Implications of trust in digital business ecosystem design: A systematic analysis of roles

Irina Rychkova[1], Jelena Zdravkovic[2] and Janis Stirna[2]

[1] University Paris 1 - Panthéon-Sorbonne, Paris, 75005, France
[2] Stockholm University, Kista, SE-16407, Sweden

Abstract

Digital technologies enable novel models of social and business interactions, where trust becomes a critical design consideration. A thorough analysis of trust issues and their implications at different enterprise levels, including strategies, processes and technological solutions, becomes an imperative part of socio-technical systems design. In this study we examine trust issues that emerge among the actors of a Digital Business Ecosystems (DBE) which, if not properly addressed, can jeopardize DBE functioning and resilience. An explicit mapping between the generic DBE roles and the social factors of trustworthiness is the main contribution of this work. We demonstrate how this mapping is used in the analysis of trust issues in the context of a Higher Education Alliance DBE. This analysis leads to the identification of explicit trustworthiness requirements that can guide (re)design of DBE strategies, processes and technical platforms.

Keywords

Enterprise Design, Trust, Trustworthiness requirements, Business Network Modeling, Digital Business Ecosystem, DBE Roles

1. Introduction

Business ecosystem refers to the interconnected business network of organizations and individuals that interact with and influence each other within a particular industry or market. It encompasses the complex web of relationships, resources, and interactions among various entities that collectively contribute to the functioning and success of the overall business environment. With the digital transformation and the increasing role of digital technologies in social interactions, the concept of digital business ecosystem (DBE) has emerged. In a DBE, entities interact and collaborate using digital technologies, and leverage data and information as key assets [1, 2].

DBEs are characterized by their dynamic and rapidly evolving nature. They require effective governance mechanisms to ensure fairness, trust, and accountability among the participants. Governance involves setting common rules, standards, and protocols for data exchange, resource sharing, and collaboration, as well as resolving conflicts, ensuring compliance, and managing risks within the DBE. A key aspect of DBEs is the diversity of actors and the roles they fulfill: in addition to the roles acting in traditional business networks, such as supplier, customer, and end user, DBEs rely in addition on some specific ones, such as for example - the *driver* role, for managing the tools that support the DBE; a *governor,* for providing and/or defining the standards and policies; a *reputation guardian* - for assessing all DBE actors' trustworthiness, reliability, solvency, and worthiness; as well as several other roles [3].

In DBE digital technology ("D") acts as a mediator in interactions between the ecosystem participants, with the expectation of increasing trust between them and for providing them with a positive experience [4]. Trust plays a crucial role in the functioning of a DBE, for its resilience. It

Companion Proceedings of the 16th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling and the 13th Enterprise Design and Engineering Working Conference, November 28 – December 1, 2023, Vienna, Austria
irina.rychkova@univ-paris1.fr (I. Rychkova); jelenaz@dsv.su.se (J. Zdravkovic); js@dsv.su.se (J. Stirna)
0000-0002-1100-0116 (I. Rychkova); 0000-0002-0870-0330 (J. Zdravkovic); 0000-0002-3669-832X (J. Stirna)

provides the foundation upon which participants collaborate and share resources and as such it is a critical design consideration for the DBE supporting digital platforms. Identifying, modeling and analyzing trust relations among social and technical DBE entities is a vital design step, which requires adequate Enterprise Modeling methods and practices. Explicit analysis of trust issues in a DBE has an impact on the DBE *strategy*, as it can be used to identify partners and their needs in terms of trust; on the DBE *operations* as it can affect the processes between DBE partners; and on the DBE *technology*, as it can help to design relevant components and to make technological choices.

In social science, trust is described as a situation in which an individual or an organization (trustor) is willing to rely on the chosen actions of another individual or organization (trustee) [5]. According to Mayer et al. [6], ability, benevolence, and integrity are the factors of (perceived) trustworthiness that characterize a trustee. In the technical domain, trust defines relationships between an individual and a technological component (trust in technology) and describes the interactions between the entities in the digital world (digital trust). Here the (perceived) trustworthiness is often connotated with security, reliability, and authenticity of digital systems, platforms, or transactions.

The gap between the social and technical definitions of trust arises due to the challenges of translating a subjective, context-dependent nature of social trust into objective, measurable terms that can be addressed by technical mechanisms. While technical (or digital) trust can provide 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.

DBEs are inherently socio-technical systems, and addressing trust in DBE requires a holistic approach that integrates both social and technical dimensions of trust. Bridging the gap between these dimensions involves recognizing the interplay between different types of trust, understanding the subjective and contextual nature of trust issues, and leveraging both social and technical mechanisms to foster trust in DBEs. The goal of this work is to explicitly address trust and its implications in DBE design.

In this paper, we examine the roles of DBE and discuss their trust relationships. First, we associate the DBE roles with social trustworthiness factors. To bridge the gap between the social and technical dimensions of trust, we propose a mapping of (social) trust issues into trustworthiness requirements (TwR) that can guide DBE design. We define trustworthiness requirements as the expectations of one actor (trustor) about trustworthiness of another actor (trustee) in a DBE. We demonstrate our findings with a case study of European universities forming a higher-education (HE) alliance, which fulfills the main criteria for being considered a DBE. We examine the trust building process among the actors of this DBE, focusing on the implications on the supporting information systems. We formulate the following research questions:

- RQ1: What are the social factors of trust defining relationships among DBE actors?
- RQ2: What are the trustworthiness requirements that guide the design and development of a DBE and its supporting systems for the case of a HE alliance?

In order to formulate the TwR for a particular role in the HE alliance DBE, first, we analyze the trust issues expressed by a corresponding DBE participant and their (social) trust factors, then we use a reference list of TwR derived from the literature [7] and identify relevant generic requirements. Finally, we illustrate how these generic requirements can be contextualized for the HE alliance. The proposed approach bridges the gap between the social and technical dimensions of trust and supports business and technology experts in guiding their design decisions and technological choices.

The remainder of this article is organized as follows: in section 2, we discuss the background of this study and its related works; in section 3, we provide a mapping of the generic DBE roles on the trustworthiness factors defined in social science. We also describe our approach for trustworthiness requirements elicitation. In section 4 we present our findings on the case study of higher-education alliance. In section 5 we discuss our results and provide our conclusions.

2. Background and related work

2.1. Trust

In the research literature on trust, the act of trust is represented as a relationship between a subject (the trustor) and an object of trust (the trustee) [5, 6, 8]. 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) [6, 8, 9]. 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 of the trustee as a design variable.

Whereas researchers in social sciences focus on trust between social entities (individuals, groups or organizations), in IS research, trust is considered as a socio-technical concept, i.e., it is defined as a relationship between social entities and technological components (information systems, applications, infrastructure, etc.), in which a technological component can be either an object (trustee) or a subject (trustor).

In modern organizations, social trust remains an important determinant of collaboration and decision making. With a constant digital transformation, trust issues that occur among social actors on the strategic and operational levels of the organizations are often addressed by socio-technical solutions developed by the IT, creating a gap between the social and technology-centric perspectives of trust. 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 [4]. 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 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 [5]. 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 [10]. Trust in technology reflects the trustor's beliefs that a specific technology has the attributes necessary to perform as expected in a given situation where negative consequences are possible [8, 11]. Table 1 presents a summary of these three types of trust, their associated trustworthiness factors and outcomes.

Table 1
Overview of trust perspectives and types

View:	Type of Trust	Trustor (subject)	Trustee (object)	Trustworthiness factors	Outcome
Social	Social Trust	Org. / Individual	Org. / Individual	Ability, benevolence, integrity	Interaction / collaboration
Technical	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 environnement
		IT object	Org. / Individual		

		IT object	IT object		

2.1.1. Trust: Social perspective

It addresses the (social) context where the trust issues among the actors arise. [6] defines trust antecedents and outcomes in their integrative model of organizational trust. 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." Propensity to trust is an intrinsic characteristic of a trustor, which can be considered as invariant. Ability, integrity and benevolence are the factors of trustworthiness that characterize a trustee; they depend on the context and the nature of a given trustor-trustee interaction. According to [6], *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 and his/her willingness to adhere to some rules and principles. Social trust is used as the basis for decision-making in diverse contexts, including enterprise strategy, governance of operations, and technology [12].

2.1.2. Trust: Technical perspective

Digital trust and trust in technology define trust in the technological domain. The trustworthiness factors of technology include usability, functionality, helpfulness, reliability and credibility of information [8, 11], as well as customizability and adaptability [4]. Digital trust reflects the trustor's beliefs that a trustee (a social entity or an IT object) has the attributes necessary to support secured digital interactions [10]. Trustworthiness factors in digital trust include privacy, security, transparency, traceability, control [13, 14].

2.1.3. Bridging the gap between the social and technical views on trust

While trustworthiness factors of digital trust and trust in technology can be formalized, measured and used to provide a foundation for technological solutions, they may not fully capture the complexities of social trust that arise from human relationships, emotions, and cultural factors. Thus, an explicit mapping between technological and social perspectives of trust is of great importance.

Requirements engineering (RE) discipline plays a crucial role in design and development of socio-technical systems. The RE process involves understanding the stakeholders' needs and expectations, as well as the social and organizational context in which the system will operate [15, 16]. We address trustworthiness of the trustee in socio-technical systems from the RE perspective. Here, trustor's expectations regarding the trustee's trustworthiness can be expressed as *trustworthiness requirements (TwR)*. We define TwR as a statement made by a trustor about the expected trustworthiness of a trustee. A TwR has to clearly express an operational, functional, design or other characteristic, which, according to trustor's beliefs, positively impacts trustworthiness of this trustee and interaction between the two. TwR can be met by incorporating certain attributes, features, or properties by the trustee, whether a social entity or a technological solution. TwR can be eventually refined into conventional FR, NFR, process requirements or contracts. The interest in requirements related to trust is not new: in [16], trust is considered as a part of soft requirements (SR) and is associated with the aspects of the social system where a technological system is used – its context; in [17], trustworthiness requirements are defined as a special class of quality requirements and relate trust with other concepts such as capability, vulnerability and risk; in [22], the role of trustworthiness in the software development lifecycle is examined and a process for elicitation and analysis of TwR is proposed. The work presented in [21] explicitly addresses TwR in supply chain management.

In this study, we examine the social trustworthiness factors that define interactions among DBE actors. First, we provide a mapping between these factors and generic DBE roles. Then, using the case

study, we illustrate how the trustworthiness factors of the trustee in a DBE can be addressed by the TwRs. As a result, we identify requirements that need to be met by the DBE roles and their supporting digital solutions, providing guidance for DBE design and evolution.

2.2. Digital business ecosystems (DBE) and roles in DBE

Actors, roles, capabilities, relationships, and digital components are essential elements of DBE [3]. The actors are individuals and organizations that take part in a DBE by fulfilling specific roles according to their capabilities. The interactions between the DBE actors are supported and mediated by different digital components such as the ecosystem digital platform and its services, smart devices, cloud storage, and other.

Roles of archetypal kind are of a high significance for the ecosystem's design as they define the DBE-specific responsibilities of the actors involved and provide underlying knowledge for the capabilities relevant to a DBE. In [3], the authors surveyed the relevant literature to identify the DBE roles and their responsibilities, leading to the following ones (Table 2).

Table 2
DBE roles and their responsibilities [3]

DBE role	Responsibility
Driver	sets up a common vision for all actors in a DBE; provides and manages a digital platform; optimizes entry barriers for joining a DBE; acquires and retain actors within a DBE; provides end-products and services to customers and end-users; collects and raise end users' events and feedback; ensures an integrated end user experience.
Aggregator	collects and combines capabilities and resources within a DBE into end-products or services, created by Modular Producer and Complementor, for offering to Customers and End-Users.
Modular Producer	provides resources within a DBE; resources can be products, services, or knowledge, created by the producer's capabilities.
Comple-mentor	using its capabilities, provides resources that complement the core resources within a DBE, with some added-value features.
Customer	buys end-products and services offered in a DBE.
End-User	consumes end-products and services offered in a DBE; provides information about its events and feedback to other DBE roles.
Governor	oversees all the actors within a DBE by defining normative artifacts, such as decisions, policies, guidelines, and ethics, related to the business concern of the DBE.
Reputation Guardian	surveys and assesses all DBE actors' trustworthiness, reliability, solvency, and worthiness.

3. Analysis of trust issues and identification of trustworthiness requirements in DBE

3.1. Research approach

This study follows the Design Science Research [18] and aims at developing a framework for the trust management in DBE types of business networks – the targeted design artifact. The need for managing trust and hence for this design artefact is expressed in [3, 19], where trust is identified as one of the important aspects of DBE design. This study paves the ground for developing the trust management framework for DBE. In this article, we report on the initial cycle of artifact design, which includes the problem identification and the framework components design and development. The theoretical view on the problem was presented in [7]; this paper is grounded on the case study and focuses on the empirical view of the problem.

We conduct a structured analysis of the archetype DBE roles and identify the trustworthiness factors that determine the interactions between these roles. The resulting mapping (Table 3) is one of the framework components developed in this study. Following the identified trustworthiness factors, we proceed with identification of trustworthiness requirements (TwR) that can be further operationalized (i.e., implemented as a part of an interactive process or a supporting information system between the corresponding DBE roles). To this end, we propose and follow a process for trust analysis (Section 3.3). This process takes trust issues expressed by the specific DBE actors as an input and leads to identification of their corresponding TwR. To support the trust analysis, we use a set of generic TwR from [7].

We demonstrate the designed artifact by examining trust in the Higher-Education Alliance DBE – our case study (Section 4). In this article, we provide the results of trust analysis for the Modular Producer role in this DBE. In particular, we show the trust issues (collected from the case), trustworthiness factors (application of our mapping), generic TwR (from [7]) and specific (contextualized) TwR defined for this role. Completeness of the elaborated set of requirements as well as their prioritization are not discussed in this study. This will be addressed during the following (validation) cycle of DSR.

3.2. Trustworthiness factors in DBE

In DBE, trust relationships are formed among their participants (social entities) and can be characterized by the following: (i) several entities can share the same DBE role and each entity can fulfill several DBE roles; (ii) within different interactions, each DBE role can be considered as a trustor (one who trusts) or as a trustee (one to be trusted).

Following [6], ability, integrity, and benevolence are the factors of trustworthiness that influence a decision of one DBE role (trustor) to engage into an interaction with another DBE role (trustee). The impact of ability, integrity, and benevolence on building trust can vary depending on the context of this interaction. More specifically, consider a situation 1, where the two individuals X and Y are respectively a patient (trustor) and a physician (trustee), and a situation 2, where the same X and Y are playing cards together: in situation 1, the Y's ability (i.e., medical proficiency and qualification) can be a major trustworthiness factor for X, whereas in situation 2, it will be rather Y's integrity (honesty, compliance with the rules). Based on that, the third characteristic of trust relationships in DBE is: (iii) Trustworthiness factors defined by a trustor for a trustee within an interaction in DBE depend on the context of this interaction and on the DBE roles they play within this interaction (as defined in Table 2).

Table 3
Social trustworthiness factors in the relationships to the DBE roles

		Trustors (subject)							
		Driver	Aggregator	Modular Producer	Complementor	Customer	End User	Governor	Reputation Guardian
Trustee (object)	Driver	A B, I	A	A, B, I	A	A	A, I	A, I	A, B, I
	Aggregator	A, I	I	A, I	A, I	A, I	A	A, I	A, B, I
	Modular Producer	A, I	A	I	A, I	A	A	A, I	A, B, I
	Complementor	A, I	A	A, I	n/a	A	A, I, B	A, I	A, B, I
	Customer	I	I	I	I	I	I	I	I
	End User	n/a	n/a	n/a	A, I	n/a	n/a	A, I	I
	Governor	I, B	I, B	I, B	I, B	I, B	I, B	A, B, I	A, B, I
	Reputation Guardian	B	B	B	B	I, B	B	A, I	n/a

Based on our previous studies on DBEs [3, 19, 20], we analyze trustor-trustee relationships between different DBE roles and identify the major social trustworthiness factors in trust building between these roles. The results are illustrated in Table 3. Each cell {i,j} defines a trustworthiness factor (or factors) for an interaction between the two DBE roles: role i (as a trustor) and role j (as a trustee). For example, the third column of the table defines the trustworthiness factors for a DBE Modular producer (MP) role towards the other roles in the DBE with which the MP interacts as a *trustor*.

The MP (trustor) - Driver (trustee) interaction in DBE is important to ensure consistent development and evolution of a service or product provided by the DBE. A, B, I in the cell {3,1} indicate that all the three factors – ability, benevolence and integrity - need to be considered when designing processes and digital platforms supporting and mediating their interactions.

Trustworthiness factors in MP – Aggregator and MP - Complementor interactions (cells {3,2}{3,4} in Table 3) include ability (A) (e.g., skills/competences of an aggregator to collect and combine capabilities and resources within a DBE) and integrity (I) (e.g., aggregator's honesty, capacity to adhere to the rules defined by DBE).

Integrity (I) is the major factor in MP – MP and MP - Customer interactions (cells {3,3}{3,5} in Table 3). Here, integrity of MP refers to their perceived honesty in delivering a high-quality service/product. Customers' integrity refers to their perceived honesty and compliance with the rules.

Trustworthiness factors in MP - Governor interactions include benevolence (B) and integrity (I). This is related to the responsibility of the governor as a trustee, which is to oversee all the actors within a DBE (Table 2).

Benevolence (B) is the major factor in MP - Reputation guardian interactions. The responsibility of the reputation guardian as a trustee is to survey and assess all DBE actors (see Table 2) and benevolence (e.g., a belief that this evaluation will be fair) provides a major contribution in building trust in these interactions.

Trustworthiness factors are not applicable to MP (trustor) - End user (trustee) interactions (indicated n/a in the cell {3,6}) since, by definition, MP role in DBE does not "rely on" or "become vulnerable from" the End user. Note that the opposite is not true: End user as a trustee has to trust the MP's ability to produce a competitive, relevant service or product. This is reflected by the ability

(A) trustworthiness factor in Table 3 (cell {6,3}). The rest of the table can be interpreted the similar way.

3.3. Analysis of trust in DBE

Table 3 maps the trustworthiness factors on DBE roles and identifies the major social factors of trust in the interactions among DBE partners. To support digital interactions between DBE partners, these factors need to be contextualized and refined into specific TwRs. We propose the following process for trust analysis in DBEs.

Consider an interaction between two specific DBE actors and the roles they play in this interaction:

1. Identify trust issue(s) of a trustor actor. This step is context-specific and can vary for different partners in the DBE. The working approach can be: empirical analysis of DBE design and operations or interviews with stakeholders.
2. Identify the trustworthiness factors of the trustee role related to this issue. This step is context-independent and defined for generic roles in DBE, c.f. Table 3.
3. Formulate TwR that express trustor's expectations about trustee's (social) trustworthiness factors from step 2 by using (technical) trustworthiness properties (i.e., system or process qualities). This step can be considered as a context design. Here we are working with engineers of the DBE to analyze the existing DBE design. The requirements can be extracted from this context or identified using a more generic reference list, derived from the previous experiences or from the literature.
4. Contextualize the TwRs by associating them with the trust issues identified in step 1. In this step, we are focusing on specific requirements of actors and the DBE as a whole. Here, the TwRs from step 3 are refined following the interviews with the actors' representatives and analysis of the usage data.

The expected outcome of this process is a set of explicit, contextualized TwRs that provide a reference to the social context and identify an operational, functional, design or other characteristic, which, according to trustor's beliefs, positively impacts the trustworthiness of this trustee and interaction between the two. In the following section we illustrate this process with the case study of Higher-Education Alliance DBE.

4. Case study: Higher-Education Alliance

4.1. About alliances in Europe

During the past decade a plethora of university alliances in the domain of higher education have emerged, with more than 40 of such alliances in Europe. Some alliances focus mainly on student mobility (e.g., Erasmus+), while others are aiming at a united Europe university both in terms of teaching and research (e.g., CIVIS, 4EU+, Una Europa). The latter type is featured in our case study (by the active participation of the authors in one of the outlined alliances). Through their activities and collaboration, these alliances strive to actively promote fundamental rights, solidarity, democracy, social cohesion, cultural diversity, and active citizenship. Therefore, the business foundation of the HE alliances could be condensed into the following knowledge square: Education, Research, Innovation and Civic Engagement. The alliances are typically co-funded by the EU Commission and the member universities.

HE alliances perform and coordinate an extensive number and variety of activities including development of educational programs and modules at Bachelor's, Master's and PhD levels; student, teacher, and researcher mobility; educational and scientific calls and events; thematic working nodes, theme-labs, promotion-related activities, governance, management of the digital infrastructure.

4.2. The roles and responsibilities of the DBE participants

HE alliances conform to the concept of DBE, because they consist of a large number of independent and self-organizing actors collaborating on various business objectives on a DBE level as well as individually. A key aspect of DBEs is actors acting in complementary roles, which is essential to maintain DBE's long-term resilience. Table 4 shows the mapping of the common actors of an HE alliance to their corresponding DBE roles and responsibilities.

Table 4
Actors and roles in the DBE of HE alliance

Actor	Description	Role in DBE	Responsibility in DBE
European Commission	The financier of an alliance.	Governor, Reputation Guardian	To control the use of fundings, monitoring of the progress, alliance promoter in EU forum
University	Alliance member, from a European university	Driver	Each university member leads one responsibility (Table 2, Driver), or all are responsible for some
Faculty teacher, researcher	Academic staff of the participating universities	Modular Producer	To develop and teach course curriculum
Node	Thematic entity	Aggregator	To propose course curriculum, assign tasks to modular producers and monitor development.
Lab	Forum for universities, businesses, citizens to meet	Complemen ntor	To organize events (conferences, seminars), present curriculum, etc.
Steering Committee	Administrative staff of participating universities.	Governor	To make decisions on operative levels, to coordinate communications and tasks of the universities.
Consultative Council	City and regional representatives, citizens, and the presidents of the member universities	Governor	To make cooperation decisions that would be applied across the participating regions
Student Council	A group of student representatives from different university members	Governor	To collect and disseminate student voices for the best interests of students: it listens, exchanges and proposes ideas on how the alliance should develop.
Student	A person registered for studying at a member university	End-User	To attend campus and online courses, take examinations, to do course evaluation

Student Ambassador	First-contact student(s) at every member university.	Reputation Guardian	To provide information about the alliance to potentially interested students.
Business member	Regional organizations and companies	Customer	To sponsor and attend some events of the alliance, provide guest lectures, etc.
Citizen	Regional citizens	Customer	To support co-creation of knowledge related to the curriculum content, collaboration with business, and other.
Communication Office	The alliance representative office in EC	Reputation Guardian	To encourage the participation of all stakeholders in building the envisioned university model.

4.3. Trust analysis for the Educational Alliance

In this section, we provide the trust analysis for the Modular Producer role (a faculty teacher or researcher) in a HE Alliance DBE. For the sake of brevity, we do not provide the analysis for the other roles in this paper.

Following the process of trust analysis (Section 3.3), we illustrate (1) the trust issues identified in the interactions between Modular producer (as trustor) and other roles in the HE alliance DBE (trustees) and (2) provide their mapping to the trustworthiness factors of DBE roles from Table 3. Next, in (3), we use the taxonomy proposed in [7] as a reference to formulate our TwR about the trustworthiness factors identified in (2). This taxonomy associates ability, integrity and benevolence with 21 TwRs derived from the literature. Finally, in (4), we contextualize the identified TwRs for the MP in the HE alliance. The summary of this analysis is presented in Table 5.

Modular producers (MP) in the HE alliance are members of teaching and research staff responsible for creating content for educational programs (course materials, practical works, projects etc.) and delivering the program to the end users. When creating common courses, one of the challenges is to ensure alignment, consistency, and uniform quality of the course modules among different MPs. Therefore, an issue expressed by a trustor-MP towards the other MPs (trustees) is:

1. *I am concerned with the quality of modules provided by other modular producers.* This issue is associated with integrity (I) of the MP role as a trustee in Table 3.

Another challenge is related to aggregation, dissemination and reuse of developed materials within common space, which are ensured by Aggregator (a node) as a trustee:

2. *I am worried that the development of a common course will not follow the established milestones and deadlines.* This issue is associated with integrity (I) and ability (A) of the Aggregator role in Table 3;
3. *I want to make sure the aggregator will not put me in competition with another modular producers* - associated with integrity (I);
4. *I am concerned that, within a common course, my content can be used or modified without my knowledge* - associated with integrity (I);
5. *I am concerned about the integration efforts and evolution of my content: upload, update, formatting should be ensured by the aggregator* - associated with ability.

Once the program is developed, MPs are also concerned with its running. The following example illustrates the trust concerns towards Driver (a university) as a trustee:

6. *I am concerned that the digital platform for course provisioning and communication with students will work without errors* - associated with the trustee's ability (A).

Towards Complementor (a lab, a third-party technology provider for) as a trustee:

7. *I am concerned with the quality of supporting services and their price (e.g., Virtual classrooms, examination tools) delivered by the complementor* - associated with the trustee's ability (A).

Towards Reputation Guardian (communication office in HE alliance):

8. *I am concerned that a fair number of students, with adequate background and academic records will be attending the course* - associated with benevolence (B) of a Reputation guardian.

Once the issues are identified (column 1 in Table 5) and associated with the trustworthiness factors (column 2 in Table 5), we formulate the TwR of the MP (as a trustor) towards the DBE (column 3 in Table 5). In [7], a taxonomy of TwR is proposed. This taxonomy associates the (social) trustworthiness factors with technical features of solutions. We use the TwR from this source as a reference. For example, issue 1 can be associated with Auditability TwR. Once relevant TwR are identified, they need to be contextualized (column 4, in Table 5). For issue 1, we propose the following contextualization of the Auditability TwR: *Any faculty teacher in the node must be able to validate the quality of the class materials produced by their peers. Every faculty teacher has to demonstrate the quality of the produced course materials.*

Note that the issues can vary among the actors playing the same DBE role (e.g., different teachers in HE alliance); they can also be shared between the roles in the DBE (e.g., issue 2 is shared by the MP and the driver role).

The process above needs to be conducted for all DBE participants to collect the list of issues and requirements for each relevant trustor-trustee interaction in the DBE.

Table 5
Trust analysis for HE Alliance Modular producers.

	(2)	(3) TwR of reference	(4) Contextualized TwR of reference
1	I	*Auditability*: Trustor must be able to validate the trustee's compliance with the rules (e.g., by executing the audit, supervising the examining the execution traces, supervising the trustee's process at run time).	Any *faculty teacher* (Modular Producer) in the *node* must be able to validate the quality of the class materials produced by their peers: fit to the program, alignment between the modules, etc. Every *faculty teacher* should be able to demonstrate the quality of the produced course materials.
2	A, I	*Performance:* Trustee must ensure an efficient distribution of resources, with respect of defined timeframe and budget. *Compliance:* Trustee has to adhere to rules, agreements or regulations.	*A node* (Aggregator) creates the educational programs, with respect to the program calendar and budget set by *the steering committee* (Governor). *A node* acts according to the rules defined by *the steering committee* (Governor) and uses the standard solutions (e.g., digital

		Integrity: Trustee must ensure correct and timely execution of activities, with respect to contract or process specifications.	portal) delivered by *a leading university* (Driver). *A node* demonstrates the program evolution to *the steering committee* and informs the *students* and *faculty teachers* about problems.
3	I	*Traceability:* Trustor has to access all information related to provenance of a physical or information object accurately and trace it to its source.	*Faculty teacher* and *faculty researcher* has to be able to access all the information related to other modular producers and to trace the produced content.
4	I	*Transparency:* Trustee's workflow must be transparent and documented. Trustee must provide an accessible and non-repudiable audit trail showing use, change and viewing of the data. *Integrity (data):* Trustee must ensure the accuracy, completeness, and consistency of data over its entire life-cycle.	A *node's* course development plan (e.g., workflow) must be transparent to the *faculty teachers* and explicitly documented. A *node* must ensure the overall accuracy, completeness, and consistency of produced content over its entire life-cycle.
5	A	*Automation of data processing*: Trustee must minimize physical and maximize digital processing of data. *Interoperability*: Trustee must show a capability to work with trustor.	A *node* must minimize physical and maximize digital processing of course materials and to enable *students* (End-User) to access it remotely. A *node* must be able to process, store and correctly integrate any numeric content from the faculty teachers.
6	A	*Availability:* All resources and software components needed for process/activity execution have to be available to the trustor, by the trustee.	Digital platform for student and course management has to be available to *students* and *faculty teachers*. The content must be accessible which is ensured by the designated *university* (Driver).
7	A	*Availability:* All resources and software components needed for process/activity execution have to be available to the trustor. *Performance:* Trustee must ensure an efficient distribution of resources, with respect of defined timeframe and budget.	All resources and software components needed for the course have to be available by the digital platform through *a university*, to *faculty teachers*. *Lab* (Complementor) must ensure an efficient distribution of resources, with respect to defined timeframe and budget.
8	B	*Accountability:* Trustee is held responsible for her actions and cannot deny them. *Authentication (data):* Trustor must be able to determine the correctness and reliability of reported data (e.g., messages, events).	*Steering committee* is responsible for her actions in marketing, dissemination of the calls and student inscription to the program. *Faculty teachers* must be able to determine the correctness and reliability of reported data (e.g.,

			application/admission ratio, information on the students).

5. Discussion and conclusions

Trust is a critical enabler of business interactions facilitating effective collaboration, efficient resource utilization, adaptive behaviors, and collective effort towards common goals. Business networks, as inherently socio-technical systems, require a holistic approach for trust analysis that integrates its social and technical dimensions. This study attempts to bridge the gap between these dimensions by incorporating the subjective and contextual nature of trust in DBE designs and management principles. Identification and analysis of trust issues among the participants of a DBE is a crucial task with a great impact on the DBE sustainability and resilience; it must be conducted upfront and it requires adequate enterprise modeling methods and practices.

In this work, we proposed a framework for structured analysis of trust among the actors of DBE. We focused on the implications on the supporting digital platforms pervading any business interaction in a DBE setting. We consider that the proposed framework can be used to support (re)design of DBE and its supporting digital platforms as follows:

- A list of requirements aggregated per Trustee-role provides a vision of what the DBE expects from this given role.
- A list of requirements aggregated per Trustor-role provides a vision of what this particular role expects from the DBE.
- Prioritization of the TwRs by identifying the TwRs most frequently expressed.
- Negotiation of the TwRs and identification of the minimal set of TwRs that will be satisfactory for a particular DBE.
- Identification and assessment of alternative organizational and technical solutions to cover the set of TwRs.

The study is a part of an overall Design Science Research project aiming to develop and implement the models and methods for resilient DBE. Within this project, we are defining the artifacts needed for incorporating the trust aspect into the DBE design: the identification and mapping of the social trustworthiness factors on the DBE roles, and a process for trust analysis serving for deriving TwRs specific to the ecosystem in design. The proposed artifacts were demonstrated to validate their usability on the case of HE alliance - a typical example of a DBE, with its high autonomy, self-organization, and cost balance principles. Concerning limitations to this study, we have performed only the initial cycle of development – the problem has been analyzed in sufficient detail to establish requirements for the artifact and its initial version has been developed and validated in an artificial setting with real life case. While this gives input to assess the validity of the artefact in broad terms, systematic evaluation in naturalistic setting is also needed.

The immediate next work will comprise further refinement of the framework and experimentation, for example., on other DBEs, to assess possible improvements for the purpose of evaluation of the framework in artificial setting which is to be followed by improvements to the framework and the guidelines for use in order to integrate the framework with a method for DBE design [23].

References

[1] Nachira, F., Dini, P., Nicolai, A.: A network of digital business ecosystems for Europe: roots, processes and perspectives. In: Nachira, F., Nicolai, A., Dini, P., Le Louarn, M., Rivera Leon, L. (eds.): Digital Business Ecosystems (pp. 1,Äí20). European Commission, Bruxelles (2007).

[2] Senyo, P.K., Liu, K., Effah, J.: Digital business ecosystem: Literature review and a framework for future research. International Journal of Information Management, 47, 52,Äí64 (2019).

[3] Tsai, C.H., Zdravkovic, J.: A Survey of Roles and Responsibilities in Digital Business Ecosystems. In: Serral, E., Stirna, J. (eds.) PoEM-Forum 2020: Proceedings of the Forum at Practice of Enterprise Modeling 2020, CEUR -WS.org (2020).

[4] Sutcliffe, A. Trust: From cognition to conceptual models and design, in LNCS, Springer, pp. 3–17. (2006)

[5] Gambetta, D.: Trust: Making and Breaking Cooperative Relations. The British Journal of Sociology. 13. 10.2307/591021. (2000).

[6] Mayer, R.C., Davis, J.H. and Schoorman, F.D.: An Integrative Model of Organizational Trust, Academy of Management Review, 20(3), pp. 709–734. (1995)

[7] Rychkova, I., Ghriba, M. (2023). Trustworthiness Requirements in Information Systems Design: Lessons Learned from the Blockchain Community. *Complex Systems Informatics and Modeling Quarterly*, (35), 67-91.

[8] Mcknight, D.H. et al.: Trust in a specific technology: An investigation of its components and measures, ACM Transactions on Management Information Systems, 2(2). (2011)

[9] Rousseau, D.M. et al. Not so different after all: A cross-discipline view of trust, Academy of Management Review, 23(3), pp. 393–404. (1998)

[10] Pietrzak, P. and Takala, J. Digital trust–a systematic literature review, In Forum Scientiae OeconomiaSep, 9(3), p. 30. (2021)

[11] Meeßen, S.M., Thielsch, M.T. and Hertel, G. Trust in Management Information Systems (MIS): A Theoretical Model, Zeitschrift fur Arbeits- und Organisationspsychologie, 64(1), pp. 6–16. (2020)

[12] Cho, J.H., Chan, K. and Adali, S. A Survey on Trust Modeling, ACM Computing Surveys, 48(2), p. 2. (2015)

[13] Mattila, J. and Seppälä, T.: Digital Trust, Platforms, and Policy, ETLA Brief, 7, p. 42. (2016)

[14] Belotti, M. et al. A Vademecum on Blockchain Technologies: When, Which, and How, IEEE Communications Surveys and Tutorials, 21(4), pp. 3796–3838. (2019)

[15] ISO/IEC: ISO/IEC 25010:2011 - Systems and software engineering – Systems and software Quality Requirements and Evaluation– System and software quality models. (2011)

[16] Sutcliffe, A., Sawyer, P. and Bencomo, N. The Implications of "Soft'' Requirements", in the 30th International Requirements Engineering Conference (RE). IEEE, (2022)

[17] Amaral, G. et al. Ontology-Based Modeling and Analysis of Trustworthiness Requirements: Preliminary Results, 12400 LNCS, pp. 342–352. (2020)

[18] Hevner, A., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. Management Information Systems Quarterly, 28(1), 75-105 (2004).

[19] Tsai, C.H., Zdravkovic, J., Stirna, J.: Requirements for a Digital Business Ecosystem Modelling Method: An Interview Study with Experts and Practitioners. In: proc. of BIR'2021, LNBIP, vol. 430, pp. 236, 252. Springer (2021)

[20] Tsai, C. H., Zdravkovic, J., Söder, F.: A method for digital business ecosystem design: situational method engineering in an action research project. Software and Systems Modeling, doi:10.1007/s10270-022-01068-z (2022)

[21] Kambilo, E., Rychkova, I., Herbaut, N., & Souveyet, C.: Addressing Trust Issues in Supply-Chain Management Systems Through Blockchain Software Patterns. In Research Challenges in Information Science: Information Science and the Connected World: 17th International

Conference, RCIS 2023, Corfu, Greece, May 23–26, 2023, Proceedings (pp. 275-290). Cham: Springer Nature Switzerland. (2023)
[22] Mohammadi, N., G.: Trustworthy Cyber-Physical Systems: A Systematic Framework towards Design and Evaluation of Trust and Trustworthiness. Springer (2019)
[23] Tsai, C.H., Zdravkovic, J., Stirna, J. (2023). A Meta-model for Digital Business Ecosystem Design. In: Nurcan, S., Opdahl, A.L., Mouratidis, H., Tsohou, A. (eds) Research Challenges in Information Science: Information Science and the Connected World. RCIS 2023. LNBIP, vol 476. Springer, Cham.