.org/10.1007/978-3-030-26619-6_20

[89] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen, and H. J. Kim, "Blockchain-based trusted electronic records preservation in cloud storage," *Comput. Mater. Contin.*, vol. 58, no. 1, pp. 135–151, 2019. Available: https://doi.org/10.32604/cmc.2019.02967

[90] J. Mendling *et al.*, "Blockchains for business process management – Challenges and opportunities," *ACM Trans. Manag. Inf. Syst.*, vol. 9, no. 1, 2018. Available: https://doi.org/10.1145/3183367

[91] X. Wang, Q. Hu, Y. Zhang, G. Zhang, W. Juan, and C. Xing, "A Kind of Decision Model Research Based on Big Data and Blockchain in eHealth," in *Web Information Systems and Applications. WISA 2018. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11242 LNCS, 2018, pp. 300–306. Available: https://doi.org/10.1007/978-3-030-02934-0_28

[92] T. Kampik, A. Najjar, and D. Calvaresi, "MAS-Aided Approval for Bypassing Decentralized Processes: An Architecture," in *Proceedings - 2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2018*, 2019, pp. 713–718. Available: https://doi.org/10.1109/WI.2018.000-6

[93] B. Nasrulin, M. Muzammal, and Q. Qu, "A Robust Spatio-Temporal Verification Protocol for Blockchain," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11233 LNCS, pp. 52–67, 2018. Available: https://doi.org/10.1007/978-3-030-02922-7_4

[94] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, "Blockchain-based business process management (BPM) framework for service composition in industry 4.0," *J. Intell. Manuf.*, vol. 31, no. 7, pp. 1737–1748, 2020. Available: https://doi.org/10.1007/s10845-018-1422-y

[95] A. B. Tran, X. Xu, I. Weber, M. Staples, and P. Rimba, "Regerator: a Registry Generator for Blockchain," *CAiSE-Forum-DC 2017*, pp. 81–88.

[96] W. Ahmed, W. Di, and D. Mukathe, “Privacy-preserving blockchain-based authentication and trust management in VANETs,” 2022. Available: https://doi.org/10.1049/ntw2.12036

[97] P. Ruotsalainen and B. Blobel, “Privacy and Trust in pHealth - Past, Present and Future,” *Stud. Health Technol. Inform.*, vol. 299, pp. 104–117, 2022. Available: https://doi.org/10.3233/SHTI220968

[98] J. O. Wobbrock and J. A. Kientz, “Research contributions in human-computer interaction,” *Interactions*, vol. 23, no. 3, pp. 38–44, 2016. Available: https://doi.org/10.1145/2907069

[99] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006. Available: https://doi.org/10.1191/1478088706qp063oa

[100] M. Lankhorst, “Beyond Enterprise Architecture,” in *Enterprise Architecture at Work*. Springer, pp. 311–316, 2005. Available: https://doi.org/10.1007/3-540-27505-3_12

[101] J. A. Zachman, “Enterprise architecture: The issue of the century.,” *Database Program. Des.*, vol. 10, no. 3, pp. 44–53, 1997.

[102] R. Ross, M. McEvilley, and J. Carrier Oren, “Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,” *NIST Spec. Publ. 800-160*, 2016. Available: https://doi.org/10.6028/NIST.SP.800-160

[103] E. Kiomba, I. Rychkova, N. Herbaut, and C. Souveyet, “Addressing Trust Issues in Supply-Chain Management Systems through Blockchain Software Patterns,” in *Research Challenges in Information Science: Information Science and the Connected World. RCIS 2023. Lecture Notes in Business Information Processing*, vol. 476, Springer, pp. 275–290, 2023. Available: https://doi.org/10.1007/978-3-031-33080-3_17