A Conceptual Model for Blockchain-Based Trust in Digital Ecosystems

Yuntian Ding, Nicolas Herbaut, Daniel Negru

A conceptual model for blockchain-based trust in digital ecosystems

Yuntian Ding[1][0009−0005−2240−721X], Nicolas Herbaut[2,3][0000−0003−1540−2099], and Daniel Negru[3][0000−0003−4116−1364]

[1] Aquitaine Science Transfert, F-33405 Talence, France
yuntian.ding@nseven.xyz
[2] Centre de Recherche en Informatique, Univ. Paris 1 Panthéon-Sorbonne, Paris, France nicolas.herbaut@univ-paris1.fr
[3] LaBRI, UMR 5800, Univ. Bordeaux, F-33400 Talence, France
dnegru@labri.Fr

Abstract. In inter-organizational business processes, divergent interests among participants often result in trust deficiencies. The question of how to initiate trust remains a largely unresolved theoretical issue. However, the advancement of Blockchain technology has led to an increase in its application for establishing trust among stakeholders in these processes. This paper introduces a conceptual model that leverages an ontology of trust to examine its significance within digital ecosystems and suggests a method to promote the integration of blockchain. We validate our approach with a practical industrial case study and outline prospective developments in the field of trust facilitation through blockchain technology.

Keywords: blockchain; trust; ontology; inter-organizational business process; content distribution

1 Introduction

As the business environment grows increasingly complex due to interconnectivity, no single entity has complete control over the entire business process. This lack of control leads actors in inter-organizational business processes to strongly desire the assurance that their operations will function correctly alongside their partners, despite potential conflicting interests, which raises trust issues [1]. In essence, establishing trust is vital because the fear that other actors may not meet expectations can discourage collaboration [2]. Therefore, identifying and categorizing the most significant trust issues in such processes is critical.

Moreover, an effective and flexible approach to establishing trust can diversify the market, presenting new opportunities. Centralized systems lack sufficient flexibility because actors must rely on a central authority that manages all process aspects, and the reliability of this authority is a concern that all actors must consider. The adoption of blockchain technology disrupts this traditional

model. Blockchain technology actualizes the idea of a shared registry, facilitating the sharing of ledgers that transactions are validated and stored in a chain of blocks. It is particularly relevant for industrial systems requiring decentralized, robust, trusted, and automated decision-making capabilities [3].

However, trust is an abstract concept and not a tangible entity that can be directly measured. Although previous research has explored modeling trust issues in inter-organizational business processes, categorizing trust issues and evaluating trust remains challenging due to the absence of a universally accepted and conceptually clear definition of trust [4]. Furthermore, despite several studies proposing blockchain-based solutions for trust issues, a research gap exists concerning their effectiveness and applicability, underscored by a lack of empirical validation [5]. Yet, in security systems, validation is crucial as it confirms that the system meets the required standards [6].

In this paper, we introduce a conceptual model of trust based on an ontology that allows for the extraction of trust components and requirements, and we examine the extent to which a blockchain-intensive system can address trust issues through its unique role within digital ecosystems.

The rest of the paper is structured as follows: Section 2 introduces the existing research on trust mechanisms and blockchain-based trust systems. In Section 3, we introduce a blockchain-based trust ontology. This conceptual model is then applied to a real-world industrial case study in Section 4. Finally, we discuss the implications of our findings and outline future research directions in Section 5 before concluding.

2 Related Work

Trust is a fundamentally abstract concept, whose definition, challenges, and requirements vary significantly across different disciplines, contexts, and types of participant relationships. This variability complicates the development of a uniform definition of trust. In response to this complexity, numerous ontologies of trust have been developed in previous research to integrate the diverse concepts related to trust. These contributions are instrumental in designing systems perceived as trustworthy. Additionally, there has been a marked increase in research efforts focused on utilizing blockchain technology for trust management.

2.1 Trust Ontology

McKnight et al. proposed an interdisciplinary typology of trust for e-commerce customer relationships, composed of four constructs [7]:

- **Disposition to Trust**: A psychological construct that reflects an individuals general willingness to rely on others.
- **Institution-based Trust**: Derived from sociological traditions, it represents trust based on the assurances provided by institutions or systems.
- **Trusting Beliefs**: The belief in the positive traits of others, even when faced with potential negative outcomes.

– **Trusting Intention**: The readiness to rely on others based on a sense of relative security, despite the possibility of negative consequences.

Amaral et al. referenced these findings in their work on the ontology of trust in both 2019 and 2021, with the latter being an expansion of the former. The 2019 publication stressed the necessity for a precise and rigorous conceptualization of trust. After reviewing various definitions, they concluded that conceptualizing trust hinges on understanding the goals and beliefs regarding the trustees intentions from the trustors perspective, the actions prompted by trust, and the associated risks. Leveraging the ontological approach and their analysis of trust in Social Systems [4], they introduced a concrete modeling tool named ROT (Reference Ontology of Trust), which is based on the foundational theory UFO (Unified Foundational Ontology) and described using the OntoUML language. They applied this tool to analyze two identified types of trust: social trust and institution-based trust [4]. Emphasizing that without uncertainty and risk, there is no trust [8], they also explored how trust relations give rise to risk. The 2021 study extended their 2019 findings, summarizing the trust concepts characteristics identified in their prior work and delving deeper into the complexity of trustors intentions, the quantification of trust, the significance of evidence of trustworthiness, and other factors influencing trust [9]. This ontology aims to facilitate the design of frameworks that allow for the quantification and reasoning about trust.

2.2 Blockchain and Trust issues

Hawlitschek et al. claim in their review that several previous works have highlighted blockchains capacity to provide an infrastructure with the potential to organize truly decentralized markets, thereby possessing transformative potential in reshaping trust dynamics. Moreover, academic literature similarly underscores blockchains potential to address trust-related challenges in peer-to-peer markets and sharing economy activities, suggesting a pivotal role for blockchain technology in resolving fundamental trust issues [10].

Sayed et al. published a review in 2023, highlighting that blockchain, through its decentralized and secure platform for transactions and record-keeping, removes the necessity for intermediaries and guarantees transparency and integrity in data exchange [11]. Previous studies have demonstrated that blockchain has the potential to foster trust among stakeholders, streamline processes, and nurture long-term relationships .

However, through these reviews, we found that there is limited research focusing on the extent to which these blockchain-intensive systems can enhance trustworthiness.

[4] Luhmann described the modern society as a complex communication system. High complexity makes systems opaque and unpredictable to each other, creating double contingency issues. This affects social order theories, with trust or distrust being key outcomes. Trust extends flexibility and uses critical information for trustworthiness, while distrust is more restrictive.[2].

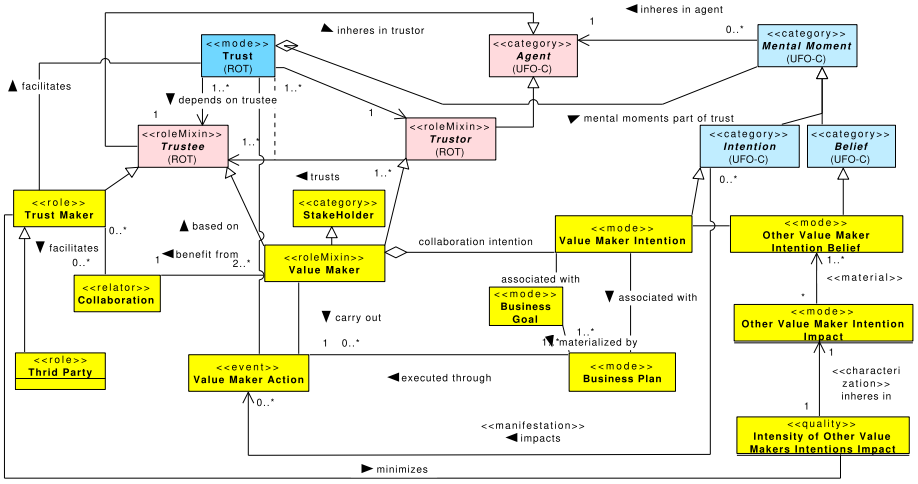

Fig. 1: Ontology of trust in digital ecosystems

3 Conceptual model

In this section, we outline a structured way to think about trust in business processes involving different organizations forming a digital ecosystem. We aim to shed light on the problems that come with sharing trust between groups that opportunistically work together if their trust requirements are fulfilled. We also explain the differences between situations where the business process stakeholders themselves creates trust and where an outside party provides it.

3.1 Ontology of trust in digital ecosystems

We formalize trust in digital ecosystems in the OntoUML shown in Figure 1, focusing on the particular roles played by process stakeholders and third parties in trust formation. We utilize the ROT [4] as a foundation for our trust mental model (in orange), which in turn employs the UFO foundational ontology proposed by Guizzardi et al. (in blue) [12].

Digital ecosystems (DE) consist of at least two `Value Makers` intending to benefit from the outcome of the `Collaboration` in the execution of an Interorganizational Business Process (IBP). They are the IBP `Stakeholders`. For instance, in the Uber Eats DE, the Value Makers are the customers, restaurants, delivery personnel, and the Uber platform itself, as they all benefit from payments or services provided through the food ordering IBP. Since every value maker relies on the collaboration of others yet also benefits from this collaboration, they are considered both `Trustor` and `Trustee` from the perspective of the IBP, marking a significant novelty in relation to ROT. The `Trust` in digital ecosystems characterizes the relationship between `Trustors` and `Trustees`, embodying a complex mental state consisting of a set of `Beliefs` regarding the intentions of other `Value Makers` and the specific

Intentions of each one. The Other Value Maker Intention Belief also considers the impact on our own Intentions through their respective Intensity. For example, when ordering a product online from a merchant with a contractual return policy, even if we harbor the belief that the product may not meet our needs, the Intensity of this beliefs impact is minimized by our entitlement to a refund. In other words, some intentions are based on the self-interests of a Value Maker, while other intentions depend on what we believe other Value Makers intention, and these intentions regarding the other Value Maker can affect ours depending on their importance.

The Intentions of Value Makers consist of a set of Business Goals, which represent the desired outcomes of the collaboration. To achieve these goals, Value Makers devise Business Plans executed through a series of Value Maker Actions. These actions can affect (positively or negatively) the Intentions of other Value Makers. For example, if an airline overbooks its flights as part of a business plan to optimize profit, we might be negatively affected by being unable to join our family for Christmas (our intention).

Value Makers are not solely responsible for fostering trust within the framework. Our conceptualization introduces Trust Makers as a distinct category of Trustee that does not contribute to the value creation of the process. Unlike Stakeholders, Trust Makers hold no intention within the IBP, serving exclusively to facilitate trust without deriving benefits from the process itself. As an illustration, consider the process of selling a painting through an auction house: the seller may seek an independent appraisal to determine a potential selling price. Here, the independent expert acts as a Trust Maker, enhancing trust without participating in the value generation of the auction.

To summarize, in IBPs, trust can be achieved directly through careful analysis of my beliefs in the intentions of other stakeholders and/or be facilitated by an independent third party that supervises the execution of the process.

Digital ecosystems can support many IBPs, involving actors that infrequently collaborate and do not necessarily know each other. In this context, deriving trust is particularly difficult and the role of a third party is paramount, but comes with significant drawbacks, as we show in the next section.

3.2 The problems of Third Parties and how blockchain can help

Achieving trust within digital ecosystems presents a significant challenge as agreements between companies are fleeting, yet these ecosystems open new avenues for collaboration and value creation across increasingly complex value chains.

In practical terms, establishing trust anew for each transaction within a digital ecosystem is inefficient. Consequently, these ecosystems often depend on Third Parties to act as trust facilitators. However, it is rarely that case that third party is just Trust Makers. In most cases, they also act as Value Makers by regulating the ecosystem to such an extent that other participants lack the flexibility to tailor the Inter-organizational Business Process (IBP) to their needs. A significant concern arises when these trust facilitators, due to the high value of trust as an asset, accumulate it, leading to monopolistic conditions. For instance, the general public is typically reluctant or unable to bypass major platforms like Google for installing applications on Android phones. A notable case involved the application provider Epic Games challenging Apple for the right to sell their games outside of the App Store, culminating in

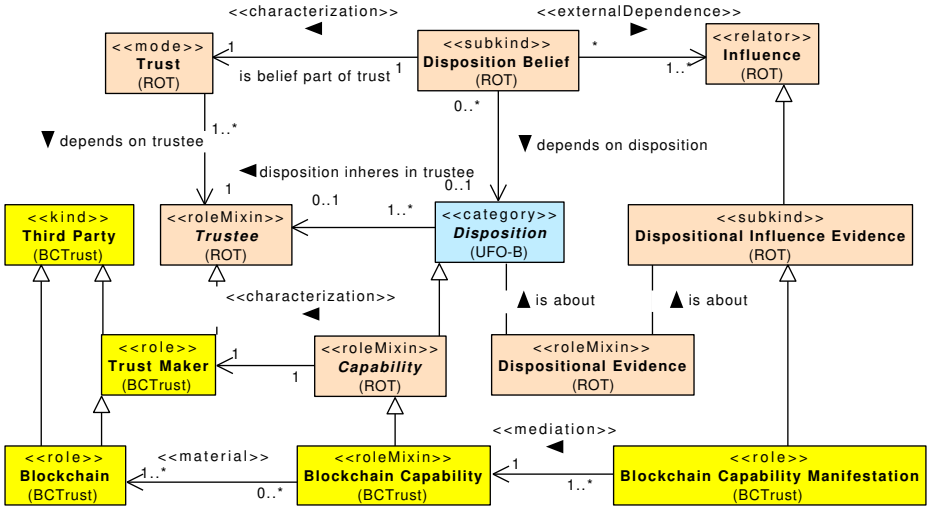

Fig. 2: Ontology of Capabilities Manifestation for Blockchain trust systems

legal action to demonstrate that the platform was in breach of the EUs Digital Markets Act (DMA) regulations [5].

Blockchain solutions are increasingly recognized for their potential to address the issues mentioned earlier, through their distinctive capabilities:

- Blockchain technology enables the creation of customized IBP via smart contracts, bringing more flexibility and versatility to the DE.
- The code executing on blockchains can be made transparent, offering auditable processes.
- Blockchain systems have the capacity to record all process execution traces, thereby ensuring data auditability for `Value Makers`, fostering a sort of indirect trust through control.

Given these features, blockchain can be viewed as a reliable and intentionless `Trust Maker` that decentralizes trust requirements by providing tools to run business processes on a decentralized infrastructure. However, as an emerging technology, established best practices and deployment strategies are still limited. Moreover, the effective utilization of blockchains capabilities hinges on specific prerequisites, the absence of which could significantly undermine its trust-enhancing proposition. In the next section, we propose a description of how we can think of ensuring those capacities to the stakeholders.

3.3 The need for capabilities Manifestation for Blockchain

Amaral et al. expanded the ROT [9] by incorporating the beliefs and intentions of a trustor, as well as evidence indicative of a trustees trustworthiness. They argued that

[5] https://www.economist.com/the-economist-explains/2021/05/02/why-are-epic-games-and-apple-going-to-court

Risks [13]	**Risk Mitigation Manifestation [13]**	**Capabilities at stake**	**Type of Evidence to provide**
sybil attack	Network joining fee, Monitor nodes, Nodes authentication	Integrity, Traceability	Network State, Type of consensus
double spending	Increase confirmed blocks, Pluggable consensus	Integrity, Traceability	Type of consensus
51% attack	Monitor computing power, Transaction Fee	Integrity, Traceability	Type of consensus
Deanonymization	Fresh keys for each transaction, Mixing techniques, Zero-knowledge proofs	Privacy	Smart Contracts design, Blockchain design
Replay Attack	Strong repeat protection, Opt-in repeat protection, Lock digital assets	Integrity, Non-Repudiation	Smart Contracts design
Bugs in code	Code Coverage	Functional Requirements Coverage	Code Coverage Report

Table 1: Mapping between Risks and mitigation, Capabilities and Evidence

`Trust` is shaped by the `Trustees Disposition`. `Disposition` refers to properties that manifest only in specific situations and may not always be evident, such as a magnets tendency to attract metal.

However, as illustrated in Figure 2, `Capabilities` generally cannot be directly assessed by the `Trustor`. Instead, it is the `Trustors` belief in these dispositions that influences `Trust`. The case of `Blockchain` serving as a `Trust Maker` is unique. As a `Trustee`, blockchain exhibits no `Intention` or business goals, owing to its inherently trustworthy design. This limits the necessity for belief in `Capabilities` to specific `Blockchain Capabilities`, demonstrated through `Blockchain Capability Manifestation`. Consequently, careful and targeted design of capability manifestations through `Dispositional Evidence` is essential to promoting trust in blockchain systems.

3.4 Evidence manifestation of Risk Mitigation

An effective blockchain-based system is contingent on the effective management of associated deployment risks, as a blockchain deployment that would be subject to mismanaged risks could not invoke its trust making capabilities. So, to demonstrate that our system possesses the claimed capabilities, we must present evidences that these risks are being properly mitigated. We ground our understanding of which risk impact blockchain systems in the work of Iqbal et al. [13]. They offer an ontological framework for managing security risks in blockchain systems. This framework serves as the foundation for our risk typology and will be expended in future work for finely describing DE specific risks and countermeasures.

Table 1 presents the mapping between potential risks and the blockchain capabilities they may affect, the measures taken to mitigate these risks, and the necessary evidence to confirm the efficacy of these risk mitigation strategies.

In blockchain systems utilizing shards, Sybil attacks pose a significant threat by flooding the network with fake transactions, aiming at the consensus process or causing network divisions, a concern highlighted by [13]. The effectiveness of detecting such attacks largely hinges on the monitoring of node behavior, which varies with the consensus mechanism in place. Concurrently, the blockchain faces vulnerabilities from double spending and 51% attacks that allow for the removal of transactions, thus endangering the networks integrity, with the risk level of these attacks being consensus-dependent. Additionally, the issue of deanonymization arises, threatening privacy as it makes it possible to trace transactions back to their originators. This risk is mitigated through careful blockchain design and the rigorous auditing of smart contract codes. Lastly, like any software, blockchains are susceptible to bugs resulting from substandard coding practices, underscoring the necessity of thorough testing, including unit and integration tests, and the publication of test results to ensure system reliability and security.

The Risk-Capability-Evidence mapping can be used to provide meaningful evidence to `Trustors` on the system the capacity to provide the advertised blockchain capabilities to ensure trust. Our conceptual model can be summarized as follows: (1) identifying the origins of trust in IBP and the pivotal role blockchain technology can serve, (2) illustrating how blockchains distinctive capabilities act as effective enablers for fostering trust, and (3) applying these capabilities to create customized evidence that enhances trust in blockchain itself. In the subsequent section, we demonstrate the application of our framework to a real-world industrial case study, N7 DE.

4 Case study: the N7 Digital Ecosystem

4.1 Motivation

The objective of N7 is to establish a digital ecosystem dedicated to the diffusion of multimedia content. This endeavor necessitates cooperation among three distinct entities: Content Owners (COs, who produce the content), Content Providers (CPs, who retail the content), and Service Providers (SPs, who ensures technical support and maintain the quality of the viewers experience). Each of these parties plays a crucial role in adding value to the ecosystem.

Existing content distribution services are facilitated through either bilateral or multilateral agreements among these stakeholders or a combination thereof. For instance, for a Ligue 1 football match featuring Olympique de Marseille, produced by the Ligue de Football Professionnelle (LFP, acting as a CO), viewers have the option to access the content via Canal+ (a premium TV service acting as both CP and SP) or Amazon Prime (acting as CP) through Amazon Web Services (AWS, acting as SP). The contracts governing the agreements between the LFP and these platforms are intricate, multi-year agreements worth hundreds of millions of euros, predicated on a concept referred to as Social Trust by the ROT [4]. This form of trust relies on the belief in the judicial systems ability to enforce contract terms, although it is not always effective[6]. Such collaborations are typically feasible only for popular services, with niche content

[6] https://www.economist.com/business/2021/02/06/why-no-one-wants-to-broadcast-frances-ligue-1

or less popular sports facing greater challenges in forming these partnerships due to economic and legal feasibility concerns.

Alternatively, viewers may resort to pirate DE, utilizing Free Live Streaming Services (FLIS) to access content illegally [14]. This involves viewers connecting to aggregator websites (acting as CPs) that stream content from FLIS Channel Providers (acting as SPs), thereby bypassing the rightful Content Owners. This illicit ecosystem thrives on deceptive advertising, malware, malicious browser extensions, and scams, posing risks to hosting companies and directly harming Content Owners by infringing on their rights.

N7 proposes a novel approach to foster a secure and productive collaboration among COs, CPs, and SPs by introducing blockchain technology as a Trust Maker. This method aims to create a digital ecosystem where trust is established through cryptographic evidence, rather than being assumed or implicitly granted.

4.2 Analyzing Trust on the N7 ecosystem

The main goal of the N7 project is to propose a system that resolves three outstanding trust issues (TU) identified that impede the three stakeholders to naturally collaborate with each other:

- TU0: Data should not be made public
- TU1: CO must ensure that CP and SP have access rights to content.
- TU2: SP must check that CP actually have the right to access the content.
- TU3: CO and CP can find out the exact number of views provided via SP.

Table 2 illustrates relevant trust requirements extracted from each trust issue.

Trust issue	**Trust Requirement**	**BC Capability**
TU0	Data provided by CO, SP and CP must be private	Privacy
TU1, TU3	CO & CP Must agree on broadcast conditions	Integrity
TU1	CO & SP Must agree on broadcast conditions	
TU1	CO Must have access to CO & SP aggrement	Traceability
TU2	SP Must prove effective service to viewer	Traceability
	CP Must verify proofs uloaded by SP	Traceability
	CO Must have access to verification results	Traceability
TU3	CO content declaration Must not be removed	Integrity
TU3	SP Must have access to CO & CP aggrement	Traceability

Table 2: Mapping between trust issues, requirements and corresponding blockchain capabilities for the N7 project

Leveraging the ontology of trust, this study delineates and categorizes trust issues into corresponding trust requirements and blockchain capabilities. Subsequently, it identifies the necessary evidence to support each Blockchain capability, as outlined in Table 1. To assess the systems trustworthiness, we gather various forms of evidence.

- Information about the state of the network.
- Type of consensus used.
- Smart contract design choices.
- A list of functional fulfillment based on the N7 system test cases

4.3 Evidence Collection

Type of blockchain and consensus N7 employs the Hyperledger Fabric (HLF) platform [15] to address trust issues. HLF operates as a consortium blockchain, where only authorized entities from multiple organizations, each with specific identities and permission, can participate in the network.

Each node stores a complete copy of the ledger, ensuring data consistency and authenticity. Moreover, HLF employs hash functions and ECDSA-256bits as an asymmetric encryption algorithm for transaction authentication. .

Regarding consensus, Hyperledger Fabric utilizes the Crash Fault Tolerant (CFT) consensus mechanism. This mechanism ensures system continuity despite crashes and failures, meaning the system can sustain the loss of nodes as long as the majority of ordering nodes remain. To prevent double-spending and 51% attacks, Hyperledger Fabric relies on its consensus mechanism.

Evidence of HLFs effectiveness and the soundness of this approach can be found in both scientific and gray literature, which provides detailed coverage of the solution and is made available to the DE stakeholders in N7 knowledge base.

Network State and Smart contracts The N7 project uses the multi-channel feature of HLF, enabling business isolation, where nodes can only manage the ledger of the channels they have joined, and cannot know of the existence of other channels. This facilitates different nodes to participate in different collaborations while protecting the privacy and security of data.

Development of smart contracts in HFL enables business rules to be automatically executed according to smart contracts written by N7. The execution results are recorded on the blockchain, providing immutability and improving the traceability and authenticity of transactions. By disclosing the source code, participants can verify the effectiveness of executions.

Acceptance Testing Automation The N7 project employs acceptance tests to verify the system behaves as expected. Interaction with the blockchain is either direct via transactions or through convenience APIs for stakeholders, making API code verification crucial.

For instance, we explore the process of content owners registering content on the blockchain ledger, analyzing both control and data flow testing. Control-Flow Graphs (CFG) illustrate the execution process initiated by input, detailing variable changes and results from browser-server interactions and Data-Flow Diagrams outlines two different types of data path:

- Normal paths can successfully lead to ledger updates and a success response.
- Exception paths interrupt the program or trigger exceptions.

Based on these two flow diagrams, we design and describe test cases in **Gherkin Syntax** to cover various data usage scenarios, including normal and exceptional paths. This ensures program effectiveness under diverse conditions. Testing evaluates if outcomes align with expectations, supporting comprehensive API resource testing and coverage metric publication.

5 Discussion and Future work

Our conceptual framework represents an initial effort to understand the benefits of utilizing blockchain technology to enhance trust in DE.

However, there are opportunities for refinement and improvement. Firstly, the relationship between risks and the evidence provided is somewhat broad and needs to be tailored more closely to specific risks in DE, rather than addressing only high-level, general risks. Further research is necessary to identify these specific risks and develop a deeper understanding of the most impactful evidence to present.

Additionally, we may have underestimated the significance of code auditability. In practical terms, it might not always be feasible for stakeholders to confirm whether the implemented smart contract accurately reflects the intended inter-business processes (IBP). This is crucial because any flaws in the smart contract could undermine the reliability of its execution records. Establishing a collection of trusted, standard patterns could mitigate this risk [16].

Moreover, the introduction of blockchain-based trust could influence the intentions of value makers within the ecosystem. If these actors perceive that they must adhere strictly to predefined rules and cannot leverage their market power to adjust business processes for their benefit, they may see reduced gain from participating in the digital ecosystem. This could potentially deter their involvement.

Lastly, it remains to be determined who should deploy and maintain the blockchain solution and how its governance should be organized. Ideally, a consortium of stakeholders would oversee these tasks. However, this approach carries the risk of a dominant group seizing control of the blockchain system and exploiting it for their own interests. Further work in understanding the governance of blockchain for digital ecosystem is required.

6 Conclusion

In summary, this paper presents a conceptual framework leveraging blockchain technology to address trust issues in digital ecosystems, illustrated through the N7 Digital Ecosystem for content distribution case study. Our findings reveal blockchain potential to enhance trust by ensuring data privacy, integrity, and traceability. However, challenges remain, including risk management, code auditability, and the governance of blockchain solutions. Future research must focus on refining the framework and exploring effective deployment and governance models to fully realize blockchains trust-enhancing capabilities in inter-organizational business processes.

Reference

[1] M. Muller, N. Ostern, D. Koljada, K. Grunert, M. Rosemann, and A. Kupper, Trust mining: Analyzing trust in collaborative business processes, *IEEE Access*, vol. 9, pp. 6504465065, 2021.

[2] N. Luhmann, *Social systems*. stanford university Press, 1995.

[3] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, A vademecum on blockchain technologies: When, which, and how, *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 37963838, 2019.

[4] G. Amaral, T. P. Sales, G. Guizzardi, and D. Porello, Towards a reference ontology of trust, in *On the move to meaningful internet systems: OTM 2019 conferences*, Springer International Publishing, 2019, pp. 321.

[5] N. P. Imperius and A. D. Alahmar, Systematic mapping of testing smart contracts for blockchain applications, *IEEE Access*, vol. 10, pp. 112845112857, 2022.

[6] C. Wang, F. Pastore, A. Goknil, and L. C. Briand, Automatic generation of acceptance test cases from use case specifications: An NLP-based approach, *IEEE Transactions on Software Engineering*, vol. 48, no. 2, pp. 585616, Feb. 2022.

[7] D. H. McKnight and N. L. Chervany, What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology, *International Journal of Electronic Commerce*, vol. 6, no. 2, pp. 3559, Dec. 2001.

[8] C. Castelfranchi and R. Falcone, *Trust theory: A sociocognitive and computational model*. Wiley, 2010.

[9] G. C. M. Amaral, T. P. Sales, G. Guizzardi, and D. Porello, Ontological foundations for trust management: Extending the reference ontology of trust, in *Proceedings of 15th international workshop on value modelling and business ontologies (VMBO 2021)*, 2021, vol. 2835.

[10] F. Hawlitschek, B. Notheisen, and T. Teubner, The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy, *Electronic Commerce Research and Applications*, vol. 29, pp. 5063, May 2018.

[11] B. SAYED and H. V. ORAL, A review on blockchain operations in construction management, *Journal of Sustainable Construction Materials and Technologies*, vol. 8, no. 2, pp. 146152, Jul. 2023.

[12] G. Guizzardi, Ontological foundations for structural conceptual models, 2005.

[13] M. Iqbal, A. Kormiltsyn, V. Dwivedi, and R. Matuleviius, Blockchain-based ontology driven reference framework for security risk management, *Data & Knowledge Engineering*, vol. 149, p. 102257, Jan. 2024.

[14] M. Zubair Rafique, T. Van Goethem, W. Joosen, C. Huygens, and N. Nikiforakis, Its free for a reason: Exploring the ecosystem of free live streaming services, in *Proceedings 2016 network and distributed system security symposium*, 2016.

[15] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukoli, S. W. Cocco, and J. Yellick, Hyperledger fabric: A distributed operating system for permissioned blockchains, in *Proceedings of the thirteenth EuroSys conference*, 2018.

[16] N. Six, N. Herbaut, and C. Salinesi, Blockchain software patterns for the design of decentralized applications: A systematic literature review, *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100061, Jun. 2022.