Review



# A Survey on Digital Trust: Towards a Validated Definition

Julija Saveljeva * and Tatjana Volkova

Posted Date: 14 April 2025

doi: 10.20944/preprints202504.1110.v1

Keywords: digital trust; systematic literature review; definition; concept validation

 doi:10.20944/preprints202504.1110.v1



*Review*

# A Survey on Digital Trust: Towards a Validated Definition

**Julija Saveljeva * and Tatjana Volkova**

BA School of Business and Finance, Riga, Latvia; tatjana.volkova@ba.lv

* Correspondence: julija.saveljeva@ba.lv

**Abstract:** Digital trust is increasingly crucial for successful interactions in modern digital environments. However, the existing literature lacks a unified definition and a comprehensive understanding of its core factors. This study addresses these gaps by conducting a systematic literature review to explore and synthesize existing definitions of digital trust and identify the fundamental factors that shape it. 86 relevant sources were analyzed, revealing that digital trust is typically conceptualized as confidence in people, processes, and technology aimed at ensuring a secure digital environment, with data protection and privacy playing critical roles. Through thematic analysis, "openness" emerged as an additional factor complementing previously established elements of the integrative model of organizational trust, such as ability, benevolence, and integrity. Based on 42 definitions, we developed a new holistic definition of digital trust. The authors evaluated its content validity, confirming its alignment with the essential factors shaping digital trust's essence. The findings highlight the multidimensional nature of digital trust and offer an operationalized framework for future measurement and application.

**Keywords:** digital trust; systematic literature review; definition; concept validation

## 1. Introduction

As technology becomes increasingly central to our lives and businesses, understanding and fostering digital trust (DT) is crucial for maximizing the potential of digital technologies and maintaining healthy relationships with them [1]. It was noted that online environments provide more significant uncertainty and perceived risk than traditional settings, making trust a key factor in reducing fear and enabling engagement [2]. As per Alpcan, Levi, and Savas [3], there is a fundamental difference between trust relationships within online and offline environments due to differences in trust establishment settings. At the same time, the concept of DT appears prominently in professional literature as a new approach to assessing the trustworthiness of digital technologies [4–7].

Research on DT has grown significantly since 2016, with studies focusing on its definition, formation process, and impact on various sectors, but is still developing in scientific literature [2]. Trust should be considered contextual and varies across different domains [8,9]. Dimitrakos connects it with the competence of the other party (trustee) in behaving dependably within a given context and relative to a specific task [10].

Many interactions between individuals and organisations have been conducted digitally in recent years. This motivates exploring new dimensions that bring the digital environment into the trust concept [11]. The authors of various papers stated that there is no single definition of DT [2,12,13]. This leads to a limited understanding of this concept and its dimensions, preventing organisations from establishing DT [13]. Sometimes alternative terms are used, such as "cyber-trust" or "online-trust" [12]. Nevertheless, no single definition or clear understanding of differentiation exists.

 doi:10.20944/preprints202504.1110.v1



Simultaneously, the researchers noticed a significant difference between "traditional" trust and DT. While DT includes the features of regular trust, as it is built on fundamental trust foundations, primarily social and psychological factors [14,15], it also has several unique characteristics due to technological or digital factors that influence it [3,14,15]. The need for DT explorations resulted in two systematic literature review research papers on DT topics published in 2021.

The first study of Tunkevichus and Rebiazina (2021) concentrated exclusively on consumer DT and identified the main trends and research directions in this field. The second systematic literature review, conducted by Pietrzak and Takala (2021), has a broader scope, focusing on the concept of DT. While this work provided valuable insights into DT at the time, several limitations highlighted the need for a new systematic literature review rather than merely a replication with newly published sources:

- The authors used only one database (Web of Science, WoS) for their research, significantly limiting the number of sources;
- The inclusion and exclusion criteria were not described in their paper [2].

The previous research has not solved the issue of various DT interpretations and lack of consensus on its characteristics despite a highlighted strong need [16]. Therefore, the aim of this research is to conduct comprehensive research on the essence of the DT concept, including its definition and key factors. Further, considering the absence of a unified definition, the authors, based on 42 existing definitions of DT, proposed their own holistic definition and tested it with the content validation method.

## 2. Materials and Methods

This study comprised two phases. First, a systematic literature review was conducted to gather comprehensive theoretical grounds for the existing definition of DT and its factor analysis. Second, the content validation method [17] was employed to demonstrate the alignment of the proposed definition of the DT concept with its key factors.

The systematic literature review was conducted based on PRISMA 2020 methodology [18]. The papers were searched in two of the world's leading bibliographic scientific databases [19] - Scopus [20] and WoS [21]. The search, using the keyword "digital trust," took place on 15 September 2024 and was restricted to 1) titles, abstracts, and keywords; 2) scientific articles and conference papers; and 3) the English language. Conference papers were included in the review, given that the concept of digital trust is still emerging.

A total of 156 records were identified in the Scopus [20] and WoS databases, with 84 [21] from the latter. After removing duplicates, 170 papers remained. All abstracts were subsequently retrieved and reviewed. The inclusion criterion was relevance to the topic of DT, while the exclusion criterion targeted engineering or computer science research where DT was merely a technical or software solution parameter. Following the initial abstract screening, 118 sources were qualified for full-text review.

The authors could not access the full texts of the 12 reports. Therefore, 106 papers were read, and 20 reports were excluded due to the previously mentioned criteria. Consequently, 86 research papers—27 conference proceedings and 59 scientific articles—were included in the theoretical analysis of the DT concept. The PRISMA 2020 flow diagram is shown in Figure 1 below.

 doi:10.20944/preprints202504.1110.v1



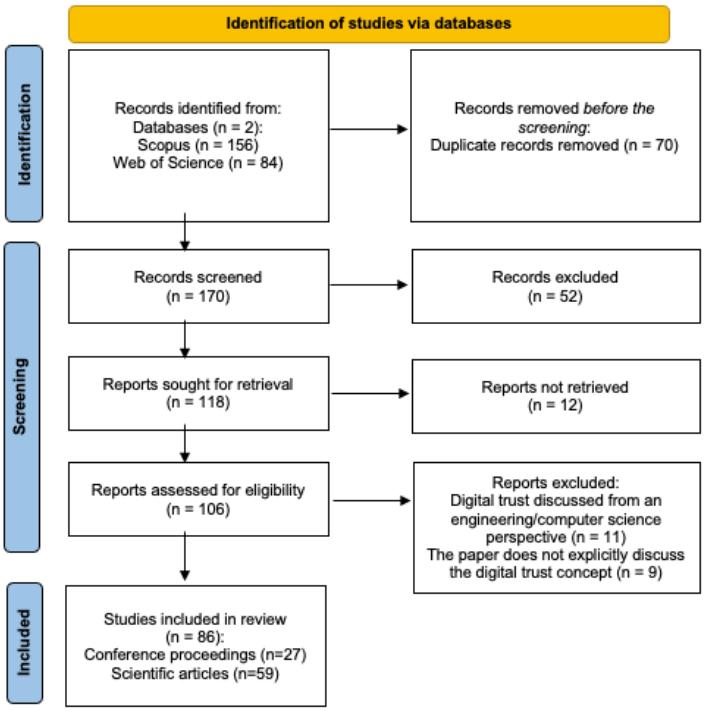


**Figure 1.** PRISMA 2020 flow diagram for systematic literature review on DT (author's own).

## 3. Systematic Literature Review Results

### *3.1. Bibliographical Analysis*

The bibliographical analysis revealed that the first publication included in the analysis appeared in 2010 as conference proceedings. Interest in DT began to increase significantly in 2019, with four papers published, peaking in 2022 with 21 publications—five times more than in 2019. With 16 papers retrieved by September 2024, there are expectations that the total number of publications in 2024 will be like or exceed that of 2022 if the publication rate remains consistent in the coming months. The papers included in the review, sorted by publication year and type, are illustrated in Figure 2.

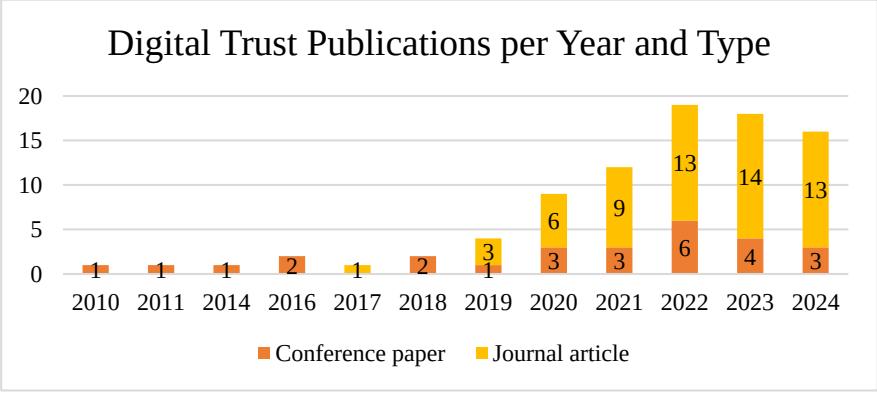


**Figure 2.** Publications included in the review sorted by year and type, 2010 – 2024 (author's own).

The keyword analysis revealed 328 keywords. A co-occurrence full-counting keyword analysis using VOSviewer [22] identified 11 keywords that appeared three or more times. The relatively small number of recurring keywords indicates a diverse focus among the analysed articles, reflecting the multifaceted nature of the DT concept.

Aside from "digital trust" (n=39) and "trust" (n=17), the most frequently mentioned keywords were "blockchain" (n=15), "digitalisation" (n=6), "digital transformation" (n=6), and "sharing economy" (n=6). These trends indicate a strong link between digital transformation and blockchain

 doi:10.20944/preprints202504.1110.v1



technology, highlighting contemporary research subjects focused on the business transition from traditional to digital environments, which enable new business models.

The clustering analysis identified four clusters, as depicted in Figure 3:

1. Blue: Devoted to governance
2. Red: Focused on digital transformation and digitalisation, strongly linking them with industrial or organisational changes.
3. Green: Related to the technological application of DT
4. Yellow: concerned with socio-economic aspects

The above highlights the significance of blockchain technology as a driver of DT and underscores the importance of policies and regulatory frameworks in this context. It also illustrates how trust is essential for adopting new digital processes and economic models.

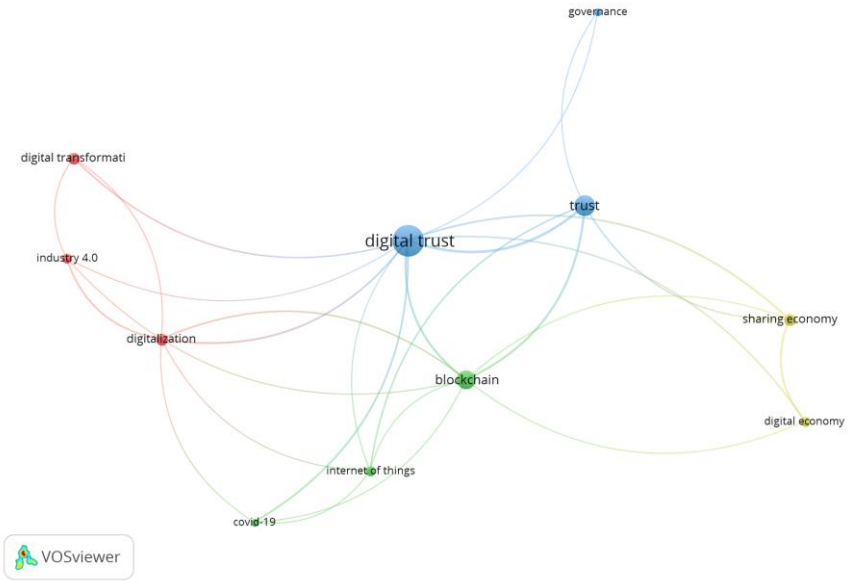


**Figure 3.** Visualisation of keywords co-occurrence clusters (author's own).

*3.2. Existing Definitions of Digital Trust*

The research revealed a wide range of definitions of DT in academia: 86 analysed papers identified 42 various definitions of DT. Some authors provided their definitions, whereas another group referred to one of a few definitions from other sources. Notably, within the wide range of the identified definitions, only five were cited several times within the scope of the analysed articles. These facts conclude that no single proven point of view exists within academia, and authors have different opinions on the DT concept.

Nevertheless, based on the analysis, the most popular definition of DT is "the confidence of stakeholders in the competence of actors, technologies and processes for establishing reliable and secure business networks", (M. F. Mubarak and Petraite 2020, p.3) which was included in the analysed papers and quoted three times [24–26], i.e. used four times.

The complete list of identified definitions is listed in Annex 1. The identified definitions can be classified into six thematic groups by applying content analysis. Some definitions encompass several themes but have been allocated to the most thematically appropriate group. The thematic distribution of the definitions is summarised in Table 1 below.

**Table 1.** DT definitions distribution by the thematic group[1].

| Group nr. | Main group's theme |
|---|---|
| Group 1 (n=12) | Confidence in people, processes and technology to create a secure digital environment |

 doi:10.20944/preprints202504.1110.v1



| | |
|---|---|
| Group 2 (n=8) | Trust in data protection, privacy, security, and ethical information handling |
| Group 3 (n=8) | Trust in the technical capability and reliability of technology |
| Group 4 (n=7) | Trust as a mental state involving cognitive, emotional, and experiential factors |
| Group 5 (n=4) | Trust as an enabler in digital relationships, interactions, and business networks |
| Group 6 (n=3) | Trust based on ethical behaviour and cultural principles |

[1] Source: created by authors.

Further, each thematic group will be detailed, with examples of common traits and definitions.

**Group 1:** confidence in people, processes and technology to create a secure digital environment. This is the most popular thematical definition type, represented by 12 examples. The common traits of these definitions are:

- Focus on the collective confidence in people, processes and technology, i.e. “holistic trust”.
- Emphasis on having a secure and reliable digital environment.
- Includes trust from various stakeholders such as users, customers, individuals, partners, and society.

As the examples, the definition of Das et al. [27], (p.360): “in the digital context, trust refers to users' confidence and reliability in the systems, services, and organisations they interact with. Users must trust that their personal information will be handled responsibly, that their privacy will be respected, and that the systems they rely on are secure from malicious actors.

**Group 2:** trust in data protection, privacy, security, and ethical information handling. This thematic group is also widely represented within DT definitions with eight examples. These definitions are focused chiefly on information security and management:

- Assurance that personal and sensitive data is protected from unauthorised access and breaches.
- Expectation in the organisations to handle data responsibly and ethically, respecting user privacy.
- Meeting stakeholders’ expectations regarding data handling practices.

It is worth mentioning that this was the type of definition proposed by Pietrzak and Takala [2], (p. 64) as the result of their systematic research on DT, which states: “Digital trust is assumed to be the measure of confidence that workers, consumers/buyers, partners, and other stakeholders have in an organisation's ability to protect data and the privacy of individuals."

**Group 3:** trust in the technical capability and reliability of technology. Eight various definitions represent this thematic group, and its common patterns may be described as:

- Confidence in technology's ability to execute tasks and transactions accurately and securely.
- Trust in the consistent performance and punctuality of digital systems, platforms, and services.
- Use specific technologies (e.g., blockchain, AI) to establish or enhance trust.

An example of such a definition is: “The consumer’s belief that the service is technically capable of ensuring the successful execution of the transaction” [28], quoted in [12], (p.433).

In this regard, it is essential to note that some researchers present blockchain technology as DT. For instance, Shin states it is “a kind of user heuristics in blockchain” [29], (p.2) or, as a default guarantee, a substitute for DT [30,31]. Nevertheless, the authors agree with Lee et al. [32], who stated that blockchain is a distributed trusted technology that does not fully substitute trust.

However, it is essential to highlight that there is a scientific discussion on this topic in the literature. Some researchers highlight that DT cannot be achieved solely through technology; it requires building trust in institutions and processes [33].

**Group 4:** Trust as a mental state that encompasses cognitive, emotional, and experiential factors. This group is characterised by seven definitions that are less digital and technical than those of the previous groups. Its common patterns are:

- Trust involves rational evaluations (competence, integrity) and emotional responses (feelings, beliefs).
- Trust is built upon past experiences and evidence of behaviour, influencing future expectations.

 doi:10.20944/preprints202504.1110.v1



- Trust affects the willingness to take risks and make decisions, even with limited verification.

Such definitions in their papers proposed Shin [29], (p.2) "digital trust as cognitive heuristics constitute information processing methods to make decisions more quickly and with less effort than more complex methods, and thus they reduce cognitive load during security assessment" and Hochstein et al. [34], (p.1) "the willingness to rely on digitally presented information when there are limited means of verification".

**Group 5:** Trust as an enabler in digital relationships, interactions, and business networks. This theme is not the most popular among the definitions and is represented by four definitions. The common thematical aspects are:

- Trust enables interactions in environments involving human actors and technological elements.
- Trust is crucial for customer acquisition, retention, and the formation of reliable business networks and partnerships.
- Technology can be an enabler that can enhance or hinder trust in digital relationships.

An example of this thematic group includes: "Digital trust represents the acquisition and retention of customers and shareholder value via providing confidence in the digital services with digital channels" [35], quoted in [36], (p.6).

**Group 6:** Trust based on ethical behaviour and cultural principles. This is the less represented thematic group, seen in three definitions. Its main characteristics are:

- Trust is based on digital partners' integrity, benevolence, and predictability.
- Trust encompasses adherence to both written and unspoken commitments to avert harm.
- It emphasises privacy, security, protection, and data management as part of an organisation's culture.

The following example may illustrate this group: "the digital trust category is also a general term to describe behavioural and cultural principles, including privacy, security, protection and data management" [37], quoted in [38], (p.544).

According to the thematic groups of definitions described above, there is no unified approach to defining DT. Consequently, it is essential to clarify this concept, as the lack of familiarity is preventing progress in scientific research and causing organisations to encounter challenges in measuring, managing, and enhancing their level of DT.

Identifying the key factors that contribute to DT is necessary to construct a comprehensive definition that reflects the multidimensional and holistic nature of the concept.

### *3.3. Key Characteristics of Digital Trust*

The actuality of a common understanding of the DT concept and its characteristics is proved by the fact that there were previous attempts to identify the characteristics of DT using a systematic literature review methodology. This is also proven by the fact that these research papers are recent. The need to have a consensus on DT and its characteristics among key stakeholders around the world was also highlighted by the World Economic Forum's Centre for Cybersecurity [16].

However, both previous studies focused on blockchain as the primary DT provider and tried to retrieve characteristics from the blockchain-related literature.

Rychkova and Ghriba [39] reviewed blockchain literature to identify 21 technology-neutral trustworthiness requirements, emphasising the importance of digital, technological, and social trust in organisational decision-making. Based on the trustworthiness factors Mayer, Davis, and Schoorman [9] mentioned, the requirements were split into three categories: ability, benevolence, and integrity.

Sharma, Agrawal, and Manupati [40] focused on adopting DT in blockchain-based supply chain management and listed its characteristics. The study identified five key characteristics of DT essential for sustainable blockchain-based supply chains: transparency, cybersecurity, data protection, accountability, reliability and provenance, and regulatory compliance. This study provided more high-level characteristics, as some factors could include several characteristics identified by Rychkova and Ghriba [39].

This systematic literature review encompassed a diverse range of sources. It focused exclusively on DT but was not restricted to the blockchain aspect. Out of 86 papers, 36 included the characteristics

 doi:10.20944/preprints202504.1110.v1



of DT, yet none appeared in a systematic review by Rychkova and Ghriba [39]. From these papers, 24 factors of DT were identified and organised into four categories and eight sub-categories.

Some authors used "trust" or "trustworthiness" as DT factors, which does not help identify elements of digital trustworthiness. Analysing various factors, it was noted that the authors meant them using different layers of granularity. Some were using exact "ability", "benevolence", and "integrity" [41]; some were naming categories, such as "security" and "responsible use" [42], whereas some were naming very detailed factors, such as "data privacy" [26] or "decentralisation" [43].

As this research seeks to identify universally applicable DT factors, all identified factors were arranged into three layers:

1. Category, based on initial trustworthiness factors introduced by Mayer, Davis and Schoorman [9];

2. Sub-category, representing the foundational elements of the category in the context of DT; and

3. Consolidated DT factors, as numerous researchers employed various elements to convey a single DT factor.

Trustworthiness requirements are linked to social science factors (ability, benevolence, and integrity) to bridge social and technological domains, following the approach of Rychkova and Ghriba [39]. As stated by Mayer et al. [9], all three categories – ability, benevolence, and integrity - are distinct yet interrelated. According to the definition of the first category, ability is "that group of skills, competencies, and characteristics that enable a party to influence within some specific domain" [9], (p.717). Considering the digital nature of trust, "ability" in this context includes:

- System's, services, and service provider's competence and performance;
- Security and control factors, i.e. internal technical capabilities required to operate reliably;
- Secure system architecture factors represent internal design choices to enhance systems or services' capabilities and perform reliably.

Such a position may be discussable. For example, it contradicts Rychkova and Ghriba's [39], classification, where the factors connected with security and control were added to category 3, "integrity". Nevertheless, such a position goes against the initial definition of "integrity", which means "that the trustee adheres to a set of principles that the trustor finds acceptable" [9], (p.719), as implemented technical controls are characteristics of products or services rather than inherent values. Table 2 below provides a comprehensive overview of the DT factors included in Category 1.

**Table 2.** DT factors included in Category 1: Ability[1].

| Category 1: Ability | Source |
|---|---|
| 1.Competence and reliable performance (cumulative n=19) | |
| 1.1. Competence (n=2) | [39,44] |
| 1.2. Performance (n=2) | [39,45] |
| 1.3. System's reliability (incl. safety and quality) (n=8) | [14,33,42,43,46–49] |
| 1.4. Operational stability (incl. availability, resilience and business continuity) (n=7) | [14,36,39,42,45,47,49] |
| 2. Security and control (cumulative n=25) | |
| 2.1. Identity and access management (inc. authentication, authorization, safe credentials and identifiability) (n=6) | [2,36,39,50–52] |
| 2.2. Confidentiality (incl. data protection and control over own data) (n=9) | [38–40,42,50,52–55] |
| 2.3. Integrity of data (incl. immutability) (n=10) | [27,32,39,42,43,45,49,50,56,57] |
| 3. Secure system architecture (cumulative n=8) | [39,56] |
| 3.1. Automation (n=2) | |
| 3.2. Decentralisation (incl. consensus algorithms, permissionless access, censorship resistance and cryptographic functions / protocols) (n=5) | [32,39,42,43,56] |

 doi:10.20944/preprints202504.1110.v1



| | |
|---|---|
| 3.3. Interoperability (n=1) | [39] |

[1] Source: created by authors.

The second category, benevolence, is "the extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive" [9], (p.718). Mayer et al. [9] describe benevolence as the perception of a positive orientation of the trustee toward the trustor. The category can be considered a blend of cognitive and emotional trust, as it arises from the trustor's subjective perception, the information available, and his experiences. Among the identified factors, this category may be classified into:

- Relational credibility includes elements like goodwill, the reliability of the supplier or service provider, and their reputation.
- User experience and the level of support received – how satisfied the trustor is with the service, their prior experiences, and the convenience of using the product or service.

In this category, it is essential to distinguish between the service's technical reliability and the user's perception of whether they can depend on the service provider. Table 3 below presents the complete list of the DT factors in the benevolence category.

**Table 3.** DT factors included in Category 2: Benevolence[1].

| Category 2: Benevolence | Source |
|---|---|
| 1. Relational credibility (cumulative n=10) | |
| 1.1. Goodwill (incl. benevolence, fairness and honesty) (n=3) | [41,58,59] |
| 1.2. Reliability (predictability of or confidence in service provider) (n=3) | [2,41,49] |
| 1.3. Reputation (incl. credibility) (n=4) | [2,57,60,61] |
| 2. User experience and support (cumulative n=12) | |
| 2.1. Satisfaction of customer service and support (incl. prompt resolution of the issues) (n=6) | [27,44–46,48,49] |
| 2.2. Positive past experience (n=3) | [47,60,61] |
| 2.3. Usability (n=3) | [39,59,60] |

[1] Source: created by authors.

According to the earlier definition of integrity, it pertains to whether an organisation operates within the values, ethics, and rules that were previously agreed upon. Based on the identified factors, this category can be divided into:

- The organisation's core ethical principles include integrity, which guides its adherence to data ethics.
- Governance and compliance encompass accountability for the organisation's actions, adherence to regulations, and the implementation of standards, including industry best practices and other frameworks.

Table 4, with all DT factors within Category 3, is depicted below.

**Table 4.** DT factors included in Category 3: Integrity[1].

| Category 3: Integrity | Source |
|---|---|
| 1. Core ethical principles (cumulative n=14) | |
| 1.1. Integrity (the principle of the organization) (n=1) | [39] |
| 1.2. Data ethics (incl. responsible use and privacy) (n=12) | [26,29,33,36,39,42,47,50,53,54,61,62] |
| 1.3. Sustainability (n=1) | [24] |
| 2. Governance and compliance (cumulative n=13) | |
| 2.1. Accountability (n=6) | [27,32,36,39,40,63] |
| 2.2. Compliance with regulations (n=6) | [15,39,40,55,62,63] |
| 2.3. Application of standards (n=1) | [60] |

[1] Source: created by authors.

 doi:10.20944/preprints202504.1110.v1



Although nearly all identified factors can be categorised into three main categories: 1. The system or organisation's competence/capacity (Ability); 2. The positive intent of organisations/service providers towards users (Benevolence); and 3. The organisation's adherence to acceptable standards and principles (Integrity), one particular set of DT factors does not entirely conform to these three pillars.

In the modern world, particularly within the digital environment, there are numerous ways to verify trustworthiness through external sources and assurances. Consequently, trust is becoming demonstrable and publicly verifiable. This concept can be described as "openness," which encompasses three factors:

- Transparency signifies open and clear information about how the service functions.
- Auditability pertains to an external party's capacity to examine the service or its provider and provide independent verification or certification. In this context, the experiences of other users may also be emphasised, whether through feedback, reviews, or word of mouth.
- Traceability refers to the ability to track processes and data flows within the service.

As this category focuses on a single aspect and includes only three factors, no sub-category has been introduced, and cumulative referencing has been calculated for the entire category. The complete list of references for this category is presented in Table 5 below.

**Table 5.** DT factors included in Category 4: Openness[1].

| Category 4: Openness (cumulative n=23) | Source |
|---|---|
| 1. Transparency (n=11) | [27,32,36,39,40,43,47,50,58,63,64] |
| 2. Auditability (incl. certification and independent verification) (n=6) | [24,32,39,47,50,61] |
| 3. Traceability (incl. data provenance) (n=6) | [2,39,40,50,51,64] |

[1] Source: created by authors.

The overall framework of the factors included in the DT concept is depicted in Figure 4 below.

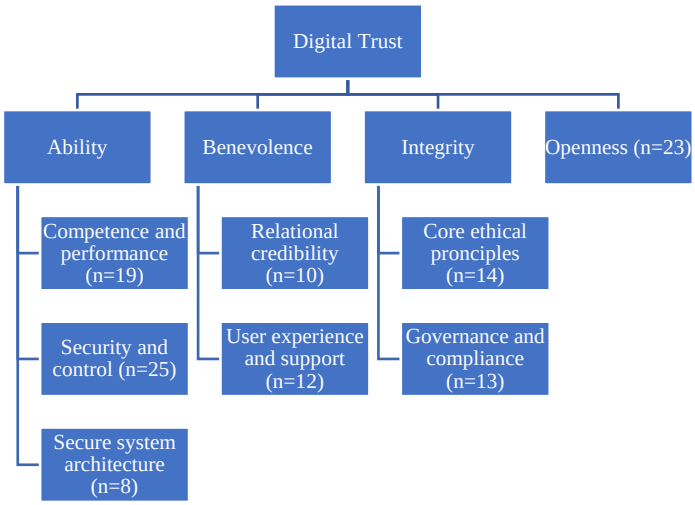


**Figure 4.** DT factors categories and sub-categories (author's own).

Based on the previously analysed DT definitions and key factors that compose the concept, the authors propose the following definition of DT: *Digital trust is the confidence that an entity or digital environment consistently demonstrates competence and reliability, maintains robust security and a secure system architecture, fosters fair and honest practices, provides a positive user experience, complies with governance and regulatory standards, and ensures auditability and traceability of data and operations.*

## 4. Digital Trust Definition Validation

 doi:10.20944/preprints202504.1110.v1



Clear conceptual definitions are very important for scientific progress and further theoretical development [65]. Even more important is to create a formal definition with precise language to prevent unclarities and repetitive reasoning [66]. As concluded in section 3.2, 42 different definitions of DT were identified within the analysed sample of papers. Although one definition appeared four times in the sample, it is difficult to label it as the dominant one. Furthermore, this definition was included in the first thematic group of definitions, and the authors of this study argue that it reflects the holistic nature of the concept.

*4.1. Definition Validation Methodology*

Considering the various existing definitions while proposing a new comprehensive one, there is a noticeable need for content validation – "the methodological process of gauging the degree to which scale items adequately sample the universe of content associated with a construct" [67], (p.1243). Although DT can be viewed as an interdisciplinary concept that merges technology with psychology, the methodology offered by Colquitt et al. [67] for industrial/organisational psychology to conduct definitional correspondence (to analyse the degree to which a scale's items or factors composing the concept correspond to its definition) and definitional distinctiveness (to analyse the extent to which a scale's items or factors composing the concept correspond more to the given definition than to other related constructs) is still regarded as relevant and was applied in this study.

The questionnaire for content validation of the definition was created using Hinkin and Tracey's approach [17]. Since it was a self-guided online survey designed to determine the degree to which the definition corresponded to the key factors that compose it, the formulation of the response scale offered by Colquitt et al. [67] in the detailed instructions (illustrated in Figure 5 below) was deemed unsuitable for the objectives of this study.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| Item does an **EXTREMELY BAD** job of measuring the **bolded** concept provided above | Item does a **VERY BAD** job of measuring the **bolded** concept provided above | Item does a **SOMEWHAT BAD** job of measuring the **bolded** concept provided above | Item does an **ADEQUATE** job of measuring the **bolded** concept provided above | Item does a **SOMEWHAT GOOD** job of measuring the **bolded** concept provided above | Item does a **VERY GOOD** job of measuring the **bolded** concept provided above | Item does an **EXTREMELY GOOD** job of measuring the **bolded** concept provided above |

**Figure 5.** The response scale for Hinkin and Tracey's approach (Source: [17]).

The respondents were informed that the research aims to validate the newly developed definition to ensure it effectively captures the essence of the DT concept. They were also informed that they would be invited to rate four definitions: three existing ones and one newly developed, in random order. They evaluated how well each survey item, i.e., each characteristic, aligns with the four provided definitions.

The authors, fluent in both English and Latvian, first created the questionnaire in English before translating it into Latvian. This was essential for effective distribution in Latvia, the authors' place of allocation, as not all potential respondents had the necessary level of English proficiency. Furthermore, the translation was validated by two native Latvian speakers who were fluent in English to ensure that both the definitions and the factors matched the original intent of the English versions.

Subsequently, the initial version of the questionnaire was piloted with five respondents to gather feedback and assess its validity. Following the pilot, the wording of the scale items was simplified, as the respondents found it difficult to grasp the essence of each factor and ascertain whether it was reflected in the provided definition. Additionally, based on the feedback, the Likert scale was reduced from 7 points to 5 points, as the respondents were uncertain about the fundamental difference between the "extremely bad/good" ratings and the "very bad/good" ratings, in line with Hinkin and Tracey's original approach[17]. The final evaluation scale ranged from 1 to 5, where:

- 1 means that the characteristic is not presented in the definition at all.
- 2 means that the characteristic is more absent than presented.
- 3 means that the characteristic is partially presented.
- 4 means that the characteristic is more presented than absent.
- 5 means that the characteristic is fully presented in the definition.

 doi:10.20944/preprints202504.1110.v1



Seven DT subcategories were operationalised to measure the validity of DT definitions. For the fourth category, known as the openness category, no subcategory was formulated; however, two of its selected factors—auditability and traceability—were operationalised. These two factors were chosen because they both essentially provide some of the transparency promised by a digitally trustworthy organisation.

The operationalised descriptions of the validation factors, which are listed in Table 6 below, were based on the factor descriptions proposed by Rychkova and Ghriba [39]. To operationalise the first three categories (F1 – F7), the authors summarised the descriptions of the factors included in the sub-category, as provided by Rychkova and Ghriba [39]. The fourth category factors (F8, F9) were created directly using the descriptions from Rychkova and Ghriba [39].

**Table 6.** Description of measurable items[1].

| Code | Category | Operationalised description |
|---|---|---|
| | | **Category 1: Ability** |
| F1 | 1.Competence and performance | The entity demonstrates competence and reliably delivers services or products. |
| F2 | 2. Security and control | The entity ensures secure access, protects data, and maintains its integrity. |
| F3 | 3. Secure system architecture | The entity employs a secure architecture and processes to ensure efficiency, control, and integration. |
| | | **Category 2: Benevolence** |
| F4 | 1. Relational credibility | The entity demonstrates fairness, honesty, and reliability, building a strong reputation. |
| F5 | 2. User experience and support | The entity ensures a positive user experience and provides responsive support. |
| | | **Category 3: Integrity** |
| F6 | 1. Core ethical principles | The entity demonstrates integrity, protects data privacy, and adopts sustainable practices. |
| F7 | 2. Governance and compliance | The entity ensures governance and compliance in accordance with regulations and standards. |
| | | **Category 4: Openness** |
| F8 | 1. Auditability | The entity ensures compliance through certifications, audits, and supervision. |
| F9 | 2. Traceability | The entity ensures traceability by providing information about data origins. |

[1] Source: created by authors.

Four definitions were provided for the respondents' judgement: the first, developed by the authors for validation; the second, the most popular existing definition, to determine whether the proposed one better captures the concept's essence; and the third and fourth, pertaining to the DT concepts of "cyber-trust" and "online trust."

Definition No. 1: "Digital trust is the confidence that an entity or digital environment consistently demonstrates competence and reliability, maintains robust security and a secure system architecture, fosters fair and honest practices, provides a positive user experience, complies with governance and regulatory standards, and ensures auditability and traceability of data and operations" (proposed by the authors).

Definition nr. 2: "Digital trust is the confidence of stakeholders in the competence of actors, technologies and processes for establishing reliable and secure business networks" [23], 3), the most popular definition within the analysed sample.

 doi:10.20944/preprints202504.1110.v1



Definition nr.3: "The user's confidence in the predictability of the 'behaviour' of software and hardware systems (digital technologies), their reliability, which is manifested in the willingness to delegate several tasks to various software and hardware systems" [68](quoted in [12] 433). This defines the related concept of "cyber-trust."

Definition nr. 4: "Consumers' perception of a web site's usefulness, security, privacy, reputation, quality, and e-vendors' willingness to customise" [69], 433). The definition of the related concept is "online trust."

Although Colquitt et al., (2019) based on an analysis of 112 studies, stated that naïve respondents may be used when applying the methodology, doctoral students are admitted as the best judges for definitional correspondence and distinctiveness. This is because they look beyond the simple meaning of definitions due to their expertise and experience. Therefore, the authors tried to obtain input from this group of respondents and distributed the questionnaire among doctoral students through Facebook [70] and LinkedIn [71] PhD student groups and personal networks. The respondents were not compensated for their participation in the survey. However, to encourage completion, participants could provide an email address to enter a prize draw of three gift cards of the winner's choice.

To ensure the necessary number of responses, and considering that, according to the methodology, the judges may also be naïve, the questionnaire was distributed among students at all levels at the university where the authors are affiliated – BA School of Business and Finance – and among professionals connected with digital topics through their networks. A total of 282 potential respondents opened the survey, 171 began to fill it out, and only 99 submitted their responses. Since Colquitt et al. [67] . stated that a minimum sample size of 100 respondents would yield sufficiently precise results, we conclude that the current sample is adequate for this study.

### *4.2. Definition Validation Study Results*

Statistical calculations in this study were conducted using Jamovi [72] software. 47 (47,5%) respondents completed the questionnaire in English, whereas 52 (52,5%) selected the Latvian language for their responses. There was an option to select ages above 65, but none of the respondents chose it. The most represented age group was 35 to 44 (n=34, 34,3%), and most respondents were under 44 (n=83, 83,8%). From the educational perspective, the most represented group was those with a master's degree (n=43, 43,4%). Most respondents (n=79, 79,8%) had obtained at least a college degree. The full demographical statistics are presented in Table 7 below.

**Table 7.** Demographical statistics[1].

| Language | N | % | Age | N | % | Education | N | % |
|---|---|---|---|---|---|---|---|---|
| English | 47 | 47,5% | 18-24 | 21 | 21,2% | High school diploma or equivalent | 20 | 20,2% |
| Latvian | 52 | 52,5% | 25-34 | 28 | 28,3% | College | 10 | 10,1% |
| | | | 35-44 | 34 | 34,3% | Bachelor's degree | 26 | 26,3% |
| | | | 45-54 | 13 | 13,3% | Master's degree | 43 | 43,4% |
| | | | 55-64 | 3 | 3,0% | | | |

[1]Source: created by authors.

Furthermore, the authors' proposed definition - definition number 1 - was analysed according to the index of definitional correspondence, known as *htc* (for Hinkin Tracey correspondence), calculated using the following formula:

htc = average definitional correspondence rating/a

The analysis of definition number 1 (D1) ratings confirmed that the judgments are not normally distributed, as anticipated in this study, based on the Shapiro-Wilk test, $p < .001$ in all instances. Furthermore, the standard deviation (SD) suggested some variation in the opinions; nonetheless, they remain largely consistent.

Following Hinkin and Tracey [17], a minimum value of 4.2 for htc provides a confirmation of content adequacy. As per Colquitt et al., (2019) the HTC value between 0.87 and 0.90 indicates strong

 doi:10.20944/preprints202504.1110.v1



content adequacy, while values from 0.84 to 0.86 suggest a moderate correlation that remains sufficient. Overall, the analysis reveals that the provided definition is moderately or strongly aligned with the key factors of the concept, enabling the authors to assert that it captures the essence of DT. While the judges noted that certain measurable items (such as competence and performance, user experience and support, and auditability) are not as strongly represented in the definition compared to others (like security and control or governance and compliance), their HTC value still indicates that the definition adequately encompasses all assessed key factors. The calculations are presented in Table 8 below.

**Table 8.** Statistical calculations of definition nr. 1[1].

| Code | Category | SD | p | Rating | htc |
|---|---|---|---|---|---|
| F1 | Competence and performance | 1.173 | <.001 | 4.18 | 0.84 |
| F2 | Security and control | 0.969 | <.001 | 4.41 | 0.88 |
| F3 | Secure system architecture | 0.959 | <.001 | 4.28 | 0.86 |
| F4 | Relational credibility | 0.956 | <.001 | 4.32 | 0.86 |
| F5 | User experience and support | 1.082 | <.001 | 4.18 | 0.84 |
| F6 | Core ethical principles | 1.036 | <.001 | 4.26 | 0.85 |
| F7 | Governance and compliance | 0.873 | <.001 | 4.48 | 0.90 |
| F8 | Auditability | 1.152 | <.001 | 4.17 | 0.83 |
| F9 | Traceability | 0.894 | <.001 | 4.34 | 0.87 |
| Overall | | | | 4.29 | 0.86 |

[1] Source: created by authors.

The statistical analysis of the second (D2), third (D3), and fourth (D4) definitions confirmed that they are also not normally distributed, which was the anticipated outcome of this research. The standard deviations for the ratings of these definitions were higher than for the first definition, indicating that the ratings displayed greater variability from the judges. The calculations are provided in Table 9 below.

**Table 9.** Statistical calculations of definitions nr. 2, 3 and 4[1].

| Code | Category | D2 SD | D2 p | D3 SD | D3 p | D4 SD | D4 p |
|---|---|---|---|---|---|---|---|
| F1 | Competence and performance | 1.003 | <.001 | 1.035 | <.001 | 1.082 | <.001 |
| F2 | Security and control | 0.955 | <.001 | 1.218 | <.001 | 1.204 | <.001 |
| F3 | Secure system architecture | 1.082 | <.001 | 1.051 | <.001 | 1.109 | <.001 |
| F4 | Relational credibility | 1.069 | <.001 | 1.190 | <.001 | 1.063 | <.001 |
| F5 | User experience and support | 1.094 | <.001 | 1.123 | <.001 | 1.071 | <.001 |
| F6 | Core ethical principles | 1.041 | <.001 | 1.211 | <.001 | 1.023 | <.001 |
| F7 | Governance and compliance | 1.114 | <.001 | 1.228 | <.001 | 1.161 | <.001 |
| F8 | Auditability | 1.264 | <.001 | 1.229 | <.001 | 1.159 | <.001 |
| F9 | Traceability | 1.161 | <.001 | 1.123 | <.001 | 1.218 | <.001 |

[1] Source: created by authors.

Afterwards, the results of the similar (D2) and alternative (D3, D4) definitions were analysed using the *htd* or Hinkin Tracey distinctiveness index, which was calculated using the formula below:

htd = Average of all (Intended Correspondence Rating – Orbiting Correspondence Rating) / ($a$ – 1), where $a$ is the number of anchors

According to Colquitt et al., [67] the HD value from 0.18 to 0.26 is moderate, whereas from 0.27 to 0.34 is strong. Following the calculations of the factors / measurable items ratings presented in Table 10 below, definition nr.2—the most popular definition of DT—is moderately distinctive from the newly proposed definition. Thus, we may conclude that the proposed definition (D1) better represents the conceptual essence of DT than the existing definition.

 doi:10.20944/preprints202504.1110.v1



In turn, definition number 3 (D3) – the definition of cyber-trust – exhibits strong distinctiveness, whereas definition number 4 (D4) – the definition of online trust – demonstrates moderate distinctiveness in comparison to the proposed D1. From this, we can conclude that the proposed D1 represents the DT concept, rather than the orbiting ones.

**Table 10.** Ratings and htd calculations for definitions nr. 2, 3 and 4[1].

| Code | Category | D1 Rating | D2 Rating | D2 htd | D3 Rating | D3 htd | D4 Rating | D4 htd |
|---|---|---|---|---|---|---|---|---|
| F1 | Competence and performance | 4.18 | 3,65 | 0,13 | 3,36 | 0,21 | 3,53 | 0,16 |
| F2 | Security and control | 4.41 | 3,62 | 0,20 | 3,31 | 0,28 | 3,59 | 0,21 |
| F3 | Secure system architecture | 4.28 | 3,47 | 0,20 | 3,43 | 0,21 | 3,35 | 0,23 |
| F4 | Relational credibility | 4.32 | 3,41 | 0,23 | 3,15 | 0,29 | 3,48 | 0,21 |
| F5 | User experience and support | 4.18 | 3,13 | 0,26 | 3,27 | 0,23 | 3,71 | 0,12 |
| F6 | Core ethical principles | 4.26 | 3,42 | 0,21 | 3,06 | 0,30 | 3,35 | 0,23 |
| F7 | Governance and compliance | 4.48 | 3,23 | 0,31 | 3,11 | 0,34 | 3,17 | 0,33 |
| F8 | Auditability | 4.17 | 3,21 | 0,24 | 3,00 | 0,29 | 3,06 | 0,28 |
| F9 | Traceability | 4.34 | 3,17 | 0,29 | 3,06 | 0,32 | 2,92 | 0,36 |
| Overall | | 4.29 | 3,37 | **0,23** | 3,20 | **0,27** | 3,35 | **0,24** |

[1] Source: created by authors.

## 5. Discussion

The thematic analysis of existing definitions of digital trust revealed six distinct approaches to the conceptual meaning of this term. The authors conceptually align with the definitions outlined in Group 1, which posits that digital trust is the confidence in people, processes, and technology to create a secure digital environment, and Group 2, which emphasises trust in data protection, privacy, security, and ethical information handling, thereby supporting a holistic and multidimensional view of this concept. While digital trust entails confidence in the enablers that foster a secure digital environment, data is the most valuable asset in the modern digital world, and its protection, along with users' privacy, must be reflected in the definition of the concept. Simultaneously, the authors contest the position concerning the definitions encompassed in Group 3, which asserts that it involves trust in the technical capability and reliability of technology. Although the importance of trustworthy and reliable technology may be a part of the definition, the technology itself, much like any isolated tool, cannot encompass all dimensions of trust-building.

The analysis of the factors that compose the essence of DT confirmed that there are various approaches towards the conceptualisation level of the factors. While some authors name such DT as "ability" and "benevolence" [41], others may go to a very granular level, mentioning "certification" [53] or "prompt resolution of the issues" [49]. Additionally, the study allowed the identification of an additional category of trust factors – "openness", that compliments Mayer et al.'s [9] previously named and highly recognised three categories – "ability", "benevolence", and "integrity". Such a result confirms the position of Alpcan et al. [3] and Dimitrakos [10], who argued that there is a distinction between trust in traditional and digital contexts, strongly influenced by the situation.

Finally, the proposed definition of DT is valid and represents all identified key factors of DT. Moreover, the new holistic definition performs better from the perspective of key factor representation and significantly differs from similar definitions of cyber and online trust. Additionally, the operationalised DT key factors may be used in the future for DT measurement.

 doi:10.20944/preprints202504.1110.v1



Future research on digital trust may focus on measuring it, particularly regarding the most effective tools for this purpose. Another prominent research topic is an innovative approach to DT communication with customers or partners.

**Author Contributions:** Conceptualization, Julija Saveljeva; methodology, Julija Saveljeva; software, Julija Saveljeva; validation, Julija Saveljeva; formal analysis, Julija Saveljeva; resources, Julija Saveljeva; data curation, Julija Saveljeva; writing—original draft preparation, Julija Saveljeva; writing—review and editing, Tatjana Volkova.; visualization, Julija Saveljeva; supervision, Tatjana Volkova.; project administration, Julija Saveljeva; funding acquisition, Julija Saveljeva. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by a grant from project nr. 5.2.1.1.i.0/2/24/I/CFLA/007, "Internal and External Consolidation of the University of Latvia.".

**Data Availability Statement:** The raw data supporting the conclusions of this article will be made available by the authors on request.

**Conflicts of Interest:** The authors declare no conflicts of interest. The funders had no role in the design of the study, in the collection, analyses, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| DT | Digital trust |
| WoS | Web of Science |

## Appendix A

*Appendix A.1*

The appendix contains the scope of the identified and analysed definition of DT. The logic of providing an authorship in the table is as follows:

- Suppose the definition was found in a source included in 86 analysed papers and copied directly from this source. In that case, the reference is included in the column source, and the field in the column "quoted in" is marked N/A (even if other authors from the scope of SLR also referenced this paper).
- If the authors of the paper quoted another source when providing the definition, the source of the quotation is referenced in the "source" column, while the paper itself is referenced in the "quoted in" column.

**Table A1.** Definitions of digital trust.

| Nr | Definition | Source | Quoted in |
|---|---|---|---|
| | Thematical Group 1 | | |
| 1 | "In the digital context, trust refers to users' confidence and reliability in the systems, services, and organizations they interact with. Users must trust that their personal information will be handled responsibly, that their privacy will be respected, and that the systems they rely on are secure from malicious actors." | [27], (p.360) | N/A14/04/2025 13:15:00 |
| 2 | "The perceived confidence individuals have in the ability of people, technology, and processes to build a secure digital environment." | [73] | [42], (p.4329) |

 doi:10.20944/preprints202504.1110.v1



| | | | |
|---|---|---|---|
| 3 | "A concept that defines confidence in the reliability of all components of digital interaction: users, processes, devices, technologies and vendors" | [74] | [12], (p.433) |
| 4 | "Digital Trust can be defined as the confidence that users have in processes, technology and people to create a secure digital world." | [51], (p.1) | N/A |
| 5 | "Digital trust underpins every digital interaction by measuring and quantifying the expectation that an entity is who or what it claims to be and that it will behave in an expected manner." | [75] | [76], (p.179) |
| 6 | "The general belief that technology, people, and processes act or are aligned in ways that will fulfill people's digital expectations, such as sense of confidence, security, or control to support the creation of a secure digital environment." | [75] | [77], (p.30) |
| 7 | "Digital trust implies a sufficient level of confidence in people, processes, and technology to build a secure digital world" | [47], (p.245) | N/A |
| 8 | "Confidence in the creation of a secure digital world" | [78] | [38], (p.539) |
| 9 | "DTrust is associated with trust in digital institutions, digital technologies and platforms, which, in other words, means the user's trust in the capability of digital institutions, companies, technologies and processes to create a safe digital world." | [57], (p.490) | N/A |
| 10 | "Digital trust can be referred to as the confidence of stakeholders on the competence of actors, technologies, and processes for establishing reliable and secure business networks." | [23], (p.3) | N/A |
| 11 | "Digital trust has been defined in practitioner circles as the confidence users have in the ability of people, technology, and processes to create a secure digital world. Yet the basis of trust placed in people, technology (e.g., devices, platforms), and processes (e.g., systems, institutions) will likely differ across digital contexts." | [79] | [80], (p.668) |
| 12 | "DT represents stakeholders' confidence in the competence of actors, technologies, platforms and processes of establishing a reliable network." | [81] | [48], (p.74) |
| | **Thematical Group 2** | | |
| 13 | "Digital trust represents the acquisition and retention of customers and shareholder value via providing confidence in the digital services with digital channels" | [35] | [36], (p.6) |
| 14 | "Reliability of information provided by trade partners, or the safety and security of the data managed by a central authority" | [82] | [40], (p.19) |
| 15 | "The confidence that a digital society attains in terms of data protection and privacy protection" | [83] | [33], (p.168) |
| 16 | "Confidence in the counterparty that stores and use consumers' digital information in such a way that this meets the expectations of consumers" | [84] | [12], (p.433) |
| 17 | "Digital trust is assumed to be the measure of confidence which workers, consumers/buyers, partners and other stakeholders | [2], (p.65) | N/A |

 doi:10.20944/preprints202504.1110.v1



| | | | |
|---|---|---|---|
| | have in the ability of an organisation to protect data and the privacy of individuals" | | |
| 18 | "The confidence placed in an organisation to collect, store, and use the digital information" | [85] | [2], (p.65) |
| 19 | "Digital trust stems from a combination of different factors (...): security, identifiability, and traceability. Quite often, however, the presence of these features can be too difficult for an individual to evaluate – and especially so in a digital environment." | [86] | [2], (p.65) |
| 20 | "Digital trust can be seen as insurance placed by data owners in an actor empowered to manage their digital data. This means that data owners feel secure with their data, by securely controlling their distribution. Their consent is required to access this data." | [87], (p.262) | N/A |
| 21 | "Digital trust refers to the belief that technology and information systems can be relied upon, secure, and well-integrated into business processes". | [88] | [89], (p.4) |
| 22 | "Digital trust, which is the users' confidence in the safety, privacy, security, reliability, and ethical handling of data by companies in the digital environment, correlates with the perceived value of the information conveyed" | [89], (p.6) | N/A |
| | **Thematical Group 3** | | |
| 23 | Digital trust is maintained through technologies like blockchain and smart contracts, replacing traditional 'implicit trust' with 'technically expressed trust'. | [90] | [91], (p.6) |
| 24 | The consumer's belief that the service is technically capable of ensuring the successful execution of the transaction | [28] | [12], (p.433) |
| 25 | "The concepts of digital trust are represented as a layered model by dividing the system into trust, credentials, control data, and trust storage abstraction levels." | [52], (p.582) | N/A |
| 26 | "Trust in the technology environment, digital trust (DT) in other words, as the belief of an individual towards a digital system regarding its reliability and punctuality in performing commercial and operational transactions." | [44], (p.7) | N/A |
| 27 | "The extent to which users believe that a platform provides reliable services and maintains a trustworthy status within relevant verification organizations." | [92] | [93], (p.5) |
| 28 | "The reliability of the system involves a shift from physical to digital and human to machine, which we refer to as digital trust, reflecting users' positive beliefs about accepting and using voice-assisted AI systems." | [94] | [49], (p.203) |
| 29 | "DT reflects the user's confidence in the digital platform's consistency and punctuality when executing operational and commercial transactions." | [44,95] | [96], (p.235) |
| | **Thematical Group 4** | | |
| 30 | "Trust is a mental state comprising (1) expectancy: the trustor expects a specific behaviour of the trustee such as providing valid information or effectively performing cooperative actions; (2) belief: the trustor believes that the expected behavior will occur, based on the evidence of the trustee's competence, good | [97] | [64], (p.107) |

 doi:10.20944/preprints202504.1110.v1



| | | | |
|---|---|---|---|
| | intention, and integrity; (3) willingness to take a risk: the trustor is willing to take the risk for (or be vulnerable) that belief in a specific context, where there is an expectation for the specific behaviour of the trustee." | | |
| 31 | "Digital trust in blockchain can be defined as enabling user heuristics made between security and privacy that reflect their level of confidence. Digital trust is a kind of user heuristics in blockchain. (…)Digital trust as cognitive heuristics constitute information processing methods to make decisions more quickly and with less effort than more complex methods, and thus they reduce cognitive load during security assessment." | [29], (p.2) | N/A |
| 32 | "A trust based either on past experience or evidence that an entity has behaved and/or will behave in accordance with the self-stated behaviour." | [61], (p.885) | N/A |
| 33 | "The combination of cognitive trust and emotional trust. Cognitive trust includes practicality, commitment to execution, honesty, benevolence, and so on. Emotional trust includes likes, beliefs, and so on." | [59], (p.4) | N/A |
| 34 | "Digital trust is defined as a "measurable belief and/or confidence" that is "accumulated from past experiences" and is an "expecting value for the future"." | [98] | [99], (p.106745) |
| 35 | "The willingness to rely on digitally presented information when there is limited means of verification" | [34], (p.1) | N/A |
| | **Thematical Group 5** | | |
| 36 | "The confidence that causes users to exercise a choice to interact, transact, and consume online. Fundamentally, it determines the quality of the interaction between those who give trust and those who guarantee to uphold said trust." | [100], (p.25) | [101], (p.3) |
| 37 | "Trust in interactions that take place in an environment where human actors and/or technological elements are involved." | [60], (p.2) | N/A |
| 38 | "Specific beliefs about the way that technology operates through a work environment" | [102] | [44], (p.7) |
| 39 | "Digital trust is a third dimension that affects digital B2B relationships. It specifically refers to trust between digital partners and it can also be influenced by the perception of the tools used. For instance, the opportunity to use technology that simulates real in-person contact reinforces trust, while only chatting has the opposite effect. According to this vision, technology represents an enabler of the relationship that can influence the formation of trust in a techno-mediated environment." | [103], (p.2107) | N/A |
| | **Thematical Group 6** | | |
| 40 | "Digital trust, or "e-trust," is characterized as one's set of specific beliefs in the e-vendor, including integrity, benevolence, ability, and predictability, that results in behavioral intentions." | [104] | [41], (p.1361) |
| 41 | "The digital trust category is also used as a general term to describe behavioral and cultural principles, including privacy, security, protection and data management" | [37] | [38], (p.544) |

 doi:10.20944/preprints202504.1110.v1



| | | | |
|---|---|---|---|
| 42 | Is consumer's confidence in a digital partner's, business' or institution's commitment (written/unwritten) to prevent all sources of harm that may arise in transacting business between the two parties (consumer and partner/business/ institution). | [105] | N/A |

## References


1. Chauhan, D. Digital Trust Is Core to Our Relationship with Technology. *Network Security* **2023**, *2023*, S1353-4858(23)70047-0, doi:10.12968/S1353-4858(23)70047-0.
2. Pietrzak, P.; Takala, J. Digital Trust– Asystematic Literature Review. *Forum Scientiae Oeconomia* **2021**, *9*, 59–71, doi:10.23762/FSO_VOL9_NO3_4.
3. Alpcan, T.; Levi, A.; Savas, E. Digital Trust Games: An Experimental Study. In Proceedings of the Lect. Notes Comput. Sci.; Baras, J., Katz, J., Altman, E., Eds.; 2011; Vol. 7037 LNCS, pp. 182–200.
4. World Economic Forum Digital Trust Available online: https://initiatives.weforum.org/digital-trust/about (accessed on 17 March 2024).
5. PwC Digital Trust and Cybersecurity Available online: https://www.pwc.com/my/en/services/digital/digital-trust-and-cybersecurity.html (accessed on 17 March 2024).
6. ISACA Digital Trust Available online: https://www.isaca.org/digital-trust (accessed on 17 March 2024).
7. Deloitte Future of Digital Trust Available online: https://www2.deloitte.com/de/de/pages/risk/articles/future-of-digital-trust.html (accessed on 17 March 2024).
8. Marsh, S. Formalising Trust as a Computational Concept. PhD, University of Stirling, 1994.
9. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An Integrative Model of Organizational Trust. *The Academy of Management Review* **1995**, *20*, 709, doi:10.2307/258792.
10. Dimitrakos, T. System Models, e-Risks and e-Trust.; Zürich, Switzerland, 2001.
11. Kożuch, B. The Dimensions of Trust in the Digital Era. In *Trust, Organizations and the Digital Economy*; Routledge: New York, 2021; pp. 15–26 ISBN 978-1-00-316596-5.
12. Tunkevichus, E.; Rebiazina, V. CONSUMER DIGITAL TRUST: THE MAIN TRENDS AND RESEARCH DIRECTIONS. *ROSSIISKII ZHURNAL MENEDZHMENTA-RUSSIAN MANAGEMENT JOURNAL* **2021**, *19*, 429–450, doi:10.21638/spbu18.2021.403.
13. Chen, X.; Li, B.; Song, D.; Wang, M. Influences of Risk-Aversion Behavior and Purchasing Option in a Cross-Border Dual-Channel Supply Chain. *Int. Trans. Oper. Res.* **2023**, doi:10.1111/itor.13345.
14. Chaudhuri, A. TRANSFORMATION WITH TRUSTWORTHY DIGITAL: POLICY DESIDERATA FOR BUSINESSES IN POST COVID-19 WORLD. *EDPACS* **2021**, *63*, 1–8, doi:10.1080/07366981.2020.1806443.
15. Zhghenti, T.; Chkareuli, V. ENHANCING ONLINE BUSINESS SECTOR: DIGITAL TRUST FORMATION PROCESS. *MARKETING AND MANAGEMENT OF INNOVATIONS* **2021**, 87–93, doi:10.21272/mmi.2021.2-07.
16. Papic, A.; Radoja, K.; Szombathelyi, D. CYBER SECURITY AWARENESS OF CROATIAN STUDENTS AND THE PERSONAL DATA PROTECTION. In Proceedings of the University of JJ Strossmayer Osijek; Simic, M., Ed.; 2022; pp. 563–574.
17. Hinkin, T.R.; Tracey, J.B. An Analysis of Variance Approach to Content Validation. *Organizational Research Methods* **1999**, *2*, 175–186, doi:10.1177/109442819922004.
18. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Syst Rev* **2021**, *10*, 89, doi:10.1186/s13643-021-01626-4.
19. Pranckutė, R. Web of Science (WoS) and Scopus: The Titans of Bibliographic Information in Today's Academic World. *Publications* **2021**, *9*, 12, doi:10.3390/publications9010012.
20. Elsevier Scopus Available online: https://www.scopus.com (accessed on 18 November 2024).
21. Clarivate Web of Science Available online: https://www.webofscience.com (accessed on 18 November 2024).
22. VOSviewer Available online: https://www.vosviewer.com// (accessed on 26 April 2024).

 doi:10.20944/preprints202504.1110.v1




23. Mubarak, M.F.; Petraite, M. Industry 4.0 Technologies, Digital Trust and Technological Orientation: What Matters in Open Innovation? *Technological Forecasting and Social Change* **2020**, *161*, 120332, doi:10.1016/j.techfore.2020.120332.
24. Mo, Z.; Liu, Y.; Lu, C.; Yu, J. Influences of Industrial Internet Platform Firms' ESG Performance and Digital Leadership on User Firms' Innovation Performance: The Mediating Role of Inter-Firm Trust. *J. Digit. Econ.* **2023**, *2*, 204–220, doi:10.1016/j.jdec.2024.01.002.
25. Han, S.; Ulhoi, J.; Song, H. Digital Trust in Supply Chain Finance: The Role of Innovative Fintech Service Provision. *J. Enterp. Inf. Manage.* **2024**, doi:10.1108/JEIM-07-2022-0238.
26. Mubarak, M.; Ghobakhloo, M.; Evans, R.; Jucevicius, G.; Prestianawati, S.; Mubarik, M. Metaverse Adoption in the Manufacturing Industry: Impact on Social and Environmental Sustainability Performance. *Asia-Pac. J. Bus. Adm.* **2024**, doi:10.1108/APJBA-02-2024-0043.
27. Das, D.; Banerjee, S.; Chatterjee, P.; Ghosh, U.; IEEE A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age. In Proceedings of the Proc. - IEEE Int. Conf. Trust, Priv. Secur. Intell. Syst. Appl., TPS-ISA; Institute of Electrical and Electronics Engineers Inc., 2023; pp. 360–369.
28. Harrison McKnight, D.; Choudhury, V.; Kacmar, C. The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *The Journal of Strategic Information Systems* **2002**, *11*, 297–323, doi:10.1016/S0963-8687(02)00020-3.
29. Shin, D. Blockchain: The Emerging Technology of Digital Trust. *TELEMATICS AND INFORMATICS* **2019**, *45*, doi:10.1016/j.tele.2019.101278.
30. Taghiyeva-Zeynalova, M.; Wang, Y.; Ta'eed, O.; ASSOC COMP MACHINERY Blockchain as a Value Enabler: Bridging Financial Assets and Intangibles. In Proceedings of the BSCI - Proc. ACM Int. Symp. Blockchain Secur. Crit. Infrastruct., co-located AsiaCCS; Association for Computing Machinery, Inc, 2019; pp. 113–119.
31. Osuagwu, O.N.; Lekan Gbadamosi, S.; Ojo, E.E. Blockchain-Based Platforms for Agricultural Supply Chains. In Proceedings of the Int. Conf. Sci., Eng. Bus. Driv. Sustain. Dev. Goals, SEB4SDG; Institute of Electrical and Electronics Engineers Inc., 2024.
32. Lee, N.; Varshney, L.; Michelson, H.; Goldsmith, P.; Davis, A. Digital Trust Substitution Technologies to Support Smallholder Livelihoods in Sub-Saharan Africa. *Global Food Secur.* **2022**, *32*, doi:10.1016/j.gfs.2021.100604.
33. Katete, G. Digital Elections and the Problem of Liquid Trust in the Kenyan Electoral Management Institution. *Int. J. Afr. Renaiss. Stud.* **2021**, *16*, 165–176, doi:10.1080/18186874.2021.1949363.
34. Hochstein, R.; Harmeling, C.; Perko, T. Toward a Theory of Consumer Digital Trust: Meta-Analytic Evidence of Its Role in the Effectiveness of User-Generated Content. *J. Acad. Mark. Sci.* **2023**, doi:10.1007/s11747-023-00982-y.
35. Neill, G. Digital Trust and Emerging Technologies; KPMG, 2015;
36. Büyüközkan, G.; Havle, C.; Feyzioglu, O. A New Digital Service Quality Model and Its Strategic Analysis in Aviation Industry Using Interval-Valued Intuitionistic Fuzzy AHP. *J. Air Transp. Manage.* **2020**, *86*, doi:10.1016/j.jairtraman.2020.101817.
37. Abraham, C.; Sims, R.; Daultrey, S.; Buff, A.; Fealey, A. March 18 2019,.
38. Aiusheeva, I.; Soyfer, T. FORMATION OF THE ENVIRONMENT OF CONFIDENCE IN SHARING ECONOMY: PROBLEMS OF CIVIL REGULATION IN RUSSIA. *INDEPENDENT JOURNAL OF MANAGEMENT & PRODUCTION* **2022**, *13*, S536–S559, doi:10.14807/ijmp.v13i4.1973.
39. Rychkova, I.; Ghriba, M. Trustworthiness Requirements in Information Systems Design: Lessons Learned from the Blockchain Community. *Complex. Syst. Inform. Model. Q.* **2023**, *2023*, 67–91, doi:10.7250/csimq.2023-35.03.
40. Sharma, V.; Agrawal, R.; Manupati, V. Blockchain Technology as an Enabler for Digital Trust in Supply Chain: Evolution, Issues and Opportunities. *INTERNATIONAL JOURNAL OF SYSTEM ASSURANCE ENGINEERING AND MANAGEMENT* **2024**, doi:10.1007/s13198-024-02471-z.
41. Zolfaghari, A.; Thomas-Francois, K.; Somogyi, S. Consumer Adoption of Digital Grocery Shopping: What Is the Impact of Consumer's Prior-to-Use Knowledge? *Br. Food J.* **2023**, *125*, 1355–1373, doi:10.1108/BFJ-02-2022-0187.

 doi:10.20944/preprints202504.1110.v1




42. Asprion, P.M.; Grieder, H.; Grimberg, F. Building Digital Trust to Protect Whistleblowers - A Blockchain-Based Reporting Channel. In Proceedings of the Proc. Annu. Hawaii Int. Conf. Syst. Sci.; Bui T.X., Ed.; IEEE Computer Society, 2023; Vol. 2023-January, pp. 4328–4337.
43. Kfoury, E.; Khoury, D.; AlSabeh, A.; Gomez, J.; Crichigno, J.; Bou-Harb, E. A Blockchain-Based Method for Decentralizing the ACME Protocol to Enhance Trust in PKI. In Proceedings of the Int. Conf. Telecommun. Signal Process., TSP; Herencsar, N., Ed.; Institute of Electrical and Electronics Engineers Inc., 2020; pp. 461–465.
44. Balci, G. Digitalization in Container Shipping: Do Perception and Satisfaction Regarding Digital Products in a Non-Technology Industry Affect Overall Customer Loyalty? *Technol. Forecast. Soc. Change* **2021**, *172*, doi:10.1016/j.techfore.2021.121016.
45. Svenson, F.; Peuser, M.; Çetin, F.; Aidoo, D.C.; Launer, M.A. Decision-Making Styles and Trust across Farmers and Bankers: Global Survey Results. *Decis. Anal. J.* **2024**, *10*, doi:10.1016/j.dajour.2024.100427.
46. Mohlmann, M. Unjustified Trust Beliefs: Trust Conflation on Sharing Economy Platforms. *Res Policy* **2021**, *50*, doi:10.1016/j.respol.2020.104173.
47. Shipunova, O.; Berezovskaya, I.; Pozdeeva, E.; Evseeva, L.; Barlybayeva, S. Digital Trust Indicators in Human-Computer Interaction. In Proceedings of the Peter the Great St. Petersburg Polytechnic University; Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Eds.; Springer Science and Business Media Deutschland GmbH, 2022; Vol. 468 LNNS, pp. 245–254.
48. Kluiters, L.; Srivastava, M.; Tyll, L. The Impact of Digital Trust on Firm Value and Governance: An Empirical Investigation of US Firms. *Soc. Bus. Rev.* **2023**, *18*, 71–103, doi:10.1108/SBR-07-2021-0119.
49. Ranieri, A.; Di Bernardo, I.; Mele, C. Serving Customers through Chatbots: Positive and Negative Effects on Customer Experience. *Journal of Service Theory and Practice* **2024**, *34*, 191–215, doi:10.1108/JSTP-01-2023-0015.
50. Deprez, J.; Ponsard, C.; Matskanis, N.; IEEE A Goal-Oriented Requirements Analysis for the Collection, Use and Exchange of Electronic Evidence across EU Countries. In Proceedings of the Proc. - IEEE Int. Requir. Eng. Conf. Workshops, REW; Institute of Electrical and Electronics Engineers Inc., 2016; pp. 106–113.
51. Chatterjee, J.; Damle, M.; Aslekar, A. Digital Trust in Industry 4.0 & 5.0: Impact of Frauds. In Proceedings of the Proc. Int. Conf. Intell. Comput. Control Syst., ICICCS; Institute of Electrical and Electronics Engineers Inc., 2023; pp. 922–928.
52. Latvakoski, J.; Kylloenen, V.; Ronkainen, J. Decentralised IOTA-Based Concepts of Digital Trust for Securing Remote Driving in an Urban Environment. *IoT.* **2023**, *4*, 582–609, doi:10.3390/iot4040025.
53. Alsamara, T.; Khalidi, F. Review Of Covid-19 And E-Commerce In The Moroccan Legal System: Challenges And Opportunities. *J. Leg. Ethical Regul. Iss.* **2020**, *23*, 1–9.
54. Soldatova, A.V.; Budrin, A.G.; Budrina, E.V.; Presnova, A.A.; Girsh, L.V. Customer Loyalty Management in the Context of Digital Transformation of Business. In Proceedings of the Proc. IEEE Int. Conf. "Qual. Manag., Transp. Inf. Secur., Inf. Technol.", T QM IS; Shaposhnikov S.O., Saint Petersburg Electrotechnical University "LETI," Prof.P.Str. 5, Saint Petersburg, Eds.; Institute of Electrical and Electronics Engineers Inc., 2021; pp. 907–910.
55. Kayhan, H. Ensuring Trust In Pharmaceutical Supply Chains By Data Protection Through A Design Approach To Blockchains. *Blockchain. Healthc. Today.* **2022**, *5*, doi:10.30953/bhty.v5.232.
56. Piccininni, M.; Rohmann, J.; Logroscino, G.; Kurth, T. Blockchain-Based Innovations for Population-Based Registries for Rare Neurodegenerative Diseases. *Front. Blockchain.* **2020**, *3*, doi:10.3389/fbloc.2020.00020.
57. Jelovac, D.; Ljubojevic, C.; Ljubojevic, L. HPC in Business: The Impact of Corporate Digital Responsibility on Building Digital Trust and Responsible Corporate Digital Governance. *Digit. Poli. Regul. Govern.* **2022**, *24*, 485–497, doi:10.1108/DPRG-11-2020-0164.
58. Kafeza, I. An Intelligent Mediation Platform for Smart Contracts in Blockchain. In Proceedings of the CEUR Workshop Proc.; Cong G., Ramanath M., Eds.; CEUR-WS, 2021; Vol. 3052.
59. Guo, Y. Digital Trust and the Reconstruction of Trust in the Digital Society: An Integrated Model Based on Trust Theory and Expectation Confirmation Theory. *Digit. Gov. Res. Pract.* **2022**, *3*, doi:10.1145/3543860.

 doi:10.20944/preprints202504.1110.v1




60. Gronier, G.; Lambert, M. A Model to Measure the Perceived Quality of Service in eGovernment. In Proceedings of the Proc. European Conf. on e-Gov., ECEG; ODonnell, D., Ed.; 2010; pp. 527–531.
61. Akram, R.; Ko, R. Digital Trust - Trusted Computing and beyond: A Position Paper. In Proceedings of the Proc. - IEEE Int. Conf. Trust, Secur. Priv. Comput. Commun., TrustCom; Institute of Electrical and Electronics Engineers Inc., 2014; pp. 884–892.
62. Khan, W.; Aalsalem, M.; Khan, M.; Arshad, Q. Enabling Consumer Trust Upon Acceptance of IoT Technologies Through Security and Privacy Model. In Proceedings of the Lect. Notes Electr. Eng.; Park, J., Jin, H., Jeong, Y., Khan, M., Eds.; Springer Verlag, 2016; Vol. 393, pp. 111–117.
63. Flew, T. The Crisis of Digital Trust in the Asia-Pacific Commentary. *INTERNATIONAL JOURNAL OF COMMUNICATION* **2019**, *13*, 4738–4750.
64. Rane, T.; Huang, J. Blockchain-Based Digital Trust Mechanism: A Use Case of Cloud Manufacturing of LDS Syringes for COVID-19 Vaccination. *J. Integr. Des. Process Sci.* **2022**, *26*, 103–129, doi:10.3233/JID-210021.
65. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Recommendations for Creating Better Concept Definitions in the Organizational, Behavioral, and Social Sciences. *Organizational Research Methods* **2016**, *19*, 159–203, doi:10.1177/1094428115624965.
66. Sell, J. Definitions and the Development of Theory in Social Psychology. *Soc Psychol Q* **2018**, *81*, 8–22, doi:10.1177/0190272518755335.
67. Colquitt, J.A.; Sabey, T.B.; Rodell, J.B.; Hill, E.T. Content Validation Guidelines: Evaluation Criteria for Definitional Correspondence and Definitional Distinctiveness. *Journal of Applied Psychology* **2019**, *104*, 1243–1265, doi:10.1037/apl0000406.
68. Vidiasova, L.; Tensina, I.; Bershadskaya, E. Cyber-Social Trust in Different Spheres: An Empirical Study in Saint-Petersburg. In *Digital Transformation and Global Society*; Alexandrov, D.A., Boukhanovsky, A.V., Chugunov, A.V., Kabanov, Y., Koltsova, O., Musabirov, I., Eds.; Communications in Computer and Information Science; Springer International Publishing: Cham, 2020; Vol. 1242, pp. 3–13 ISBN 978-3-030-65217-3.
69. Wu, G.; Hu, X.; Wu, Y. Effects of Perceived Interactivity, Perceived Web Assurance and Disposition to Trust on Initial Online Trust. *Journal of Computer-Mediated Communication* **2010**, *16*, 1–26, doi:10.1111/j.1083-6101.2010.01528.x.
70. Facebook Available online: https://www.facebook.com/ (accessed on 21 February 2025).
71. Linkedin Available online: https://www.linkedin.com/ (accessed on 21 February 2025).
72. jamovi The Jamovi Project 2022.
73. Ritter, J. Digital Trust Available online: https://www.techtarget.com/whatis/definition/digital-trust (accessed on 11 March 2024).
74. Orekhova, E. Digital Trust as a Contributor to Development under Uncertainty and Turbulence. *Bulletin of the Saratov State Socio-Economic University* **2020**, *3*, 24–27.
75. Marcial, D.E.; Launer, M.A. Towards the Measurement of Digital Trust in the Workplace: A Proposed Framework. **2019**, doi:10.5281/ZENODO.3595295.
76. Marcial, D.E.; Arcelo, A.; Montemayor, J.; Launer, M. DIGITAL TRUST IN THE ACADEME: PEOPLE, SOFTWARE, AND HARDWARE. *INFORMATION TECHNOLOGIES AND LEARNING TOOLS* **2022**, *89*, 178–189, doi:10.33407/itlt.v89i3.4881.
77. Launer, M.; Çetin, F.; Paliszkiewicz, J. Digital Trust in the Workplace: Testing a New Instrument on a Multicultural Sample. *Forum Scientiae Oeconomia* **2022**, *10*, 29–47, doi:10.23762/FSO_VOL10_NO1_2.
78. Frenehard, T. GRC Tuesdays: Building Digital Trust, What Does It Really Mean? Available online: https://community.sap.com/t5/technology-blogs-by-sap/grc-tuesdays-building-digital-trust-what-does-it-really-mean/ba-p/13412611 (accessed on 11 April 2024).
79. PwC *The Journey to Digital Trust.*; PricewaterhouseCoopers.: London, UK, 2019;
80. Ferraro, C.; Wheeler, M.; Pallant, J.; Wilson, S.; Oldmeadow, J. Not so Trustless after All: Trust in Web3 Technology and Opportunities for Brands. *Bus. Horiz.* **2023**, *66*, 667–678, doi:10.1016/j.bushor.2023.01.007.
81. Bhattacharjee, S.; Gopal, R.D.; Lertwachara, K.; Marsden, J.R. Impact of Legal Threats on Online Music Sharing Activity: An Analysis of Music Industry Legal Actions. *SSRN Journal* **2005**, doi:10.2139/ssrn.816704.

 doi:10.20944/preprints202504.1110.v1




82. Wang, Y.; Han, J.H.; Beynon-Davies, P. Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda. *SCM* **2019**, *24*, 62–84, doi:10.1108/SCM-03-2018-0148.
83. Gangneux, J. Digital Citizenship in a Datafied Society: By Arne Hintz, Lina Dencik and Karin Wahl-Jorgensen, Cambridge, UK, Polity Press, 2019,180 Pp., £15.99 (Hardback), ISBN 9781509527168. *Information, Communication & Society* **2019**, *22*, 2211–2213, doi:10.1080/1369118X.2019.1635186.
84. Li, F.; Betts, S.C. Trust: What It Is And What It Is Not. *IBER* **2003**, *2*, doi:10.19030/iber.v2i7.3825.
85. Accenture *Digital Trust in the IoT Era*; Accenture Consulting, 2015;
86. Mattila, J.; Seppälä, T. Digital Trust, Platforms, and Policy 2016.
87. Goint, M.; Bertelle, C.; Duvallet, C. Establish Trust for Sharing Data for Smart Territories Thanks to Consents Notarized by Blockchain. In Proceedings of the Universite de Rouen Normandie; Prieto, J., Partida, A., Leitao, P., Pinto, A., Eds.; Springer Science and Business Media Deutschland GmbH, 2022; Vol. 320 LNNS, pp. 261–271.
88. Launer, M.; Çetin, F.; Paliszkiewicz, J. Digital Trust in the Workplace: Testing a New Instrument on a Multicultural Sample. *Forum Scientiae Oeconomia* **2022**, *10*, 29–47, doi:10.23762/FSO_VOL10_NO1_2.
89. Sartono, Y.; Siti Astuti, E.; Wilopo, W.; Noerman, T. Sustainable Digital Transformation: Its Impact on Perceived Value and Adoption Intention of Industry 4.0 in Moderating Effects of Uncertainty Avoidance. *F1000 Res.* **2024**, *13*, doi:10.12688/f1000research.152228.1.
90. Gromek, M. Clarifying the Blurry Lines of FinTech: Opening the Pandora's Box of FinTech Categorization. In *The Rise and Development of FinTech Accounts of Disruption from Sweden and Beyond*; Routledge, 2018.
91. Pashkov, P.; Pelykh, V. A Conceptual Framework of Developing Ecosystem Strategies for Digital Financial Services. In Proceedings of the CEUR Workshop Proc.; Telnov Y., Plekhanov Russian University of Economics, A.D. of A.I. and I.S., Stremyanny lane 36, Moscow, Fiodorov I., Plekhanov Russian University of Economics, A.D. of A.I.T. and I.S., Stremyanny lane 36, Moscow, Eds.; CEUR-WS, 2021; Vol. 2919, pp. 48–58.
92. Sundararajan, A. Commentary: The Twilight of Brand and Consumerism? Digital Trust, Cultural Meaning, and the Quest for Connection in the Sharing Economy. *Journal of Marketing* **2019**, *83*, 32–35, doi:10.1177/0022242919868965.
93. Ko, G.; Amankwah-Amoah, J.; Appiah, G.; Larimo, J. Non-Market Strategies and Building Digital Trust in Sharing Economy Platforms. *AIMS Research Publication* **2023**, *2*, 1–10, doi:10.22624/AIMS/CSEAN-SMART2023P3.
94. Fernandes, T.; Oliveira, E. Understanding Consumers' Acceptance of Automated Technologies in Service Encounters: Drivers of Digital Voice Assistants Adoption. *Journal of Business Research* **2021**, *122*, 180–191, doi:10.1016/j.jbusres.2020.08.058.
95. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly* **1989**, *13*, 319, doi:10.2307/249008.
96. Loh, H.; Lee, J.; Gu, Y.; Chen, H.; Tay, H. The Effects of Digital Platforms on Customers' Satisfaction in International Shipping Business. *Rev. Int. Bus. Strategy* **2024**, *34*, 231–244, doi:10.1108/RIBS-07-2023-0072.
97. Huang, J.; Nicol, D.M. Trust Mechanisms for Cloud Computing. *J Cloud Comput Adv Syst Appl* **2013**, *2*, 9, doi:10.1186/2192-113X-2-9.
98. International Telecommunication Union Telecommunication Standardization (ITU-T) Series Y: Global Information Infrastructure, Internet Protocol Aspects, Next-Generation Networks, Internet of Things and Smart Cities; Geneva, Switzerland, 2017;
99. Ting, H.; Kang, X.; Li, T.; Wang, H.; Chu, C. On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study. *IEEE Access* **2021**, *9*, 106743–106783, doi:10.1109/ACCESS.2021.3100767.
100. Bhaskar, C.; Chaturvedi, R.S.; Filipovic, c.; Brewer, G. *Digital Intelligence Index*; The Fletcher School: Medford, 2021;
101. Venter, I.M.; Cranfield, D.J.; Tick, A.; Blignaut, R.J.; Renaud, K.V. 'Lockdown': Digital and Emergency eLearning Technologies—A Student Perspective. *Electronics (Switzerland)* **2022**, *11*, doi:10.3390/electronics11182941.

 doi:10.20944/preprints202504.1110.v1




102. Akbari, M.; Rezvani, A.; Shahriari, E.; Zúñiga, M.Á.; Pouladian, H. Acceptance of 5 G Technology: Mediation Role of Trust and Concentration. *Journal of Engineering and Technology Management* **2020**, *57*, 101585, doi:10.1016/j.jengtecman.2020.101585.
103. Corsaro, D.; D'Amico, V. How the Digital Transformation from COVID-19 Affected the Relational Approaches in B2B. *J. Bus. Ind. Mark.* **2022**, *37*, 2095–2115, doi:10.1108/JBIM-05-2021-0266.
104. Gefen; Karahanna; Straub Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly* **2003**, *27*, 51, doi:10.2307/30036519.
105. Thomas-Francois, K.; Somogyi, S.; Zolfaghari, A. The Cultural Acceptance of Digital Food Shopping: Conceptualisation, Scale Development and Validation. *Int. J. Retail Disrtib. Manage.* **2023**, *51*, 306–326, doi:10.1108/IJRDM-11-2021-0552.