IPIC 2024 10th International Physical Internet Conference May 29-31, 2024 | Savannah, GA USA

Unlocking the Potential of the Physical Internet: a Trust-enabling Decentralized Process Sharing Connector

Shiqi Sun[1] , Philippe Michiels[2], Cathy Macharis[1],
An Cant[2], Dries Van Bever[2], Koen Mommens[1]

1. Mobilise Research Group, Vrije Universiteit Brussel, Brussels, Belgium
2. Imec, Leuven, Belgium

Corresponding author: shiqi.sun@vub.be

Abstract: *The Physical Internet (PI) hinges on extensive collaboration across logistics stakeholders. Although the benefits have been confirmed by numerous studies and despite its potential for business success, there is a noticeable reluctance to adopt and implement concepts such as PI. We put forward that this hesitancy is in no small part attributed to trust. Therefore, we establish a trust framework that provides a better understanding of trust and its concerns in the context of PI. This paper aims to reason about trust in relation to architecture with commercial stakeholders.*

In our research, we introduce a novel, decentralized, connector-based architecture leveraging dataspaces and event-based data sharing. This architecture prioritizes data ownership and transparency, enabling universal process sharing while eliminating the need for fully centralized platforms.

Surveys demonstrated that the proposed architecture, initially unfamiliar to some, ultimately fostered greater trust due to its federated nature. We conclude by advocating for a transparent design approach to expedite PI adoption and collaboration, highlighting the persistent challenges in this domain, and setting the stage for future research.

Keywords: *Physical Internet Connector, Trust, Process Sharing, Logistics Data Spaces*

Physical Internet (PI) Roadmap Fitness*: Select the most relevant area(s) for your paper according to the PI roadmaps adopted in Europe and Japan:* ☐ *PI Nodes (Customer Interfaces, Logistic Hubs, Deployment Centers, Factories),* ☐ *Transportation Equipment,* ☒ *PI Networks,* ☒ *System of Logistics Networks,* ☒ *Vertical Supply Consolidation,* ☒ *Horizontal Supply Chain Alignment,* ☐ *Logistics/Commercial Data Platform,* ☒ *Access and Adoption,* ☒ *Governance.*

Targeted Delivery Mode-s*:* ☒ *Paper,* ☐ *Poster,* ☐ *Flash Video,* ☒ *In-Person presentation*

1 Introduction

The Physical Internet (PI) aims to create an open, global logistics system inspired by the interconnectedness of the digital internet (Montreuil et al., 2012). This fosters collaboration among participants, leading to more efficient and sustainable logistics (El Omri, 2009). Decentralized architectures like blockchain hold promise for secure and transparent data sharing within PI (Meyer et al., 2019). Additionally, PI leverages automation, distributed intelligence, and smart contracts to facilitate collaboration (Cortes-Murcia et al., 2022; Wang et al., 2016).Despite its potential to improve logistics performance, achieving the envisioned level of collaboration in PI remains a challenge. Trust is a critical but often overlooked factor, as evidenced by the limited success of centralized collaboration platforms like Tradelens (Louw-Reimer et al., 2021; Prandtstetter et al., 2016; Simmer et al., 2017).

Our paper addresses the trust challenge by establishing a trust framework for logistics collaboration in Section 2. This framework derives from established academic frameworks that

although valuable, are not suitable for communication with a non-academic and non-technical audience. Therefore, we have derived eight key trust drivers: *Confidentiality*, *Control*, *Altruism*, *Interest*, *Adoption*, *Compliance*, *Transparency*, and *Reputation*, which we validate with key logistics stakeholders in Section 3. We then propose a trust-enabled architecture for PI in Section 4, building on dataspace principles and process-sharing concepts. In Section 5, we assess stakeholder perception of trust for this architecture, after which we present our findings and directions for further research in Section 6.

2 Establishing a Trust Framework for PI

2.1 Existing Trust Models

Trust is crucial for collaboration in PI, which involves multiple diverse stakeholders like shippers, logistics service providers (LSPs), and receivers (Pan et al., 2019). Existing trust models often have complex factors because it is often multidisciplinary (Moorman et al., 1993; Rotter, 1980; Rousseau et al., 1998). Here, we concentrate on key trust aspects relevant to PI. Beyond the typical focus on the inter-organisational aspect, this also requires us to look at trust factors related to innovative technologies and automation, two aspects that are often overlooked but considered very sensitive to logistics stakeholders (see **Figure 1**).

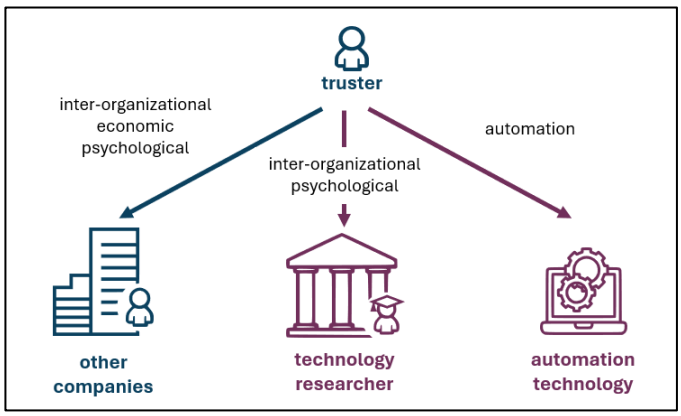

Figure 1 *Aspects of trust in the context of PI. Existing models typically focus on trust in relation to other companies. New technologies and automations need to be trusted before they are adopted.*

Inter-Organizational Trust: This emphasizes trust in business relationships. Three key factors are (Mayer et al., 1995):

- **Ability**: Belief in a partner's competence (e.g., efficient operations).
- **Benevolence**: Perceived willingness to prioritize shared interests (e.g., fair profit sharing).
- **Integrity**: Adherence to established principles (e.g., ethical conduct).

Psychological Trust: This refers to faith in others' promises (Cho et al., 2015; Rotter, 1980). It aligns with individual-level interpretations of integrity and benevolence from the inter-organizational perspective.

Automation Trust: This is the belief in a system's ability to perform correctly (Lee et al., 2004). It's crucial as PI uses automation heavily. Both *overtrust* and *undertrust* can be detrimental.

Economic Trust: Collaboration in PI can lead to economic benefits for all participants (Cho et al., 2015). This potential gain is a driver of trust.

2.2 Trust Drivers for the Physical Internet

The above trust framework under review is typically elaborate and well-founded but also complex and academically focused. When engaging with logistics stakeholders, we need a clear and concise trust framework. Taking the abovementioned aspects and factors into consideration, we have distilled the following eight trust drivers to outline trust in PI: *confidentiality*, *control*, *altruism*, *interest*, *adoption*, *compliance*, *transparency* and *reputation*. The trust drivers are formally defined in **Table 1**.

Our framework translates the complex trust aspects above into clear terms for better communication. These trust drivers allow us to engage with logistics stakeholders to discuss trust in the Physical Internet using plain and understandable terms. Consequently, any architectural decisions can be justified by referring to the trust drivers as well.

Table 1 *Definition of the Trust Drivers for PI*

Trust Driver	Explanation
Adoption	The belief that a critical mass in the ecosystem will adopt common policies, and technologies to affect joint outcomes.
Altruism	The willingness to put collective benefits first to fulfil individual interests within collaborative settings.
Compliance	Adherence to agreed norms, standards, and obligations, ensuring reliability and predictability in collaborations.
Confidentiality	The assurance that data and cargo information are accessible only to authorized parties, safeguarding against unauthorized exposure.
Control	The ability to exercise authority over one's data and cargo, ensuring decisions align with individual or organizational preferences.
Interest	The anticipated individual/organizational gains derived from participation in collaborative endeavours.
Reputation	The perceived reliability based on an entity's historical behaviour and adherence to ethical standards. Reputation can be objectified with governance.
Transparency	The clarity and availability of relevant information and the traceability of assets, fostering openness and accountability.

3 Validation of the Trust Framework

3.1 Methodology

To assess the relevance and completeness of the proposed trust drivers, we conducted a survey with a limited group of nine key logistics stakeholders (shippers, LSPs, etc.) in an interactive workshop. In this survey we focused on two questions.

- **Part 1: Trust Driver Importance**
    - Participants were asked to rate the importance of each of the eight trust drivers in **Table 1**.
    - There were also queries about potential missing trust concerns in order to assess the completeness of the trust framework.
- **Part 2: Architectural Preferences**

- Participants were presented with three different collaboration platform models: centralized, decentralized with a trusted third party, and fully decentralized (peer-to-peer).
- They were asked to assess each model's trustworthiness based on the proposed trust drivers.

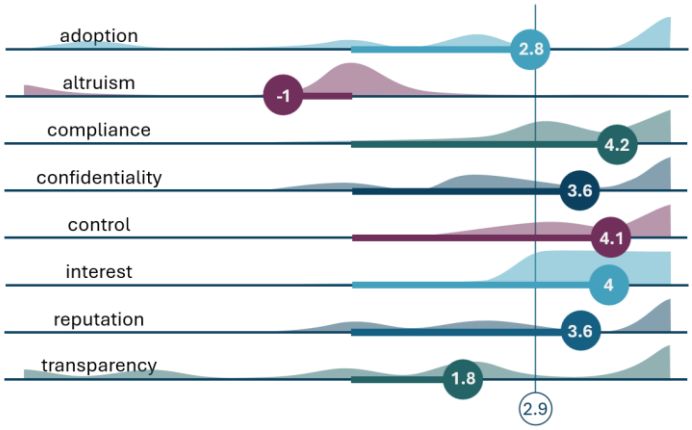

Figure 2 Perceived importance scores of the trust drivers along with voting distribution.

3.2 Findings

Most trust drivers were deemed important. Altruism is a clear outlier, while transparency scores relatively low as well (as shown in Figure 2). It is unclear at this point if this is because altruism is truly irrelevant. A possible explanation is that the role and importance of altruism in a collaborative setting is misunderstood. Transparency in turn, can be interpreted in several ways, which could attribute to its low score.

In addition to the proposed trust drivers, prior relationships, 3rd party endorsement, mandatory use of standards, timeliness and security were presented as additional concerns. However, these can all be traced back to one or more of the existing trust drivers, providing reasonable confidence in the trust mode's completeness.

Part 2 of the survey indicated a preference for a centralized platform for information sharing. Interestingly, when a decentralized model with a trusted third-party governing body was introduced, trust levels significantly increased. This suggests a preference for decentralized architectures with some centralized oversight. The fully decentralized model received mixed reviews, with trust levels averaging between the previous two architectures, but left some stakeholders expressing concerns about potential security issues.

Overall, this survey confirms the relevance and completeness of the proposed set of trust drivers and sheds light on stakeholder sensitivity to separate trust concerns. Although with a limited population, designing PI as a decentralized architecture with a trusted third party appears to be the most promising approach for encouraging collaboration in PI.

4 Design for a Trustworthy Physical Internet

This section introduces a novel reference architecture for PI that builds on existing initiatives and prioritizes trust. The industry often operates within a "platform logic" mindset, requiring participants to connect to numerous platforms. This leads to some issues: the risk of a single platform gaining excessive control and disrupting the balance of power, known as **Dominant Platform Risk**, an increased integration burden for small and medium-sized enterprises, i.e., **Complexity for SMEs** and partly resulting from this a **Vendor Lock-in**.

4.1 Technical Foundation and Innovations

As established in the survey above, logistics stakeholders, hesitant to share data and distrustful of centralized platforms, prefer a decentral architecture with governance. Since dataspaces enable secure and controlled data sharing and collaboration between different parties (Nagel & Lycklama, 2021), we posit that dataspace architecture can serve as a solid foundation for trustworthy collaboration in logistics and thus, for the Physical Internet as well.

Some logistics dataspace initiatives such as *iShare* in the Netherlands and *Catena-X* in Germany are gaining momentum. In parallel, the *FEDeRATED* project (van Bockel et al., 2023) introduced novel concepts for event-based data sharing and process orchestration for decentralized collaboration. Finally, our previous work in the *PILL* project (Michiels et al., 2024) focuses on PI discoverability using abstract PI concepts as initially described in (Montreuil et al., 2010). Bringing together these ingredients, we propose a decentral, federated architecture in line with dataspaces with trustful collaboration between logistics stakeholders in mind.

4.2 Layered Architecture

The architecture combines the results and insights from several existing technologies, projects and initiatives. The layered design in **Figure 3** separates five concerns, which we discuss in detail below. This layering of concerns is analogous to the layering of the internet and fosters interoperability and scalability.

Figure 3 *A layered design for PI connectivity with a clear separation of concerns. The design is inspired by dataspace architecture, which addresses several shared concerns.*

4.2.1 Connectivity: Physical Internet Connector (PIC)

A PIC is an extension of a dataspace connector. Data space connectors facilitate trusted data exchange between stakeholders. This can be operational data such as electronic invoices or B/Ls, logistics events, etc. But our architecture adds the following PI-specific extensions that allow to:

- Connect to specific PI communities, governed by a neutral instance,
- Manage and publish network state (Cassan et al., 2023),
- Synchronize network state locally,
- Manage agreements with process-sharing support,
- Orchestrate processes bilaterally.

An easily deployable PIC can lower entry barriers for accessing and integrating with the PI.

4.2.2 Identity & Trust: Governance with Dataspace Components

An open PI ecosystem requires identities usable across ecosystems. This necessitates a uniform trust framework where credentials can be verified by independent trusted parties. The W3C Decentralized Identity (DID) and Verifiable Credentials (VC) specifications provide the foundation for such a system.

Additionally, PI communities can govern their networks. Like dataspaces, this governance could include a *Participant Management Service* (ParIS), which is used to register members

and manage key metadata and a *Federated Service Catalog*, which lists (technical) services offered by participants.

4.2.3 Discoverability: Publishing and Synchronizing Network State

LSPs publish their PI Network State, which is essential for others to discover them. The network state service can also provide detailed, up-to-date data like availability and pricing.
In addition to the common federated dataspace services above a *Federated Network State* service can be used to help participants synchronize their local copy of the network state for routing and other purposes.

4.2.4 Agreements: Extending Policies with Process Descriptions

Network state publication should include conditions under which logistics services are offered. This includes legal agreements and a machine-readable process description with the following components:

1. **Data Format and Semantics:** E.g., PEPPOL XML format with semantic definitions.
2. **Process Roles:** Identifies participants in the process (e.g., supplier, customer).
3. **Formal Process Description:** Uses states and transitions with allowed roles for each step.

This information can be accompanied by policy clauses like service level agreements and terms of use. The FEDeRATED ontology describes how logistics processes can be captured in terms of events and orchestrated according to a process description. An example is given below in **Figure 4**.

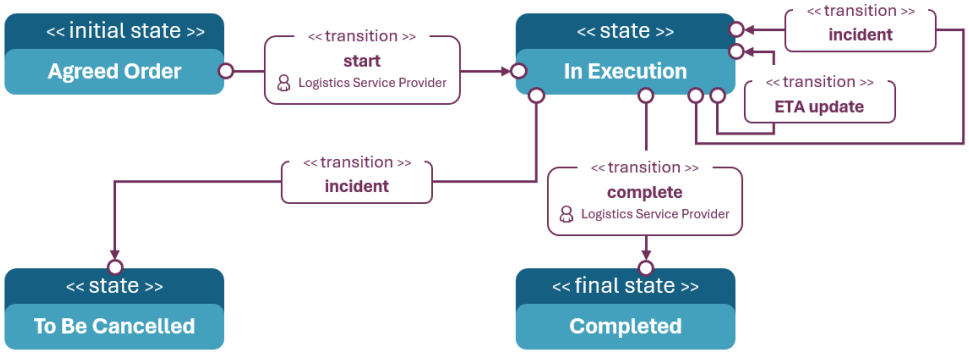

Figure 4 *A description of a process, or interaction pattern based on* (Van Gessel et al., 2023)

4.2.5 Process Sharing: Decentral Logistics Process Orchestration

The final addition is the engine that allows process execution based on the agreed-upon process description (see **Figure 5**). Prior work on event-based data sharing and process orchestration in the FEDeRATED project has led to an implementation demonstrating such a system.

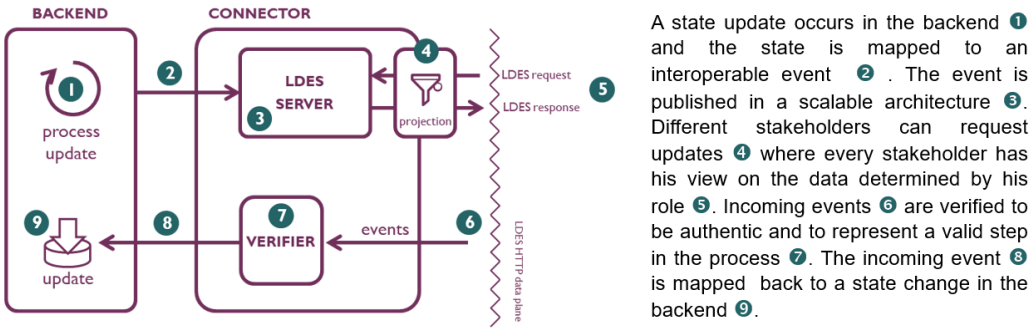

Figure 5 *A high-level design for an event-driven API for decentral logistics process orchestration. (Source: imec)*

4.3 Reflection of Trust Drivers in the PI Reference Architecture

The reference architecture is designed with trust in mind. To underpin this claim, we revisit the trust drivers and explain how the reference architecture addresses them in **Table 2**.

Table 2 *Overview of how the Trust Drivers are reflected in the Reference Architecture.*

Trust Driver	Description in Reference Architecture
Adoption	• **Standardized Approach**: Uses established technologies and open standards (e.g., W3C DID/VC). • **Modular Design**: Allows phased adoption of individual components (e.g., PIC). • **Reduced Vendor Lock-in**: Decentralization avoids reliance on a single platform provider.
Altruism	• **Focus on Collective Benefits**: Simplifies collaboration, potentially leading to increased efficiency and cost reductions for all. • **Transparent Network**: Promotes visibility through discoverability of services and real-time network state sharing. • **Bilateral Agreements**: Enables direct agreements for negotiation of mutually beneficial terms.
Compliance	• **Machine-Readable Agreements**: Formalizes agreements with process descriptions and policy clauses for clarity. • **Automated Enforcement (potential)**: Integrates process engine with automated compliance checks based on policies. • **Audit Trail**: Event-based data sharing creates a verifiable record of actions for accountability.
Confidentiality	• **Decentralized Data Storage**: Stores data within individual, controlled dataspaces, not a central platform. • **Access Control Mechanisms**: Leverages DIDs and VCs for granular access control based on roles and permissions. • **Data Minimization**: Encourages "need-to-know" principle, sharing only essential data. • **Data Encryption**: Uses standard encryption for data in transit between stakeholders.
Control	• **Participant-Owned Connectors**: Each participant has its own PIC, granting control over data flow and network integration. • **Process Description Flexibility**: Agreements can include formal, machine-readable process descriptions defining roles and responsibilities. • **Decentralized Orchestration**: Process execution relies on event-based data sharing, not a central authority. • **Revocable Credentials**: Enables revoking previously awarded credentials if needed.
Interest	• **Reduced Entry Barriers**: Open standards and existing technologies like dataspaces lower joining costs and complexity. • **Improved Resource Utilization**: Facilitates efficient resource allocation and service discovery, potentially leading to cost savings. • **Focus on Value Creation**: Streamlines collaboration, allowing participants to focus on core competencies and value creation.
Reputation	• **Decentralized Governance**: Enables building reputations based on past performance and adherence to agreements. • **Verifiable Credentials**: Allows showcasing credentials and qualifications to establish trust and expertise. • **Public Network State**: Network state information (e.g., service availability, performance) contributes to building trust.
Transparency	• **Discoverable Services**: LSPs can publish network state and service offerings for easy discovery. • **Real-Time Data Sharing**: Enables controlled data sharing for maintaining visibility into collaborative processes. • **Traceability**: Supports data and cargo traceability through event-based logs for tracking movement of goods and data.

5 Trust-based Evaluation of the Architecture

This section evaluates how well the proposed architecture addresses the eight trust drivers identified earlier. To achieve this, a follow-up survey was conducted with the same participants as the initial survey. The results are shown in **Figure 6** and **Figure 7**.

Our interpretation of this preliminary survey is summarized in **Table 3**. For the future refinement and validation of the architecture, we consider the following improvement points:

- Not all aspects of the architecture are fully understood by all participants, leading to some discrepancies between initial importance scores and responses to coverage.
- Clearer definitions of trust drivers using more examples could be helpful in future surveys.
- The perceived importance of trust drivers should be weighed when interpreting the results. For instance, one initially rated low in importance (like adoption) might still be a significant concern if participants perceive the architecture as not addressing it well.

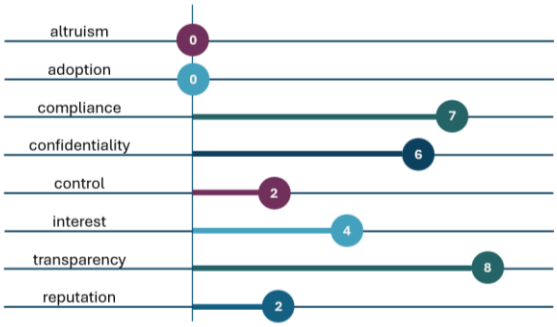

Figure 6 *Survey result: what trust drivers are well-covered by the architecture?*

Figure 7 *Survey result: what trust drivers are* ***not*** *well-covered by the architecture?*

Table 3 *A brief interpretation of the fit-gap survey results.*

Trust Driver	Survey Scores		Discussion
Adoption	**Importance:** **Covered:** **Less covered:**	Low: 2.8 No High: 6	Disconnect between initial rating and later concerns. Participants likely understand critical mass is necessary but are concerned about stakeholder integration challenges. The architecture itself can't guarantee neutral governance, but it can facilitate transparency and fair access.
Altruism	**Importance:** **Covered:** **Less covered:**	Very Low: -1 No High: 6	A negative initial score might be a misunderstanding. The architecture does not explicitly address altruism, which may be a concern for some. More clarity might be needed.
Compliance	**Importance:** **Covered:** **Less covered:**	High: 4.2 Well Covered: 7 Low: 1	Positive finding. Compliance was rated highly important, and most participants felt the architecture addressed it well.
Confidentiality	**Importance:** **Covered:** **Less covered:**	Moderate: 3.6 Good: 6 No	Moderately important concern initially. Most participants felt the architecture adequately addresses confidentiality.
Control	**Importance:** **Covered:** **Less covered:**	High: 4.1 Low: 2 Low: 1	Discrepancy. Rated highly important, but few felt control was well-covered. A clearer explanation of how the architecture addresses control is needed.
Interest	**Importance:** **Covered:** **Less covered:**	High: 4.0 Moderate: 4 Moderate: 3	Significant concern. While some felt the architecture addressed it, there is room for improvement.
Reputation	**Importance:** **Covered:** **Less covered:**	Moderate: 3.6 High: 8 Moderate: 3	Moderate importance. The architecture seems to need further explanation regarding how it addresses reputation.

Transparency	**Importance:**	Low: 1.8	Initially rated low, but became a concern for some. The high rating for architecture coverage is positive, but some participants still lack clarity on how transparency is implemented.
	Covered:	High: 8	
	Less covered:	Moderate: 3	

6 Conclusions and Further Work

This paper explored trust within PI and identified eight key trust drivers influencing logistics stakeholder collaboration. We proposed a trustworthy architecture by implementing dataspace principles and adding support for decentral process orchestration. Exploratory surveys with a limited group of logistics stakeholders validated the trust drivers and assessed the architecture's effectiveness.

The identified trust drivers appear comprehensive for PI. Survey participants favoured a decentralized, federated PI design, aligning well with the proposed dataspace-inspired architecture. The architecture addresses stakeholder trust concerns, but broadening the survey to more stakeholders is needed to assess its effectiveness with greater certainty.

Widespread stakeholder adoption is crucial for a true Physical Internet and is identified as a major challenge. While trust can encourage adoption, the survey highlighted a need for improved clarity regarding the architecture's principles. Participants struggled with concepts like data control, decentralized orchestration, and federated services. Addressing this communication gap is essential for broader adoption.

These results are a starting point for further research on a larger scale. Surveys with a broader audience, more participants and a focus on clear trust driver definitions will provide deeper insights into stakeholder concerns. Our insights will be used to further refine the architecture with trust in mind. Ultimately, through iterative surveys and practical testing within Living Labs, we aim to establish a robust foundation of trust within the Physical Internet, empowering increased collaboration and paving the way for a truly interconnected PI that unlocks its full potential.

7 References

Cassan, C., Michiels[2], P., Sun, S., Lemos[2], V., Dries, ;, Bever[2], V., Cant[2], A., Fink[2], J., & Macharis, C. (2023). Data Sharing in the Physical Internet: A Capability-Based Approach for Trustless Logistic Networks. *Proceeding of the 9th International Physical Internet Conference*, 156–165.

Cho, J. H., Chan, K., & Adali, S. (2015). A Survey on Trust Modeling. *ACM Computing Surveys*, *48*(2). https://doi.org/10.1145/2815595

Cortes-Murcia, D. L., Guerrero, W. J., & Montoya-Torres, J. R. (2022). Supply chain management, game-changing technologies, and physical internet: A systematic meta-review of literature. *IEEE Access*, *PP*, 1–1. https://doi.org/10.1109/access.2022.3181154

El Omri, A. (2009). *Cooperation in supply chains : alliance formation and profit allocation among independent firms* [Ecole Centrale Paris]. https://theses.hal.science/tel-00453322/fr/

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, *46*(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392

Louw-Reimer, J., Nielsen, J. L. M., Bjørn-Andersen, N., & Kouwenhoven, N. (2021). *Boosting the Effectiveness of Containerised Supply Chains: A Case Study of TradeLens* (pp. 95–115). https://doi.org/10.1007/978-3-030-72785-7_6

Meyer, T., Kuhn, M., & Hartmann, E. (2019). Blockchain technology enabling the Physical Internet: A synergetic application framework. *Computers and Industrial Engineering*, *136*(July), 5–17. https://doi.org/10.1016/j.cie.2019.07.006

Michiels, P., Sun, S., Lemos, V., Van Bever, D., Cant, A., & Macharis, C. (2024). *PILL: Physical Internet Living Lab*. https://www.imec-int.com/en/pill

Montreuil, B., Meller, R. D., & Ballot, E. (2010). Towards a Physical Internet: the impact on logistics facilities and material handling systems design and innovation. *11th IMHRC Proceedings (Milwaukee, Wisconsin. USA – 2010)*, 40.

Montreuil, B., Meller, R. D., & Ballot, E. (2012). Physical internet foundations. In *IFAC Proceedings Volumes (IFAC-PapersOnline)* (Vol. 14, Issue PART 1). IFAC. https://doi.org/10.3182/20120523-3-RO-2023.00444

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors Affecting Trust in Market Research Relationships. *Journal of Marketing*, *57*(1), 81. https://doi.org/10.2307/1252059

Nagel, L., & Lycklama, D. (2021). *OPEN DEI Position Paper Design Principles for Data Spaces*. https://doi.org/10.5281/zenodo.5244997

Pan, S., Trentesaux, D., Ballot, E., & Huang, G. Q. (2019). Horizontal collaborative transport: survey of solutions and practical implementation issues. *International Journal of Production Research*, *57*(15–16), 5340–5361. https://doi.org/10.1080/00207543.2019.1574040

Prandtstetter, M., Sarah, L. P., Alexandra, P., Gernot, H., Wolfgang, L., & Ponweiser, W. (2016). *Introduction to Synchromodal Networks in Austria*. *1*, 1–6.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, *35*(1), 1–7. https://doi.org/10.1037/0003-066X.35.1.1

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different After All : a Cross- Discipline View of Trust. *The Academy of Management Review*, *23*(3), 393–404. https://www.jstor.org/stable/259285

Simmer, L., Pfoser, S., Grabner, M., Schauer, O., & Putz, L. M. (2017). From horizontal collaboration to the physical internet - A case study from Austria. *International Journal of Transport Development and Integration*, *1*(2), 129–136. https://doi.org/10.2495/TDI-V1-N2-129-136

van Bockel, R., & Benvenuti, M. (2023). *FEDeRATED : EU project for decentralized data collaboration in logistics*. https://www.federatedplatforms.eu/

Van Gessel, T., & Hofman, W. (2023). *An Interaction Pattern Ontology for Data Sharing about Logistics Activities*. http://ceur-ws.org

Wang, J., Fan, G., Yan, F., Zhang, Y., & Sun, S. (2016). Research on initiative scheduling mode for a physical internet-based manufacturing system. *The International Journal of Advanced Manufacturing Technology*, *84*(1–4), 47–58. https://doi.org/10.1007/s00170-015-7915-3