UNIVERSITY OF TURKU
Turku School of Economics

Unlocking Trust in Digital Product Passport

An fsQCA & Multiple Linear Regression Approach

Subject/Department:
Master's thesis
Turku School of Economics (TSE)
Tilburg School of Economics and Management (TiSEM)

Author:
A.N.A. (Anne) van den Eijnden

Supervisor(s):
Dr. F. (Farhan) Ahmad (TSE)
Dr. E.A.M. (Emiel) Caron (TiSEM)

29.07.2024
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master's thesis

Subject: Trust in Digital Product Passports
Author(s): Anne van den Eijnden
Title: Unlocking Trust: Investigating the Impact of Design Requirements on Trust in the Digital Product Passport
Supervisor(s): Dr. F. (Farhan) Ahmad, Dr. E.A.M. (Emiel) Caron
Number of pages: 61 pages + 11 pages
Date: 29.07.2024

This thesis investigates the factors influencing trust in Digital Product Passports (DPPs), in terms of the information they provide and the systems themselves. Also, the relation between trust in the DPP information, the DPP system, and behavioral intention to use the DPP was tested. A survey was conducted among potential future users of DPPs within an organizational context, focusing on multiple trust precursors related to DPP design requirements. The data was analyzed using a fuzzy-set Qualitative Comparative Analysis to identify factors and their combinations that lead to high or low trust in DPP information and systems, and using multiple linear regression to test the relation between the trust factors and behavioral intention.

Key findings include unique location identifiers, data calculation transparency, and third-party certification as core conditions for trust in DPP information, and secure authentication mechanisms for data editing as a single predictor for high trust in DPP systems. However, the study also found that trust alone may not be sufficient to ensure the use of DPPs in decision-making processes related to circularity and sustainability.

The research contributes to the limited academic literature on DPPs by advancing the understanding of trust in DPPs and similar initiatives. It provides validated survey measures for analyzing trust precursors within information systems and demonstrates the potential of the fsQCA method for understanding complex constructs like trust.

The study acknowledges limitations such as the limited literature on DPPs, constraints in data collection, and potential bias in the fsQCA method. Future research could extend this study by testing specific propositions, exploring more or different trust precursors, performing longitudinal studies, and the needs of organizations to see the DPP as more than just a legal requirement.

Keywords: Digital Product Passports, Trust in Data, Trust in Information Systems, Circularity, Design Requirements.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Digital Product Passports (DPPs) for industrial and electric vehicle batteries will be phased in from 2024. Also, in the textile and construction sector, works are done to start the introduction in the coming years. The European Commission has legislated the implementation of DPPs in the Eco-design for Sustainable Products Regulation (ESPR) (Regulation (EU) 2024/1781 of the European Parliament and of the Council, 2024) officially published in June 2024, and the Circular Economy Action Plan (CEAP) (Stretton, 2022).

The goal of the DPPs is to collect and share data on a product and its supply chain throughout the complete value chain, therefore improving the understanding of the materials and products used by all parties involved, including consumers, and their associated environmental impact. The whole supply chain will need to work together to specify the vital information needed to create the passport in order to improve the reuse, reconditioning, remanufacturing, and recycling of products. Therefore the core values that DPPs generate are their traceability (Heeß et al., 2024) and transparency (Jansen et al., 2023). When these are maximized, the first steps can be taken to move to a more circular economy within Europe (Rinaldi et al., 2022).

Since the introduction of this plan in 2020 by the European Commission (Götz et al., 2022), research has been conducted on the implementation of these DPPs. Research has focused on data standardization and the platforms needed to achieve this sharing of data between different organizations. Plociennik et al. (2022) indicated that there are multiple non-technical barriers to overcome to achieve the core objectives of the DPP. One of these barriers is the agreement on common standards to improve interoperability between organizations (Jansen et al., 2023), which currently, standardization organizations are working on (CEN CENELEC, 2024). Further, studies have been done that concentrate solely on specific data and information needs (Berger et al., 2023). And while this research is important to make sure DPPs are well developed, no literature that was found has dived into specific factors that contribute to the adoption of the DPPs in an organizational context, and how to achieve those factors.

Trust is a key factor often studied and considered significant in research towards IT adoption (Salahshour Rad et al., 2018). To broaden the research towards DPPs, this thesis

will focus on the impact of trust on the adoption and use of DPPs in the coming years, and explore precursors that could be implemented to improve this level of trust.

For the DPP to be adopted successfully, individuals within organizations must be willing to share their data with others in the ecosystem in a trustworthy manner (W. Liu et al., 2021; Otto & Jarke, 2019). This is required so all the necessary information can be shared within the value chain and with (other) (re)manufacturers and end-of-life actors (Plociennik et al., 2022). For instance, data and information about product composition and hazardousness are important for the end-of-life actors but not every organization is willing to share this information in the first place.

In the organizational value chain setting, this trust works in two directions. Stakeholders must trust others not to misuse the data they share, and they must trust, e.g., the correctness, authenticity, and completeness of the data that they receive from others (Heeß et al., 2024). To enable these two directions, one could focus on multiple types of trust, for example, trust in the DPP system, trust in the DPP information, and the stakeholders' inter-organizational trust within the value chain. Besides these, other types of trust related to the success of DPP include consumer trust towards the organizations and a two-way trust between authorities and their legislation about DPP and the organizations implementing it, i.e., regulation compliance and legislation trust.

So, while various types of trust can influence the success of DPP, this study will focus on the trust, as perceived by actors along the value chain that will use the DPP in an organizational setting, in the DPP system and the DPP information. The justification for this focus is twofold. Firstly, these types of trust directly impact these stakeholders' willingness to use the DPP, as emphasized in previous research (Alkhater et al., 2018; Kusuma & Pramunita, 2011). If stakeholders do not trust the system or the information it provides, they may be unwilling to engage with the DPP therefore hindering its overall success. Secondly, while other types of trust, such as inter-organizational trust and consumer trust, are undoubtedly important, they fall outside the scope of this study, which is situated within the field of information systems research.

1.1 Research Questions

This research seeks to address this critical gap in research regarding DPPs by exploring the following questions:

RQ1: Which factors, and their combinations, affect high or low trust, or both, in the Digital Product Passport?

RQ2: What is the effect of trust in the Digital Product Passport on the behavioral intention to use the Digital Product Passport in the decision-making processes regarding circularity and sustainability?

Recognizing that trust is multifaceted and complex, this study will employ a configurational approach, using fsQCA to answer the first research question. This approach acknowledges that it is not a single factor, but rather combinations of factors, that lead to high (or low) trust. The considered factors are discussed in Section 2.2. By examining these factors in configurations, this study aims to provide a more nuanced understanding of how trust can be fostered within DPPs.

The second research question will be answered using multiple linear regression analysis. This variance-based analysis builds on the basic linear regression approach and aims to determine and understand the connection between several independent variables and one dependent variable. In this case, the independent variables will be two types of trust (Section 2.1), and the dependent variable will be the behavioral intention (Section 2.3).

In interrogating these questions, this study aims to shed light on the precursors through which trust can be increased within DPPs. It seeks to understand what individual stakeholders deem important for the success of the DPP. In particular, this study will focus on several key factors that influence trust, transparency, traceability, and security. In the end, this study aims to contribute to the current knowledge of DPPs by providing insights into DPP trust precursors that enhance stakeholders' trust in DPPs and similar data-sharing initiatives along the value chain. Therefore, this study contributes to both theoretical and practical value.

The rest of this thesis is structured as follows, first, prior research is presented, focusing on trust in systems and information, design requirements of DPPs, possible trust precursors for the DPP, and behavioral intention regarding DPP. In Section 3, the research framework is presented which will be analyzed by the methodology presented in Section 4. Section 5 will present the results of the quantitative study and Section 6 discusses these results comparing them to prior research. Finally, Section 7 will provide a conclusion regarding this research including contributions, limitations, and paths for further research.

2 Literature Review

This chapter presents prior research on several topics that contribute to the necessary understanding of trust, design requirements of DPPs, and possible DPP trust precursors. These concepts are essential for finding an answer to the research questions.

First, the concept of trust is demystified, focusing on its role in both data and information systems. Second, the design requirements of DPPs are outlined, discussing both information-based and system-based requirements. Finally, various DPP trust precursors are presented, detailing how information presentation and system features can foster trust.

2.1 Trust

When looking at how people develop trust in a system, the concept of interpersonal trust should be understood first. Within the literature, multiple definitions for the concept of trust are provided which shows the complex nature of this concept. In one way, trust is based on the expectation of truthful behavior of others towards ourselves (Sztompka (2007) in (Ejdys, 2018)). Another definition, by (Mayer et al., 1995), is a party's readiness to be open to the action of another party in exchange for the expectation that the other party would carry out a specific task that is important to the trustor, regardless of the other party's capacity for oversight or control. This definition is based on the fact that interpersonal trust always happens between a trustee and a trustor and is the basis for an interaction between the two counterparts (Kivijärvi et al., 2013).

Based on the previously given definitions of trust, a concept often referred to as technological trust is special in the way that the trustee is an 'inanimate' technology instead of one or multiple human beings (Giffin, 1967; Lippert & Forman, 2006; Xu et al., 2014). Therefore, a trusting relationship will never be bi-directional, as it is in interpersonal trust (Lippert & Swiercz, 2005), and it is not possible to evaluate the technology's trustworthiness by assessing the constructs of its competence, benevolence, and integrity (Mayer et al., 1995), which are antecedents of trustworthiness that are widely used and accepted in research.

So, the relation between interpersonal trust and trust in an information system is that we want trust in a system to be comparable to interpersonal trust, except that a user interacts with a system rather than another person. To trust a system, users should expect it to offer true information and prevent exploitation or abuse of their information. So, what data can

be shown to increase the level of trust that a user feels towards the information in the DPP, and what trust precursors can be implemented into the DPP system that enhances the level of trust of a user using the DPP system?

2.1.1 Trust in Data

First, Thielsch et al. (2018) show that users should evaluate a management information system's trustworthiness and features by determining how reliable the information it offers, i.e., *credibility of the provided information*. This could be about the consistency and accuracy of the data within the DPP or how data is gathered and processed. Meeßen et al. (2019) use this previous work and mention that users can assess the trustworthiness of an information system before they have used it, basing their opinions on e.g., discussions with coworkers, managers, or technical support personnel, or based on their initial opinion of the user interface. This is relevant in the case of DPPs as, in most sectors, DPPs are not yet implemented practices so their trustworthiness has to be based on one of these other aspects.

Further, Acikgoz et al. (2023) found that trust in specific applications is positively influenced by information adoption, which is determined by characteristics like *usefulness*, *credibility*, and *quality of information*. Their research highlights an interesting approach to analyzing trust, particularly relevant to the DPP's focus on enhancing transparency throughout the value chain by sharing information. Also, Yoon & Lee (2019) showed that *data quality* was significantly related to the trust of the data (re)users.

Further, factors regarding collection methods, measurements, or variables come forward in research regarding trust in data. According to Wallis et al. (2007) habitat biologists asked about the selection of data-collection tools and the calibration process used by data providers before reusing the data. Besides this, Faniel & Jacobsen (2010) discovered that the trust that data (re)users had in the reliability of the data was boosted when the users understood how data producers gathered and measured the data. This indicates the importance of *transparency* regarding data collection methods, measurements, measurement devices, and formulas for the intent of making decisions based on the DPP.

Moreover, Schmidthuber et al. (2023) showed that, within the context of public performance information, giving users access to raw data increases their trust in public performance reports. Also, when a source of the data is given, citizens are more likely to believe statements made about public performance. These results contribute to how both

the *transparency* of collected data and *traceability* of the data provider contribute to a higher level of trust.

2.1.2 Trust in Information Systems

First, as competence, benevolence, and integrity (Mayer et al., 1995) are not useful for assessing the trust in a system, Mcknight et al. (2011) adapted these antecedents of trust (Mayer et al., 1995) to the context of trust between people and technology. They redefined *functionality* as the technology's competence, *helpfulness* as the technology's benevolence, and *integrity* as its reliability. In the context of the DPP, this translates to how well the data assists decision-making and how reliably it operates. In previous research, technological trust has been found to rely on a lot of different antecedents.

Another focus on trust in systems is put into online banking, where trust is an important aspect for people to adopt financial technology services. Zhang et al. (2023) focused on the customer trust towards financial technology services and how it affected its adoption. By focusing on the Technology Acceptance Model, and the Theory of Planned Behavior, they developed a model to see how *data security*, *perceived usefulness*, and *perceived ease of use* affected this customer trust.

Further, Chang & Seow (2016) propose three trusting attributes towards trusting technology. First, *openness* refers to features that allow consumers to access information about the gathering, usage, and disclosure of their personal data. Second, *consent* refers to a person’s specific, freely given approval for the gathering, usage, or sharing of personal data. And lastly, *access* comprises the systems that let people see their personal data and get information on how it is used and shared. Mainly consent could be translated to the DPP system by letting data providers decide on who can access what details of the organization’s sensitive data that they share within the DPP.

2.2 Digital Product Passports

Focusing on DPPs and trust, one article is available that dives into this within an organizational context (Heeß et al., 2024). They have focused their research on enhancing trust in data sharing within global supply chains in the low-carbon hydrogen market, using DPPs. Therefore, this research has used DPPs as a means to enhance trust within the supply chain and what is needed in the DPPs to do this, compared to enhancing trust in

DPPs itself. On the other hand, the list of design principles presented is useful to cover a broader context besides the low-carbon hydrogen market, as discussed below.

Based on recent research, the main focus has been on what is technically needed to be able to implement DPPs. Some research has focused specifically on blockchain solutions (Greiner et al., 2024; Ribeiro da Silva et al., 2023) or data space solutions (Koppelaar et al., 2023). However, most research has resulted in design requirements to consider in further development of the DPP. Therefore, design requirements are used as input for this study to scope the focus of this research.

Regarding research on DPPs in general, previous research is limited offering only a small amount of academic literature on this topic. This is because the introduction of DPPs by the European Commission happened in 2022, and before this year there was little to no research being done on the topic. Abstract and citation database Scopus[1] shows three results for the search query "Digital Product Passport*" that mention this term in their article from before 2022, compared to 71 from 2022 onwards. As such, this does indicate that there is progress being made in the development of this topic, and therefore, new research on DPPs is published each month.

Besides this, European Commission-funded consortiums like CIRPASS (Gupta et al., 2024; Wagner et al., 2023) are focusing on the development and implementation of the DPP within Europe. In these consortiums, industry players come together to research the best ways to implement the DPP. The results of these studies are also used within this research as grey literature, compared to white literature being academically published articles.

To begin with, Heeß et al. (2024), after setting up three meta-requirements for the DPP, presented six design principles for a hydrogen DPP with their aim, context, mechanism, and rationale, where the mechanism in most cases reflects a more specific design requirement. After multiple rounds of interviews, the design principles were: a holistic data approach, data privacy, decentralized data administration, forgery-proof data, automated passport processing, and interoperability.

Further, Boukhatmi et al. (2023) presented 3 design principles and 11 design requirements for photovoltaic installations, i.e., solar panels. Using a design science research approach,

[1] Scopus - Document search

they came to the following requirements: accessibility, completeness, consistency, efficiency, interoperability, security, sensitivity, traceability, transparency, time performance, and visibility.

Lastly, CIRPASS (Gupta et al., 2024; Wagner et al., 2023) has provided an overview of legal and voluntary requirements regarding the DPP system and the needed information. In their non-peer-reviewed report, they provide a cross-sector and sector-specific overview of these requirements, including the organization's legal and location IDs and third-party certifications (Wagner et al., 2023), decentralized data storage, and authentication requirements (Gupta et al., 2024).

Based on the above literature review, 7 design requirements are collected to be used in this research. In the following sections, they are distinguished as information-based requirements and system-based requirements. From these design requirements, 8 DPP trust precursors are reviewed that potentially enhance trust in the DPP in light of a specific design requirement.

To be able to discuss the design requirements of DPPs, we need to determine what these requirements entail. Prior research distinguishes between design principles and design requirements. First, design principles are developed to be employed in new situations and reflect prescriptive knowledge of design (Möller et al., 2020). They are considered a more general construct that helps future design problems in different fields. On the other hand, design requirements are the first stage of the product development process. Design requirements are essential for reducing the possibility of implementing user needs that are not well-specified (Li & Ahmed-Kristensen, 2015). When setting the scope of this research, the focus lies on design requirements as DPPs are already in their development stage and it would be most beneficial to review the design requirements that are determined in previous research. Therefore, the outcomes of this research could contribute to the further development of the DPPs.

2.2.1 Information-based Requirements

The Information-based requirements focus on the content of the DPP, what data it should contain, and whether extra information is needed. It is acknowledged that the data in the DPP has not always been analyzed and interpreted enough for it to be called information, however, the term ‘information’ is used throughout the rest of this thesis to refer to everything that can be read from the DPP. The requirements that focus on the information

in the DPP are data collection transparency, data calculation transparency, product traceability, data traceability, and third-party certification.

To begin with, transparency is created through data sharing within the value chain (Boukhatmi et al., 2023). This is also one of the goals of the DPP in itself, however, it is interesting to see how this feeling of transparency can be further increased besides only sharing the data that the organizations are obligated to share. Sharing more (meta-)data could be an important factor for trust as it provides more context to the data that is shown which could for example increase the credibility of the data (Acikgoz et al., 2023; Kratz & Strasser, 2015; Thielsch et al., 2018).

Based on transparency, it would be good to see how data presented in the DPP is collected or calculated (Berg et al., 2022; Faniel & Jacobsen, 2010; Wallis et al., 2007). Within academia, it is shown that knowing how data is collected or measured increases trust when other researchers reuse the data (Faniel & Jacobsen, 2010; Wallis et al., 2007). When a data viewer can see how data has been collected (or calculated) it could increase their trust in this information as it reduces the risk that data is not added to 'fill in the blanks' but is determined critically. Examples of this could be making visible the sources of raw data, such as sensor readings and specific algorithms or formulas used for processing the data. Additionally, a step-by-step explanation of the data handling process could be shown. This information would be shown alongside the actual data values.

Further, regarding traceability, multiple types could be interesting for the DPP. First, product traceability can show the product's life cycle history (Boukhatmi et al., 2023), including where the product and its components come from and a further component breakdown of what is processed into the product. As this product traceability reaches for a higher level of completeness of the data, this could positively affect the level of trust towards the data in the DPP (Acikgoz et al., 2023).

This product traceability can be enhanced by showing a data lineage tracking diagram of the information on products added to the current product. This would lead to a tree-like structure that splits the product into its smaller parts, showing the relevant DPPs of these components. Data lineage diagrams often show how data flows through a workflow (Stitz et al., 2016; Yazici & Aktas, 2022) but can also apply to a supply chain. The diagram will improve the traceability of the products within the DPP by showing the journey that the data has taken from its source to its current state, including all intermediate components. This will also show more clearly where which component is produced and where the

information that is provided about the component stems from, regarding location or organization. It can also include transformations, processes, systems, and people that have interacted with the data

On the other hand, one could also focus on data traceability where the question is who collected or calculated the data presented in the DPP. This could be traced back to an organization, a facility, or a specific geological location (Boukhatmi et al., 2023; Wagner et al., 2023). This information will show you what organization or facility is responsible for the correctness of the data. When this information is visible it could also increase the importance of data correctness for the organization associated, thus enhancing the quality of the information. Therefore, it could have a positive result on trust in this information (Acikgoz et al., 2023; Thielsch et al., 2018).

To enable this trust, data traceability can be enhanced by including Unique Location Identifiers (ULI) that are tagged to specific data. Wagner et al. (2023) proposes a two-way identification where the 'legal' (the organization) is further specified with the 'location' (specific facility), ULIs are used for this. This way it can be seen who (organization) made what claim (data) and where the data was gathered (location). An example of this is GS1's Global Location Number (GLN) (GS1 US, 2022) that can be used by organizations to identify their different locations. This contributes to streamlining communication and data exchange between trading partners, ensuring accurate and consistent location information.

Lastly, to improve the trust in the correctness of the data and whether the data complies with the regulations presented in the ESPR or any addition to this regulation defined in delegated acts, third-party certification could be implemented into the DPP-system. By introducing a trusted external entity into the dataflow that validates the data, the credibility of that data could be increased, in turn, affecting the data viewer's trust (Anisetti et al., 2014; Acikgoz et al., 2023; Thielsch et al., 2018). Also, shows the importance of including a third-party certifier in the system architecture that checks the data of the product to the regulations. Moreover, in the non-peer-reviewed work by CIRPASS, it is specified that third-party certification is important for the compliance of the data to the regulations presented by the EC. Research, including work by Boukhatmi et al. (2023) and non-peer-reviewed work by CIRPASS (Wagner et al., 2023), highlights the importance of including a third-party certifier in the system architecture. This certifier

checks the product data against regulations, thereby increasing trust in the data's correctness (Jiang et al., 2008) and compliance with requirements.

Having an independent authority or organization check the values that are presented in the DPP provides an extra dimension to the interpretation of the data. After a manufacturer registers a DPP, a certification is requested. A third-party certifier will look at the data and whether it has been collected or calculated according to the determined standards and requirements (Boukhatmi et al., 2023).

To conclude, four information-based design requirements were found in the literature that could contribute to trust in the information found in the DPP. First, transparency enables stakeholders to see how the data is collected and how it is processed into the information that is shown in the DPP. Second, traceability can be achieved using data lineage tracking to improve product data traceability and unique location identifiers can be used to improve data provider traceability. Further, regarding the correctness of the data, third-party certification can help stakeholders see compliance with the requirements set on presented information. Besides information-based design requirements, the literature also presents a set of system-based design requirements, presented below.

2.2.2 System-based Requirements

Regarding system-based requirements, the focus is not on the data and its contents but on the mechanisms and functions of the system that could contribute to a higher level of trust in the DPP system. The requirements that focus on the DPP system are accessibility management, decentralized data storage, and secure authentication.

First of all, access management is important to make sure that no one that is not eligible to view the data, can view the data. Consumers that want to view a DPP only see a subset of all the information available in the DPP but there could also be distinctions of data that is available within the value chain. For example, a recycler of products may have to access different data than a wholesaler or a retailer. Boukhatmi et al. (2023) propose a login format that defines organizations or people within members and guests that have different access and role permissions. This access control could contribute to the data security of the data providers, which, in turn, could contribute to the enhancement of trust in the DPP system (Zhang et al., 2023).

Focusing on accessibility, the use of verifiable identities in DPPs could improve trust as it allows people to create and own their identity while organizations are credible to validate this identity (Copeland & Copeland, 2017). This way, a data viewer that asks for access to the DPP provides their identity to the data provider or host of the data and one of the latter determines, based on this identity, whether it can view the DPP and what information will be visible to this data viewer. This way certain data and information can be kept invisible to specific data users (Boukhatmi et al., 2023). The process that goes along with verifiable identities is that the holder presents the credentials issued by the issuer to the verifier, and the verifier checks these credentials. This way the holder only needs to present some information to the verifier and not to the issuer whose data the holder wants to access. In the case of DPPs this would mean that the data viewer is the holder trying to access the data, the data owner or host of the data is the verifier as they want to verify the data viewer's identity, and the issuer is a third-party, possibly government-managed, that issues the data viewer a digital identity, see Figure 1.

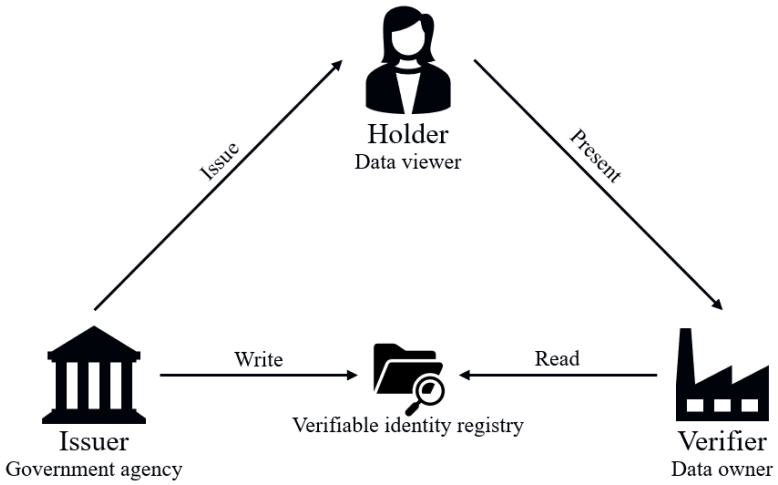

Figure 1. Verifiable identities, actors, and process for DPP

Second, Gupta et al. (2024), part of the CIRPASS consortium, presents decentralized data storage as one of the essential requirements for the DPP system. A decentralized data storage means that not all data is stored in one repository but is distributed over more than one repository. This reduces the risk of failure of a single point and prevents the need for an agreement on a storage space (Heeß et al., 2024). However, to nuance, the ESPR (SOURCE) states that there should always be a backup available of the DPP. Also, in this way organizations that would like to only store their data on their repositories can do so. This decentralized system contributes to data security (Zhang et al., 2023) and integrity (Mcknight et al., 2011) of the system.

Lastly, a tamper-proof DPP architecture is essential to ensure that data cannot be changed by unauthorized organizations or individuals (Gupta et al., 2024; Heeß et al., 2024). Secure authentication mechanisms are needed so that only authorized stakeholders can acquire editing access to the relevant DPP. For instance, a repairer might need to edit the data of the components of the product that the DPP belongs to if they repair the product such that components are changed or otherwise affected. However, a distributor should not have the ability to edit this data as they will not change anything to the components of the product.

Moreover, as stakeholders in the value chain will need to update the data concerning the use and reuse of products, organizations should request access to edit the data separately from requesting access to view the data. Implementing robust authentication mechanisms and verifiable identities could be beneficial for this purpose. This level of security could affect the trust levels of the users towards the DPP (Zhang et al., 2023).

To conclude, system-based requirements and their possible trust precursors are verifiable identities to manage accessibility to the DPP data, decentralized data storage to reduce the risks that go along with centralized data storages, and lastly, secure authentication mechanisms for data editing access.

2.3 Behavioral Intention

To see what the effects are of trust in DPP, another factor that is of great importance is the behavioral intention of using the DPP in decision-making processes regarding circularity and sustainability. Behavioral intention is defined as the perceived likelihood that a person will engage in a specific behavior (Fishbein & Ajzen, 1977). Earlier studies found a positive correlation between behavioral intentions and actual behavior in information systems (Agarwal and Prasad, 1997; Davis, 1989). The findings show that effective usage of information technology is dependent on a positive intention to use the IT system. As DPPs are still in their development process it would be unable to check the actual usage, but therefore behavioral intention is an interesting factor.

Previous studies have shown that trust has a real effect on the behavioral intention component (Hamidi & Chavoshi, 2018). As a result, it is thought to have a significant role in how well information systems and behavior are accepted. Additionally, Tung et al. (2008) demonstrate the importance of this relationship in the literature on healthcare information systems.

Furthermore, research by Alkhater et al. (2018) revealed that trust was a key component that positively impacted an organization's choice to employ cloud services. This study has been performed in the context of the adoption of cloud within private sector organizations.

Also, (Kusuma & Pramunita, 2011) have shown that trust has a positive relation with the behavioral intention of using e-procurement. This, and the other previous research, show the importance of trust in different contexts and how it affects individuals and organizations in the use of an information system.

Further, within the context of sustainability, Pienwisetkaew et al. (2023) found that trust is positively related to the users' behavioral intentions for using an agricultural waste management platform. The study focused specifically on agricultural waste management within the context of circular-economy-based platforms. Besides trust, privacy is another important factor that affects the behavioral intention to use the system within this research.

Besides this, Chen & Zhao (2023) has shown that perceived trust significantly increases the intention to employ green financial security intelligence services. When users feel that intelligence services can deliver better decision-making suggestions, they will be more likely to employ these green intelligence services. Intelligence services are often a base for decision-making processes and provide useful information to base decisions on regarding sustainability factors.

Moreover, Kašparová (2023) analyzed the intention to use business intelligence tools in decision-making processes using the Unified Theory of Acceptance and Use of Technology 2 (Venkatesh et al., 2012). This model ends typically in analyzing the actual use and what factors, such as the behavioral intention, affect this. However, since the DPP is not yet an implemented mechanism, the focus for now will be on the behavioral intention to use the DPP in the decision-making processes regarding circularity and sustainability.

Within this study, behavioral intention is of interest because it is important to understand whether individuals within organizations view the DPP as a mere legal requirement. Specifically, the aim is to understand whether the information provided by upstream suppliers in the value chain is being utilized as intended by the DPP for making decisions on circularity and sustainability, or if it is not being used at all. It can be seen that the relation between trust and behavioral intention is a concept often studied in the context

of technology adoption, and therefore it is also fitting within the context of DPPs. Also, within the context of sustainability and circularity, the concept of behavioral intention to use information systems comes back (Chen & Zhao, 2023; Pienwisetkaew et al., 2023).

2.4 Summary of Prior Research

To summarize, based on the literature search, a set of design requirements and related DPP trust precursors are defined that will be used as input for the remainder of this thesis. An overview of these requirements and precursors is shown in Table 1. Besides this, the concept of trust and its implications within systems and information within systems is understood. And lastly, the concept of the behavioral intention of using (green) information systems has been reviewed.

Table 1. Design requirements of DPP and their trust precursors

No.	Design Requirement	DPP trust precursors
		Information-based
1	Transparency	Showing data collection methods in the DPP Showing data calculation methods in the DPP
2	Product traceability	Data lineage tracking diagrams for component-DPPs
3	Data traceability	Unique location identifiers of legal entities tagged to the data
4	Certification	Third-party certification on data compliance to requirements
		System-based
5	Accessibility	Verifiable identities for access management to the DPP
6	Decentralized data storage	A decentralized system without assigning a single authority to control the data
7	Security	Secure authentication mechanisms for stakeholders with editing access

3 Research Approach

Based on the previous section and the scope of this research, 7 design requirements are defined of which 4 are information-based and 3 are system-based. The design requirements will be analyzed, through the precursors presented in Section 2.2, on how they affect trust in the context of the DPP. Figure 2 presents the research framework and how it will be used in the remainder of this research.

To capture the complexity of how the DPP trust precursors affect either trust in the DPP information or the DPP system, fuzzy-set qualitative comparative analysis (fsQCA) to connect configurational analysis (Ragin, 2009). This theory assumes asymmetric relationships and accommodates equifinality (Ragin, 2000).

First, the assumption of asymmetric relationships allows for nonlinearity in causality, as the factors contributing to one result may differ from those contributing to its absence (Woodside, 2014). This would mean that different DPP trust precursors contribute to the presence of trust compared to its absence. By taking this assumption into account, data points that might have appeared as ‘noise’ within regression-based methods, for example where third-party certification is low and trust in the DPP information is high, are important evidence for asymmetry (Y. Liu et al., 2017). This is particularly important because, even if a user evaluates an IS attribute negatively, they may nevertheless adopt it due to good evaluations of other attributes.

Second, equifinality refers to situations in which two or more sets of conditions can result in the same outcome (Fiss, 2011). This could result in a combination of verifiable identities and decentralized data storage leading to high trust, as well as a configuration of decentralized data storage and secure authentication mechanisms for data editing. This is useful since multiple precursors are under consideration and it is highly likely that not only one configuration will be the determinant for either high or low trust, even though this is still possible.

However, what has to be kept in mind when comparing fsQCA to regression-based methods is that they have different assumptions and interpretations which means that they cannot be compared exactly one to one (Y. Liu et al., 2017). Looking at the research framework, presented in Figure 2, the configurational approach seems fitting to use on the left side of the framework because multiple independent variables that can work together in different sets are analyzed on their effect on trust. Their contributions to trust,

even though literature shows this is likely positive, see Section 2.2, could well be negative, which are also valuable insights to gather.

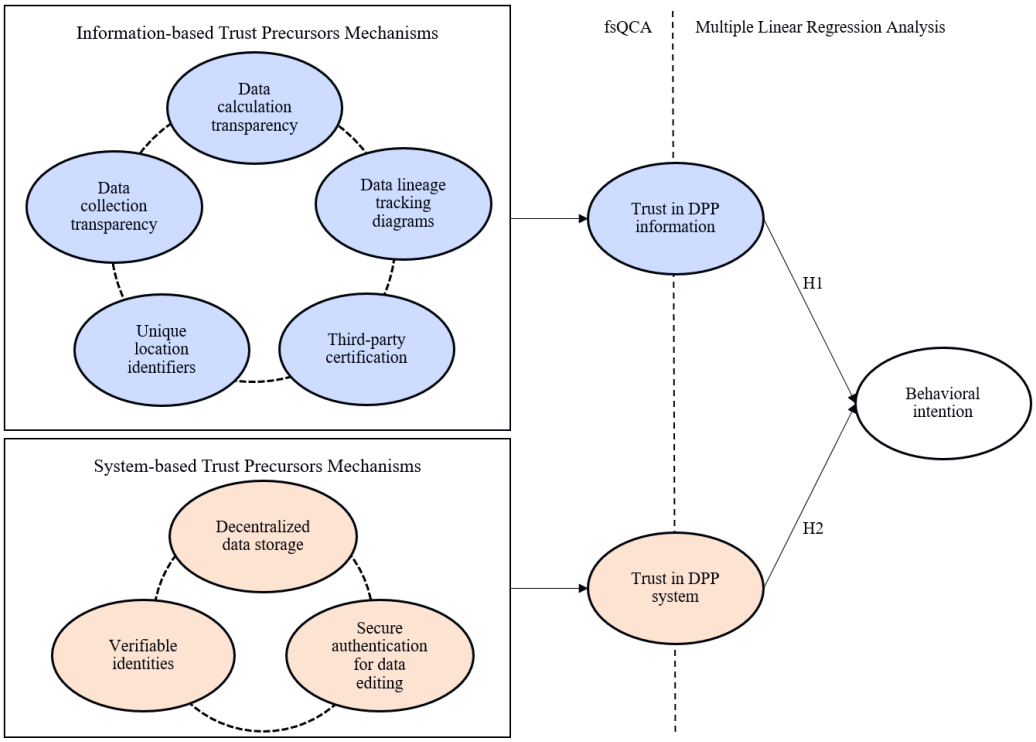

Figure 2. Research framework

For the right side of Trust in DPP, divided by the dotted line, two hypotheses are formed to evaluate the effect of trust on behavioral intention. Trust, in this research, is separated on information and system level. To analyze these relationships, a variance-based approach is used. This approach will provide a straightforward and interpretable way to understand the relationships between the trust variables and the behavioral intention as it enables to calculate the proportion of the dependent variable's variation that may be linked to each independent variable and any interactions between the independent variables (Hassouna, 2023). The hypotheses to be analyzed are:

H1: Trust in the information in the DPP is positively related to the behavioral intention to use the DPP in the decision-making process regarding circularity and sustainability

H2: Trust in the DPP system is positively related to the behavioral intention to use the DPP in the decision-making process regarding circularity and sustainability

4 Methodology

This chapter will provide insights on how the data for this research is gathered and analyzed. First, the selected methodology for this research is described. Second, it describes how the data is collected. Next, the data analysis methods are introduced and the use of AI tools are discussed, and lastly, how all the previous points are done ethically is stated.

4.1 Selection of Methodology

This study employs both a complexity theory and a quantitative approach to investigate the research questions defined in Section 1.1. To begin with, the effect of the design requirements and its precursors on trust towards the DPP are analyzed using a configurational approach (complexity theory) to show the complex relation between the DPP trust precursors and the variables of trust in the DPP information and DPP system. Using this approach, it is kept in mind that the precursors can have asymmetric relations (Woodside, 2014) and can be present in different configurations leading to the same outcome (Ragin, 2009), as discussed in Section 3.

In the second part of the research, a quantitative approach is used to analyze the quantitative relationship between the independent trust variables, and the behavioral intention. This is useful to get broader insights from different but relevant sectors and organizations. Compared to a qualitative approach, a quantitative approach offers a more objective examination of data, which is useful for measuring the extent of certain behavior (Evrin, 2021).

The primary data collection method used in this research is a survey designed to gather responses from relevant stakeholders. Relevant stakeholders in this research are employees within value chains that will have to either implement or work with a DPP, or both, in the near future (King et al., 2023).

4.2 Data Collection Methods

The survey will be introduced with a current prototype of the DPP (Avery Dennison Corporation, 2023) and the respondents will be asked to base their answers on this prototype. This prototype is an example of a DPP of a sweater, showing, among others, its material information, its journey, and its environmental impact. Next to this, there is

an explanation provided on what DPPs entail, shown in Appendix 2. This will make sure that the knowledge of the respondents about DPP is, at least, raised to a minimal level of understanding which will make their answers more valuable. As indicated in Section 2.1.1, users can evaluate the trustworthiness of an information system before using it by basing their thoughts on their first impression of the user interface (Meeßen et al., 2019). Also, for the conditions, short explanations to show what they entail are given to make sure the respondents at all times know, to a certain extent, what they are answering on. This has been done to mitigate the limitation regarding the scarce knowledge of participants regarding DPPs and the conditions used in this study. The information provided in the survey is shown in Appendix 2.

The survey is done electronically using an online survey platform, Qualtrics[2], provided by Tilburg University. Relevant participants for this study are people who have to work with DPPs, either provide or use data, in an organizational setting. At first, the survey is aimed at sectors that will have to implement the DPPs first, such as textiles, construction, batteries, and electronics. However, any insights from individuals within organizations that will have to work with DPPs are welcomed.

Participants are invited to complete the questionnaire through personalized email invitations, social media channels (LinkedIn and WhatsApp), and professional networking. Thus, convenience sampling is used. Additionally, snowball sampling techniques are utilized to encourage existing participants to share the survey link with their contacts who meet the selection criteria. These sampling techniques offer a time and cost-effective method for data collection as personally inviting people to fill in the survey, as noticed during the time of data collection has worked best.

The survey has been open for respondents from the 31st of May 2024 to the 9th of July 2024. During this time, 65 respondents completed the survey without skipping one question, out of 128 total responses. Using a question asking for the respondent's job title, irrelevant responses are taken out of the dataset. For the analysis, only complete responses are used. Table 3 summarizes the demographics of the sample of survey participants. Note that one respondent's organization can be present in multiple places in the value chain and therefore, the addition of all percentages within this category does not add up to 100%.

[2] Qualtrics XM

4.2.1 Measures

The survey instrument consists of structured questionnaire items designed to measure the trust level in the DPP information and its system and the conditions as described in Table 1. Whenever possible, established measures are used for the conditions (Gupta et al., 2024; Venkatesh et al., 2003, 2016; Wu et al., 2021; Zhang et al., 2023). For the other conditions, the measurements are based on statements from previous research regarding that specific condition (Aslam & Mrissa, 2023; Brunner et al., 2021; Cui et al., 2018; Darnall et al., 2018; Dujak et al., 2017; Ghorbel et al., 2022; Guntzburger et al., 2021; Narang & Gupta, 2018; Salman et al., 2015; Tewari & Gupta, 2020). The measurement constructs along with their relevant sources can be found in Appendix 1. First, a 5-point Likert scale will be used to make sure the responses are valuable, but the survey is not too hard to complete, as could happen with, for example, a 7-point Likert scale. This reduces the risks of respondents not pursuing to the end of the survey.

4.2.1.1 Construct Validity

The construct validity testing, using Pearson's correlation, provided strong evidence that the constructs were valid. All measures significantly correlate with their respective constructs, showing that they are appropriate and effective indicators of these constructs. This significant correlation indicates that the measures accurately capture the intended constructs and are not influenced by other factors.

Besides this, convergent validity was determined by calculating the average variance extracted (AVE). The AVE of all constructs exceeds the threshold value of 0.5 with the AVE of trust in the DPP information being the lowest with 0.558.

Lastly, using the squares of all the AVE values, discriminant validity is assessed. All constructs were deemed valid in this test because the Fornell and Larcker criteria (Wong, 2013) are met when the square root of each construct's AVE is higher than its correlation with other constructs. All results are summarized in Table 2.

4.2.1.2 Reliability

Reliability is tested using Cronbach's Alpha (Cronbach, 1951). During this analysis, one measure was found that, when deleted, resulted in a significant increase in Cronbach's Alpha. This was the case for the second question related to trust in the information in the

DPP, ‘I believe the DPP would include few uncertainties’. This measure is deleted for further analysis as it does not effectively contribute to the reliability of the construct. Deleting the measure results in Cronbach’s Alpha going up from 0.589 to 0.738. The reason for the unreliability of the measure could be the wording of the measure, ‘I believe the DPP would include few uncertainties’, where the word ‘few’ might cause unclearness in the statement.

From that point on the construct related to data calculation transparency has the lowest reliability score (0.624), however, as it is above 0.6, and deleting one of the measures does not make a drastic change in the resulting Cronbach’s Alpha, none of the measures are deleted for further analysis.

Table 2. Construct reliability, convergent validity, and discriminant validity results

	VI	BI	C	CAT	COT	DDS	DLT	ULI	S	TI	TS
Cronbach's alpha	0.765	0.894	0.832	0.624	0.756	0.815	0.722	0.760	0.761	0.738*	0.856
AVE	0.584	0.825	0.748	0.565	0.644	0.716	0.570	0.658	0.676	0.558	0.773
VI	0.764										
BI	0.189	0.909									
C	0.463	0.125	0.865								
CAT	-0.052	-0.084	0.081	0.751							
COT	0.031	0.047	0.205	0.693	0.803						
DDS	0.448	0.234	0.360	0.025	0.220	0.846					
DLT	0.339	0.035	0.339	0.217	0.272	0.241	0.755				
ULI	0.492	0.020	0.231	0.265	0.228	0.349	0.256	0.811			
S	0.334	0.228	0.252	0.134	0.255	0.281	0.125	0.258	0.822		
TI	0.411	0.279	0.267	-0.279	-0.245	0.131	0.100	0.149	0.167	0.747	
TS	0.374	0.341	0.130	-0.240	-0.183	0.276	-0.061	0.095	0.299	0.537	0.879

* Cronbach’s alpha when measure T2 deleted
VI: verifiable identities; BI: behavioral intention; C: third-party certification; CAT: data calculation transparency; COT: data collection transparency; DDS: decentralized data storage; DLT: data lineage tracking; ULI: unique location identifiers; S: secure authentication for data editing; TI: trust in DPP information; TS: trust in DPP system

4.3 Data Analysis Methods

To be able to answer the two research questions, provided in Section 1.1, this study involves two separate data analyses. The first analysis focuses on the first research question and uses fuzzy set Qualitative Comparative Analysis (fsQCA) to retrieve a set of conditions that are predicted to enhance trust in the information in the DPP and the DPP system. The second analysis uses multiple linear regression to see whether there is

a relation between the levels of both versions of trust and the behavioral intention to use the DPP in the decision-making process regarding sustainability and circularity.

Table 3. Demographics of 65 survey participants

	%		%
Age		**Place in the value chain**	
18-24 years old	4.6%	Raw material supplier	6.2%
25-34 years old	36.9%	Component supplier	9.2%
35-44 years old	18.5%	Manufacturer/producer	33.8%
45-54 years old	18.5%	Quality control/assurance	9.2%
55-64 years old	18.5%	Packaging	7.7%
65+ years old	3.1%	Logistics and distribution	10.8%
DPP knowledge		Wholesale	7.7%
Unfamiliar	13.8%	Retail	12.3%
Neutral	24.6%	Repairer/ recycler/ remanufacturer	7.7%
Familiar	61.5%	IT	15.4%
Sector		Research/ Consultancy	24.6%
Textiles	9.2%	Others	9.2%
Construction	21.5%	**Base of operations**	
Electronics	10.8%	The Netherlands	89.2%
Batteries	1.5%	Belgium	3.1%
Others	56.9%	Portugal	1.5%
Number of employees in the organization		Bulgaria	1.5%
Less than 10	15.4%	Switzerland	1.5%
Between 10 and 49	13.8%	Sweden	1.5%
Between 50 and 249	24.6%	Ireland	1.5%
250 or more	46.2%		

4.3.1 FsQCA on DPP Trust Precursors and Trust

To analyze the gathered data and see what conditions and combinations of conditions influence trust in the DPP, a fuzzy set Qualitative Comparative Analysis (fsQCA) will be used. In fsQCA, the variables that are analyzed are called conditions. Bridging the gap between quantitative and qualitative methodologies, it explores various potential solutions for enhancing trust in DPPs rather than just identifying a single optimal one, a limitation often encountered in traditional variance-based analyses (Pappas & Woodside, 2021). Some conditions might not matter on their own but become important when combined with others, while some are crucial by themselves. Compared to variance-based

analyses, fsQCA puts the variables in a non-competing environment and takes into account the relations between these variables when determining the effect on the outcome variable (Mendel & Korjani, 2013; Pappas & Woodside, 2021). FsQCA shows us which factors are essential and which combinations are most influential. Furthermore, because system design must meet varying user demands, fsQCA's ability to calculate multiple solutions for different user types exceeds the constraints of regression analysis (Pappas & Woodside, 2021).

4.3.1.1 Data Calibration and Truth Table Analysis

Performing fsQCA consists of different steps. After gathering all the data through the survey, validating and checking the reliability of the measurements, and aggregating the validated and reliable constructs, these constructs are calibrated to a (0,1) fuzzy set membership where 0 is a full non-member of the set and 1 a full member of the set. The thresholds on which the data is calibrated are determined by the researcher. Calibrating the data is done to meet the needs of both quantitative and qualitative researchers by understanding relevant and irrelevant variations and positioning cases relative to one another (Vis, 2012).

To calibrate the values in this study, the 5, 50, and 95 percentiles for each variable were determined. As can be seen in Table 4, for the variable TI (trust in DPP information) the 50 and 95 percentile are both 4.0 which will lead to problems during the calibration within fsQCA. Therefore, for the calibration of TI and its conditions (COT, CAT, DLT, ULI, and C), calibration values fitting for Likert scales of 5 are used, namely 2, 3, and 4 (Pappas & Woodside, 2021). Because it is recommended to use the 5, 50, and 95 percentiles, these values are kept for the variables TS, VI, DDS, and S. After calibrating, the truth table analysis has been done as presented in the following sections.

Table 4. Calculated percentiles per variable

Percentile	TI	COT	CAT	DLT	ULI	C	TS	VI	DDS	S
5	2.50 *(2)*	2.43 *(2)*	3.00 *(2)*	2.77 *(2)*	2.43 *(2)*	2.43 *(2)*	2.42	2.81	2.00	3.00
50	4.00 *(3)*	4.00 *(3)*	4.00 *(3)*	4.00 *(3)*	4.00 *(3)*	4.00 *(3)*	4.00	3.75	3.33	4.00
95	4.00 *(4)*	5.00 *(4)*	5.00 *(4)*	4.33 *(4)*	5.00 *(4)*	5.00 *(4)*	5.00	5.00	4.92	5.00

After the data is calibrated, truth tables are generated for both high and low trust in the information in the DPP and the DPP system. For the first, the causal conditions are the

information-based conditions from Table 1, and for the latter, the causal conditions are the system-based conditions from Table 1. Next, a frequency threshold is established to guarantee that a minimum number of examples are gathered for assessing the relationships (Pappas & Woodside, 2021). As the sample in this study is relatively small (<150), the threshold is set at 1. This means that any combination that that does not occur is removed from further analysis and anything on and above the frequency threshold is included which would include solutions that would be seen as outliers in a variance-based analysis. Besides a frequency threshold, a consistency threshold should be set which is recommended to be set at a minimum of 0.75 (Rihoux & Ragin, 2009) and preferably it is set at a natural breaking point in the derived consistency values (Pappas & Woodside, 2021). For this analysis, a raw consistency threshold of 0.85 is used to make sure the analysis produces effective results. Besides this, a PRI consistency threshold of 0.70 is used to make sure the results for high and low trust do not overlay each other.

Computing this truth table results in three solutions, a complex solution, a parsimonious solution, and an intermediate solution (Pappas & Woodside, 2021). The first displays all of the potential combinations of conditions when typical logical processes are used. The second is a simplified form of the complex solution and shows the most significant requirements that must be included in every solution. And lastly, the intermediate solution is part of the complex solution, which includes the parsimonious one. Therefore, the intermediate solution and parsimonious solutions are used for the interpretation of the results. The results of this analysis are presented in Section 5.1.

4.3.2 Multiple Linear Regression on Trust and Behavioral Intention

To test the relation between the two trust variables and behavioral intention, multiple linear regression analysis is done. Its purpose is to identify and learn more about the relationship between multiple independent variables and a single dependent variable and extends on the simple linear regression method (Weissberg, 1980 in (Oztekin, 2011)).

In this study, the dependent variable (Y) is the behavioral intention to use the DPP in the decision-making process regarding sustainability and circularity. There are two independent variables, namely trust in the information within the DPP (X_1) and trust in the DPP system (X_2). The basic form of the two-independent-variable simple linear regression model is:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \epsilon$$

Where:

- β_0 is the y-intercept, meaning, the value of Y when both X_1 and X_2 are 0.
- β_1 and β_2 are the coefficients of X_1 and X_2, and represent the change in Y that results from a one-unit change in X_1 and X_2, respectively.
- ϵ is the error term, which represents the variation between the actual and predicted values of Y

There are a few limitations to this method that should be mitigated as much as possible and kept in mind when performing the analysis. First, it is assumed that the independent and dependent variables have a linear relationship and that the errors have a normal distribution with constant variance. When these assumptions are not met, biased or inefficient estimates can be deducted. To test the assumptions, checks on linearity and constant variance are done using a predicted probability plot and a scatterplot. Second, to make sure that the independent variables are not highly correlated, which would make it hard to determine the effect of them separately, the Variance Inflation Factor (VIF) is checked which indicates minimal concern when it is below 5.0.

After the data measures have been validated and checked for reliability and the measures are aggregated to the construct level, the multiple linear regression analysis is performed with the use of statistics software. At first, the relationship is tested on the whole dataset and, to check for specific cases and possibly different end users, the demographics, as presented in Table 3, are used to check for significance in specific cases, e.g., a specific sector or an organization with more than 250 employees. The results of this analysis are presented in Section 5.2.

4.4 Use of AI-tools

Within this research, Copilot[3], by Microsoft, is used to improve the readability of this thesis. As English is the researcher's second language, the AI tool is used to improve the structure and grammar of sentences, determine synonyms used in the text, and check for clarity of the written text.

The researcher claims that the outputs of the AI tool are understood, assessed, and critically evaluated before implementing them into the text of this thesis. Results that are

[3] Copilot (microsoft.com)

not considered to be true or do not provide any improvement to the text, from the eyes of the researcher, are not used.

4.5 Research Ethics

This research adheres to ethical guidelines governing research. Participants are provided with informed consent information outlining the purpose of the study, their rights as participants, and confidentiality assurances, as shown in Appendix 3. Data confidentiality and anonymity are maintained throughout the study, with identifiable information kept confidential and data aggregated for analysis purposes.

In terms of data sharing and access, the data collected will be kept confidential and only accessible to the researcher conducting this study. No other parties will be granted access to this data. As for long-term preservation and sustainability, the dataset will be destroyed upon the conclusion of the study to maintain the confidentiality of the participants. While the results of the study will be made public, no data will be traceable back to any individual who participated in the survey. This approach ensures the privacy and rights of all participants are respected throughout the research process. An overview of the research data management plan can be found in Appendix 4.

5 Results

This section will dive into the results of both the fsQCA and multiple linear regression analysis presented in the previous section. First, the fsQCA results are presented including the calibration methods, and the results for the DPP information and DPP system are separated. Afterward, the results of the multiple linear regression are presented, including the assumptions testing.

5.1 FsQCA

This section will provide the results of the fsQCA. To present the outputs of the analysis, the notation system suggested by (Ragin, 2009) was used. The outputs consist of the peripheral conditions from the intermediate solutions along with the core conditions from the parsimonious solution. Core conditions present a strong relation. Table 5 and Table 6present these solutions along with a legend presented in the note. These tables also present the raw consistency, raw coverage, and unique coverage per configuration and the overall solution consistency and coverage.

5.1.1 Information-based Conditions for High and Low Trust in the DPP Information

First, Table 5 shows the outcome of the analysis of the 5 information-based conditions in relation to trust in the DPP information. This has resulted in four configurations that explain high trust and one configuration that explains low trust in the DPP information. This illustrates that the performance of no single condition would be superior to combinations of conditions.

The overall solution coverage of the high trust configurations is 0.878 which shows that the extent to which the trust in the DPP information may be explained by the information-based conditions is high. For low trust, this extent of explanation is relatively low (0.304). Both overall solution consistencies are above the minimum threshold of 0.75 and the overall solution consistency of high trust is above the suggested threshold (0.80) (Pappas & Woodside, 2021).

Table 5. Sufficient configurations for high and low trust in the DPP information

	High trust				Low trust
Configuration	HI1	HI2	HI3	HI4	LI1
Data collection transparency	•	•		⊗	•
Data calculation transparency	●	•	●	⊗	•
Data lineage tracking		•	•	⊗	⊗
Unique location identifier	⊗	●	●	●	⊗
Third-party certification	●		●	•	
Consistency	1	0.877	0.894	1	0.762
Raw coverage	0.149	0.784	0.799	0.042	0.304
Unique coverage	0.021	0.015	0.030	0.009	0.304
Overall solution consistency		0.885			0.762
Overall solution coverage		0.844			0.304

Note: black circles (•) indicate the presence of a condition and circles with 'x' (⊗) indicate its absence. Large circle (●) or bold circle with 'x' ⊗; core condition, small circle peripheral condition, blank space; 'don't care' condition

The first configuration for high trust in the DPP information, HI1, indicates that when core conditions data calculation transparency and third-party certification are present, data collection transparency is present, and unique location identifiers are absent, regardless of data lineage tracking, trust in the DPP information is high. This configuration has a consistency of 1 which would indicate that the configuration is perfectly consistent with the outcome, however, coverage is low (14.9%) meaning that it is only supported by a small part of the participants.

Second, HI2 indicates that when core condition unique location identifiers are present, and data collection transparency, data calculation transparency, and data lineage tracking are also present, regardless of third-party certification, a high level of trust in the DPP information is expected. HI2 has a decent consistency of 0.877 and is supported by 78.4% of the participants.

Third, HI3 indicates a high level of trust in the DPP information when a set of core conditions is present, including data calculation transparency, unique location identifiers, and third-party certification, along with data lineage tracking as a peripheral condition.

HI3's consistency and coverage are higher than that of HI2's, namely 0.894 and 0.799, respectively.

The last configuration, HI4, suggests that trust in the DPP information is high when the core condition unique location identifiers are present, along with third-party certification, and data collection transparency, data calculation transparency, and data lineage tracking are absent. Similar to H1I, this configuration has a consistency of 1, suggesting that it is perfectly consistent with the outcome, however, it is only supported by 4.2% of the participants.

Considering low trust in the DPP information, the one configuration, with core conditions data lineage tracking and unique location identifiers being absent, along with the presence of data collection transparency and data calculation transparency, has a relatively low consistency, of only 0.765. Also, the extent to which the configuration is supported by the participants is relatively low, namely 30.4%.

5.1.2 System-based Conditions for High and Low Trust in the DPP System

Second, the results of the fsQCA, testing the relation between system-based conditions and trust in the DPP system, are shown in Table 6. It can be seen that this analysis resulted in one configuration for high trust and three configurations for low trust in the DPP system. For high trust, this is less than the first analysis, however, this is also influenced by the fact that fewer conditions were used as input which leads to fewer configurations (2^n) in the first place.

Regarding the high trust configurations, the solution coverage is high (0.831). This indicates that the extent to which this trust is explained by the two configurations is high. Further, the overall solution coverage for low trust is relatively high as well (0.726), so the extent to which the configurations explain low trust in the DPP system is relatively high as well. Further, the overall solution consistencies for both low trust in the DPP system is above the recommended threshold of 0.75 (Pappas & Woodside, 2021), this is not the case for the overall solution consistency of high trust in the DPP system (0.668).

Table 6. Sufficient configurations for high and low trust in the DPP system

	High Trust	Low Trust		
Configuration	HS1	LS1	LS2	LS3
Verifiable identities			⊗	⊗
Decentralized data storage		⊗		⊗
Secure authentication for data editing	•	⊗	⊗	
Consistency	0.668	0.949	0.898	0.898
Raw coverage	0.831	0.574	0.579	0.568
Unique coverage	0.831	0.076	0.081	0.071
Overall solution consistency	0.668		0.868	
Overall solution coverage	0.831		0.726	

Note: black circles (●) indicate the presence of a condition and circles with 'x' (⊗) indicate its absence. Large circle (●) or bold circle with 'x' ⊗; core condition, small circle peripheral condition, blank space; 'don't care' condition

The first and only configuration for high trust presents secure authentication for data editing as a peripheral condition. It suggests that the participants of this study indicate a high level of trust in the information DPP system when there is a high level of secure authentication mechanisms for data editing rights. Therefore, these secure authentication mechanisms for editing rights can be seen as a single predictor for high trust in the DPP system from the view of employees who will work with this system after deployment of the DPP within their relative field. This is also shown by the coverage of this configuration, namely 0.831. However, the consistency of this configuration is not that high, namely 0.668.

Regarding the configurations for low trust in the DPP system, LS1 suggests that the absence of decentralized data storage and the absence of secure authentication for data editing, regardless of verifiable identities leads to low trust in the DPP system. This combination is also a core condition for low trust in the DPP system and is supported by 57.4% of the participants. This configuration is most likely to lead to low trust in the DPP system as it has the highest consistency score of 0.949.

Second, configuration LS2 indicates that low trust in the DPP system is achieved through the absence of verifiable identities and secure authentication mechanisms for data editing, regardless of decentralized data storage. Same as for LS1, this combination of absent conditions is considered a core condition for low trust in the DPP system and is supported by the highest number of participants, namely 57.9%.

Lastly, configuration LS3 indicates that low trust in the DPP system is caused by the absence of verifiable identities and secure authentication mechanisms for data editing. Similar to the previous configurations, this combination is also a core condition. Further, this configuration is supported by 56.8% of employees who will work with the system after deployment and participated in this study. Both LS2 and LS3 have a consistency score of 0.898 and therefore are less likely to lead to low trust than LS1 but still have acceptable consistency values.

5.2 Multiple Linear Regression Analysis

To answer research question 2, multiple linear regression is done with the behavioral intention being its dependent variable. The two independent variables are trust in the DPP information and trust in the DPP system. As multiple linear regression is sensitive to outliers, an outlier analysis is performed. This resulted in one response that could be seen as an outlier, however after manually looking at the specific response, no specific reason why it should be taken out the analysis, such as 'flat-lining', was found. To be able to perform the regression analysis, the assumptions, as presented in Section 4.3.2 have to be tested. Afterward, the multiple linear regression analysis is done and presented.

5.2.1 Assumption testing

As explained in Section 4.3.2, multiple linear regression is based on a set of assumptions that have to be met when performing the analysis. First, linearity is checked using a prediction-probability plot, as shown in Figure 3. It can be seen that the data follows the reference line in a linear way and no outstanding data points above or below the reference line are found.

Second, a scatterplot is created to check the assumption of constant variance, as shown in Figure 4. Most data points are equally distributed around both x equals 0 and y equals 0. There is one outstanding data point, but as explained before, there was no reason for deleting this response from the data. Because of the distribution of data points around 0, the constant variance assumption is met.

Lastly, to check for multicollinearity, the VIF is checked and presented in Table 77. The VIF of both independent variables is 1.289 which indicates minimal concern for multicollinearity. Thus, the independent variables are not highly correlated and the effect of them can be determined separately.

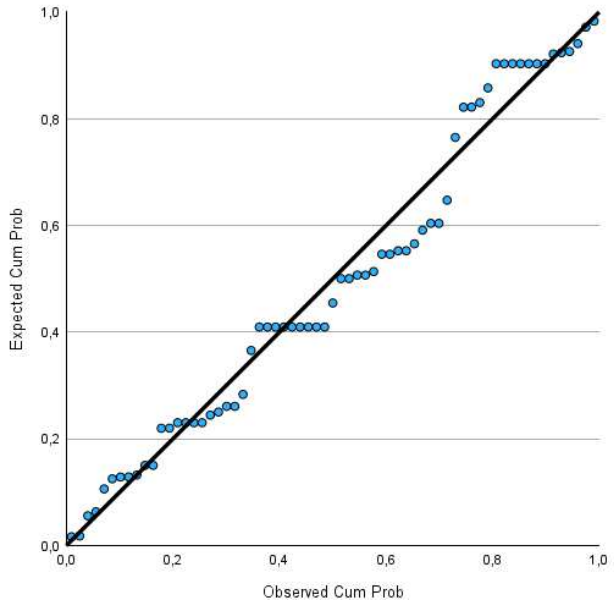

Figure 3. Predicted probability plot with behavioral intention as dependent variable and trust in the DPP system and trust in the DPP information as independent variables

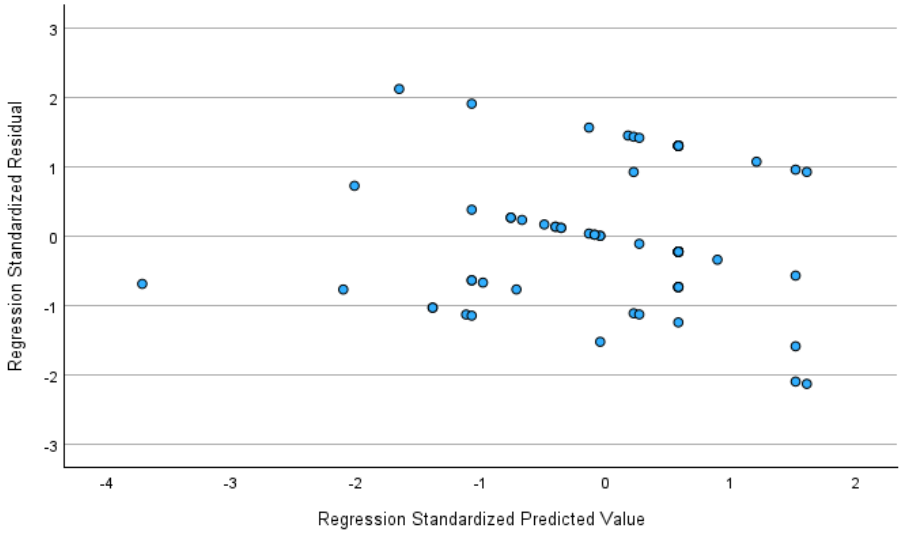

Figure 4. Scatter plot with behavioral intention as the dependent variable and both trust in the DPP system and trust in the DPP information as the independent variables

5.2.2 Trust to Behavioral Intention

As the assumptions of multiple linear regression are met, the multiple linear regression analysis is performed. The results are presented in Table 77. To begin with, the regression model included a constant term with a value of 2.561. This constant term was statistically significant with a t-value of 4.921 and a p-value of <.001, indicating that the model significantly differs from zero.

Table 7. Multiple linear regression with behavioral intention as the dependent variable and both trust in the DPP system and trust in the DPP information as the independent variables

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	2.561	0.520		4.921	<0.001		
	TI	0.172	0.162	0.153	1.057	0.294	.680	1.472
	TS	0.225	0.136	0.239	1.658	0.102	.680	1.472

Second, the independent variable trust in the DPP information (TI) had an unstandardized coefficient (B) of 0.172, representing the change in behavioral intention for a one-unit change in the trust in DPP information, while holding trust in the DPP system constant, and a standardized coefficient (Beta) of 0.153. On the other hand, the t-value of 1.057 resulted in a p-value of 0.294, which is not statistically significant at the commonly used .05 level. This suggests that trust in the DPP information does not have a significant unique contribution to the prediction of the behavioral intention to use the DPP in the decision-making process regarding circularity and sustainability when controlling for the other variables in the model. Therefore, hypothesis 1 (see Section 3) cannot be supported.

Third, the independent variable trust in the DPP system had an unstandardized coefficient (B) of 0.225, representing the change in behavioral intention for a one-unit change in the trust in the DPP system, while holding trust in the DPP information constant, and a standardized coefficient (Beta) of 0.239, meaning that it would have a greater effect on behavioral intention than trust in the DPP information. However, the t-value of 1.658 resulted in a p-value of 0.102, which is also not statistically significant at the .05 level. This suggests that trust in the DPP system does not have a significant unique contribution to the prediction of behavioral intention to use the DPP in the decision-making process regarding circularity and sustainability when controlling for the other variables in the model. Therefore, hypothesis 2 (see Section 3) cannot be supported.

After running the model without any control variables, the model was run for all descriptive variables, as presented in Table 3, separately and in consecutive groups like more than 50 employees, so including ‘between 50 and 249 employees’, and ‘250 or more employees’. However, for none of the smaller groups of respondents, the model was significant at the 0.05 level, for neither of the independent variables.

6 Discussion

The following discussion seeks to illustrate the findings of this study concerning the gap identified in research regarding DPPs. Central to this investigation were two key research questions: Which DPP trust precursors, and combinations thereof, positively affect trust in the DPP? And, what is the effect of trust in the DPP on the behavioral intention to use the DPP in decision-making processes regarding circularity and sustainability? These questions guided the investigation of trust precursors within DPPs, intending to understand what individual stakeholders deem important for the success of the DPP. The discussion that follows will dive into the interpretations and implications of the findings, comparing them with existing literature, acknowledging the limitations of the study, and suggesting future research directions.

6.1 Interpretation of Findings

6.1.1 Conditions and Trust

First, the relation between the DPP trust precursors and the two variants of trust is discussed, with first, information-based trust and second, system-based trust.

6.1.1.1 Information-based Trust

The fsQCA approach indicates that there exist different and often substitutable configurations for high and low trust in the DPP information and the DPP system. Four configurations may lead to high trust in the DPP information and one configuration may lead to low trust in the DPP information. One configuration may lead to high trust in the DPP system and three configurations may lead to low trust in the DPP system.

Regarding high trust in the DPP information, there is not one trust precursor that is present in all configurations. This shows that no single precursor in itself can produce high trust, instead, it requires a combination of precursors that must work together for stakeholders to perceive high trust. Unique location identifiers are present in 3 out of 4 configurations and absent in the other (HI1). If there are no unique location identifiers, third-party certification, data collection transparency, and data calculation transparency may together contribute to high levels of trust in the DPP information. Data lineage tracking did not appear in this configuration meaning that stakeholders can still perceive high trust in the DPP information without data lineage tracking in the DPP.

This first configuration is mostly focused on the credibility of the data, which is consistent with previous research analyzed in Section 2.1.1 (Acikgoz et al., 2023; Thielsch et al., 2018), as it has been previously found that the credibility of the information has a positive effect on trust and it increases the transparency related to the data (Faniel & Jacobsen, 2010; Schmidthuber et al., 2023; Wallis et al., 2007). On the other hand, this configuration is not in accordance with the literature as it disregards data lineage tracking which contributes to the completeness of information (Thielsch et al., 2018) and implies unique location identifiers not being there, while they contribute to the correctness of the data (Acikgoz et al., 2023; Schmidthuber et al., 2023). As can be seen before, this configuration is also not supported by many participants in this research, but it did show up due to its high consistency.

The second configuration (HI2) for high trust in the DPP information reflects the findings of the former literature as it covers a wider set of antecedents of trust. First, both data collection and calculation transparency contribute to the transparency (Faniel & Jacobsen, 2010; Schmidthuber et al., 2023; Wallis et al., 2007) and credibility of the information (Acikgoz et al., 2023; Thielsch et al., 2018) of the DPP by showing how data is collected and transformed into the information that can be found in the DPP.

Second, data lineage tracking contributes to the completeness of the information (Thielsch et al., 2018) by showing component DPPs to maximize the traceability of the components of the product at hand.

Third, as a fundamental prerequisite, the availability of unique location identifiers enhances the accuracy of data (Acikgoz et al., 2023; Thielsch et al., 2018) and the traceability of data providers (Schmidthuber et al., 2023) by facilitating efficient communication and data sharing among trading partners.

Lastly, since third-party certification does not appear in this configuration, meaning that high trust in the DPP information can still be achieved without this precursor. It is positive to see that this configuration, which is supported by existing literature, is supported by a large part of the participants which shows that it has high potential to cause a high level of trust in the DPP information.

The third configuration (HI3), similar to the second one, also reflects the findings of the literature (Acikgoz et al., 2023; Faniel & Jacobsen, 2010; Schmidthuber et al., 2023; Thielsch et al., 2018; Wallis et al., 2007), as, compared to the second configuration, data

collection transparency is interchanged with third-party certification, adding another core condition to the configuration. This means that stakeholders can still have high trust in the DPP information when data collection transparency is low. This combination still contributes well to the credibility of the information (Acikgoz et al., 2023; Thielsch et al., 2018) as the data is checked against regulations. This has a positive effect on the stakeholders' perceived trust in the DPP information. Also, comparable to the second configuration for high trust in the DPP information, is that it is supported by a large part of the participants of the study, with nearly 80%.

Further, the last configuration (HI4) for high trust in the DPP information is more contradictory to the literature. It still follows the literature because it presents the availability of unique location identifiers and third-party certification to contribute to completeness (Thielsch et al., 2018), traceability of the data provider (Schmidthuber et al., 2023), and the quality of the data (Acikgoz et al., 2023; Thielsch et al., 2018; Yoon & Lee, 2019), which in turn has a positive effect on trust in information. However, it suggests that even without data collection transparency, data calculation transparency, and data lineage tracking, stakeholders can still perceive a high level of trust in the DPP information if the other factors are in place.

One could argue that the amount of information can be too much (Thielsch et al., 2018) and therefore not all trust precursors can work together, however, these precursors are still expected to have a positive effect on the credibility, transparency, and completeness of the information (Acikgoz et al., 2023; Faniel & Jacobsen, 2010; Kratz & Strasser, 2015; Schmidthuber et al., 2023; Thielsch et al., 2018; Wallis et al., 2007). This configuration is only supported by 4.2% of the participants which is fitting as the configuration is contradictory to the literature.

Looking at configuration LI1, stakeholders will have low trust in the DPP information when data lineage tracking and unique location identifiers are not there, both being core conditions. Since third-party certification does not appear in this configuration, stakeholders can still perceive a low level of trust in the DPP information when certifications are or are not part of the DPP.

This configuration is in line with the literature as the trust precursors that are low or not there would contribute to the completeness (Thielsch et al., 2018) and correctness (Acikgoz et al., 2023; Thielsch et al., 2018) of the data, and the traceability of the data provider (Schmidthuber, 2022), leading to a higher level of trust. However, data lineage

tracking could also provide a too large amount of data leading to low trust in the information provided (Thielsch et al., 2018).

On the other hand, a low level of trust in the DPP information being achieved with high data collection and data calculation transparency is not consistent with previous studies as these trust precursors would contribute to the credibility of the data (Kratz & Strasser, 2015) and transparency of the data, which in turn would have a positive effect on trust and, thus, should lead to high trust instead of low trust in the DPP information (Acikgoz et al., 2023; Faniel & Jacobsen, 2010; Schmidthuber et al., 2023; Thielsch et al., 2018; Wallis et al., 2007). This configuration is supported by 30.4% of the participants of this study which shows that the configuration is not that likely to occur, compared to, for example, HI2 and HI3.

Overall it can be seen that the configurations that are most consistent with the literature are supported by the largest groups of participants (HI1 and HI2). However, as there is only one configuration that passed the thresholds for low trust in the DPP information, it could well be that there are other factors that affect the low perception of trust in the DPP information.

Looking at the core conditions of both high and low trust, it can be seen that unique location identifiers play the most important role for stakeholders in predicting high or low trust. Data calculation transparency and third-party certification also have a strong relation with the stakeholders' perception of high trust in the DPP information as they are a core condition in both HI1 and HI3. Besides the case that unique location identifiers are not there, leading to a low level of trust in the DPP information, not having data lineage tracking also has this same result. Further, the results show that trust is often the result of a combination of factors, rather than a single factor, which aligns with previous research (Lippert, 2001).

6.1.1.2 System-based Trust

Looking at the fsQCA results of trust in the DPP system, only one configuration met the thresholds to come out of the truth table analysis. This configuration indicates that stakeholders perceive secure authentication mechanisms for data editing as the only predictor for high trust in the DPP system. This means that it can achieve high trust by itself, instead of requiring a combination of precursors to achieve high trust in the DPP system. The availability of secure authentication mechanisms within DPPs aligns with

what's been found in academic studies. It plays a key role in ensuring the data provider's security (Heeß et al., 2024). This, in turn, leads to people having greater trust in the system (Yoon & Lee, 2019; Zhang et al., 2023).

Ignoring both verifiable identities and decentralized data storage means that they do not affect the results enough to come up in the configuration and that stakeholders still can perceive a high level of trust when they are not part of the DPP system. This contradicts existing literature as it has been shown that the use of verifiable identities and decentralized data storage contribute to data security and integrity. These factors, in turn, contribute to a higher level of trust (Mcknight et al., 2011; Zhang et al., 2023). This configuration is, besides supported by existing research, also supported by 83.1% of the participants.

The reason that there is only one configuration for high trust might be that the trust precursors are overlaying too much as they all focus on a form of security or that there are other factors outside of the model that possibly affect the trust precursors or trust in the DPP system directly.

Further, stakeholders will have a low level of trust in the DPP system when two out of three of the precursors for the DPP system are not available. This holds for the three results with all of them having either, a highly decentralized data storage and highly secure authentication for editing rights (LS1), verifiable identities and a highly secure authentication (LS2), or a highly decentralized storage and verifiable identities in place (LS3). This is consistent with the literature as the precursors would have a positive effect on the security of the system in multiple ways (Heeß et al., 2024; Tewari & Gupta, 2020) and this, in turn, would have a positive effect on the trust in the system (Yoon & Lee, 2019; Zhang et al., 2023).

For each configuration, one precursor does not appear in the configuration meaning that when the other two are not part of the DPP system, it does not matter whether the third precursor is or is not part of the system, still, stakeholders will perceive a low level of trust in the DPP system.

Looking at the consistency scores, stakeholders are most likely to perceive a low level of trust when there is a low level of decentralized data storage and a low level of secure authentication mechanisms for data editing (LS1), along with a coverage of 57.4%. However, the other two combinations (LS2 and LS3) also have high consistency and are

supported by a large part of the participants, with coverages of 57.9% and 56.8% respectively.

All the combinations within the configurations of low trust in the DPP system are core conditions. This implies that when two of the three system-based conditions are missing, stakeholders are more likely to perceive a low level of trust towards the DPP system.

6.1.2 Trust & Behavioral Intention

The multiple linear regression analysis was conducted to examine the relationship between behavioral intention to use the DPP in the decision-making process regarding circularity and sustainability and the two independent variables; trust in the DPP information and trust in the DPP system. The model suggests that neither trust in the DPP system, nor trust in the DPP information significantly contribute to the prediction of the behavioral intention to use the DPP.

While the unstandardized coefficient for trust in the DPP system was higher than that for trust in the DPP information, indicating a greater effect on behavioral intention, this did not translate into a significant contribution to the model. This could suggest that while there may be a relationship between trust in the DPP system and behavioral intention, other factors, not included in the model, may be influencing this relationship.

These findings are not indicated in previous literature, as there are multiple studies performed that showed how trust positively affects the behavioral intention to use a system (Alkhater et al., 2018; Hamidi & Chavoshi, 2018; Kašparová, 2023; Kusuma & Pramunita, 2011; Tung et al., 2008). What could be the case is that the DPP system may not captivate what participants see as a digital system, as by itself it will not provide help to the user, it will provide information that the user can use but besides that, there is not a lot of interaction.

Also, it could be the case that for now, organizations are mostly focusing on the need to comply with the regulations that introduce DPPs and all the uses that the DPP could have that are not yet in consideration. As DPPs become more established and standardized over time, more opportunities might come up for organizations to include the information from the DPP in their decision-making processes, and individuals within organizations might get a better view of the DPP to assess their intentions to use the information found in the DPP.

6.2 Contributions

6.2.1 Theoretical Contributions

This study makes several major contributions to the current body of research on DPPs and trust in information systems. To begin with, as the current research into Digital Product Passports is still limited at this point, one of the theoretical contributions is the advanced understanding of trust in DPPs, similar data-sharing initiatives along the value chain, and digital platforms and technologies in general. The focus on design requirements provides an overview of the current status of research on DPPs. Also, the focus on DPP trust precursors contributes to research towards trust formation in information systems as it shows what trust precursors are perceived as trustworthy by users (Acikgoz et al., 2023; Meeßen et al., 2019; Thielsch et al., 2018; Yoon & Lee, 2019).

Moreover, this research has provided additional insights into how certain mechanisms, that can be implemented into information systems, contribute to the perceived level of trust of an end user. The results indicated that the availability of unique location identifiers, contributing to data provider traceability, was important to develop a high level of trust towards the information shown in the DPP, confirming the outcomes by Schmidthuber et al. (2023). Also, transparency of data calculation methods had an important role in configurations that may lead to a high level of trust in the DPP information, which was previously shown by Faniel & Jacobsen (2010). Additionally, third-party certification was another important contributor to the perception of a high level of trust by the relevant stakeholders, confirming the research of Acikgoz et al. (2023) and Thielsch et al. (2018).

Furthermore, this study differs from typical trust in information systems research (Schmidthuber et al., 2023; Zhang et al., 2023) in that it assessed important components of an upcoming, not yet fully designed, IT system. This encourages innovation and raises practical issues for policymakers and DPP service providers alike, bridging the gap between academia and business. This contribution may appear to be more practical than theoretical, but it may also be taken as a critique of existing trust in information systems research, which frequently lags behind business innovations. It shows academia opportunities to engage their knowledge and efforts in unexplored but crucial areas on

the critical path for near-term IT systems and ecosystems, rather than relying solely on incumbent systems as units of study.

Regarding trust in the DPP system, secure authentication mechanisms for data editing act as the single precursor that may lead to a high level of trust in the system. Even though the other two precursors, verifiable identities and decentralized data storage, might contribute to security as well, the presence of secure authentication mechanisms confirmed the previous work of Chang & Seow (2016) and Zhang et al. (2023).

Considering the data collection methods, this study provides a list of validated and reliable survey measures for analyzing DPP trust precursors. Based on previous research regarding these trust precursors, measures have been formed, validated, and analyzed.

Further, by using the fsQCA method, integrating quantitative and qualitative approaches, improvements in the understanding of how various factors interact to contribute to trust in information systems are done. This may provide insights that quantitative or qualitative methods alone may not capture. Also, the use of the fsQCA method in analyzing the concept of trust contributes to the development and refinement of theories on trust showing a not yet often used method on this complicated construct. Possibly it can help challenge existing assumptions, propose new hypotheses, and provide new empirical evidence on the concept of trust in information systems research (Giffin, 1967; Lippert & Forman, 2006; Lippert & Swiercz, 2005; Xu et al., 2014).

6.2.2 Practical Contributions

After the data analysis and relating the results to prior research, this research provides insight into DPP trust precursors that, considered by organizational users, would enhance their trust in the DPP information and system. These results contribute to the current research being done on DPPs and they can help system designers and developers make decisions on what trust precursors to include to increase the completeness, credibility, and correctness of the information in the DPP (Acikgoz et al., 2023; Faniel & Jacobsen, 2010; Schmidthuber et al., 2023; Thielsch et al., 2018; Wallis et al., 2007) and the security and integrity of the DPP system (Mcknight et al., 2011; Zhang et al., 2023).

This study showed that unique location identifiers, data calculation transparency, and third-party certification are core conditions for configurations to lead to high trust in the DPP information. When implementing those trust precursors, the chance that the

information is trusted by organizational users is increased. Moreover, secure authentication mechanisms for data editing acted as the only predictor for a high level of trust in the DPP system, These results can be used by system designers and developers when developing the DPP to increase the level of perceived trust in the DPP, which contributes to its adoption (Salahshour Rad et al., 2018).

Besides this, this study was unable to show the relationship between trust in the information of the DPP and the DPP system and the behavioral intention to use the system in the decision-making process regarding circularity and sustainability. However, this did show that there is more needed than trust alone to make sure that organizations will use the DPP for its purpose to improve the circularity and sustainability of their business and not see it as only legislation to adhere to or that users can assess their intentions yet when they will interact with the DPP.

Strategies to encourage organizations to use DPPs for improving decision-making regarding circularity and sustainability are, e.g., demonstrating the practical benefits of DPPs and positioning them as tools for business improvement rather than just compliance mechanisms. DPP service providers, after having an up-and-running system, could show these practical benefits such that businesses are moving forward to a more circular economy.

6.3 Limitations and Directions for Future Research

To begin with, there are a few limitations to this study in terms of the data collection method. Due to the limited timeframe in which the study had to be done, only a limited sample of respondents could be gathered. The researcher focused a lot of their time on finding participants, however, response rates for these types of studies are always rather low. Besides this, another limitation in terms of data collection is the limited understanding of DPPs and trust precursors used in this study. It was considered beforehand that not all respondents had the necessary knowledge to answer all questions in a valuable way.

To mitigate this, the concept of the DPP was explained and a demo was provided to base their answers on. Also, for all trust precursors used in this study, an explanation and, when necessary, a visual aid was provided to raise the understanding of the concept to a basic level. The feedback on the explanation of these concepts was mostly positive. Lastly, as often with survey-based data collection, the sample gathered in the study could be biased

due to the use of convenience and snowball sampling, the data gathered might suffer from sample bias, and therefore the results may not be generalizable to all potential users of the DPPs. Besides this, there are always risks with using self-reported data as there may be issues with the accuracy or honesty of responses, these limitations should be kept in mind when interpreting the results.

Third, looking at the data gathered and who responded to the survey (Table 3), there might be a bias regarding the familiarity of the respondents with the DPP. Individuals who are more familiar with the DPP at this point might be more involved with the development of the DPP than individuals who are less familiar with the DPP. This might result in a bias in terms of that they would rather not be part of the development of an untrustworthy DPP which might have affected their responses.

Fourth, regarding the data analysis method, fsQCA is highly dependent on the decisions of the researcher, which can introduce subjective bias. By explaining all the decisions made in this thesis, the study should be reproducible for other researchers. While this is a common issue in research methods, it is still a limitation worthy to be mentioned.

Regarding future studies, there are a lot of possibilities to extend the research on DPPs, trust in information systems, and the use of fsQCA. To begin with, the results of these, and possibly other studies, could be used to test for specific propositions on existing or to-be-implemented systems, as also proposed by Pappas & Woodside (2021). This could show how well systems adhere to the configurations that may lead to high trust in either the DPP information or the DPP system.

Second, to further extend this research, the study could be repeated using more or different trust precursors that enforce trust antecedents. This could lead to additional insights into what trust precursors affect trust in the DPP information and the DPP system. Besides this, extending the sample could lead to additional or different insights for specific end users within the organizational context. Also, the study could be focused on consumers and what their perceptions are in terms of trust in the DPP information and the DPP system. Performing this study in a longitudinal format over the coming years could be valuable in understanding how trust in DPPs develops and changes over the time of implementation and thereafter.

Lastly, as this study did not succeed in showing that trust would have a positive relation to the behavioral intention to use the DPP in the decision-making process regarding

circularity and sustainability, another direction for future research could focus on the needs of organizations to make the DPP a valuable asset to use in this decision-making process. Case studies or in-depth interviews could provide insights into what organizational end users need to see the DPP as more than a regulation to adhere to.

7 Conclusion

This thesis has focused on answering two questions. The first question focused on what factors, and their combinations influenced the level of trust in the DPP. This was separately analyzed for the DPP information and DPP system. Through a survey, set out to individuals who will be working with the DPP in the future, within an organizational context, data was gathered on multiple DPP trust precursors relating to a certain design requirement of DPPs.

After the data collection, a fuzzy-set Qualitative Comparative Analysis was done to see what factors, or combinations of factors, would lead to high or low trust in the DPP information and high or low trust in the DPP system. This approach was done to capture the complexity of trust as a construct. The precursors under analysis for trust in the DPP information were data calculation transparency, data collection transparency, data lineage tracking diagrams, unique location identifiers, and third-party certification. For trust in the DPP system, the precursors were decentralized data storage, verifiable identities, and secure authentication for data editing.

Unique location identifiers, as a fundamental need, are crucial for predicting whether users would have high or low levels of trust in the DPP information. This is because when unique location identifiers are included in the DPP, it may lead to a high level of trust and when they are not there, it may lead to a low level of trust. Next to this, data calculation transparency and third-party certification also have a strong relation with high trust in the DPP information. Besides a low level of data provider traceability, without unique location identifiers, stakeholders also perceive a low level of trust when there is a low level of product data traceability, without data lineage tracking. No single precursor can be seen as a single predictor for either low or high trust in the DPP system.

Further, regarding trust in the DPP system, secure authentication mechanisms for data editing came out as the single predictor for high trust. There was only one configuration leading to high trust which could be because there were only three conditions, the precursors, that were used as input for the dependent variable. On the other hand, for low trust in the DPP system, three configurations were determined, all resulting in two out of three conditions being absent. With all configurations being core conditions, it can be generalized that stakeholders perceive a low level of trust when two of the three precursors for trust in the DPP system are low or not there.

Next, the second question that this thesis tried to answer was whether trust has any effect on the behavioral intention to use the DPP in the decision-making processes regarding circularity and sustainability. Using the same survey data, a multiple linear regression analysis was performed to check the relations between the independent variables, trust in the DPP information and trust in the DPP system, with the dependent variable of behavioral intention. However, both relations were found insignificant. There could be a couple of reasons for this, as even though there is a system behind it, for some users within the organizational context, the DPP will just provide information without a lot of interaction with the system. Also, a possibility is that organizations for now are focusing on just complying with the regulations and are not yet thinking about how it can help or inform them, or both, in their decision-making processes. Possibly, once the DPP is more established, this perception might change.

Focusing on contributions, theoretically, this study contributes to the limited academic research on DPPs by advancing the understanding of trust in DPPs and similar initiatives. Also this study highlights the importance of assessing components of emerging IT systems to foster innovation and address practical issues, bridging the gap between academia and business, and critiquing existing trust research for lagging behind business innovations., Further, it provides validated survey measures for analyzing trust precursors within information systems and shows possibilities for the fsQCA method to understand how various factors contribute to trust in information systems.

On the practical side, this research provides insights into trust precursors in DPP that can enhance the user's trust in the information found in the DPP and the DPP system. These findings can be used as input in the design and implementation phase for the gradual introduction of DPPs in the coming years. However, this study has also highlighted that trust alone may not be sufficient to ensure the DPP's use in decision-making processes related to circularity and sustainability.

Lastly, the study acknowledges limitations such as limited literature on DPPs, constraints in data collection, and potential bias in the fsQCA method. Future research could extend this study by testing specific propositions on existing or to-be-implemented systems, exploring more or different trust precursors, and focusing on specific end users or consumers. Longitudinal studies could provide valuable insights into how trust in DPPs evolves. Future research could also explore what organizations need to see the DPP as more than just a regulation to adhere to.

8 References

Acikgoz, F., Busalim, A., Gaskin, J., & Asadi, S. (2023). An Integrated Model for Information Adoption&Trust in Mobile Social Commerce. *Journal of Computer Information Systems*, 1–23. https://doi.org/10.1080/08874417.2023.2251449

Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*, *35*(1), 38–54. https://doi.org/10.1016/j.tele.2017.09.017

Anisetti, M., Ardagna, C. A., & Damiani, E. (2014). A Certification-Based Trust Model for Autonomic Cloud Computing Systems. *2014 International Conference on Cloud and Autonomic Computing*, 212–219. https://doi.org/10.1109/ICCAC.2014.8

Aslam, S., & Mrissa, M. (2023). A framework for privacy-aware and secure decentralized data storage. *Computer Science and Information Systems*, *20*(3), 1235–1261.

Avery Dennison Corporation. (2023, April 18). *Hoodie*. https://consumer-apps-sandbox.atma.io/dppMkAnatomy/dppMkAnatomy/8d30eadc-5190-424c-ac0b-a40e86ae4b58/?labelId=303431711C5B0C4000000066&language=en-US

Berg, H., Kulinna, R., Stöcker, C., Guth-Orlowski, S., Thiermann, R., & Porepp, N. (2022). *Overcoming information asymmetry in the plastics value chain with digital product passports: How decentralised identifiers and verifiable credentials can enable a circular economy for plastics* (Vol. 197). Wuppertal Institut für Klima, Umwelt, Energie. https://doi.org/10.48506/opus-7940

Berger, K., Baumgartner, R. J., Weinzerl, M., Bachler, J., Preston, K., & Schöggl, J.-P. (2023). Data requirements and availabilities for a digital battery passport – A value chain actor perspective. *Cleaner Production Letters*, *4*, 100032. https://doi.org/10.1016/j.clpl.2023.100032

Boukhatmi, Ä., Nyffenegger, R., & Grösser, S. N. (2023). Designing a digital platform to foster data-enhanced circular practices in the European solar industry. *Journal of Cleaner Production*, *418*, 137992. https://doi.org/10.1016/j.jclepro.2023.137992

Brunner, C., Eibl, G., Fröhlich, P., Sackl, A., & Engel, D. (2021). *Who Stores the Private Key? An Exploratory Study about User Preferences of Key Management*

for Blockchain-based Applications. 23–32. https://doi.org/10.5220/0010173200230032

CEN CENELEC. (2024). *Sustainability*. Work Programme 2024. https://wp2024.cencenelec.eu/horizontal-topics/sustainability/

Chang, K.-C., & Seow, Y. (2016). Adoption intention on cloud storage services: The role of technology trust, privacy and security concerns. *PACIS 2016 Proceedings*. https://aisel.aisnet.org/pacis2016/79

Chen, H., & Zhao, X. (2023). Use intention of green financial security intelligence service based on UTAUT. *Environment, Development and Sustainability*, *25*(10), 10709–10742. https://doi.org/10.1007/s10668-022-02501-5

Circularise. (n.d.). *Circularise Digital Product Passports*. Retrieved May 27, 2024, from https://www.circularise.com/dpp

Copeland, R., & Copeland, M. (2017). Independently Verifiable Identity Scheme (IVIS). *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, 196–198. https://doi.org/10.1109/ICIN.2017.7899410

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Cui, H., Deng, R. H., & Li, Y. (2018). Attribute-based cloud storage with secure provenance over encrypted data. *Future Generation Computer Systems*, *79*, 461–472. https://doi.org/10.1016/j.future.2017.10.010

Darnall, N., Ji, H., & Vázquez-Brust, D. A. (2018). Third-Party Certification, Sponsorship, and Consumers' Ecolabel Use. *Journal of Business Ethics*, *150*(4), 953–969. https://doi.org/10.1007/s10551-016-3138-2

Dujak, D., Zdziarska, M., & Kolinski, A. (2017). GLN Standard as a facilitator of physical location identification within process of distribution. *LogForum*, *13*(3), 247–261. https://doi.org/10.17270/j.log.2017.3.1

Ejdys, J. (2018). Building technology trust in ICT application at a university. *International Journal of Emerging Markets*, *13*(5), 980–997. https://doi.org/10.1108/IJoEM-07-2017-0234

Evrin, V. (2021). Risk Assessment and Analysis Methods: Qualitative and Quantitative. *ISACA*, *2*. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

Faniel, I. M., & Jacobsen, T. E. (2010). Reusing Scientific Data: How Earthquake Engineering Researchers Assess the Reusability of Colleagues' Data. *Computer*

Supported Cooperative Work (CSCW), *19*(3), 355–375. https://doi.org/10.1007/s10606-010-9117-8

Fishbein, M., & Ajzen, I. (1977). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. *Philosophy and Rhetoric*, *10*(2), 130–132.

Fiss, P. C. (2011). Building Better Causal Theories: A Fuzzy Set Approach to Typologies in Organization Research. *Academy of Management Journal*, *54*(2), 393–420. https://doi.org/10.5465/amj.2011.60263120

Ghorbel, A., Ghorbel, M., & Jmaiel, M. (2022). Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain. *International Journal of Information Security*, *21*(3), 489–508. https://doi.org/10.1007/s10207-021-00565-4

Giffin, K. (1967). The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychological Bulletin*, *68*(2), 104–120. https://doi.org/10.1037/h0024833

Götz, T., Berg, H., Jansen, M., Adisorn, T., Cembrero, D., Markkanen, S., & Chowdhury, T. (2022). *Digital Product Passport: The ticket to achieving a climate neutral and circular European economy?* (6). https://circulareconomy.europa.eu/platform/en/knowledge/digital-product-passport-ticket-achieving-climate-neutral-and-circular-european-economy

Greiner, M., Seidenfad, K., Langewisch, C., Hofmann, A., & Lechner, U. (2024). The Digital Product Passport: Enabling Interoperable Information Flows Through Blockchain Consortia for Sustainability. In F. Phillipson, G. Eichler, C. Erfurth, & G. Fahrnberger (Eds.), *Innovations for Community Services* (pp. 377–396). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60433-1_21

GS1 US. (2022). *An Introduction to the Global Location Number (GLN)* (3.0). https://www.gs1us.org/content/dam/gs1us/documents/industries-insights/standards/An-Introduction-to-Global-Location-Number-GLN.pdf

Guntzburger, Y., Peignier, I., & de Marcellis-Warin, N. (2021). The consumers' (mis)perceptions of ecolabels' regulatory schemes for food products: Insights from Canada. *British Food Journal*, *124*(11), 3497–3521. https://doi.org/10.1108/BFJ-05-2021-0546

Gupta, M., Alcagaya, A., Bendzuck, K., Berg, H., Bernier, C., Böll, M., Dao, A., Gayko, J., Lehmacher, W., Merkx, J., Olsson, S., Osterwalder, M., Ruiz Lopez, A., Schneider, A., Wagner, E., Wautelet, T., & Wenning, R. (2024). *Cross-*

sector and sector-specific DPP roadmaps (Version 1.2). CIRPASS. https://cirpassproject.eu/wp-content/uploads/2024/03/CIRPASS_Cross-sector_and_sector-specific_DPP_roadmaps_1.2_2024-03-27.pdf

Hale, M. (2023, May 16). *Verifiable Credentials as a Model for Digital Identity*. https://www.redbelly.network/blog/verifiable-credentials-as-a-model-for-digital-identity

Hamidi, H., & Chavoshi, A. (2018). Analysis of the essential factors for the adoption of mobile learning in higher education: A case study of students of the University of Technology. *Telematics and Informatics*, *35*(4), 1053–1070. https://doi.org/10.1016/j.tele.2017.09.016

Hassouna, A. (2023). Multivariable Analysis. In A. Hassouna (Ed.), *Statistics for Clinicians: How Much Should a Doctor Know?* (pp. 247–338). Springer International Publishing. https://doi.org/10.1007/978-3-031-20758-7_3

Heeß, P., Rockstuhl, J., Körner, M.-F., & Strüker, J. (2024). Enhancing trust in global supply chains: Conceptualizing Digital Product Passports for a low-carbon hydrogen market. *Electronic Markets*, *34*(1), 10. https://doi.org/10.1007/s12525-024-00690-7

Jansen, M., Meisen, T., Plociennik, C., Berg, H., Pomp, A., & Windholz, W. (2023). Stop Guessing in the Dark: Identified Requirements for Digital Product Passport Systems. *Systems*, *11*(3), Article 3. https://doi.org/10.3390/systems11030123

Kašparová, P. (2023). Intention to use business intelligence tools in decision making processes: Applying a UTAUT 2 model. *Central European Journal of Operations Research*, *31*(3), 991–1008. https://doi.org/10.1007/s10100-022-00827-z

King, M. R. N., Timms, P. D., & Mountney, S. (2023). A proposed universal definition of a Digital Product Passport Ecosystem (DPPE): Worldviews, discrete capabilities, stakeholder requirements and concerns. *Journal of Cleaner Production*, *384*, 135538. https://doi.org/10.1016/j.jclepro.2022.135538

Kivijärvi, H., Leppänen, A., & Hallikainen, P. (2013). Technology Trust: From Antecedents to Perceived Performance Effects. *2013 46th Hawaii International Conference on System Sciences*, 4586–4595. https://doi.org/10.1109/HICSS.2013.510

Koppelaar, R. H. E. M., Pamidi, S., Hajósi, E., Herreras, L., Leroy, P., Jung, H.-Y., Concheso, A., Daniel, R., Francisco, F. B., Parrado, C., Dell'Ambrogio, S.,

Guggiari, F., Leone, D., & Fontana, A. (2023). A Digital Product Passport for Critical Raw Materials Reuse and Recycling. *Sustainability*, *15*(2), Article 2. https://doi.org/10.3390/su15021405

Kratz, J. E., & Strasser, C. (2015). Researcher Perspectives on Publication and Peer Review of Data. *PLOS ONE*, *10*(2), e0117619. https://doi.org/10.1371/journal.pone.0117619

Kusuma, H., & Pramunita, R. (2011). The effect of risk and trust on the behavioral intention of using E-procurement system. *European Journal of Economics, Finance and Administrative Sciences*, 138–145.

Li, X., & Ahmed-Kristensen, S. (2015). UNDERSTAND THE DESIGN REQUIREMENT IN COMPANIES. *DS 80-5 Proceedings of the 20th International Conference on Engineering Design (ICED 15) Vol 5: Design Methods and Tools - Part 1, Milan, Italy, 27-30.07.15*, 063–074.

Lippert, S. K. (2001). An exploratory study into the relevance of trust in the context of information systems technology [Ph.D., The George Washington University]. In *ProQuest Dissertations and Theses*. https://www.proquest.com/docview/251607510/abstract/B777665082484F4FPQ/1

Lippert, S. K., & Forman, H. (2006). A supply chain study of technology trust and antecedents to technology internalization consequences. *International Journal of Physical Distribution & Logistics Management*, *36*(4), 271–288. https://doi.org/10.1108/09600030610672046

Lippert, S. K., & Swiercz, P. M. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science*, *31*(5), 340–353. https://doi.org/10.1177/0165551505055399

Liu, W., Shao, X.-F., Wu, C.-H., & Qiao, P. (2021). A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development. *Journal of Cleaner Production*, *298*, 126763. https://doi.org/10.1016/j.jclepro.2021.126763

Liu, Y., Mezei, J., Kostakos, V., & Li, H. (2017). Applying configurational analysis to IS behavioural research: A methodological alternative for modelling combinatorial complexities. *Information Systems Journal*, *27*(1), 59–89. https://doi.org/10.1111/isj.12094

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.2307/258792

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2), 12:1-12:25. https://doi.org/10.1145/1985347.1985353

Meeßen, S., Thielsch, M., & Hertel, G. (2019). Trust in Management Information Systems (MIS) A Theoretical Model. *Zeitschrift Für Arbeits- Und Organisationspsychologie*, *64*, 6–16. https://doi.org/10.1026/0932-4089/a000306

Mendel, J. M., & Korjani, M. M. (2013). Theoretical aspects of Fuzzy Set Qualitative Comparative Analysis (fsQCA). *Information Sciences*, *237*, 137–161. https://doi.org/10.1016/j.ins.2013.02.048

Möller, F., Guggenberger, T. M., & Otto, B. (2020). Towards a Method for Design Principle Development in Information Systems. In S. Hofmann, O. Müller, & M. Rossi (Eds.), *Designing for Digital Transformation. Co-Creating Services with Citizens and Industry* (pp. 208–220). Springer International Publishing. https://doi.org/10.1007/978-3-030-64823-7_20

Narang, A., & Gupta, D. (2018). A Review on Different Security Issues and Challenges in Cloud Computing. *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 121–125. https://doi.org/10.1109/GUCON.2018.8675099

Otto, B., & Jarke, M. (2019). Designing a multi-sided data platform: Findings from the International Data Spaces case. *Electronic Markets*, *29*(4), 561–580. https://doi.org/10.1007/s12525-019-00362-x

Oztekin, A. (2011). A decision support system for usability evaluation of web-based information systems. *Expert Systems with Applications*, *38*(3), 2110–2118. https://doi.org/10.1016/j.eswa.2010.07.151

Pappas, I. O., & Woodside, A. G. (2021). Fuzzy-set Qualitative Comparative Analysis (fsQCA): Guidelines for research practice in Information Systems and marketing. *International Journal of Information Management*, *58*, 102310. https://doi.org/10.1016/j.ijinfomgt.2021.102310

Pienwisetkaew, T., Wongsaichia, S., Pinyosap, B., Prasertsil, S., Poonsakpaisarn, K., & Ketkaew, C. (2023). The Behavioral Intention to Adopt Circular Economy-Based Digital Technology for Agricultural Waste Valorization. *Foods*, *12*(12), Article 12. https://doi.org/10.3390/foods12122341

Plociennik, C., Pourjafarian, M., Saleh, S., Hagedorn, T., Carmo Precci Lopes, A. do, Vogelgesang, M., Baehr, J., Kellerer, B., Jansen, M., Berg, H., Ruskowski, M., Schebek, L., & Ciroth, A. (2022). *Requirements for a Digital Product Passport to Boost the Circular Economy*. 1485–1494. https://dl.gi.de/handle/20.500.12116/39501

Ragin, C. C. (2000). *Fuzzy-Set Social Science*. University of Chicago Press.

Ragin, C. C. (2009). *Redesigning Social Inquiry: Fuzzy Sets and Beyond*. University of Chicago Press.

Regulation (EU) 2024/1781 of the European Parliament and of the Council, 2024/1781 (2024). http://data.europa.eu/eli/reg/2024/1781/oj/eng

Ribeiro da Silva, E., Lohmer, J., Rohla, M., & Angelis, J. (2023). Unleashing the circular economy in the electric vehicle battery supply chain: A case study on data sharing and blockchain potential. *Resources, Conservation and Recycling*, *193*, 106969. https://doi.org/10.1016/j.resconrec.2023.106969

Rihoux, B., & Ragin, C. C. (2009). *Configurational Comparative Methods: Qualitative Comparative Analysis (QCA) and Related Techniques*. SAGE.

Salahshour Rad, M., Nilashi, M., & Mohamed Dahlan, H. (2018). Information technology adoption: A review of the literature and classification. *Universal Access in the Information Society*, *17*(2), 361–390. https://doi.org/10.1007/s10209-017-0534-z

Salman, O., Elhajj, I., Kayssi, A., & Chehab, A. (2015). An architecture for the Internet of Things with decentralized data and centralized control. *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*, 1–8. https://doi.org/10.1109/AICCSA.2015.7507265

Schmidthuber, L., Willems, J., & Krabina, B. (2023). Trust in public performance information: The effect of data accessibility and data source. *Public Administration Review*, *83*(2), 279–295. https://doi.org/10.1111/puar.13603

Stitz, H., Luger, S., Streit, M., & Gehlenborg, N. (2016). AVOCADO: Visualization of Workflow–Derived Data Provenance for Reproducible Biomedical Research. *Computer Graphics Forum*, *35*(3), 481–490. https://doi.org/10.1111/cgf.12924

Stretton, C. (2022, April 20). Digital product passports (DPP): What, how, and why? *Circularise*. https://www.circularise.com/blogs/digital-product-passports-dpp-what-how-and-why

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, *108*, 909–920. https://doi.org/10.1016/j.future.2018.04.027

Thielsch, M. T., Meeßen, S. M., & Hertel, G. (2018). Trust and distrust in information systems at the workplace. *PeerJ*, *6*, e5483. https://doi.org/10.7717/peerj.5483

Tung, F.-C., Chang, S.-C., & Chou, C.-M. (2008). An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics*, *77*(5), 324–335. https://doi.org/10.1016/j.ijmedinf.2007.06.006

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems*, *17*(5). https://doi.org/10.17705/1jais.00428

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

Vis, B. (2012). The Comparative Advantages of fsQCA and Regression Analysis for Moderately Large-N Analyses. *Sociological Methods & Research*, *41*(1), 168–198. https://doi.org/10.1177/0049124112442142

Wagner, E., Rukanova, B., Bernier, C., Wautelet, T., Ayed, A.-C., Böll, M., Gayko, J., Schneider, A., Bendzuck, K., & Dalwigk, von, I. (2023). *D2.1 Mapping of legal and voluntary requirements and screening of emerging DPP-related pilots*. CIRPASS. https://cirpassproject.eu/wp-content/uploads/2023/07/D2.1_July_2023.pdf

Wallis, J. C., Borgman, C. L., Mayernik, M. S., Pepe, A., Ramanathan, N., & Hansen, M. (2007). Know Thy Sensor: Trust, Data Quality, and Data Integrity in Scientific Digital Libraries. In L. Kovács, N. Fuhr, & C. Meghini (Eds.),

Research and Advanced Technology for Digital Libraries (pp. 380–391). Springer. https://doi.org/10.1007/978-3-540-74851-9_32

Wong, K. (2013). Partial least square structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*, 1–32.

Woodside, A. G. (2014). Embrace•perform•model: Complexity theory, contrarian case analysis, and multiple realities. *Journal of Business Research*, *67*(12), 2495–2503. https://doi.org/10.1016/j.jbusres.2014.07.006

Wu, X., Xiong, J., Yan, J., & Wang, Y. (2021). Perceived quality of traceability information and its effect on purchase intention towards organic food. *Journal of Marketing Management*. https://www.tandfonline.com/doi/full/10.1080/0267257X.2021.1910328

Xu, J., Le, K., Deitermann, A., & Montague, E. (2014). How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology. *Applied Ergonomics*, *45*(6), 1495–1503. https://doi.org/10.1016/j.apergo.2014.04.012

Yazici, I. M., & Aktas, M. S. (2022). A novel visualization approach for data provenance. *Concurrency and Computation: Practice and Experience*, *34*(9), e6523. https://doi.org/10.1002/cpe.6523

Yoon, A., & Lee, Y. Y. (2019). Factors of trust in data reuse. *Online Information Review*, *43*(7), 1245–1262. https://doi.org/10.1108/OIR-01-2019-0014

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical Analysis From Commercial Bank Users in Pakistan. *Sage Open*, *13*(3), 21582440231181388. https://doi.org/10.1177/21582440231181388

Appendices

Appendix 1. Survey Measurements

Table 8. Survey measurements and their sources (1/3)

Construct	ID	Measurement (EN)	Adapted from	Based on
Information-based trust	T1	I would regard the information provided by the DPP as reliable	(Acikgoz et al., 2023)	
	T2	I believe the DPP would include few uncertainties	(Acikgoz et al., 2023)	
	T3	In general, I could rely on the information found in the DPP	(Acikgoz et al., 2023)	
System-based trust	T4	I would trust the DPP system to retain my company information secure and safe	(Zhang et al., 2023)	
	T5	I would have confidence that the DPP system is trustable	(Zhang et al., 2023)	
	T6	I would be confident in my data security whenever using the DPP system	(Zhang et al., 2023)	
Data collection transparency	COT1	I believe the data collection methods used for the data in the DPP should be transparent	(Venkatesh et al., 2016)	
	COT2	I think all stakeholders should have access to the data collection methods used for the data in the DPP	(Venkatesh et al., 2016)	
	COT3	I believe there should be opportunities for stakeholders to provide feedback on the data collection methods used for the data in the DPP	(Venkatesh et al., 2016)	
Data calculation transparency	CAT1	I believe the data calculation methods used for the data in the DPP should be transparent	(Venkatesh et al., 2016)	
	CAT2	I think all stakeholders should have access to the data calculation methods used for the data in the DPP	(Venkatesh et al., 2016)	
	CAT3	I believe there should be opportunities for stakeholders to provide feedback on the data calculation methods used for the data in the DPP	(Venkatesh et al., 2016)	

Table 9. Survey measurements and their sources, continued (2/3)

Construct	ID	Measurement (EN)	Adapted from	Based on
Data lineage tracking traceability	DLT1	I expect that data lineage tracking diagrams in the DPP will help me evaluate a product's lifecycle more effectively	(Wu et al., 2021)	
	DLT2	I think the information from the data lineage tracking diagram in the DPP will be helpful	(Wu et al., 2021)	
	DLT3	Data lineage tracking diagrams in the DPP provide me with sufficient objective information about a product's lifecycle	(Wu et al., 2021)	
Unique Location Identifiers	ULI1	Tagging data in the DPP with a unique location identifier of its initial organizational source helps me identify the origin of the data		(Dujak et al., 2017)
	ULI2	Tagging data in the DPP with a unique location identifier of its initial organizational source increases the value of the data for me		(Dujak et al., 2017)
	ULI3	I think unique location identifiers are effective in ensuring the traceability of data providers that input data in the DPP		(Cui et al., 2018)
Third-party certification on data compliance	C1	I believe third-party certification of data in the DPP for data compliance with requirements is crucial		(Guntzburger et al., 2021)
	C2	I am confident that third-party certification of data in the DPP for data compliance enhances the legitimacy of the provided data		(Darnall et al., 2018)
	C3	Third-party certification of data in the DPP provides me with reassurance regarding data compliance		(Narang & Gupta, 2018)

Table 10. Survey measurements and their sources, continued (3/3)

Construct	ID	Measurement (EN)	Adapted from	Based on
Verifiable identities for accessibility	VI1	I believe the use of verifiable identities decrease the risk of data misuse		(Ghorbel et al., 2022)
	VI2	I think the use of verifiable identities enhance the access to data relevant to me		(Brunner et al., 2021)
	VI3	Verifying the identities of data viewers reassures me as the data provider when sharing sensitive data		(Ghorbel et al., 2022)
	VI4	Verifying the identities of data providers reassures me as the data viewer that the data is real		(Ghorbel et al., 2022)
Decentralized data storage	DDS1	I believe decentralized data storage offers greater protection for my data privacy compared to centralized systems		(Aslam & Mrissa, 2023)
	DDS2	I am confident that decentralized data storage improves the security of data in the DPP compared to centralized systems		(Aslam & Mrissa, 2023)
	DDS3	I feel I have more control over my data in a decentralized storage system compared to centralized systems		(Salman et al., 2015)
Secure authentication for editing rights	S1	I believe secure authentication mechanisms for editing rights improve control over my data in the DPP		(Tewari & Gupta, 2020)
	S2	I believe secure authentication safeguards the integrity of the data in the DPP by preventing unauthorized modifications		(Tewari & Gupta, 2020)
	S3	A secure authentication process boosts my confidence in the overall security of my data in the DPP		(Tewari & Gupta, 2020)
Behavioral intention	BI1	I intend to use the DPP system in the future for decision-making regarding circularity	(Venkatesh et al., 2003)	
	BI2	I predict that I would use the DPP system in the future for decision-making regarding circularity	(Venkatesh et al., 2003)	
	BI3	I plan to use the DPP system in the future for decision-making regarding circularity	(Venkatesh et al., 2003)	

Appendix 2. Information Provided in Survey

Appendix 2.1. Digital Product Passports

Digital Product Passports (DPPs) are digital records that provide comprehensive information about a product's lifecycle, including its origins, materials, manufacturing processes, and environmental impact. DPPs can support circular economy practices by making it easier to recycle, repair, or repurpose products, thereby reducing waste and promoting sustainability. As an example, it could be compared to the Nutri-score (used in France, Belgium, Germany, Luxembourg, the Netherlands, Spain, and Switzerland) which helps consumers make healthier food choices but then focused on all physical products with a wide range of lifecycle information concerning sustainability, ethical production, and comprehensive product details.

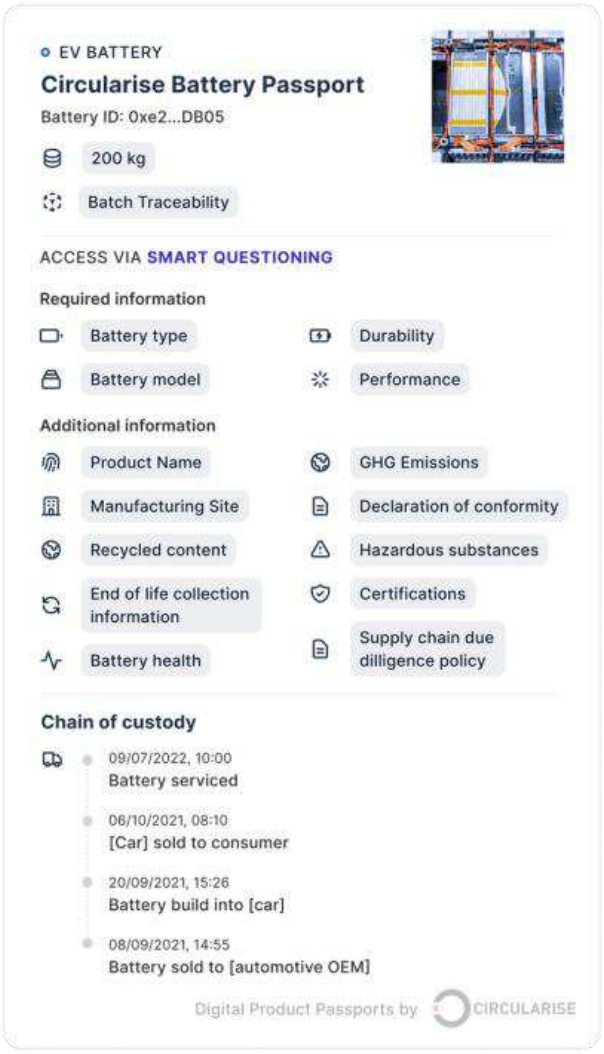

Figure 5. An example of a DPP (Circularise, n.d.)

Appendix 2.2. Data Collection and Calculation Transparency

Visualizing data collection and calculation methods would include making visible the sources of raw data, such as sensor readings and specific algorithms or formulas used for processing the data. Additionally, a step-by-step explanation of the data handling process can be shown. This information would be shown alongside the actual data values.

Appendix 2.3. Data Lineage Tracking Traceability

Data lineage refers to the lifecycle of data, including its origins, where it moves over time, and what happens to it. It's about understanding the journey that data has taken from its source to its current state. This can include transformations, processes, systems, and people that have interacted with the data. Data lineage is often visualized in a lineage diagram, which provides a clear view of the data's history and context. In the DPP this would translate to being able to visit the DPP data of raw materials or components that are processed into the product.

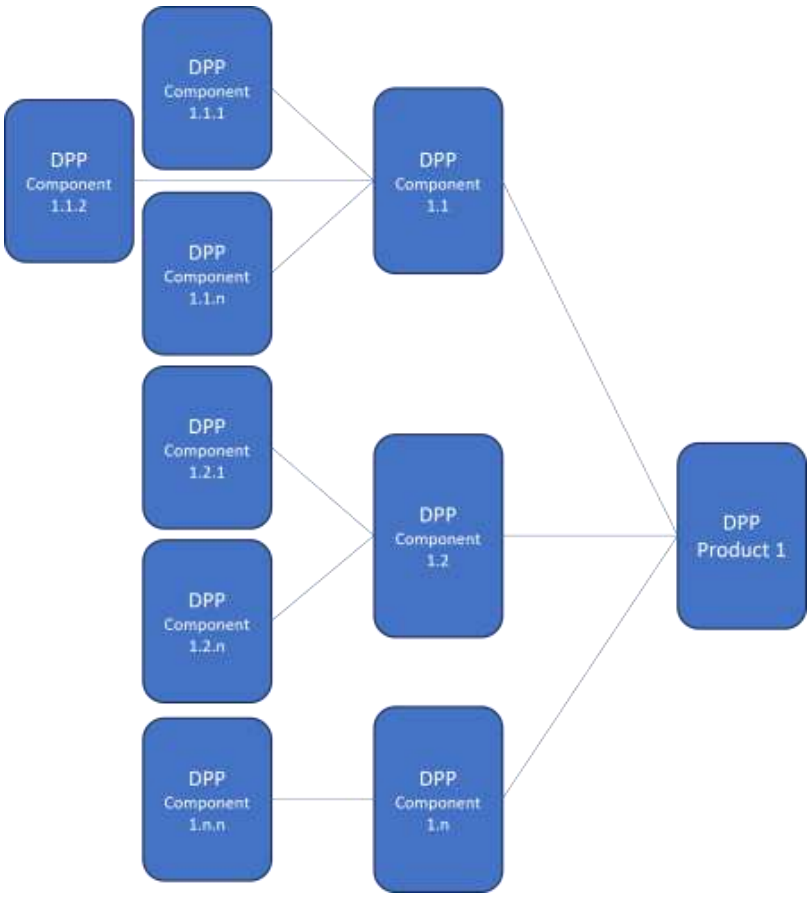

Figure 6. An example of digital lineage tracking

Appendix 2.4. Data Provider Traceability

Unique Location Identifiers (ULI) are used to identify physical locations and legal entities within supply chains. It enables precise identification of locations, such as warehouses, production facilities, and offices, facilitating efficient logistics and operations. ULIs help streamline communication and data exchange between trading partners, ensuring accurate and consistent location information. An example of this is GS1's Global Location Number that can be used by organizations to identify their different locations.

Figure 7. An example of a ULI (GS1 US, 2022)

Appendix 2.5. Third-Party Certification

Third-party certification for data compliance involves an independent organization evaluating and verifying that a company's data practices meet specific standards and regulatory requirements. This could be, for example, on data collection level, data storage level, or data processing.

Appendix 2.6. Verifiable Identities for Accessibility

Verifiable identities for accessibility involve using authenticated and secure digital identities to grant individuals access to information and services. This ensures that only authorized users can access sensitive or restricted data. By employing verifiable identities, organizations can streamline access management, making it easier to provide tailored access to the right users. An example of this would be 'Sign in with Google', but in the case of the DPP the Issuer could be, for example, a governmental institution.

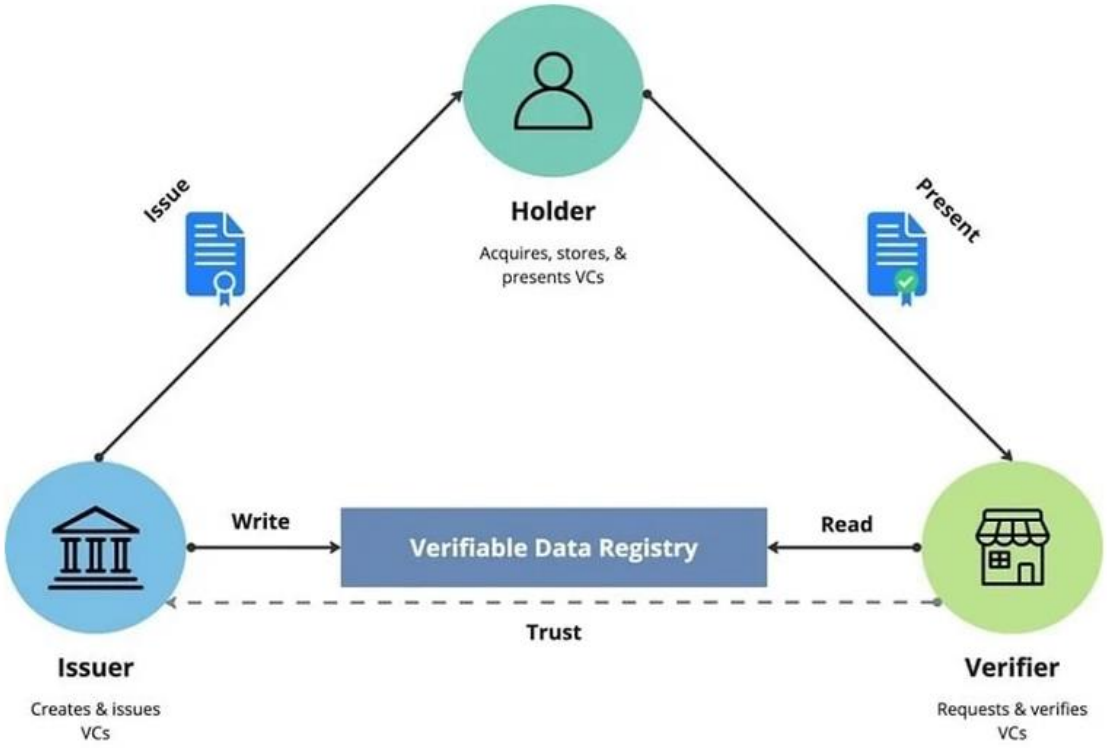

Figure 8. An example of verifiable credentials (Hale, 2023)

Appendix 2.7. Decentralized Data Storage

Decentralized data storage distributes data across multiple nodes or locations rather than storing it in a central server. As data is not concentrated in one location it is less prone to failure of that one location, as would be the case in a centralized storage.

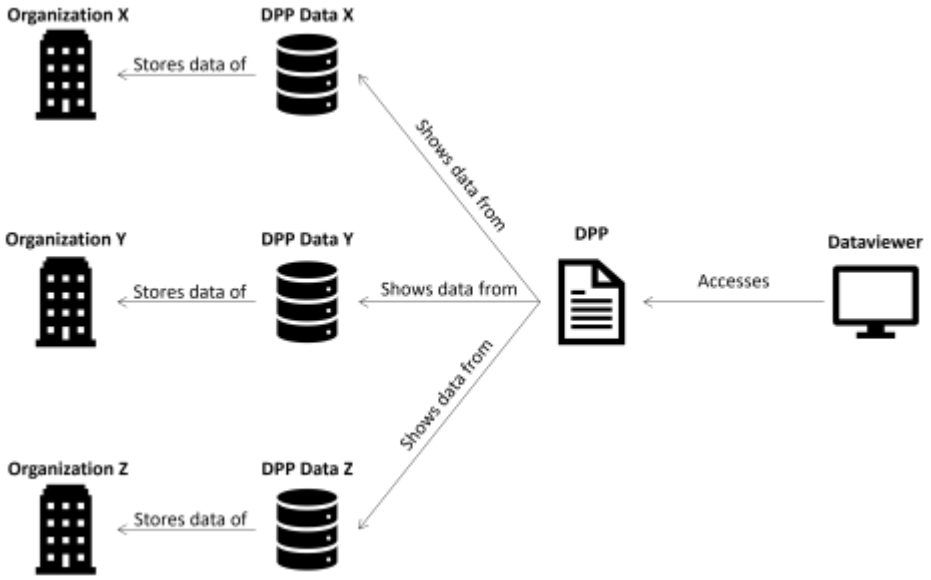

Figure 9. An example of a decentralized data storage

Appendix 2.8. Secure Authentication for Editing Rights

Secure authentication for editing rights involves implementing robust user authentication mechanisms to control access to editing privileges within a system or platform. By requiring users to verify their identity through secure authentication methods, organizations can ensure that only authorized individuals can make changes to specific data or content.

Appendix 2.9. Circularity

Circularity is a concept in sustainability that promotes the efficient use of resources. It involves designing products and systems in a way that minimizes waste and maximizes the reuse and recycling of materials. The goal is to create a closed-loop system where waste is eliminated and resources are continually used and reused. This approach contrasts with the traditional linear economy, which follows a ‘take-make-waste’ model.

Appendix 3. Invitation Letter

Dear reader,

As a Master's student at Tilburg University (NL) and the University of Turku (FI), I, in collaboration with TNO, would like to invite you to participate in a research study on the topic of trust in digital product passports (DPPs). These passports are introduced by the European Commission to help create a circular economy of products through sharing data and information about products and their ecological impact throughout the value chain. From 2027, the gradual introduction will happen in the electronic vehicle battery, textiles, and construction sectors. Therefore, it would be valuable to gather insights on how to increase the user's trust in this passport for a more effortless adoption.

By participating in this survey (approx. 15 min.), you will contribute to a deeper understanding of the factors shaping trust in digital product passports and the effects thereof.

The goals of this survey are as follows:

- To identify key data management factors influencing trust in DPPs that can be implemented when designing the DPP system;
- To explore the impact of trust on the intention to utilize the DPP for its intended purposes;
- To gather insights from professionals and stakeholders who will be using digital product passports.

Adherence to ethical guidelines governing research is ensured. Your participation in this study is voluntary and anonymous, and you have the right to withdraw at any time without consequence. Additionally, all data collected will be handled with the highest confidentiality, and your responses will only be used for this research purpose. Once the research has been completed, all the data will be discarded.

To participate in the survey, please click here.

Thank you in advance for your time and participation. Should you have any questions or require further information, please do not hesitate to contact me at a.n.a.vdneijnden@tilburguniversity.edu.

Kind regards,

Anne van den Eijnden

Tilburg University | University of Turku | TNO

Appendix 4. Research Data Management Plan

The research data management plan is based on the University of Glasgow's five questions. The questions are answered as follows:

- What data will be created?
    - Quantitative and descriptive data will be gathered in terms of survey responses.
- How will the data be documented and described?
    - Descriptive statistics will provide an overview of all participants in the study to create an overview of the respondents. This way no specific cases can be retrieved from the data presented in the final report. Further, all results from the data will be presented in one overview for the same purpose.
- How will you manage ethics and intellectual property rights?
    - Participating in the study is voluntary and participants can stop their participation at any point in the survey. The responses to the survey will be anonymized and the data will be used only for the purpose of this research and will therefore not be available to any other parties.
- What are the plans for data sharing and access?
    - Data will not be shared and will be visible only to the researcher of this study. No access is provided to other parties.
- What is the strategy for long-term preservation and sustainability?
    - The dataset will be destroyed after the finalization of the study, to maintain confidentiality of the participants. The results of the study will be public, but no data will be traceable to any person who filled in the survey.