

UNIVERSITÄT
BAYREUTH

Designing Trust and Verifiability in Digital Energy Systems

Dissertation
zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft
der Rechts- und Wirtschaftswissenschaftlichen Fakultät
der Universität Bayreuth

Vorgelegt
von
Till Zwede
aus
Buchholz in der Nordheide

Dekan:	Prof. Dr. Claas Christian Germelmann
Erstberichterstatter:	Prof. Dr. Jens Strüker
Zweitberichterstatter:	Prof. Dr. Nils Urbach
Tag der mündlichen Prüfung:	15. September 2026

“Wer überzeugt ist, nichts verändern zu können, richtet Schaden an – aus Gedankenlosigkeit, aus Bequemlichkeit.”

Iryna Fingerova

Acknowledgments

This dissertation marks an important – if not the most important (that part remains to be seen) – milestone of my academic career, and it would not have been possible without a lot of explicit and implicit support along this journey, and the life that led up to it. I want to extend my deepest gratitude to everyone who has played a role in my life leading up to this moment. I wouldn't be the same had I not met and shared time with you.

A very special thank you goes to my family – Dinah, André, Benthe, and Thore – who set and softly steered me on a path where I could pursue my own dreams and goals, while always teaching me the important lessons and values for life. I sincerely appreciate the support you have always extended toward me, and the valuable time we've spent together.

A big thank you goes out to my friends. To those who have known me since childhood and still make time for me despite the distance between us – Ole and Dawid, thank you for a friendship that needs no catching up. And to those I met along the way, in Bayreuth and beyond, who became such an important part of my life these past years – Michael, Julia, Jan, Timo, Basti, Duda, Felix, Linda, Marvin, Marike, Marc, and Paula, thank you for making this chapter unforgettable. I deeply value the positive impact you all have on my life – through laughter, games, evenings and nights out, insightful or lighthearted conversations, and more. Spending time with you has given me the energy and perspective that make everything else in life easier.

I owe equal thanks to my co-authors – especially Matthias, Marvin, Paula, and Lynne – whose ideas, feedback, and teamwork made this research far stronger than I could have made it alone.

My mentors and supervisors were just as essential to this journey.
Thank you, Johannes, for guiding my master's thesis and, in doing so, helping me realize that I wanted to become an expert and design new solutions in the energy domain.
Thank you, Marc, for always providing easily accessible guidance and mentorship in research, and for the friendship that has grown alongside it.

And most centrally, thank you, Jens, for enabling this entire journey – for providing honest and right guidance and support, for letting me take responsibility and learn all the necessary soft and hard skills that allowed me to become an expert in a field I deeply value, and that leave me feeling more than ready for the next steps in my career. Just as formative for my personal growth was your flexibility in supporting me as I started my own company.

That start-up journey – and the experiences I gathered with my co-founders (now friends) Valentin, Vincent, and Jens (not my supervisor!), together with our employees, and business partners – was incredible, and taught me more in that short time than any traditional career path could have.

And lastly, to Lynne, my partner: none of this would have been possible without you. Your daily support, and the long days and nights we spent together – working, researching, having fun – have pulled me through these last, very extraordinary, years. Your perspective has always helped me, especially in times of difficult decisions, and your encouragement and love have pushed me through so many barriers and toward so many milestones. I look forward to the rest of my life with you and the family that I adopt with that promise. This is our milestone – and it will get even better from here.

Abstract

The renewable energy transition is restructuring electricity systems, necessitating the coordination of many spatially distributed and heterogeneous actors and assets. This coordination requires data sharing to ensure efficient, secure, and sustainable operation. At this scale, actors can no longer trust the data they receive from often unknown counterparties, and manually verifying each sender and datum becomes prohibitively inefficient. Verification must therefore become digital and automatable to scale. While such verifiable data sharing promises to create value through co-creation, the data carrying this value are often sensitive, and disclosure risks loss of control and competitive or privacy-related harm. A data-sharing dilemma results: data create value only once a relying party can establish that they are correct, yet establishing this must not force those who hold the data into indiscriminate disclosure.

Positioned at the intersection of Information Systems, Green IS, and Energy Informatics, this dissertation asks how verifiable data sharing and the necessary trustworthy infrastructure can be designed to support value creation in decentralized digital energy systems while addressing privacy concerns and loss-of-control risks. Integrating nine research papers within the Design Science Research paradigm, it addresses a theoretical and design-oriented gap along a single arc: from the value drivers and acceptance requirements that make verifiable data sharing worthwhile, through the design knowledge that realizes it, to the governance conditions under which that knowledge creates value at system scale.

The overarching finding is that verifiability is not a substitute for trust but a means of relocating it, from the counterparties an actor shares data with toward the technologies and infrastructures that mediate data sharing. This trust shift recurs across the explanatory and the design argument. On the explanatory side, three value drivers emerge. Technology-enabled data sovereignty reshapes the interplay of trust, control, and perceived risk, enabling control instead of reliance on a counterpart's goodwill. Sustainability data create value through purpose-fit and not availability, and digital verifiability turns a credence attribute into a credibility signal that outperforms third-party certification at the point of choice. Acceptance of these applications turns not on social influence, as in classical acceptance models, but on comprehensibility and trust in technology.

On the design side, the dissertation contributes layered design knowledge: it derives generalizable design principles for cross-organizational energy and sustainability data sharing. It then develops a trustworthy infrastructure, the Trust Diamond and its Decentralized Flexibility Provision Architecture, in which revocable delegation substitutes a verifiable data lineage for trust in the intermediary. And it designs mechanisms that render individual claims verifiable under privacy constraints through succinct zero-knowledge proofs and newly developed shielded, fractional non-fungible tokens. The results make data sharing verifiable downstream of measurement but presuppose the truth of the source – the oracle problem, beyond this dissertation's scope. A capability-oriented rather than technology-deterministic policy perspective completes the arc with the governance conditions for deployment. The dissertation thereby contributes design-oriented knowledge for trustworthy and verifiable data sharing under explicit privacy, control, and governance constraints.

Table of Contents

1 Introduction **1**

1.1 Motivation 1

1.2 Research Aim 3

1.3 Structure of the Thesis and Overview of Embedded Research Papers 8

2 Trust & Verifiability as Value Drivers in Digital Energy Systems **10**

2.1 Interorganizational Trust in Digital Data Ecosystems 12

2.2 The Value of Verifiable Digital Energy Data and Attributes 15

2.3 User Acceptance of Verifiable Digital Data Sharing Solutions 19

2.4 Synthesis 21

3 Designing Trustworthy and Verifiable Digital Energy Data Infrastructure **23**

3.1 Design Principles for Digital Energy Data Sharing 24

3.1.1 Emission Data Sharing in Battery Value Chains 25

3.1.2 The Concrete Data Sharing Dilemma in Battery Value Chains 26

3.1.3 Two Design Approaches Informing Digital Energy Data Sharing 26

3.1.4 Data Usability Across Actors and Time 28

3.1.5 The Confidentiality–Traceability Tension 29

3.1.6 Operational and Ecosystem Viability 31

3.1.7 From Requirements to a Built Energy-Domain Instance 32

3.1.8 Design Principles for Digital Energy Data Sharing – Synthesis 34

3.2 Trustworthy Digital Energy Data Infrastructure 35

3.2.1 The Infrastructure Challenge in Small-Scale Flexibility Provision 35

3.2.2 Roles as Central Infrastructure Building Blocks 36

3.2.3 The Trust Diamond 37

3.2.4 The Trust Shift on an Infrastructure Level 37

3.2.5 The Decentralized Flexibility Provision Architecture 39

3.2.6 A Contrasting Infrastructural Pattern: Green Electricity Labeling 40

3.2.7 The Oracle Problem as a Boundary Condition 41

3.2.8 Performance as Feasibility Evidence 42

3.2.9 Trustworthy Digital Energy Data Infrastructure – Synthesis 42

3.3 Mechanisms for Verifiable Digital Energy Data Sharing 43

3.3.1 Abstracting Verifiability from Transparency 44

3.3.2 Securing the Accounting Step: Green Electricity Labeling 44
3.3.3 Securing the Value in Motion: Shielded Fractionalized NFTs 46
3.3.4 The Common Logic behind Two Mechanism Designs 47
3.3.5 Evidence on Feasibility and Embeddedness 47
3.3.6 Mechanisms for Verifiable Digital Energy Data Sharing – Synthesis 49
3.4 Designing Trustworthy & Verifiable Digital Energy Data Infrastructure – Synthesis 50

4 Conclusion **53**
4.1 Summary, Policy Implications & Outlook 53
4.2 Acknowledgement of Previous & Related Work 60

Bibliography **63**

A Overview of Research Papers **74**
A.1 Research Papers Included in This Dissertation 74
A.2 Index of Further Papers 75
A.3 Individual Contribution to the Included Research Papers 76

B Research Papers **79**
B.1 Research Paper P1: The Impact of Technology-Enabled Data Sovereignty on Trust and Control in Data Platform Ecosystems 79
B.2 Research Paper P2: From Fragments to Conceptual Clarity: A Taxonomy for Effective ESG Data Management 82
B.3 Research Paper P3: From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour 85
B.4 Research Paper P4: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications 86
B.5 Research Paper P5: Data Spaces for Battery Value Chains: Uncovering Design Principles for Emission Data Sharing 87
B.6 Research Paper P6: Designing Practical Blockchain-Based Green Electricity Labeling With Succinct Non-Interactive Zero-Knowledge Proofs 90
B.7 Research Paper P7: Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs 93
B.8 Research Paper P8: Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision . . 94
B.9 Research Paper P9: Governing Digital Technologies in Decentralized Energy Systems: A Qualitative Assessment of Capabilities and Policy Implications 95

List of Figures

Figure 1.1: Cumulative argument of the dissertation: from trust and verifiability as value drivers for data sharing to design knowledge for trustworthy infrastructure, verifiable mechanisms, and effective governance in decentralized digital energy systems. 7
Figure 1.2: Structure of the following chapters and associated papers within the cumulative dissertation. 8

Figure 2.1: Developed Model (Ehaus et al., 2026) 14
Figure 2.2: The final taxonomy on ESG data, comprising three meta-dimensions (MD), 17 dimensions, and 63 characteristics, partly exclusive (E) and non-exclusive (N) (Zwede, Valett, et al., 2026). 16
Figure 2.3: Estimated utility coefficients and predicted choice probabilities for the headphone and T-shirt models (Geist et al., 2026). 18
Figure 2.4: Self-Sovereign-Identity Acceptance Model (Guggenberger et al., 2023). 20
Figure 2.5: Specific Argument of Chapter 2 within the dissertation. Interorganizational trust and user acceptance enable value creation from verifiable data, serving as antecedents for the following chapters. 22

Figure 3.1: Specific Argument of Chapter 3 within the dissertation. Design principles for Digital Energy Data Sharing inform Trustworthy Digital Energy Data Infrastructure. That architecture itself is enabled by the specific Mechanisms for Verifiable Digital Energy Data Sharing. 24
Figure 3.2: Mapping of the 30 meta-requirements to six key requirements and six design principles for emission-data-sharing data spaces (Babel et al., 2026). 28
Figure 3.3: The Trust Diamond for energy flexibility provision, extending the issuer–holder–verifier trust triangle with the aggregator as a delegated-holder intermediary (Zwede et al., 2025). 38
Figure 3.4: The Decentralized Flexibility Provision Architecture operationalizing the Trust Diamond for small-scale flexibility provision (Zwede et al., 2025). 40
Figure 3.5: Division of labor in P6's proving scheme: a global zk-SNARK over private inputs establishes aggregate accounting consistency, while local Merkle proofs establish per-stakeholder inclusion (Zwede, Mertel, et al., 2026). 45
Figure 3.6: Process of minting and transferring shielded fractional proof-of-origin certificates for verifiable carbon-emission tracing (Babel et al., 2022). 48

Figure 4.1: Revisited cumulative argument of the dissertation: trust and verifiability as value drivers, design knowledge for trustworthy infrastructure and verifiable mechanisms, and the governance conditions for their deployment – connected by the recurring relocation of trust onto mediating technology. 55

List of Tables

Table 2.1: The three levels at which trust and verifiability act as value drivers in Chapter 2. 12

Table 3.1: Contrasting the two requirements-layer contributions of Section 3.1. 27
Table 3.2: The six design principles for emission-data-sharing data spaces (Babel et al., 2026), the design problem each addresses, and its role in the dissertation argument. 31
Table 3.3: Actor-role configuration of the Trust Diamond for verifiable flexibility provision (Zwede et al., 2025). 38
Table 3.4: The two mechanism patterns of Section 3.3 compared. 49
Table 3.5: Cumulative contribution of Chapter 3 across its three design levels. 51

Table 4.1: Contribution boundaries between the embedded papers and the dissertation-level synthesis. 61

Copyright Statement

The following chapters are partly comprised of content taken from the research articles in this thesis. To improve the readability of the text, I have omitted the standard labeling of these citations.

1 Introduction

1.1 Motivation

The renewable energy transition is restructuring electricity systems from the centralized dispatch of a few large generators toward the coordination of many distributed actors and assets. Generation and consumption become spatially distributed, ownership structures grow more heterogeneous, and electrification couples electricity ever more tightly with heating, mobility, and industry (Bühler et al., 2019; Goedeking & Meckling, 2024; Maldet et al., 2024; Thomaßen et al., 2021). This shift turns system operation into a coordination and governance problem: reliable and efficient operation now depends on the effective orchestration of numerous distributed actors, assets, data flows, and market roles instead of on centrally dispatched generation alone (European Commission, 2020b; Körner et al., 2022). At the core of this problem lies the exchange of data between these actors. Established coordination mechanisms were designed for a small number of large, centrally organized, and mutually known participants, where the trustworthiness of a counterpart and the correctness of its data could be presumed or checked manually (Hirth & Glismann, 2018; Lind et al., 2019). Once coordination instead spans many decentralized and often unfamiliar actors, this assumption no longer holds: actors can no longer simply trust one another or the data they exchange (Strüker et al., 2013). Where such implicit trust can no longer be presumed, the correctness of a counterpart and its data must instead be established explicitly. Doing so by hand – checking each counterpart, role, and datum case by case – remains feasible among a few mutually known participants, but the cost of such manual verification grows with the number of interacting actors and becomes prohibitive at the scale of a decentralized energy system (Körner et al., 2022). The correctness of data, roles, attributes, and identities must accordingly become *verifiable* in a form that can be checked automatically as opposed to manually, so that coordination can be scaled beyond individually negotiated bilateral relationships. Automating verification through end-to-end digitalization is what promises to keep it viable at this scale, lowering its cost by an order of magnitude; it is hence *digital* verifiability, and not verification in general, that this dissertation pursues (Körner et al., 2022; Sedlmeir, Smethurst, et al., 2021).

This requirement – to make data sharing trustworthy and verifiable across many decentralized actors – is at its core an information-systems problem going beyond a purely energy-technical one (Kotlarsky et al., 2023). Information Systems (IS) research provides the conceptual and methodological repertoire for designing and understanding how distributed actors coordinate and create value through shared data (Püchel et al., 2024). Green IS directs this repertoire toward environmentally sustainable development – for which the energy transition is a fundamental pillar – by treating information systems not as mere efficiency tools but as novel and digital enablers of sustainable practices (Seidel et al., 2013; vom Brocke et al., 2013; Watson et al., 2010). Energy Informatics, in turn, concerns the concrete design and implementation of such systems in the energy sector, specifying the information structures and coordination mechanisms that sustainable

energy systems require (Goebel et al., 2014; Schmeck et al., 2022). At the intersection of these lenses, the dissertation does not stop at explaining why data sharing may prove difficult but sets out to develop knowledge for making it trustworthy, verifiable, and ultimately valuable to the energy system. A recurring answer runs through this work: making data verifiable does not remove the need for trust but relocates it – from the actors one shares data with toward the technologies and infrastructures that mediate the exchange. Meanwhile, one central requirement surfaces – while data must be made verifiable, those who hold it must not be forced into undue disclosure.

Sharing such data across organizations is what creates value – improving processes, enabling new services and business models, and generating joint value – yet the very data that carry this value are often sensitive. Disclosing them exposes the sharing organization to loss of control, opportunistic use, unintended knowledge spillovers, and competitive or privacy-related harm (Fassnacht et al., 2023): plainly disclosed, energy data originating from household assets may reveal personal information protected under data-protection law (European Commission, 2023), or – in the case of industrial assets – may reveal trade secrets and production patterns that competitors could reconstruct (Brucker & Yalman, 2022), eroding privacy or competitive advantage. Evidence from similar sensitive datasets shows that precisely such concerns measurably lower actors' willingness to share data in the first place (Cichy et al., 2021). Here lies a central tension: information should be automatically verifiable, yet the underlying data need to be protected. The tension is not dissolved by the two obvious workarounds. Restricting disclosure to a few selected, trusted counterparts leaves each recipient unable to *verify* what it receives unless the source discloses prohibitively more information, and – arguably more importantly – such bilateral, need-to-know exchange does not scale to the many unfamiliar actors a decentralized energy system must coordinate (Körner et al., 2022; Strüker et al., 2013). Withholding or encrypting the data, conversely, protect them but forecloses its use: data a counterpart can neither read nor check cannot inform its decisions or be relied upon in coordination. A data-sharing dilemma results: data create value in the energy system only once a relying party can interpret them and establish that they are correct, yet establishing this must not force those who hold the data into indiscriminate disclosure (Sedlmeir et al., 2022). Work on privacy-enhancing computation makes the same point from the technical side: the obstacle is *not only* privacy, but the joint reconfiguration of trust, control, and risk that ultimately decide whether sensitive data are shared at all (Agahari et al., 2022). Where this dilemma is left unresolved, the actors expected to share data will not accept the corresponding solutions – and without their acceptance, the data is not shared and their value is not materialized (Benbasat & Barki, 2007; Rieger et al., 2022). One concrete example of this dilemma becomes visible in electricity grid operation, where operators need verifiable flexibility data to ensure stable system operation, while the master and operational data of small-scale devices are highly privacy-sensitive and, for prosumers, fall under data-protection law (Ferrag et al., 2018; Körner et al., 2022). The same structural tension recurs in adjacent domains – green-electricity labeling and carbon-emission tracing across supply chains – from which design knowledge can be drawn and to which it can be extended (Sedlmeir, Völter, & Strüker, 2021; Ströher et al., 2025). Designing verifiable data sharing solutions thus comprises a socio-technical challenge, spanning trust, control, privacy, and verification across organizational and personal boundaries.

Technological building blocks for verification and the preservation of privacy have recently been discussed in the literature: digital identities, verifiable credentials, distributed ledgers, and zero-knowledge proofs have been proposed across a range of fields including Green IS and energy informatics (Goldwasser et al., 1989; Sedlmeir, Smethurst, et al., 2021). Yet they have largely been studied in isolated use cases and from technology-specific perspectives, leaving their impact on data sharing and data use in information systems in general, and digital energy systems specifically, neither theoretically well understood nor practically realized (Körner et al., 2022). Two gaps follow. The first is theoretical: it remains insufficiently theorized how these technologies actually shape data sharing and use – in particular, how organizations come to trust technology-mediated data-sharing arrangements and what leads end users to actually adopt them, before data can be shared in value-creating ways (Agahari et al., 2022; Benbasat & Barki, 2007; Das & Teng, 2001). The second is design-oriented: the field still lacks design principles for these comparatively novel arrangements, verification mechanisms tailored to the roles, constraints, and incentives of the energy system, and trustworthy architectures that integrate both into viable and value-generating artifacts (Gregor et al., 2020; Principato et al., 2023). This dissertation aims to address both of these gaps by developing a theoretical understanding of the mechanisms of data sharing and creating socio-technical design knowledge and resulting practical architectures for trustworthy and verifiable energy-data infrastructure.

Resolving these questions is as pressing as ever. Currently, EU policy calls for more integrated planning and operation across energy carriers, infrastructures, sectors, and data flows, yet a systematic understanding of which digital capabilities decentralized digital electricity systems actually require is still missing (European Commission, 2020b, 2022; European Commission: Directorate-General for Energy et al., 2024). Questions of theoretical understanding (Chapter 2), of designing trustworthy and verifiable systems (Chapter 3), and of enabling policy (Chapter 4) should therefore not be treated in isolation (Kotlarsky et al., 2023). Only their interplay can unlock the potential of IS research for the energy transition and, with it, for global decarbonization.

1.2 Research Aim

The motivation framed trustworthy and verifiable data sharing in decentralized digital energy systems as a socio-technical design problem with two significant gaps: a theoretical gap, concerning how verifiable, technology-mediated data sharing creates value, and a design-oriented gap, concerning how such data sharing can be enabled through information systems design. This dissertation studies neither the digitalization of the energy sector in general nor isolated digital technologies. It pursues the narrower phenomenon of verifiable data sharing and the necessary trustworthy infrastructure and sets out to contribute to both gaps through this lens. A brief terminological note frames what follows. This dissertation is concerned with data *sharing* in the broad, organizational sense – the constellation of participating actors, the access and usage policies among them, and the conditions under which data may be transferred at all – and reserves data *exchange* for the narrower technical transfer of data between two parties. A precise definition

follows in Section 3.1.2. Against this background, the overarching research question guiding this dissertation is:

> *How can verifiable data sharing and the necessary trustworthy infrastructure be designed to support value creation in decentralized digital energy systems while addressing privacy concerns and loss-of-control risks?*

The question rests on two related but distinct constructs. In line with P1, this dissertation understands trust as the willingness of actors to accept vulnerability under conditions of uncertainty and perceived risk (Mayer et al., 1995). Verifiability, by contrast, denotes the possibility of leveraging information systems to ensure the truthfulness of data, claims, attributes, or computations in contrast to accepting them as asserted (Sedlmeir, Smethurst, et al., 2021). The two are closely linked but not interchangeable. Verifiability can take the place of *some* of the trust an actor would otherwise have to extend toward another: a party that can check a claim for itself does not need to simply believe the counterpart that asserts it. But verifiability can neither take the place of *all* of that trust, nor does it do so automatically – the checking party must still trust that the verification mechanism is sound and honestly operated. How exactly the two relate – specifically, how verifiability relocates trust from counterparties toward the technologies and infrastructures that mediate data sharing – is itself an object of this work and developed in Chapter 2.

To answer the research question, the dissertation pursues five research objectives (ROs) along a single arc – from the necessary conditions for value creation, through three aspects of system design of increasing integration, to the governance implications for effective deployment. RO1 addresses the theoretical gap (Chapter 2); RO2–RO4 address the design gap on three interdependent levels (Chapter 3); RO5 adds the governance and policy implications (Chapter 4). Because RO2–RO4 are constructive rather than merely explanatory – they call for the design, implementation, and evaluation of artifacts – the dissertation pursues them within the design science research (DSR) paradigm, which provides the methodological repertoire for developing and validating prescriptive design knowledge (Gregor & Hevner, 2013; Hevner et al., 2004; Peffers et al., 2007).

1. **RO1: Understand how trust and user acceptance shape the value potential of verifiable data sharing (Chapter 2).**
   To design verifiable mechanisms and trustworthy infrastructures we must first understand why actors participate in data sharing and under what conditions that exchange creates value (Grover & Kohli, 2012). RO1 establishes this explanatory foundation and in doing so addresses the theoretical gap along three strands. First, on trust (Section 2.1), P1 shows that verifiable interorganizational data sharing, operationalized as technology-enabled data sovereignty, reshapes the interplay of trust, control, and perceived risk in decentralized platform ecosystems (Ehaus et al., 2026). Its central result is that verifiable data control mechanisms relocate part of the trust actors must extend: where they once had to trust the counterpart, they must increasingly trust the technology and the infrastructure that mediate data sharing instances. This trust shift is what allows data sharing to scale beyond bilateral relationships where it must be negotiated case by case. P2 complements

this strand by establishing that the shared data themselves must be conceptually clear, governable, and purpose-fit for sustainability-related data to be shared across organizational boundaries (Zwede, Valett, et al., 2026). Second, on value (Section 2.2), data are valuable only when they are perceived as credible, interpretable, and manageable attributes, making them relevant to organizational decision making. From the organizational perspective, P2 provides a taxonomy that brings conceptual order to fragmented ESG data and links their characteristics to concrete usage contexts for value creation (Zwede, Valett, et al., 2026). From the demand side, P3 demonstrates empirically that digital verifiability of carbon information increases their value as credibility signals which in turn raises consumers' willingness to pay for products with digitally verifiable attributes (Geist et al., 2026; Spence, 1973). Third, on acceptance (Section 2.3), even potentially verifiable and value-adding solutions create value only if the expected users adopt them (Benbasat & Barki, 2007). P4 identifies, through a qualitative study, the conditions under which users accept self-sovereign identity applications and contributes acceptance variables beyond established technology-acceptance models (Guggenberger et al., 2023); P3 adds the corresponding demand-side perspective. Together, the three strands construct the core value drivers that verifiability mechanisms and trustworthy architectures must satisfy – and reveal a common pattern, as the relocation of trust toward mediating technology recurs at the organizational (P1), demand-side (P3), and user (P4) levels.

2. **RO2: Develop design principles for cross-organizational energy and sustainability data sharing (Section 3.1).**
   RO1 established *that* verifiable data sharing can create value and *under which conditions*; RO2 takes the first step in turning those conditions into prescriptive design knowledge. The first design question is not yet which infrastructure or mechanism to build, but what any such solution must provide – the requirements a cross-organizational arrangement has to satisfy once the relevant data are distributed across many actors with divergent incentives and confidentiality needs. Design principles capture this requirements-level knowledge and thereby precede and constrain the infrastructure and mechanisms that are later developed in RO3 and RO4 (Gregor et al., 2020). As such, P5 derives design principles for an emission-data *data space* in complex battery value chains, where product-carbon-footprint assessment depends on primary data from several upstream actors and traceable data may expose sensitive process information putting participants' competitive advantage at risk (Babel et al., 2026; Jarke et al., 2019). P6 complements these with design principles distilled from an implemented and evaluated system for the improved labeling of green electricity between consumers and producers, grounding the principles in a working artifact beyond conceptual requirements alone (Zwede, Mertel, et al., 2026). RO2 thus bridges from the value drivers of RO1 to the concrete design of verifiable data sharing in trustworthy data ecosystems across organizational boundaries.

3. **RO3: Design a trustworthy infrastructure for verifiable and privacy-preserving data sharing (Section 3.2).**
   Design principles specify *what* a cross-organizational data-sharing arrangement must support, but not *who* satisfies those requirements or how the responsibilities for issuing, holding, verifying, and delegating data are distributed among actors; answering that moves the design from principles to infrastructure. Such an infrastructure must make governance principles and technical mechanisms fit for the roles of participating actors and their interaction patterns (Sedlmeir, Smethurst, et al., 2021). P8 develops such an infrastructure design – the decentralized flexibility-provision architecture, grounded in the accompanying Trust Diamond – a prototype implementation for small-scale flexibility provision, combining wallet-based identity management, zero-knowledge proofs for data minimization, and an intermediary that aggregates flexibility while shielding device-level data (Zwede et al., 2025). P6 contributes a second, implemented and evaluated architecture that reconciles public data auditability with disclosure control and scalability for green electricity labeling (Zwede, Mertel, et al., 2026). In the terms of the DSR lens adopted above, RO3 contributes both an instantiated architecture and the design knowledge it embodies: it highlights how the trust that RO1 found relocating onto technology can be vested in an infrastructure built to bear it – credibly, auditably, and enforceably – by leveraging the design principles proposed by RO2.

4. **RO4: Design sovereign data-sharing mechanisms that enable verifiable proof of claims under privacy constraints (Section 3.3).**
   Where RO3 focuses on the trust element and organizes *who* may verify *what* across the infrastructure, RO4 turns to the individual claim: it operates at the mechanism level, where the granular verifiability of a single claim is needed but plainly disclosing the data behind it raises privacy, confidentiality, and scalability concerns (Goldwasser et al., 1989). P7 introduces shielded, fractional non-fungible tokens combined with off-chain bilateral data exchange to provide verifiable carbon-emission tracing along electricity supply chains at high resolution while keeping sensitive data confidential (Babel et al., 2022). P6 contributes the complementary mechanism for green-electricity labeling, using succinct zero-knowledge proofs and Merkle trees to prove specific claims about energy provenance on a global and an individual level without revealing the sensitive underlying data (Zwede, Mertel, et al., 2026). As with RO3, the contribution is twofold – the technically instantiated mechanisms and the generalizable privacy-preserving verification logic they embody: RO4 thereby supplies the mechanism-level design knowledge that the infrastructure of RO3 presupposes, addressing the design gap at its most granular level.

5. **RO5: Derive governance and policy implications for the effective deployment of digital technologies in decentralized electricity systems (Chapter 4).**
   The design contributions of RO2-RO4 do not operate in an institutional vacuum; their value depends on enabling conditions in the regulatory-, market-, and data-governance domains (European Parliament and Council of the European Union, 2023). P9 assesses,

through a qualitative multi-method study, which capabilities certain digital technologies can provide to the governance and operation of decentralized electricity systems and which policy measures enable their effective deployment (Zwede, Heeß, et al., 2026). RO5 ensures that the dissertation closes not with isolated artifacts alone, but with a clear value proposition that those artifacts can contribute to the energy transition while also expressing the necessary regulatory implications for effective adoption.

Taken together, these objectives aim to comprehensively answer the stated research question. To this end, the dissertation's cumulative contribution lies in a layered body of design-oriented knowledge for verifiable data sharing and the necessary trustworthy infrastructure in decentralized digital energy systems – the details of which will be laid out throughout this dissertation (cf. Figure 1.1).

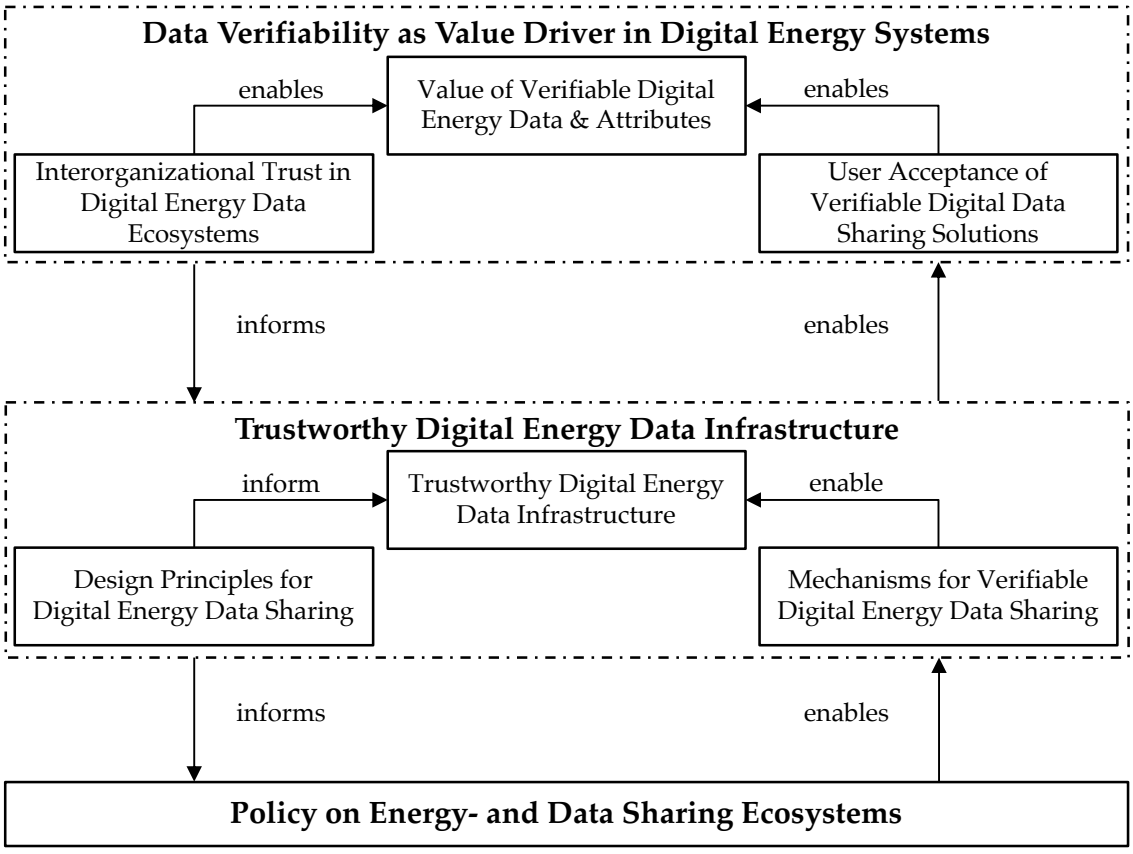


Figure 1.1: Cumulative argument of the dissertation: from trust and verifiability as value drivers for data sharing to design knowledge for trustworthy infrastructure, verifiable mechanisms, and effective governance in decentralized digital energy systems.

This layering specifies what the dissertation contributes to each field it engages with. To IS, it advances the understanding and design of data-sharing arrangements in decentralized data sharing instances where trust, control, risk, and value creation are jointly shaped in organizational interaction through technological mechanisms (Kotlarsky et al., 2023). To Energy Informatics, it develops information systems, verification mechanisms, and infrastructure designs for concrete coordination problems – flexibility provision, green-electricity labeling, and carbon-emission

tracing. Lastly, to Green IS, it presents how information systems can support sustainability-oriented decisions and management along complex value-chains while specifically advancing the energy transition, setting up a concrete impact on global decarbonization.

The next section maps these papers onto the dissertation's chapters.

1.3 Structure of the Thesis and Overview of Embedded Research Papers

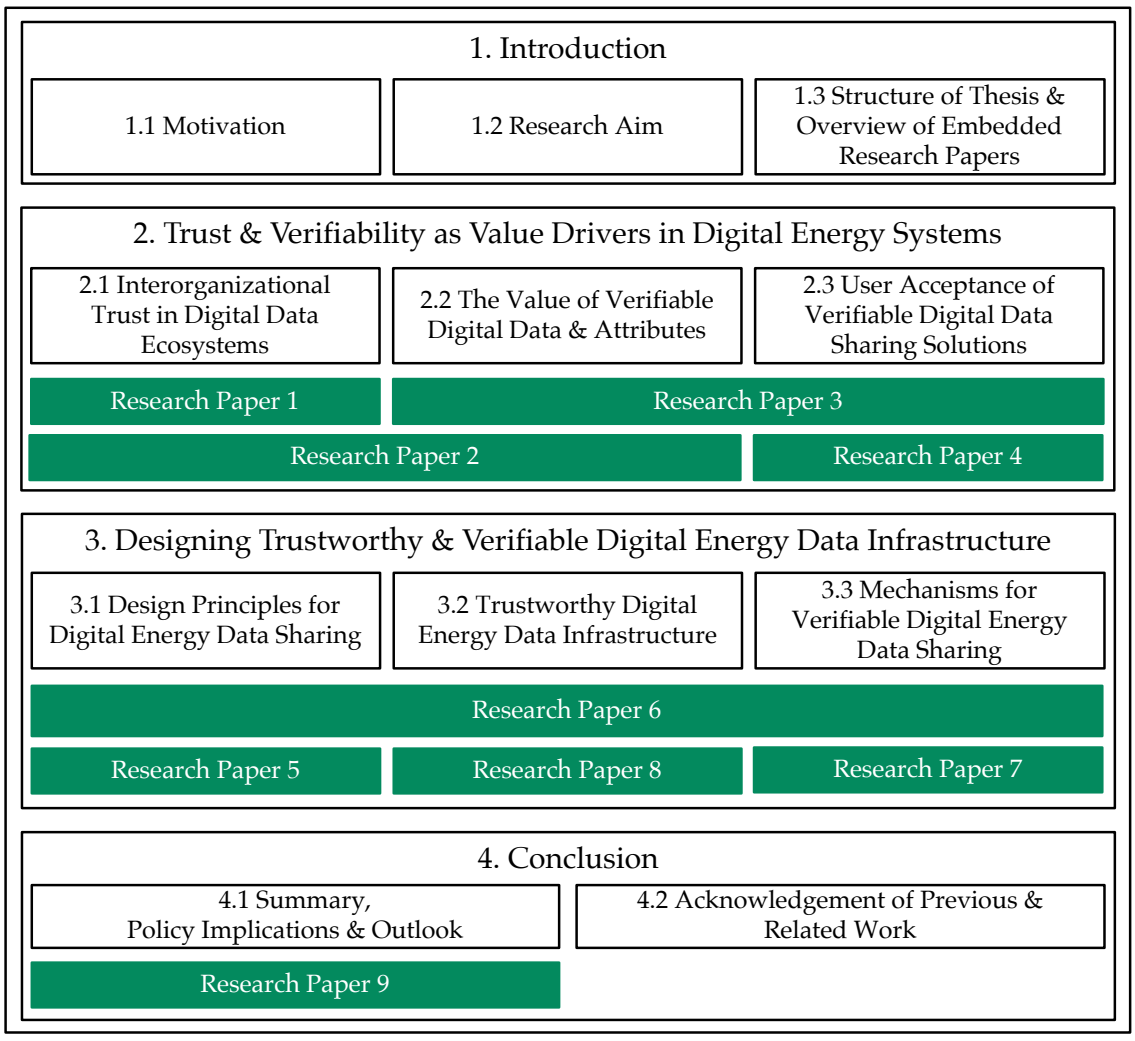


Figure 1.2: Structure of the following chapters and associated papers within the cumulative dissertation.

This dissertation is cumulative: its nine embedded papers (P1–P9) are integrated into a single dissertation-level argument and explicitly not arranged chronologically or by technology. Its structure follows the red thread developed in the preceding sections – the decentralization of digital energy systems makes coordination data-dependent; this dependence produces a data-sharing dilemma shaped by tensions between trust, control, privacy, and verifiability; and resolving these

tensions calls for socio-technical design knowledge for verifiable data sharing mechanisms and the necessary trustworthy infrastructure. The three main chapters follow the arc of the research aim, from the conditions of value creation, through the design responses that create it, to the governance conditions for their deployment. Figure 1.2 summarizes this logic and locates each chapter within it.

Chapter 2, *Trust and Verifiability as Value Drivers in Digital Energy Systems*, develops the explanatory side of the argument and closes the theoretical gap: it establishes why and under which conditions verifiable data sharing creates value before the dissertation turns to how it can be designed. Section 2.1 examines interorganizational trust through P1's notion of technology-enabled data sovereignty (Ehaus et al., 2026) and P2's perspective on organizations perception of sustainability data. Section 2.2 shifts from actor relationships to the data themselves, drawing on P2 (a taxonomy of fragmented ESG data) and P3 (the value of verifiable carbon information) (Geist et al., 2026; Zwede, Valett, et al., 2026). Section 2.3 adds the user-facing view, drawing on P4 – complemented by the demand-side perspective of P3 (Guggenberger et al., 2023). Together, these sections establish technology-enabled data sovereignty, verifiable sustainability data, and technology acceptance as value drivers within the scope of the dissertation.

Chapter 3, *Designing Trustworthy and Verifiable Digital Energy Data Infrastructure*, leverages the identified value drivers to devise design knowledge, closing the design gap across three interdependent levels. Section 3.1 derives design principles for cross-organizational energy and sustainability data sharing, drawing on P5's *data space* for emission-data-sharing along battery value chains and on P6's design principles derived from a green-electricity labeling system (Babel et al., 2026; Zwede, Mertel, et al., 2026). Section 3.2 moves to the infrastructure level, drawing on P8's decentralized flexibility-provision architecture and its accompanying Trust Diamond, complemented by the architecture of P6 (Zwede, Mertel, et al., 2026; Zwede et al., 2025). Section 3.3 turns to the underlying verification mechanisms, drawing on P7's shielded, fractional non-fungible tokens for verifiable carbon-emission tracing and on P6's succinct zero-knowledge proofs for verifiable green-electricity labeling (Babel et al., 2022; Zwede, Mertel, et al., 2026).

Chapter 4, *Conclusion*, steps back from the individual artifacts to their joint contribution and dependencies. Section 4.1 summarizes how the embedded papers jointly answer the research question and derives policy implications and an outlook, drawing on P9 and its assessment of the digital capabilities and enabling policy for decentralized electricity systems (Zwede, Heeß, et al., 2026). Section 4.2 acknowledges previous and related work and clarifies the relationship between the embedded papers, related publications, and the cumulative dissertation contribution.

2 Trust & Verifiability as Value Drivers in Digital Energy Systems

Decentralized digital energy systems create value by coordinating distributed actors and assets: ensuring reliable and efficient system operation, provisioning flexibility, enabling market participation, and accounting for sustainable energy provenance. Realizing these forms of value depends on sharing data across organizations, assets, users, and institutions, a dependence that historic centralized energy architectures did not face (Goebel et al., 2014; Schmeck et al., 2022; Watson et al., 2010). The design-oriented chapters that follow develop the infrastructure, principles, and mechanisms for such exchange. This chapter establishes why that exchange creates value in the first place, and accordingly defines what characteristics any effective design must deliver.

To that end, the mere technical ability of a system to move data between actors does not by itself create value; value in data sharing is co-created through use, not conferred by availability (Grover & Kohli, 2012; Haki et al., 2019). Building on this premise, this dissertation organizes the conditions for such value creation into three aspects, each located at a different system level and each substantiated by embedded papers of this chapter. Actors must be willing to share data, despite the risk that disclosure entails (the organizational level, P1). The shared data must be interpretable and credible enough to inform a decision (the data-object level, P2 and P3). And the applications through which data are exchanged must be accepted by the people who operate and use them (the user level, P4). Where any one of these fails, value does not materialize: data are withheld, or they are shared but cannot be used, or they could be used but the application is not accepted. The three conditions are proposed as the structuring elements through which this chapter reads its four embedded papers.

Trust and verifiability are the two levers this dissertation foregrounds for satisfying these conditions. They serve as central enablers: trust describes the willingness to accept vulnerability under uncertainty and perceived risk (Mayer et al., 1995), and verifiability is the possibility of leveraging information systems to ensure the truthfulness of data, claims, attributes, or computations instead of accepting them as asserted (Sedlmeir, Smethurst, et al., 2021). Neither is exhaustive. External factors – among them price sensitivity, institutional rollout, and data governance – shape value alongside these two constructs and recur throughout the chapter as boundaries on what trust and verifiability alone can achieve. What distinguishes trust and verifiability from these factors, and motivates the dissertation's focus on them, is that they can be deliberately designed: a data-sharing arrangement can be built to make claims verifiable and to render itself trustworthy, whereas price levels or regulatory rollout largely lie beyond a designer's reach. The two are coupled but distinct: verifiability can substitute for part of the trust an actor would otherwise have to extend toward another, yet it neither presupposes nor guarantees it.

This coupling yields the chapter's fundamental claim, which the three levels substantiate in turn. Verifiability and the technical control it supports do not remove trust from data sharing; they relocate it. Across all three levels, the object of trust moves from the parties one transacts with toward the technology that mediates the transaction and the actors who operate it. At the organizational level, P1 demonstrates technology-enabled data sovereignty shifting reliance from trust between organizations toward trust in technology. At the data-object level, P3 highlights consumers favoring digitally verifiable carbon information over institutional certification, anchoring credibility in a verification mechanism rather than a certifier's reputation. At the user level, P4 shows trust in the software and the parties operating it as a direct condition of acceptance. Hence three independent evidence bases exhibit the same effect – a *trust shift* as the empirical backbone of this chapter.

Within this argument, a *value driver* is an enabling condition under which trustworthy and verifiable data sharing supports value creation: organizational willingness to share credible and decision-relevant data and attributes – despite associated risk, and user acceptance of the applications that carry such data. The claim is not that trust or verifiability automatically produce value, but that they are the conditions under which the design responses of the following chapter can enable value creation through data sharing.

Three distinctions discipline the argument and recur throughout. The first separates *verification* from *verifiability*: verification is a checked status a datum acquires within a management process, whereas verifiability is the property that a claim can be independently checked by a relying party who cannot inspect its source. A verified datum is not yet a verifiable claim for an outside actor. The second separates the two kinds of disclosure risk that the data-sharing dilemma folds together. *Privacy* denotes the personal, data-protection-governed concern that arises when shared data reveal information about identifiable individuals, as governed by regimes such as the GDPR (European Commission, 2023); *confidentiality* denotes the firm-level, competitive concern that arises when shared data reveal trade secrets, process characteristics, or strategic information a firm has reason to protect (Brucker & Yalman, 2022). The two frequently coincide in energy data – smart-meter readings are at once personal and commercially revealing – yet they answer to different institutions and dominate at different points of the value chain, and the design chapter distinguishes them where that difference bears on the design. The third concerns the object of trust. Trust in the *parties* one deals with – counterpart organizations, credential issuers, verifiers, operators – is distinct from trust in the *technology* that mediates the exchange. The *trust shift* is precisely a rebalancing of trust from the former toward the latter. Distinguishing these objects allows the chapter to describe that shift without conflating it with a loss of trust.

The chapter proceeds across the three levels. Section 2.1 addresses the organizational level, drawing on P1 to demonstrate why bilateral data sharing between organizations – being highly prevalent in decentralized systems – may remain difficult despite its value potential and how technology-enabled data sovereignty can relocate trust to enable it to scale. Section 2.2 turns to the data object, drawing on P2 and P3 to highlight that data create value through purpose-fit and that digital verifiability can make a credence attribute decision-relevant. Section 2.3 addresses

the user, drawing on P4 to show that the applications operationalizing verifiable data sharing are accepted only when they are useful, manageable, trusted, and comprehensible. Table 2.1 maps this structure.

Table 2.1: The three levels at which trust and verifiability act as value drivers in Chapter 2.

Section	Level	Value-driver logic	Primary evidence
2.1	Organization & ecosystem	Technology-enabled data sovereignty enables control and relocates trust from counterparties toward technology, reducing perceived risk in data sharing.	P1 (Ehaus et al., 2026)
2.2	Data object & decision	Data create value through purpose-fit; digital verifiability makes a credence attribute credible and decision-relevant.	P2, P3 (Geist et al., 2026; Zwede, Valett, et al., 2026)
2.3	User & application	Verifiable applications are accepted only when useful, manageable, trusted, and comprehensible.	P4 (Guggenberger et al., 2023)

2.1 Interorganizational Trust in Digital Data Ecosystems

Designing trustworthy and verifiable data sharing first requires an organizational explanation of why data are not shared automatically, even when sharing promises value. Decentralized digital energy systems are a paradigmatic instance of decentralized data ecosystems in which generators, consumers, prosumers, aggregators, grid operators, market platforms, and more must coordinate through data that no single central entity holds. In such ecosystems, coordination depends on interorganizational sharing of data among heterogeneous, loosely coupled, and dynamically participating actors that pursue individual goals, may occupy several roles at once, and often interact without prior relationships (Gelhaar & Otto, 2020; Nischak et al., 2017; Oliveira et al., 2018, 2019). Neither stable bilateral trust nor a universally trusted central intermediary can be taken for granted. The organizational question is not whether technically usable data exist and can be shared, but whether actors are willing to disclose them under these conditions.

This willingness is constrained by a structural dilemma. Interorganizational data sharing can improve processes, enable new services and business models, and create joint value, yet the act of disclosure exposes the sharing organization to loss of control, opportunistic use, unintended knowledge spillovers, and competitive or privacy-related harm (Cichy et al., 2021; Fassnacht et al., 2023). As a result, actors may recognize the value potential of sharing while still withholding data, because the exchange creates vulnerability that availability alone does not sufficiently offset. This is the organizational form of the data-sharing dilemma: data become valuable in the energy system only once shared, but sharing must not expose those who hold the data to undue risk.

To describe the underlying mechanisms of this dilemma, literature refers to trust, control, and perceived risk as distinct and non-interchangeable constructs that explain different parts of

willingness – or lack thereof – to share data (Das & Teng, 2001; Mayer et al., 1995; Rousseau et al., 1998; Zaheer et al., 1998). Trust concerns an organization's willingness to accept vulnerability based on positive expectations about another party's intentions and behavior; control concerns the attempt to ensure that participants act in conformity with predefined rules, expectations, or strategies (Eisenhardt, 1985; Kirsch, 1997; Piccoli & Ives, 2003); and perceived risk captures the assessment of possible negative outcomes under uncertainty (Das & Teng, 2001; Ibbott & O'Keefe, 2004). Treating these as unilaterally dependent constructs would imply that more trust alone could resolve the data sharing dilemma. However, it cannot, because decentralized data ecosystems lack the very conditions under which interorganizational trust is normally built – repeated interaction, an established relationship history, and prior knowledge of the counterpart – which heterogeneous, loosely coupled, and dynamically participating actors rarely share (Gallivan & Depledge, 2003; Rousseau et al., 1998).

Those same conditions also weaken the conventional means of exercising control. Informal control rests on repeated interaction, shared norms, and relational history, none of which can be assumed among short-lived and weakly embedded ecosystem relationships (Das & Teng, 2001; Gallivan & Depledge, 2003). Formal, in this case technically embedded, control becomes the salient mechanism, enacted through contracts, standards, monitoring, and enforceable restrictions on data access and use (Dyer & Chu, 2003; Van den Broek & van Veenstra, 2015). This emphasis is reinforced by emerging architectural principles such as zero-trust, which replace implicit trust assumptions with the continuous verification of interactions (Kindervag et al., 2010; Rose et al., 2020). The organizational problem thus shifts from how to persuade actors to increasingly trust one another, to how the formal control provided by data sharing mechanisms can reduce the need for unconditional bilateral trust in the first place.

Technology-enabled data sovereignty proposes to supply exactly that kind of mechanism. It denotes a socio-technical combination of governance structures and digital technologies that jointly enable controlled, policy-compliant, auditable, and verifiable data sharing across organizational boundaries (Abbas et al., 2024; Hellmeier & von Scherenberg, 2023; Hummel et al., 2021; von Scherenberg et al., 2024). Its technical core is a set of privacy-enhancing technologies – secure multi-party computation, zero-knowledge proofs, and self-sovereign identities – that allow organizations to define, enforce, and verify how their data are accessed and used after disclosure (Agahari et al., 2022; Gossen et al., 2022; Xue & Wang, 2022). These are precisely the verifiable data-sharing mechanisms the dissertation aims to later design for the energy domain (Section 3.3); here they matter not for how they work but for what they change organizationally. By embedding control in governable and technically enforced arrangements in place of relational expectation alone, technology-enabled data sovereignty makes control a realizable property of the exchange instead of a promise contingent on a counterpart's goodwill.

This reconfiguration is the substance of P1's conceptual model (Figure 2.1) (Ehaus et al., 2026). The model describes a consistent effect: technology-enabled data sovereignty enables control, control reduces perceived risk, and lower perceived risk raises the willingness to share data, which in turn enables value creation. Two features of the model are decisive for the chapter. First, the

trust–control relationship is not a fixed substitution or complementarity but is use-case-specific – it is the most heavily evidenced pattern in P1's corpus and resists a single characterization. Second, and most importantly, technology-enabled data sovereignty does not raise trust uniformly: it reduces organizations' reliance on *trust between parties* while increasing the need for *trust in the technology* and infrastructure that mediate data exchange (Li et al., 2008; Söllner et al., 2016).

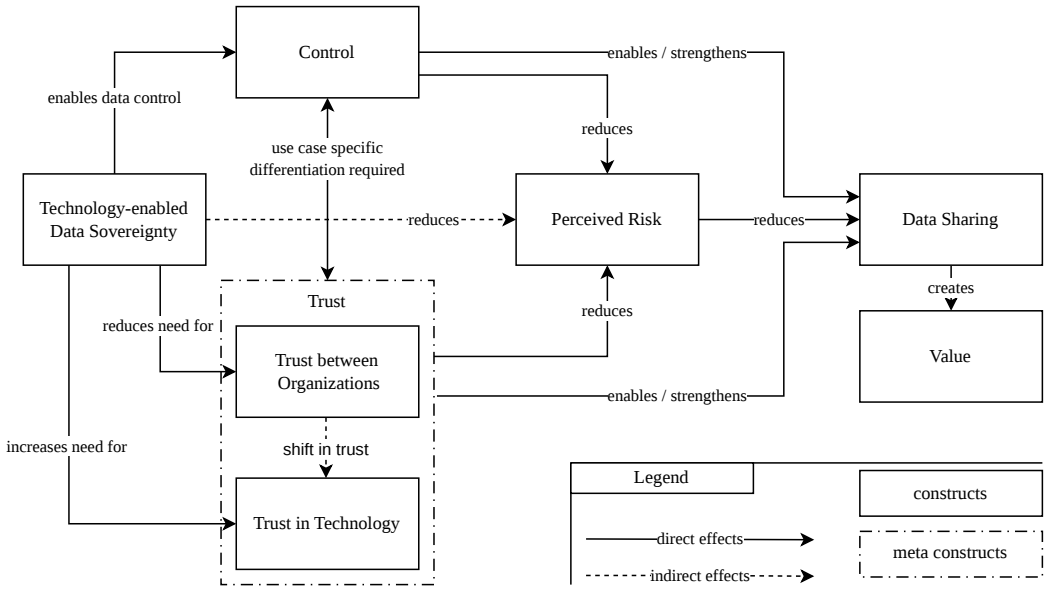


Figure 2.1: Developed Model (Ehaus et al., 2026)

This second feature is the chapter's fundamental claim in its organizational form: a *shift in trust*, not its removal. Where prior work casts trust and control as substitutes or complements (Edelenbos & Eshuis, 2012; Gallivan & Depledge, 2003), P1 highlights that technology-enabled control can partially substitute for trust between parties while simultaneously elevating trust in the technical infrastructure on which that control now depends (Söllner et al., 2016). Trust is not dispensed with; its object moves – from the counterpart toward the technology, its governance, and the actors operating it. This shift is also a redistribution of dependency: actors must now trust that governance is legitimate, that infrastructure operators behave appropriately, and that technical controls are correctly implemented and enforceable.

The practical payoff of this trust shift is scalability. As long as confidence must be vested in each counterpart individually, data sharing has to be negotiated bilaterally and case by case, which hardly scales to the number of actors a decentralized energy system comprises. Relocating part of that trust onto a shared infrastructure is what allows coordination to extend beyond bilateral relationships. This relocation makes the infrastructure itself the load-bearing element: because trust has moved onto it, the infrastructure must now *earn* that trust beyond merely connecting participants. A trustworthy energy-data-sharing infrastructure is consequently a response to an organizational risk-and-control problem and it must deliver credible, auditable, and enforceable control by design – the design task taken up in Section 3.2.

Relocating trust onto infrastructure presupposes, however, that what is shared is itself governable through formal control mechanisms. These mechanisms can enforce access and use only against data whose decision rights, responsibilities, and verification status are well defined (Chua et al., 2022; Khatri & Brown, 2010). As a result, the trust shift turns the analysis from the bilateral sharing relationship to the shared object: even under trustworthy and controlled data sharing, value depends on what kind of data are shared, which attributes they carry, and whether those attributes can be interpreted and verified to ultimately generate value by the parties relying on them. P1 grounds the interorganizational mechanism developed here in an analysis of the literature and of five real-world initiatives, including the project on decentralized flexibility provision "DEER" (Ehaus et al., 2026); it specifies the mechanism that Chapter 3 subsequently instantiates and designs for the energy domain. Section 2.2 turns to the data object and asks why verifiable energy- and sustainability-related data become valuable only when their attributes are interpretable, credible, and fit for a specific purpose.

2.2 The Value of Verifiable Digital Energy Data and Attributes

Section 2.1 established that technology-enabled data sovereignty can enable interorganizational data sharing by relocating trust from the intersection between individual organizations onto the data sharing infrastructure. This data sharing itself is necessary for value creation but not sufficient for it. Once data can be shared under trustworthy and verifiable conditions, their value depends on properties of the data themselves: a shared datum creates value only when it is interpretable, governable, comparable, credible, and fit for the purpose it is meant to serve (Ixmeier et al., 2024; Wang et al., 2025). This section shifts the level of analysis from the sharing relationship to the data object and its use, and asks under which conditions verifiable energy- and sustainability-related data become value-relevant.

Environmental, social, and governance (ESG) data are heterogeneous, fragmented, voluminous, and context-dependent, and they remain ambiguously defined and inconsistently operationalized across organizational settings (Krasikov & Legner, 2023; Wang et al., 2025). Energy-related data, on which decentralized energy systems increasingly rely, face the same challenges. The same numerical value – a product carbon footprint, an emission factor, a quantity of energy, a certificate – can carry different meaning depending on its context, data management scheme, and intended use. Their conceptual ambiguity, not merely their technical integration, is what obstructs cross-boundary usability and value creation.

P2 addresses this ambiguity by bringing conceptual clarity to ESG data through what it presents as the first systematic taxonomy of ESG data (cf. Figure 2.2 (Zwede, Valett, et al., 2026). Developed and evaluated over four iterations against 180 ESG data objects from academic, regulatory, and practitioner sources, the taxonomy organizes ESG data along three meta-dimensions – *context*, *data management*, and *data usage* – comprising 17 dimensions and 63 characteristics (Kundisch et al., 2021; Nickerson et al., 2013). Context specifies what the data describe and under which boundary conditions; data management specifies how they are structured, processed, and validated; and

data usage links them to functional purpose, disclosure standards, and internal and external stakeholders. Within this structure, *verification* denotes a characteristic of a datum describing whether and how it has acquired a checked status within a management process, and is therefore a property of the data. It comprises a central data-management characteristic, ranging from no verification – where a datum is accepted as asserted – through manual and semi-automated to automated validation.

MD	Dimension	Characteristic						E/N
Context	Data Classification	Environmental		Social		Governance		E
	Data Source	Internal		External				N
	Data Type	Primary		Secondary				E
	Data Temporality	Persistent Data	Historical	Real-time	Forecasted			E
	Data Scope	Downstream		In-house		Upstream		N
	Data Aggregation	Company-level		Location-level		Product-level		E
	Sector	Energy & Utilities		Financial Services		Consumer Goods & Retail		N
		Manufacturing		Technology & Telecom		Transportation & Logistics		
Data Management	Data Structure	Unstructured		Structured				E
	Data Format	Qualitative		Quantitative				E
	Data Collection & Dissemination	Manual		Semi-automated		Automated		E
	Data Processing & Analytics	Manual		Semi-automated		Automated		E
	Data Verification	None	Manual	Semi-automated	Automated			E
Data Usage	Functional Purpose	Performance & Optimisation	Strategy & Development	Risk, Reporting & Compliance	Communication & Engagement			N
	Disclosure Standard	Internal use only	ESRS	GRI	CDP	SBTI	GDPR	N
	Judgement Rule	Binary Threshold		Score / Rating		Qualitative Audits		N
	Internal Groups	Top-level Management	Finance & Controlling	Procurement & Logistics	R&D & Production			N
		Legal & Compliance		Marketing & Sales		Human Resources		
	External Groups	Internal use only		Customers		Civil Society		N
		Rating Agencies & Capital Providers		Regulatory Authorities & Auditors		Suppliers		

Figure 2.2: The final taxonomy on ESG data, comprising three meta-dimensions (MD), 17 dimensions, and 63 characteristics, partly exclusive (E) and non-exclusive (N) (Zwede, Valett, et al., 2026).

The taxonomy's central finding is that the value of ESG data is governed not only by their literal content but significantly by their purpose. Across the 180 mapped objects, *functional purpose* emerged as the dominant structuring element: ESG data are usage-dependent constructs whose meaning and relevance are shaped predominantly by the organizational purpose for which they are mobilized rather than interpreted in isolation (Chua et al., 2022; Püchel et al., 2024; Seidel et al., 2013). P2 distinguishes four such purposes – performance and optimization, strategy and development, risk, reporting and compliance, and communication and engagement – and shows that the same data object takes on different characteristics and corresponding value potential depending on which purpose it serves. Value, in this account, is realized through situation-appropriate use, and verification comprises one characteristic that is crucial for a given purpose.

P2's taxonomy makes a further observation that the dissertation builds directly upon: across the mapped objects, verification is predominantly manual, and automated validation is rare (Zwede, Valett, et al., 2026). This finding is highly relevant, because manual verification does not scale at ecosystem level. A datum checked by hand inside one organization yields a status that an external party must take on trust; it does not let that party check the claim itself without disclosing

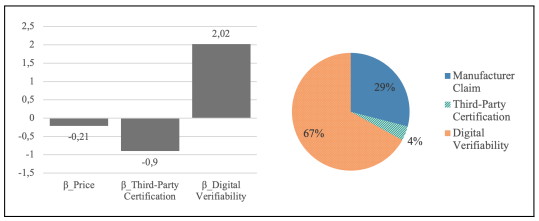
sensitive information. Converting verification into evidence that an outside actor can validate independently – and, at scale, automatically – requires the datum itself to be *verifiable*. This is the precise point at which P2's data-management characteristic meets the dissertation's broader construct: verification is a status reached inside a process, whereas verifiability is the property that a claim can be checked by a relying party who may not be able to inspect its source. The need for verifiability becomes acute exactly when a datum's functional purpose is external, lying beyond the scope of one organization, and digital verification mechanisms are what make independent, automated verifiability possible – the capability this dissertation later designs for the energy domain (Section 3.2).

The product carbon footprint is P2's own exemplar of such an external purpose. P2 classifies it under communication and engagement: an externally shared, product-level metric, aggregated across the lifecycle and along potentially complex value chains. Its value depends on outside stakeholders believing it, yet those stakeholders cannot verify it by inspecting the product (Zwede, Valett, et al., 2026). Such a claim demands verifiability and is the point at which P2's focus on the data-object meets the demand side.

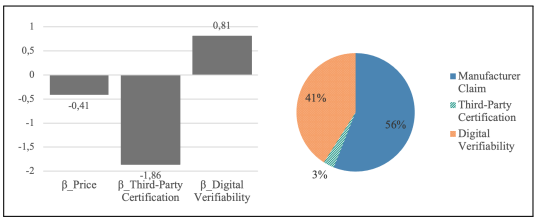
P3 takes up precisely this externally directed claim and asks whether digital verifiability turns it into decision-relevant value. It frames product-level carbon information as a *credence attribute* – a property consumers cannot verify by inspection or consumption – which creates an information asymmetry between producers who hold the data and consumers who must rely on its disclosure (Atkinson & Rosenthal, 2014; Darby & Karni, 1973; Perrini et al., 2010; Spence, 1973). Under such asymmetry, credibility must be conveyed by a signal. P3 compares three signals that differ in how they establish credibility – an unverified manufacturer claim, third-party certification resting on institutional reputation, and digitally verifiable carbon information that builds credibility through cryptographic, privacy-preserving proofs (Babel et al., 2022; Beck et al., 2018; Heiss et al., 2023; Treiblmaier & Garaus, 2023). Digital verifiability thus represents a categorically different basis for belief: assurance grounded in the reliability of a verification mechanism in place of the standing of a certifying body.

In a Best-Worst Scaling experiment with 122 participants, analyzed through multinomial logit models estimated separately for a high-involvement product (headphones) and a low-involvement product (T-shirts), digital verifiability is the most valued signal in both cases (Figure 2.3) (Geist et al., 2026). For headphones, digital verification raises systematic utility strongly relative to the manufacturer-claim reference ($\beta = +2.02$), whereas third-party certification actually *lowers* perceived value ($\beta = -0.90$); the corresponding predicted choice probabilities are 67% for digital verification, 29% for the manufacturer claim, and 4% for third-party certification, and the advantage of digital over third-party verification is statistically significant ($p = 0.025$). The striking result is the ordering: not only does digital verifiability outperform third-party certification, but third-party certification scores below a bare, unverified manufacturer claim. Once price is controlled for, digital verifiability emerges as the dominant determinant of perceived utility.

Digital verifiability's decision-relevance is moderated by product involvement and price sensitivity: for T-shirts the positive utility contribution persists but attenuates ($\beta = +0.81$), third-party



(a) Estimated β-coefficients (left) and predicted choice probabilities (right) for the headphone model (Geist et al., 2026).



(b) Estimated β-coefficients (left) and predicted choice probabilities (right) for the T-shirt model (Geist et al., 2026).

Figure 2.3: Estimated utility coefficients and predicted choice probabilities for the headphone and T-shirt models (Geist et al., 2026).

certification is penalized more sharply ($\beta = -1.86$), and the price coefficient is more strongly negative ($\beta = -0.405$) with the difference still significant at $p = 0.042$ (Geist et al., 2026). This means verifiability as a signal is perceived as most valuable precisely where involvement and prices are highest and where choice is most reliant on information quality, but remains a value-adding factor in low-involvement, low-value settings (Evans & Stanovich, 2013; Simon, 1955).

This preference order describes the demand-side instance of the trust shift developed in Section 2.1. Consumers favor digital verification because they anchor their judgment in the perceived reliability and credibility of the underlying system instead of the reputation of an institutional certifier (Pavlou & Gefen, 2004; Samuel et al., 2022; Treiblmaier & Garaus, 2023; Völter et al., 2023). Trust again moves from the third-party – the certifier – toward the verification technology – the same relocation P1 identifies between organizations, now reproduced at the level of an individual decision. That two independent evidence bases, organizational and consumer-facing, exhibit the same effect is the first convergence the chapter's synthesis builds on.

Taken together, P2 and P3 specify the data-object side of the dissertation's value argument as one claim seen at two altitudes. P2 demonstrates, at the level of organizational data management, that ESG data create value through purpose-fit, and that verification is one central characteristic a usage pattern may require. P3 takes one such purpose – the externally communicated product carbon footprint, P2's own exemplar – and highlights that when its credibility is supplied by digital verifiability, the attribute becomes decision-relevant and can outweigh institutional certification at the point of choice. The implication for trustworthy energy-data infrastructure is direct: it must preserve and communicate the value-bearing attributes of energy data that allow a relying party to interpret, believe and ultimately use them in a valuable manner. The mechanisms that make such attributes independently checkable without disclosing the underlying data are the subject of Section 3.2; P3 establishes their decision-relevance through stated preferences in controlled choice tasks, a foundation that Chapter 3 operationalizes for the energy domain.

Even where data are governable, purpose-fit, and verifiable, however, their value is mediated by the applications through which they are issued, presented, and checked. A verifiable attribute that users cannot understand or are unwilling to engage with realizes no value at the point of use. Here, Section 2.3 turns from the value of verifiable data attributes to the acceptance of the applications that operationalize them.

2.3 User Acceptance of Verifiable Digital Data Sharing Solutions

Sections 2.1 and 2.2 established that verifiable mechanisms could strengthen data sharing between organizations when it is designed in a way that preserves the decision relevance of the shared data object. Both conditions, however, are realized through applications that must be operated and used: a verifiable attribute is issued, stored, presented, and checked through software, and if the people expected to use that software do not actually use it, the verifiability remains technically intact but practically irrelevant (Benbasat & Barki, 2007; Rieger et al., 2022). This section adds the third and final condition of the chapter's value argument. It asks under which conditions users accept the applications that operationalize verifiable data sharing, and highlights that technology acceptance is not a downstream usability concern but a constitutive requirement for value to materialize.

The relevant users in this paper are individuals who interact with verifiable data sharing technology in the form of self-sovereign identity (SSI) applications – receiving, holding, selectively presenting, and reviewing verifiable credentials. SSI applications are a holder-mediated form of verifiable data sharing, in which data are exchanged through a cryptographically verifiable credential that the user controls. P4 examines these users through a qualitative interview study built around an SSI demonstrator in which an income-tax certificate is issued as a verifiable credential, held in a wallet, and selectively presented to a verifier (Guggenberger et al., 2023). Hence P4 supplies the user-facing acceptance conditions that any SSI-like verifiable data-sharing application must satisfy, conditions that the corresponding mechanisms of Chapter 3 aim to meet.

From thirteen interviews, analyzed against the more generally applicable Technology Acceptance Model 2 (TAM2) as a baseline, P4 derives the SSI Acceptance Model: fourteen acceptance-relevant categories grouped into framework conditions, software characteristics, and user characteristics (Figure 2.4) (Davis, 1985; Guggenberger et al., 2023; Venkatesh & Davis, 2000; Vogelsang et al., 2013). Two of its results matter most for the chapter's argument. The first is structural. Three constructs act as *direct* determinants of the intention to use an SSI application – perceived usefulness, perceived ease of use, and trust – while the remaining factors operate through them. Notably, the social-influence constructs that TAM2 treats as central – image, subjective norm, job relevance, and voluntariness – proved irrelevant for SSI acceptance and drop out of the model entirely. Acceptance of verifiable data-sharing applications is therefore driven not by social conformity but by perceived usefulness, ease of use, and ultimately trust in the technology.

The second result is the construct that does the most work for verifiable data sharing specifically: comprehensibility. Absent from TAM2 and induced from the interviews, comprehensibility denotes users' ability to understand the process steps and benefits of an application before, during, and after use, and it feeds all three direct determinants—perceived usefulness, perceived ease of use, and trust (Guggenberger et al., 2023). Its prominence follows from what SSI applications ask of users. Verifiability adds procedural steps – credentials must be created, received, stored, selected, presented, and verified – and rests on cryptographic constructs that are opaque to most users. A credential may be technically verifiable while remaining meaningless to the person

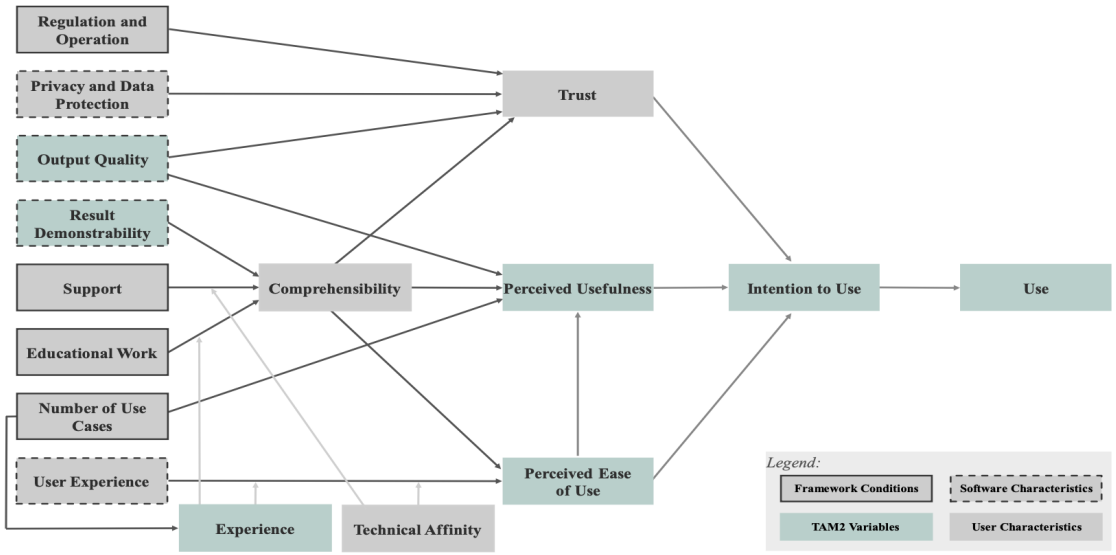


Figure 2.4: Self-Sovereign-Identity Acceptance Model (Guggenberger et al., 2023).

presenting it if they cannot see or make sense of what is shared, with whom, and to what end. P4 demonstrates that comprehensibility is built through concrete, designable means: educational work that conveys the application's purpose and mechanics before use, support that guides users through the steps during use, and result demonstrability that lets users review afterward which data they disclosed (Guggenberger et al., 2023). This is the user-level form of the dissertation's recurring requirement that verifiability be made intelligible beyond mere implementation.

Trust again occupies a central place, but its object distinguishes this level from the organizational one. In P4, trust is extended into the SSI software and the involved parties – the wallet provider, the credential issuer, and the verifier (Guggenberger et al., 2023; McKnight et al., 2011). The underlying logic is the same as in Section 2.1: a willingness to accept vulnerability under uncertainty, since users will not necessarily be able to validate the inner workings of the software and are thus vulnerable to its malfunction. What distinguishes this level is what builds that trust. P4 identifies four trust-building conditions, three of which are designable properties of the application and its rollout. Comprehensibility, already established above, raises trust by letting users understand what they do. Privacy and data protection raise it when users perceive that only necessary data are requested and that disclosure is minimized. To that end, selective disclosure – realized in SSI through zero-knowledge proofs – provides an appropriate lever, though P4 rightfully states that it underlies the privacy paradox, in which actual behavior may not align with stated concerns (Dimodugno et al., 2021; Kokolakis, 2017; Preukschat & Reed, 2021). Output quality raises acceptance when the software functions reliably and transmits data correctly. And regulation and operation additionally raise it through institutional anchors – trusted rollout actors such as government bodies, recognizable seals, preinstalled wallets (Guggenberger et al., 2023). A separate factor, the number of available use cases, drives intention to use through perceived usefulness: an application valued in only one isolated interaction is not perceived as useful enough to adopt (Guggenberger et al., 2023). It follows that even a technology premised on

decentralization and user control depends, for its acceptance, on trust that the application, its surrounding institutions, and operators must actively build.

Across the three levels the chapter traverses, the object of trust moves consistently toward the technology and the parties that operate it – from a counterpart organization (P1), to a verification mechanism (P3), to the software and its operators (P4). The user-level analysis shows that the infrastructure onto which trust has shifted must also earn that trust at the point of individual interaction.

P3 and P4 meet at the boundary between the data and the application, and together they map the demand side onto the two objects the design chapter must build. P3 demonstrates that digital verifiability raises the value of a claim at the moment of decision; P4 highlights that the application carrying such a claim is accepted only when it is comprehensible, useful, and trusted. Read together these two studies point in two mutually supporting directions: value is driven by the verifiability of the data, and acceptance is driven by the trustworthiness of the application that carries it. This yields the design brief the chapter hands forward – mechanisms must be designed to be verifiable, and the architecture that carries them must be designed to be trustworthy. Verifiability at the data level does not by itself produce acceptance at the application level; a verifiable attribute and a trustworthy, acceptable application are distinct achievements, and valuable data sharing requires both.

P4 grounds this brief in an SSI demonstrator and contributes transferable acceptance constructs and hypotheses rather than validated energy-sector adoption, a foundation the design chapter operationalizes for trustworthy and verifiable data sharing in decentralized energy systems.

2.4 Synthesis

This chapter integrated P1 through P4 into one coherent argument (cf. Figure 2.5): trustworthy and verifiable data sharing creates value in decentralized digital energy systems under three conditions, at the organizational level (P1), the data object (P2, P3), and the user (P4). Within this argument, the dissertation advances the notion that these conditions are cumulative instead of substitutable. An organization may share data no relying party can interpret; a datum may be verifiable yet carried by an application no one will use; an application may be accepted while the surrounding ecosystem lacks accountable governance. The claim of this chapter is that all three levels need to be satisfied collectively for value to materialize, with none single-handedly compensating for the absence of another.

Across all three levels, the chapter's central finding is the same: within a data-sharing instance, verifiability does not substitute for trust but relocates it. P1, P3, and P4 each show the object of trust moving from the parties one transacts with toward the technology that mediates the exchange and the actors who operate it – from a counterpart organization (P1), to a verification mechanism valued above institutional certification (P3), to the wallet software and the issuers and verifiers behind it (P4). Three independent evidence bases, at three levels of analysis, exhibit one

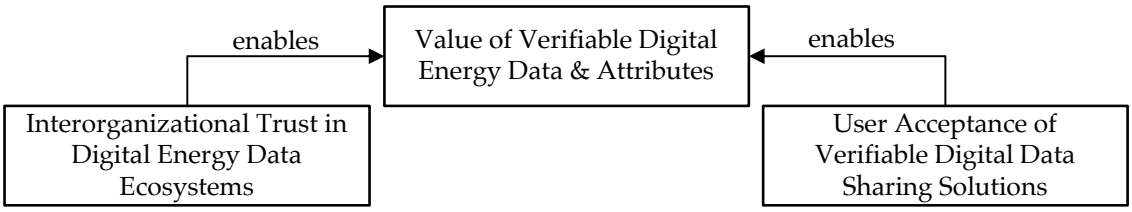


Figure 2.5: Specific Argument of Chapter 2 within the dissertation. Interorganizational trust and user acceptance enable value creation from verifiable data, serving as antecedents for the following chapters.

common movement – the *trust shift* that forms the empirical backbone of this chapter, and whose recurrence the design chapter will trace further.

This trust shift and its requirements set the agenda for the design chapter. Technology that mediates digital energy data sharing must be built to bear the trust that is now placed upon it: it requires verifiable mechanisms and trustworthy architecture. The three value drivers established here become the three design objects of Chapter 3: design principles for accountable cross-organizational data sharing (Section 3.1), a trustworthy infrastructure for verifiable digital energy data (Section 3.2), and mechanisms for verifiable digital energy data sharing (Section 3.3).

For Information Systems, the chapter contributes an account of trust that accommodates its relocation onto technology, holding that decentralized data ecosystems require trust-control arrangements going beyond access alone. For Green IS, it highlights that sustainability data create value not by disclosure but through purpose-fit and through credibility which can be supplied through digital verifiability where institutional reputation is insufficient. For Energy Informatics, it specifies why coordination in decentralized energy systems depends on infrastructures and mechanisms that make selected energy- and sustainability-related claims verifiable without assuming unrestricted transparency.

3 Designing Trustworthy and Verifiable Digital Energy Data Infrastructure

Chapter 2 closed with a design brief. Having highlighted that verifiability does not remove trust from data sharing but relocates it – from the parties one shares data with toward the technology that mediates the sharing and the actors who operate it – it handed forward a design objective: that technology must now be built to bear it. Mechanisms must be designed to be verifiable, and the architecture that carries them must be designed to be trustworthy. This chapter takes up that brief. After explaining *why* trust and verifiability create value in decentralized digital energy systems, I now focus on showing *how* trustworthy and verifiable data sharing can be designed under the privacy, confidentiality, and control constraints those systems impose.

The corresponding design challenge is socio-technical and layered. In decentralized digital energy systems, coordination depends on data that are generated and controlled by many different actors – manufacturers, device owners, aggregators, grid operators, certificate issuers, utilities, and other institutional stakeholders – each typically holding only the data its own processes produce. These data must become usable for system coordination and management, including flexibility provision, energy labeling and corresponding financial- and sustainability accounting, yet the same data can reveal commercially sensitive process information, device-level operational patterns, consumer behavior, or strategic intelligence. The challenge is hence not to maximize transparency, it is to design arrangements in which selected claims can become inspectable, attributable, and reliable to a relying party – i.e. verifiable – *without* forcing the actors who hold the data to disclose all of their detail or surrender control over it. This is the data-sharing dilemma of the introduction, now in its design form: how to make selected claims verifiable while the data behind them stay protected.

The chapter develops its response as *design knowledge for trustworthy and verifiable digital energy data sharing*. One distinction governs that knowledge throughout and is best stated at the outset. Verifiable data sharing does not mean that digital mechanisms establish the real-world truth of the underlying source data. It means that selected claims or attributes can be checked against defined properties – authenticity, integrity, provenance, inclusion, consistency, or authorization – while the assumptions concerning how the data were issued and measured remain explicit. The truth of the source is presupposed, not proven; what is designed is the verifiability of everything downstream of it. This distinction is most present at the infrastructure layer, where Section 3.2.7 develops it as the dissertation's oracle boundary, but it holds across the whole chapter.

On this basis the chapter proceeds across three complementary levels (cf. Figure 3.1), each answering a different design question and each developed primarily through one embedded paper, with P6 connecting them. Section 3.1 establishes the principle level (RO2): what characteristics

must a cross-organizational energy data-sharing arrangement satisfy before any infrastructure or mechanism can be built? It draws on P5's design principles for emission-data sharing in battery value chains and on P6's principles abstracted from a built green-electricity labeling system. Section 3.2 establishes the infrastructure level (RO3): how are the responsibilities for issuing, holding, delegating, aggregating, and verifying claims distributed across actors? It draws on P8's wallet-based architecture for flexibility provision and contrasts it with the architecture of P6. Section 3.3 establishes the mechanism level (RO4): how is a single claim rendered checkable without disclosing the data behind it? It draws on P7's shielded fractionalized Non-Fungible Token (NFT) approach for emissions tracing and P6's proof construction for green-electricity accounting. The three levels are cumulative and mutually conditioning – principles specify what an arrangement must support, infrastructure distributes the responsibilities that satisfy them, and mechanisms render the necessary claims checkable. Section 3.4 integrates them into the chapter's layered contribution.

The underlying papers' four settings – battery emission data, small-scale flexibility provision, green-electricity labeling, and emission-certificate tracing – partly differ in their objects of exchange, their actors, and their technologies. They are adjacent sustainability and energy data contexts, not a single use case, and the chapter does not treat any one of them as representative for the entirety and multitude of digital energy systems. What they share is the dissertation's central dilemma: decentralized actors require data-dependent coordination, while excessive transparency would undermine confidentiality, privacy, or control. The chapter develops design-oriented knowledge for one part of the research aim, and not a technology-driven argument for data spaces, wallets, blockchains, or zero-knowledge proofs as general solutions. Section 3.4 states that contribution and its bounds in full; Chapter 4 turns to the governance and policy conditions required to enable corresponding solutions to create value.

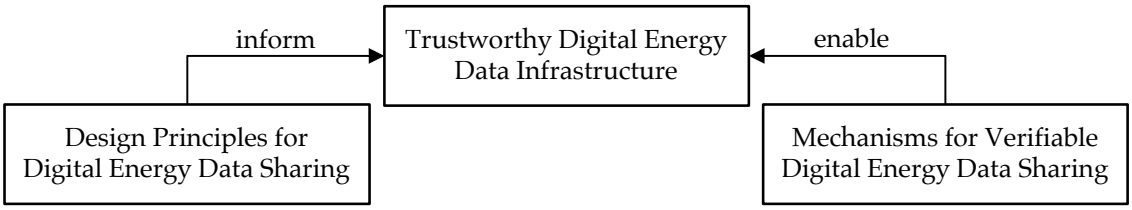


Figure 3.1: Specific Argument of Chapter 3 within the dissertation. Design principles for Digital Energy Data Sharing inform Trustworthy Digital Energy Data Infrastructure. That architecture itself is enabled by the specific Mechanisms for Verifiable Digital Energy Data Sharing.

3.1 Design Principles for Digital Energy Data Sharing

The chapter opening set out why the design response must begin with requirements: before an infrastructure can carry verifiable claims (Section 3.2) or mechanisms can render them checkable (Section 3.3), it must be clear what a cross-organizational data-sharing arrangement has to support in the first place. This section specifies that requirements layer. It does so from two complementary evidentiary bases: P5 derives design principles for cross-organizational data sharing from a

structured analysis of requirements, and P6 derives them from a system that was built and evaluated (Babel et al., 2026; Zwede, Mertel, et al., 2026). Read together, they specify what digital energy data sharing must support and demonstrate that the central tension between confidentiality and verifiability – declared earlier – can be reconciled through appropriate design.

3.1.1 Emission Data Sharing in Battery Value Chains

The empirical anchor of P5 is emission-data sharing in battery value chains. The battery value chain is not treated here as a stand-in for the energy system as a whole, nor as a product comparable to electricity. It is, rather, a particularly demanding instance of the same socio-technical sharing problem that recurs throughout digital data sharing instances: many distributed actors, divergent and partly conflicting incentives, sensitive primary data, and a need to make claims that cross organizational boundaries and remain credible to a relying party who cannot inspect their source. An arrangement that holds under this complexity travels well; if design principles can govern data sharing across a long, heterogeneous, and competitively sensitive battery value chain, the requirement structure they encode applies also where distributed energy actors must share sensitive yet verifiable data. Here, the generalization the section develops runs through the structure of the sharing problem, not through any resemblance between batteries and electricity.

What makes the case of the battery value chain demanding is the dependence of product-level carbon accounting on *primary* data. A product carbon footprint (PCF) quantifies the emissions attributable to a product across its life cycle, yet for complex and long-lived goods such as lithium-ion batteries the relevant emission data are seldom held in one place; they are fragmented across upstream value-chain actors, each controlling only the data generated through its own processes (Bhatia et al., 2011; Gebhardt et al., 2022; Peiseler et al., 2022; Stampatori et al., 2020). Where primary data are unavailable, PCFs are currently computed from secondary sources – industry averages, estimates, and other arbitrary database values – which are generic, frequently outdated, and insensitive to the specific product, supplier, or production conditions – such as the share of renewable energy in the production of a specific batch, a major leverage for a battery's PCF (Jaeger et al., 2022; Lin et al., 2021; Patchell, 2018; Sica et al., 2022).

Such PCFs cannot distinguish the climate impact of two otherwise comparable batteries and as a result can't enable the carbon-management and procurement decisions they are meant to inform. On average, production of a battery electric vehicle (BEV) is moreover roughly twice as emission-intensive as that of a conventional vehicle, which concentrates a large part of a battery's lifetime climate impact in exactly the value-chain stages where primary data are hardest to obtain (Helms et al., 2019; Kim et al., 2016). Regulation compounds the pressure: the European Battery Regulation mandates a carbon-footprint declaration for every battery above two kilowatt-hours entering the market, while broader instruments such as the Corporate Sustainability Reporting Directive (CSRD) and Corporate Sustainability Due Diligence Directive (CSDDD) tighten cross-organizational sustainability disclosure obligations for all industries (European Commission, 2020c; Müller et al., 2023). Improving PCFs thus requires sharing primary emission data across firm boundaries without revealing unduly sensitive and competitively advantageous

information – and it is this requirement that activates the dissertation's central data sharing dilemma in concrete form.

3.1.2 The Concrete Data Sharing Dilemma in Battery Value Chains

Primary emission data are, in carbon-accounting terms, *activity data*: records of the energy consumed, materials used, and processes run to manufacture a component (Bhatia et al., 2011). These are the very data firms regard as trade secrets, since they can be reverse-engineered into insights about production processes, sourcing relationships, and operational efficiencies (Brucker & Yalman, 2022; Peiseler et al., 2022). The binding constraint in this setting is firm-level confidentiality in place of personal privacy. P5 treats privacy and confidentiality as a single key requirement and, from its company-centric perspective, lets confidentiality subsume but exceed the protection of personal data: it covers personal data where present, but extends to any commercially sensitive information a firm classifies as worthy of safeguarding (Kiemel et al., 2022; Stenzel & Waichman, 2023). This is consistent with the distinction drawn in Chapter 2, where *privacy* denoted the personal, data-protection-governed concern and *confidentiality* the firm-level, competitive one; in the battery value chain the latter dominates. The result is the dissertation's data-sharing dilemma in concrete form: more granular primary data improve the PCF and the decisions it supports, yet the same granularity threatens the competitive position of the firm disclosing it, so overall economically beneficial sharing is withheld on individual firms' confidentiality grounds.

Two terminological commitments frame the rest of the section. First, following the usage P5 adopts, *data sharing* is distinguished from *data exchange*: data exchange denotes the technical transfer of data between two parties, whereas data sharing is the broader, organizational concept encompassing actor constellations, access and usage policies, and the conditions under which transfer is permitted at all (Jussen et al., 2023). This dissertation is concerned with data sharing in that broader sense, and the design principles below are requirements on the sharing arrangement, not merely on the technical exchange channel. Second, the section adopts a deliberately bounded notion of a *data space* as a distributed arrangement in which data remain at their source and are shared only under defined conditions, rather than pooled in central storage (Otto, 2022; Pettenpohl et al., 2022). A data space in this sense is oriented toward a specific group of stakeholders and is not synonymous with a deployed infrastructure, a complete governance regime, or the broader *data ecosystem* of loosely coupled actors that jointly create value from data across multiple data spaces (Gelhaar et al., 2021; Schleimer et al., 2023). Its intermediate position between an unmet sharing need and an implementable infrastructure allows the development of actionable design principles.

3.1.3 Two Design Approaches Informing Digital Energy Data Sharing

P5 and P6 – the latter, introduced above, a system for green-electricity labeling that was built and evaluated – approach this requirements layer from opposite methodological directions, reaching a complementary contribution. P5 conducts a structured literature review of 47 publications,

extracts 30 meta-requirements, synthesizes them into six key requirements, and formulates six design principles (cf. Figure 3.2) that it refines and confirms across three build–evaluate cycles with fourteen semi-structured expert interviews, following a formative, purely technical evaluation strategy (Babel et al., 2026; Gregor et al., 2020; Möller et al., 2020; Venable et al., 2014). Because data-space implementations remain scarce and in an early stage of development, P5 deliberately contributes *nascent*, artificial design theory – prescriptive Ω-knowledge that abstracts from any single situated artifact – and not evidence from a deployed system (Gregor & Hevner, 2013; Peffers et al., 2007). P6, this section's supplementary, build-grounded contribution, proceeds in the other direction: it builds a working prototype for green-electricity labeling, evaluates it through performance tests and ten expert interviews, and only then abstracts four nascent design principles from the artifact (Hevner et al., 2004; Zwede, Mertel, et al., 2026). The two bracket the requirements layer from the literature side and from the build side, and where their principles converge that convergence is evidentially stronger for resting on both.

The bridge from P5 to digital energy data sharing more broadly is structural. P5's principles are derived on emission data, but the structure that generates them – distributed actors, divergent incentives, sensitive primary data, and a need for verifiable cross-boundary claims – is the generic structure of digital energy data sharing. Emission data are one energy-relevant data class among several, alongside generation, consumption, flexibility, and certificate data, and they are among the most complex, all-encompassing, and, as a result, confidentiality-sensitive of these. This section reads P5's six principles as requirements for digital energy data sharing for which emission data are the worked instance, and reads P6 as a second, concrete energy-domain instance – green-electricity labeling – that shares the same sharing structure while carrying a different and equally sensitive data class, smart-meter generation and consumption data. P5 itself locates its contribution at the intersection of Green IS, Energy Informatics, and digital decarbonization and claims generalizability beyond the battery case to complex, long-lived goods (Babel et al., 2026; Goebel et al., 2014); this dissertation extends that claim along the dimension that actually carries it, the data sharing dilemma stretching beyond any single product. The six principles are developed below in three pairs – data usability, the confidentiality–traceability tension, and ecosystem viability – and Table 3.2 summarizes each principle, the problem it addresses, and its role in the dissertation argument. Table 3.1 contrasts the two contributions along their evidentiary basis, data class, scope, and output.

Table 3.1: Contrasting the two requirements-layer contributions of Section 3.1.

	P5 (Babel et al., 2026)	**P6** (Zwede, Mertel, et al., 2026)
Evidentiary basis	Requirements-grounded: SLR (47 sources), 30 meta-requirements, 6 key requirements, 3 build–evaluate cycles, 14 expert interviews	Artifact-grounded: built prototype, performance tests, 10 expert interviews
Data class	Primary emission / PCF data	Smart-meter generation and consumption data
Scope of output	6 nascent design principles developed through artificial design theory	4 nascent design principles abstracted from a working artifact
Maturity claim	No situated artifact; use-case-specific	Proof-of-concept; not broadly deployed

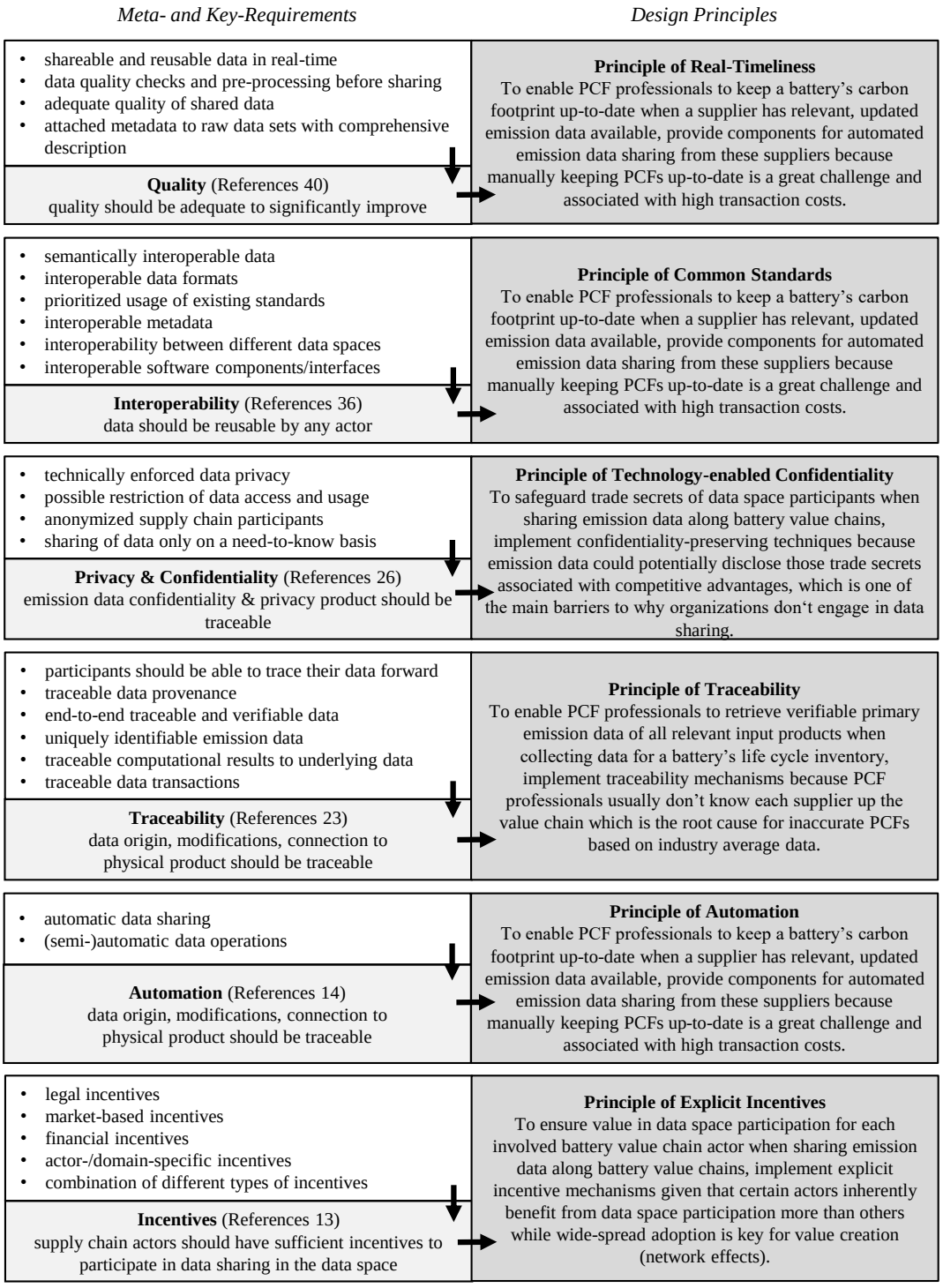


Figure 3.2: Mapping of the 30 meta-requirements to six key requirements and six design principles for emission-data-sharing data spaces (Babel et al., 2026).

3.1.4 Data Usability Across Actors and Time

The first pair of principles concerns whether shared data are usable at all – current enough to be decision-relevant, and interoperable enough to be interpreted across actors. *Real Timeliness*

addresses temporal representativeness. Emission data are not static: within a single battery model, the carbon footprint of an individual unit depends largely on dynamic inputs, foremost the electricity mix drawn during production (Babel et al., 2026). A PCF computed from static annual averages cannot reflect this variation, so the principle calls for sharing dynamic emission data with sufficient timeliness that PCF professionals can represent unit- and time-specific differences – approaching, in the limit, the "live carbon footprints" that are computed in step with production (De Soete, 2016). The electricity-mix dependency is worth dwelling on, because it already ties emission data to energy-system data: the attribute that makes a battery's footprint dynamic is itself a property of the electricity system, an instance of the same dependence on highly granular energy-system data that is directly addressed for green-electricity labeling in P6.

Common Standards addresses interoperability – across data formats, syntax, and semantics, and across the heterogeneous systems, jurisdictions, and PCF methodologies that value-chain actors employ (Babel et al., 2026; Jaeger et al., 2022). The requirement should not be understood in a mere technical sense. The same term can denote different things to different actors – "battery" may mean a cell to one firm, a pack to another, and a module to a third, or carry an unrelated meaning entirely – so machines need explicit, shared, and unambiguous descriptors to interpret shared data correctly, which standards and common ontologies supply (Clark et al., 2022). This makes interoperability a precondition for verifiability, not only a separate concern. A claim can be independently checked only if it is specified, structured, and interpretable in the first place; the verification mechanisms developed later in this chapter operate on claims and attributes, and an attribute that cannot be unambiguously interpreted cannot be meaningfully verified. Real Timeliness and Common Standards together determine whether shared energy data are decision-relevant and checkable before any question of trust or proof arises.

3.1.5 The Confidentiality–Traceability Tension

The second pair of principles captures this section's trust-and-control tension, and their interaction is the central design-level implication P5 contributes to the dissertation. *Technology-enabled Confidentiality* responds to the concern, established above, that primary emission data can be reverse-engineered into trade secrets. Instead of resolving this organizationally – by simply declining to share – the principle calls for confidentiality to be built into the sharing arrangement through technical means, drawing on a repertoire of confidentiality- and privacy-preserving techniques including homomorphic encryption, differential privacy, secure multi-party computation, k-anonymity, zero-knowledge proofs, and usage control (Babel et al., 2022, 2026; Brucker & Yalman, 2022). *Traceability* addresses the complementary requirement to follow emission data along the value chain: to trace provenance back to its source, to maintain a continuous chain of custody that allows allocations to be verified and double-counting prevented, to trace computational results back to the data and methods that produced them, and to trace data forward so that providers can see how their data were used (Babel et al., 2026; Patchell, 2018). Traceability serves two concrete purposes in carbon accounting – identifying which upstream actors to engage for primary data, and locating the emission hot spots that reduction efforts are most efficiently directed at.

As established in Chapter 2, traceability must not be conflated with verifiability. Traceability concerns lineage and provenance – the ability to follow data and computational relations through the chain. Verifiability concerns whether a relying party can independently check a claim against defined properties such as authenticity, integrity, provenance, or authorization. Traceability can support verifiability, but it does not by itself establish that the traced data are true; a complete and faithful lineage of an incorrect figure remains incorrect.

The tension between the two principles is direct. Traceability is what makes emission data useful – it enables emission-based decisions and supports verification – yet the more traceable the data, the more they expose. Firms hesitate to share traceability-relevant data precisely because doing so risks reputational damage where climate performance is poor and uniquely attributable, permits reverse-engineering of production and sourcing processes, and reveals the existence and identity of business relationships that are themselves competitively sensitive (Babel et al., 2026; Brucker & Yalman, 2022; Peiseler et al., 2022). Confidentiality and traceability work against each other: each increment of traceability that makes the data more valuable for carbon management is an increment of disclosure that makes them less safe to share.

P5's experts and several industry initiatives converge on a partial resolution: *upstream aggregation* accounting, often described as the "one-up-one-down" principle, as pursued by bodies such as the Global Battery Alliance, Catena-X, and the Partnership for Carbon Transparency (Babel et al., 2026; Kaplan & Ramanna, 2021; Piétron et al., 2023). Under this scheme each actor accounts only for its own scope 1 and 2 emissions and adds them to the aggregated PCFs of the input materials it receives from its immediate suppliers, exchanging information only with its direct upstream and downstream partners. This lowers transaction costs, raises the share of primary data in the overall PCF, and eases the double-counting problems that arise when responsibility for shared emissions is contested, all while letting each actor keep its supplier relationships and granular activity data confidential (Babel et al., 2026; Bhatia et al., 2011).

The cost of this resolution is often framed as pure loss, but within this dissertation it has a more pronounced role. Aggregation does forgo a global, supplier-level map of emission hot spots, and it collapses provenance verifiability and peer-to-peer verification of underlying primary data beyond the immediate tier-1 relationship (Babel et al., 2026). Yet the same scheme preserves a meaningful and arguably better-aligned form of decision-relevance. An actor that receives aggregated PCFs from its tier-1 suppliers can still compare them and select the lower-carbon supplier, and the prospect of being selected gives each tier-1 supplier its own incentive to reduce the footprint it declares – which it can only do by engaging its *own* upstream in turn. The decarbonization incentive is hence distributed recursively along the chain rather than concentrated in a single actor holding a global map. This approach might be slower than centralized hot-spot optimization and it does relinquish a chain-wide overview, but it keeps supplier relationships and activity data confidential, and in doing so it protects the competitive advantage and fair-competition conditions that make actors willing to participate at all. On this reading, confidentiality is not merely a constraint the design must tolerate; it is part of what enables broad participation – and as a result the data sharing itself. This parallels the acceptance logic developed in P4 in Chapter 2, where

privacy and data-protection concerns shape trust and, through it, the intention to use a verifiable data-sharing solution: there the concern is personal privacy at the level of the individual user and the application, here it is firm-level confidentiality at the level of the sharing arrangement, but in both cases data protection is a precondition for participation.

Table 3.2: The six design principles for emission-data-sharing data spaces (Babel et al., 2026), the design problem each addresses, and its role in the dissertation argument.

Design principle	Design problem addressed	Role in the dissertation argument
Real Timeliness	Temporal representativeness of dynamic emission data	Ties data quality to decision-relevant PCF assessment and to energy-system data
Common Standards	Interoperability across heterogeneous actors and systems	Establishes interoperability as a precondition for verifiability
Technology-enabled Confidentiality	Reverse-engineering of sensitive process and sourcing data	Connects the sharing dilemma to a concrete, technical design requirement
Traceability	Provenance, chain of custody, and computational lineage	Highlights why inspectability matters, while remaining distinct from verifiability
Automation	Cost and infeasibility of manual PCF upkeep	Shows that sharing arrangements must support continuous updating
Explicit Incentivization	Uneven actor benefit and participation barriers	Connects technical sharing to ecosystem participation

3.1.6 Operational and Ecosystem Viability

The third pair of principles turns from the properties of the data to whether a sharing arrangement can be sustained and populated over time. *Automation* addresses the effort of keeping PCFs current. Data collection is already the most labor-intensive part of PCF assessment, and stricter requirements multiply it: the Battery Regulation effectively demands a fresh assessment whenever the energy mix changes, which renders manual upkeep infeasible for any sizeable product portfolio (Babel et al., 2026; De Soete, 2016; European Commission, 2020a). The principle therefore calls for components that share updated emission data automatically as conditions change, inverting the conventional pull model so that data sources push updates to the PCFs that depend on them, for instance through publish–subscribe patterns (Babel et al., 2026). Automation does not stand alone here: it presupposes the interoperability that Common Standards establishes, since data can be ingested and recomputed automatically only where formats, interfaces, and semantics are shared. The two principles compound – interoperability is what makes the timeliness sought by Real Timeliness achievable in practice and the recursive, near-continuous updating that one-up-one-down accounting would otherwise make prohibitively costly becomes tractable once sharing is automated over interoperable interfaces.

Explicit Incentivization addresses participation. A data space exhibits public-good and two-sided-market characteristics: early adopters bear the cost of bootstrapping a sharing ecosystem while its benefits remain low until enough others join, which invites free-riding and can stall adoption before network effects take hold (Babel et al., 2026; Gelhaar et al., 2023). Because the benefits and costs of sharing are distributed unevenly across value-chain actors, explicit incentive mechanisms are needed so that each actor can recognize value in participating. P5's experts agree that regulation

is the most powerful lever for inducing data sharing, but they also note that regulatory and market pressures sit *upstream* of the data space and cannot be engineered by its designer (Babel et al., 2026). On the design-controllable incentives the evidence is genuinely unsettled: the data-market concept promoted by initiatives such as the International Data Spaces Association (IDSA) and Gaia-X is regarded by some of P5's experts as lacking a real-world business case for emission data specifically, even as others observe firms already paying premiums for sustainability information. The section reports this as an open question, since the viability of paid emission-data markets is not something the present evidence can settle.

3.1.7 From Requirements to a Built Energy-Domain Instance

Taken together, P5's six principles specify what a cross-organizational emission-data-sharing arrangement must support – data that are timely (Real Timeliness) and interoperable (Common Standards), protected yet inspectable (Technology-enabled Confidentiality and Traceability), and maintainable and attractive to join (Automation and Explicit Incentivization) – and, along the structural argument of Section 3.1.3, this dissertation reads them as requirements for digital energy data sharing more broadly. They also localize the dissertation's central tension at a specific point: confidentiality and verifiability collide, and the field's habitual resolution – aggregation backed by institutional verification – reconciles them only partially. What P5 establishes by analysis, P6 establishes by construction, in a second, independent instance of a comparable data sharing structure – one that carries genuine energy-system data, smart-meter generation and consumption data, in place of emission data.

Green-electricity labeling is a setting to which P5's requirements also apply: it exhibits the same fundamental data sharing structure while carrying a different and equally sensitive data class. It involves many distributed generators and consumers; it depends on smart-meter data that are highly sensitive because they reveal economic and behavioral patterns and are correspondingly regulated as personal data under data-protection law such as the European General Data Protection Regulation (European Commission, 2023); and it turns on a verifiable provenance claim – that a given quantity of consumed electricity was matched by renewable generation (Zwede, Mertel, et al., 2026). Guarantees of Origin (GOs) certify exactly this, but conventional systems are opaque, coarse in their temporal resolution – often only providing yearly aggregates – and offer end users no means to check the underlying accounting independently. In particular, conventional GO schemes are prone to perceived double-spending of green electricity through the sale of certificates across country borders while accounting for them only on a yearly basis, which is the concrete mechanism behind the greenwashing that a verifiable labeling system must foreclose. P6 builds a system to close that gap and abstracts four nascent design principles from it – principles that, in its own framing, address the general class of information systems in which stakeholders must verify claims about sensitive data without disclosing the data themselves (Zwede, Mertel, et al., 2026). The four fall into two pairs.

The first pair concerns how to engineer a verifiable system efficiently. *DP1* holds that proof systems should be designed around actor-specific incentives and attack surfaces: Instead of encoding all

available data into one comprehensive proof, designers should first identify which actors have both the incentive and the ability to manipulate which data, and verify only what is needed to rule out those specific fraud vectors (Zwede, Mertel, et al., 2026). *DP2* holds that cryptographic primitives should be selected based on their end-to-end performance in the target architecture, since a primitive that is efficient in one component can become the bottleneck once its interaction with the rest of the system is considered. In P6, for instance, a proof system that was efficient at proving the aggregate energy balance performed poorly once it also had to prove the signatures that establish the data's provenance, so a primitive that is locally optimal for one sub-proof need not be optimal for the system as a whole – which makes primitive selection an architectural rather than a component-level decision (Zwede, Mertel, et al., 2026). Both principles treat verifiability as something to be engineered against real incentives and real performance budgets, not assumed.

The second pair concerns how to structure verifiability so that it coexists with confidentiality, and these are the principles that most directly answer the tension P5 localized. *DP3* holds that blockchains should be used as immutable verification layers instead of computational data-processing infrastructures: sensitive and high-volume data should be processed off-chain, while only compact commitments and verification results are published on-chain (Zwede, Mertel, et al., 2026). This enables selective transparency despite global verifiability – a relying party can confirm that the agreed accounting rules were followed without the underlying operational data ever being exposed – and it reconciles openness and verifiability with confidentiality and scalability.

The scalability gain is a central benefit of the system design: on-chain computation is costly in compute and, on public ledgers, in direct monetary terms, leading to poor scalability. So moving the heavy processing off-chain and publishing only compact commitments keeps computation efficient and scalable even as the underlying data volume grows. *DP4* holds that local inclusion proofs should be combined with global consistency proofs: each stakeholder can verify that its own data were correctly included in an aggregate, while the aggregate as a whole is proven to satisfy the required global constraints, with the blockchain providing a shared, immutable reference point for the Merkle roots that anchors each stakeholder's proof verification to a consistent shared layer. This layered structure lets many actors obtain assurance about a collective outcome while each accesses only its own slice of the underlying data – precisely the assurance that upstream aggregation forfeited beyond tier-1, here re-established through a cryptographic mechanism. P6's experts confirmed the objectives these principles serve: verifiability as the means to rule out the double-spending of green electricity and the "greenwashing" it enables, zero-knowledge proofs as the means to preserve privacy while retaining that verifiability, alongside architectural decisions that enable openness and scalability (Zwede, Mertel, et al., 2026).

The two sets of principles stand in a clear relation. P5's principles say *what* such a sharing arrangement must support – requirements derived on emission data and abstracted here to digital energy data sharing – and establish that cryptographic verification can in principle reconcile confidentiality with verifiability. P6's principles say *how* to engineer and structure a system that does so, and demonstrate their capabilities in a built energy-domain artifact. The requirements layer and its first build-grounded refinement thus meet on the same claim approached from

two directions: confidentiality and verifiability need not be traded off, provided the sharing arrangement is designed to separate what must be proven from what must be disclosed.

3.1.8 Design Principles for Digital Energy Data Sharing – Synthesis

This section has developed the requirements layer of the dissertation's design response and generalized it from emission data to digital energy data sharing. P5 establishes, by structured analysis, which properties a cross-organizational data-sharing arrangement must exhibit and diagnoses where its central tension lies: confidentiality and traceability pull against each other, and the field's institutional fix – aggregation backed by third-party verification – reconciles them only partially and rests on a form of assurance that P5's own analysis finds opaque and inconsistent. P6 confirms and extends this from a built artifact in a specific energy systems setting, demonstrating that the confidentiality–verifiability tension can be reconciled by design and that verification can be relocated from an institution onto a technical mechanism.

This relocation is the trust shift of Chapter 2 reappearing at the verification function. Where the field would have a relying party trust an auditor – a party – to attest that an accounting is correct, the cryptographic alternative has it trust a verification mechanism instead, anchoring credibility in the integrity of a proof system as opposed to the standing of an institution (Babel et al., 2026; Boiral & Heras-Saizarbitoria, 2020; Perego & Kolk, 2012). This is the supply-side counterpart to the demand-side result of P3: where Chapter 2 highlighted consumers valuing digitally verifiable carbon information above third-party certification, the present section shows the same movement among the firms that must produce such information, with zero-knowledge proofs and related techniques offering verifiable evidence under minimal disclosure (Babel et al., 2022; Geist et al., 2026; Goldwasser et al., 1989; Hellani et al., 2021; Principato et al., 2023). That the same relocation appears on both sides of the market strengthens the dissertation's claim that it is a structural feature of verifiable data sharing instances and not just an isolated artifact of any explicit setting.

The contribution of this section is bounded in two respects that should be stated plainly. P5 contributes nascent, artificial design theory: it is evaluated by experts but not through a situated deployment, and it offers no evidence of end-user acceptance. Its principles were derived on emission data; this dissertation generalizes them to digital energy data sharing along the data sharing dilemma beyond any single product (Section 3.1.3), but that broader reach is argued and remains to be empirically substantiated across further energy data classes (Babel et al., 2026). P6 contributes a proof-of-concept: it is built and evaluated but not deployed, and it leaves open the integrity of its data feed-in, the trusted-setup requirement of its proof system, and the governance needed to prevent double-generation across separate implementations (Zwede, Mertel, et al., 2026). These boundaries mark the work that the following sections and chapters take up.

What the requirements layer cannot do is specify how the responsibilities it implies should be distributed across concrete actors. P5 and P6 establish what must be supported and that cryptographic verification can reconcile the central tension, but not who issues a claim, who holds and delegates it, who aggregates and presents it, and who ultimately verifies it – nor how these

roles are organized when no single actor can or should see all the underlying data. Answering that requires moving from principles to an infrastructure design that can carry them. This is why the design response further sets out to present a *trustworthy architecture* in which these roles and verification responsibilities are organized so that the relocated trust has something to rest on, and *mechanisms for verifiable data sharing* that make the individual claims checkable under disclosure constraints. Section 3.2 develops the first of these, turning from what a sharing arrangement must support to how its actor roles and verification responsibilities can be structured.

3.2 Trustworthy Digital Energy Data Infrastructure

Section 3.1 established what a cross-organizational data-sharing arrangement must support, and demonstrated that cryptographic verification can in principle reconcile confidentiality with verifiability instead of trading one against the other. What the requirements layer could not specify is how the responsibilities it implies are distributed across concrete actors: who issues a claim, who holds and delegates it, who aggregates and presents it, and who ultimately verifies it, when no single actor can or should see all the underlying data. This section answers that question. It develops the infrastructure layer of the dissertation's design response, asking who verifies what, through which configuration of roles, and under which privacy and control constraints.

Trustworthy infrastructure is understood here in the narrow sense that it denotes the socio-technical arrangement of actors, credentials, delegated rights, aggregated claims, and verification responsibilities that lets actors rely on selected claims about assets and services without centralized disclosure of the data behind those claims. The concern here is not every communication or market-clearing component of a decentralized energy system, but specifically the arrangement that makes claims about assets, delegated rights, and aggregated services verifiable across organizational boundaries. The section develops this layer primarily through P8, which designs and implements such an infrastructure for the use case of small-scale flexibility provision, and contrasts it with the architecture of P6 as a second, structurally different arrangement that addresses the same verification-distribution challenge for the labeling of green electricity (Zwede, Mertel, et al., 2026; Zwede et al., 2025).

3.2.1 The Infrastructure Challenge in Small-Scale Flexibility Provision

The decarbonization of heating, transport, and industry proceeds through electrification, which multiplies the number of small-scale flexibility devices (FDs) – heat pumps, electric vehicles, and battery storage systems – connected to the low-voltage grid, while the intermittency of renewable generation makes grid congestion both more frequent and more costly to manage (Fridgen et al., 2020; Hirth & Glismann, 2018; Lind et al., 2019; Priesmann et al., 2021). Coordinating the flexibility of these distributed devices is a promising and, because these devices are already connected to the grid, comparatively cheap lever for congestion management, but exploiting it requires processing large volumes of privacy-sensitive device data at short intervals, since grid operators (GOs) must

continuously balance supply and demand within the constraints of the network to keep the grid stable (Körner et al., 2022; Loschan et al., 2023).

The structural obstacle is an information asymmetry rooted in the metering boundary. The vast majority of small-scale devices sit *behind the meter* of a household or firm, and the meter constitutes the system boundary of the GO: the operator has no direct access to the primary data of the devices behind it (Körner et al., 2024). Agency theory helps to understand the dynamics behind this gap more precisely (Eisenhardt, 1989; Meckling & Jensen, 1976). The FD owner is an agent holding private information that the GO, as principal, cannot observe – whether a device is genuinely prequalified to provide flexibility, and whether flexibility offered was actually delivered. The conventional response to such asymmetry is monitoring or bonding, but here that response is defeated by the very privacy-sensitivity of the data that would resolve it: the device-level master and operational data that would settle the question reveal private consumption behavior or industrial production patterns and so cannot simply be disclosed (Ferrag et al., 2018; Hinterstocker et al., 2017). This is the hinge to the trust shift. Verifiable claims allow the principal to check the agent's assertions without the agent disclosing the underlying data, substituting verification for the trust – or the costly monitoring – that the asymmetry would otherwise demand. The infrastructure problem is therefore not that the GO needs more data, but that it needs *trustworthy claims* – about which devices are prequalified, about the flexibility on offer, and about flexibility actually delivered – organized so that it can rely on them without the underlying device data being disclosed to it.

3.2.2 Roles as Central Infrastructure Building Blocks

P8 leverages an architecture based on wallet-based identity management to address this challenge. Its contribution to the dissertation lies mainly at the level of the *role architecture* this entails as a prerequisite to the specific choice of technology. A wallet-based, self-sovereign identity arrangement consists of a small set of roles: an *issuer* that defines, issues, and can revoke Verifiable Credentials (VCs); a *holder* that stores credentials in a wallet and presents selected claims from them as a Verifiable Presentation (VP); and a *verifier* that checks the origin and validity of the presented claims (Babel, Willburger, et al., 2025; Mühle et al., 2018; Sedlmeir, Smethurst, et al., 2021; Tobin & Reed, 2017). Zero-knowledge proofs – here realized as zk-SNARKs – let a holder disclose only the claims it chooses while keeping the remaining contents of a credential secret, so that the verifier learns that a claim holds without learning the data behind it – i.e. proving the holder is an adult, without revealing their date of birth (Goldwasser et al., 1989).

A VC and a VP are not synonyms for device-level operational data; they are the means by which *selected claims about an asset's attributes* become verifiable to a relying party without the underlying data being shared. Through this characteristic they contribute greatly to solving the dissertation's underlying data sharing dilemma. As such this arrangement demonstrates the infrastructural level of data sovereignty as described in Chapter 2: the self-determination of an actor to control its data while still sharing what a counterpart legitimately needs (Gramlich et al., 2023; Hummel et al., 2021; von Scherenberg et al., 2024). The roles, on the other hand, are the function through

which the confidentiality–verifiability reconciliation identified in Section 3.1 is actually allocated to actors.

3.2.3 The Trust Diamond

The conceptual centerpiece of P8 is the *Trust Diamond*, which extends the conventional issuer–holder–verifier trust triangle of self-sovereign identity by inserting an additional role – the aggregator – between the device owner and the grid operator (Mühle et al., 2018; Zwede et al., 2025). Earlier extensions of the trust triangle added a governance authority for global rule-setting (Lacity & Carmel, 2022); P8's extension is different, adding a market intermediary that the flexibility use case requires for three connected reasons: a single household's flexibility is too small to be market-relevant, so many devices must be pooled into tradeable volumes; the resulting aggregated provision carries operational and market risk that some party must bear and manage; and grid operators have neither the mandate nor the interest to handle the privacy-sensitive, personal device data that direct coordination would force upon them. The resulting configuration assigns four roles (Figure 3.3; Table 3.3). A trusted third party (TTP), typically the original equipment manufacturer (OEM) of a device, acts as *issuer*, attesting device characteristics and prequalification status in a VC. The FD owner is the *holder and delegator* of that credential. The aggregator first acts as *verifier* of the owner's credential and then, once the owner delegates the credential's use, as a *delegated holder* that pools the delegated credentials of many FD owners and presents a single aggregated claim over all of them onward to the GO. The GO is the *terminal verifier* of those aggregated claims for the purpose of grid management.

For this configuration to function, the GO must only trust the issuer: the value of a device credential rests on the OEM's attestation being correct. This is not a novel assumption – it is the standard trust anchor of any credential system. What the Trust Diamond changes is everything downstream of issuance. Crucially, delegation is revocable through an identity registry, so that an FD owner can withdraw an aggregator's authority to act on its behalf and switch to another aggregator. This revocability is what allows the role configuration to sit inside a competitive market for aggregation that prevents locking owners to a single intermediary, improving overall market performance (Amprion et al., 2024). The Trust Diamond is, then, a role configuration for distributing and forwarding verifiability of claims across actors; it is not a complete governance or market-design model for flexibility provision.

3.2.4 The Trust Shift on an Infrastructure Level

From the Trust Diamond, P8 derives two design principles (Gregor et al., 2020; Zwede et al., 2025). These belong at the infrastructure layer as opposed to the requirements-layer principles of Section 3.1, since they concern a different object: where P5's and P6's principles concern what a sharing arrangement must support and how to engineer a proof system, P8's principles concern how *roles* are distributed across a verifiable intermediated data chain – a claim central to the Trust Diamond and the decentralized flexibility-provision architecture, which is why they appear here.

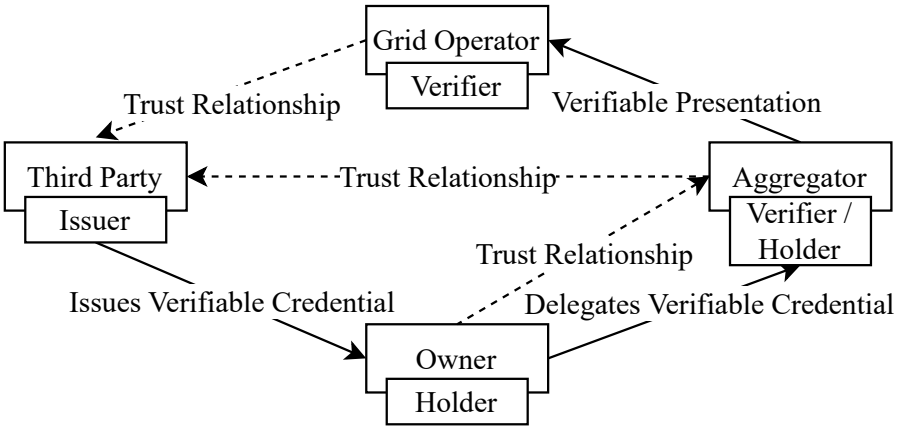


Figure 3.3: The Trust Diamond for energy flexibility provision, extending the issuer–holder–verifier trust triangle with the aggregator as a delegated-holder intermediary (Zwede et al., 2025).

Table 3.3: Actor-role configuration of the Trust Diamond for verifiable flexibility provision (Zwede et al., 2025).

Actor	Infrastructure role	Claim / data object	Verification responsibility
TTP/ OEM	Issuer	Device characteristics and prequalification claims	Issues credentials; their correctness remains a source-data assumption under the oracle problem
FD owner	Holder / delegator	Device credentials and local flexibility information	Holds credentials and delegates their use; can revoke delegation and switch aggregator
Aggregator	Verifier / delegated holder	Delegated credentials; aggregated offers and delivered-flexibility claims	Verifies device-level credentials, aggregates, and presents verifiable aggregated claims
GO	Terminal verifier	Aggregated flexibility offers and delivered-flexibility claims	Verifies aggregated claims without access to device-level data

The first principle, *Verifiability through Delegation*, carries the section's central finding. By delegating a credential from the holder (the FD owner) to the aggregator, the design removes the trust relationship between aggregator and GO that prior trust-triangle arrangements would have required, and replaces it with a verifiable data lineage (Babel, Willburger, et al., 2025; Sedlmeir, Smethurst, et al., 2021; Zwede et al., 2025). The aggregator becomes an intermediary that *does not need to be entirely trusted*: it cannot lie on behalf of the holder, because the GO verifies the forwarded claims independently against the issuer's attestation. This is precisely the trust shift of Chapter 2, now instantiated at the infrastructure layer. Trust between parties – the GO having to trust the aggregator's word – is substituted by trust in a verifiable mechanism, the delegated-credential lineage that the GO can check for itself. The principle also yields a concrete operational benefit: because the GO verifies aggregated offers independently, the aggregator is constrained from double-counting, for instance from submitting offers based on the same underlying flexibility more than once (Babel & Sedlmeir, 2023).

The second principle, *Mediated Sovereignty*, governs the privacy side of the same intermediated chain. Combining data aggregation with Zero-Knowledge Proof (ZKP)-based selective disclosure,

it lets the FD owner share verifiable data through a self-sovereignly chosen and revocable intermediary while retaining what P8 terms derived data sovereignty: the owner sets the terms of its participation – time, location, and horizon – and its detailed device data reach only the trusted aggregator, never the GO (Amprion et al., 2024; Zwede et al., 2025). Aggregation here adds a layer of anonymization on top of the data minimization that the ZKPs already provide, since the GO sees only a combined claim across many devices. The resulting privacy benefit runs in both directions: the FD owner's data are protected, and the GO's own burden of managing and protecting sensitive device-level data is reduced, because those data never reach it. Together, the two principles distribute verifiability and sovereignty across the intermediated chain so that the GO obtains trustworthy aggregated claims while device owners retain control of their data.

3.2.5 The Decentralized Flexibility Provision Architecture

P8 operationalizes the Trust Diamond in the *Decentralized Flexibility Provision Architecture* (Figure 3.4), an implemented and field-tested artifact that highlights how credential issuance, delegation, aggregation, and verification combine in one concrete energy data sharing use case – the provision of decentralized flexibility (Zwede et al., 2025). On the owner's side, a local *Flexibility Component* pairs a flexibility agent – which orchestrates the owner's devices and computes their local flexibility offer – with a Self-sovereign Identity (SSI) agent that manages the wallet, its credentials, and their presentation. On the other side, a cloud-based *aggregator*, coupled with a *verification component*, assembles aggregated offers, disaggregates activation requests from the GO, and produces the proofs that accompany aggregated claims. Both sides bind to a shared identity registry that provides the cryptographic trust anchors against which credentials and delegations are checked. The GO interfaces only through a standardized API and receives only aggregated flexibility data that it can verify.

The architectural decision this imposes is the decoupling of identity verification from data transport: credential verification runs through the SSI agents and the identity registry, while flexibility data move over a separate messaging layer. Because trust is anchored in the former and not in the transport, new actors can be added to the messaging layer without weakening the trust guarantees of the system – which is what lets the arrangement scale in the number of participants without renegotiating trust pairwise. One capability the design needs, delegation, is not yet available in broadly available standard wallet libraries and was implemented separately (Babel & Sedlmeir, 2023). This architecture instantiates the requirements-layer principles of Section 3.1 at the level of concrete components: the end-to-end digitization ensures *automation*, which in turn leads to timeliness of communication so that flexibility can be provided within the appropriate market window, the decoupled identity layer and standardized API operationalize *Common Standards*, the credential-and-delegation flow realizes *Technology-enabled Confidentiality* by keeping device data with the owner and aggregator, and the shared identity registry supplies the provenance anchor that *Traceability* requires. The architecture should be read as an infrastructure artifact: a demonstration that the role configuration of the Trust Diamond can be realized with available components, not as a finished product.

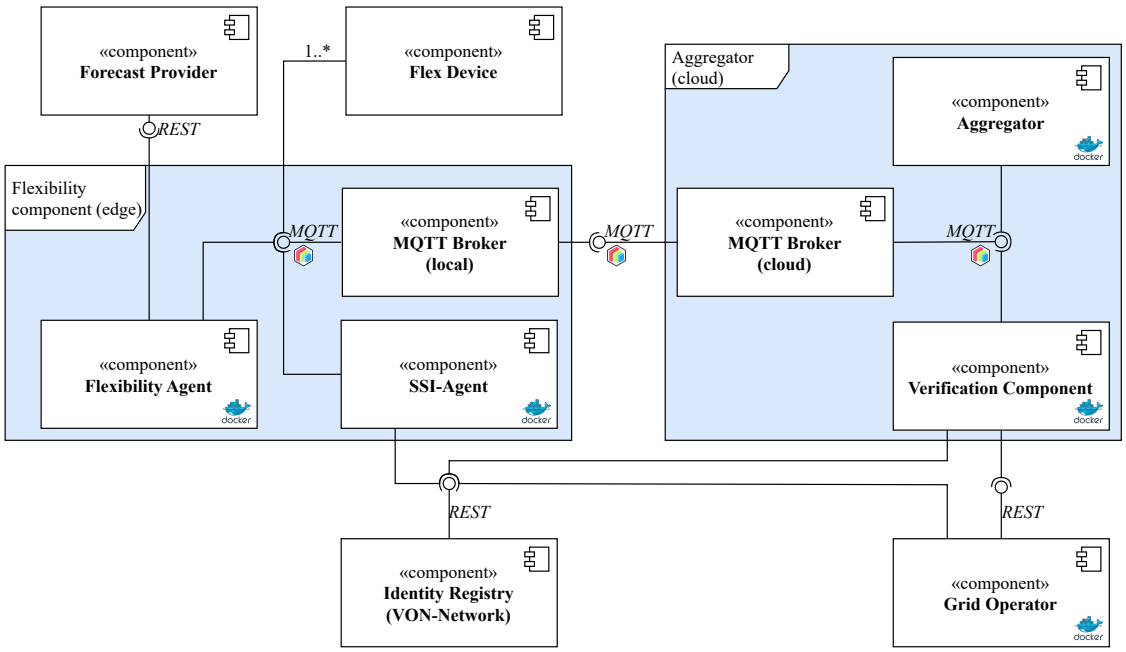


Figure 3.4: The Decentralized Flexibility Provision Architecture operationalizing the Trust Diamond for small-scale flexibility provision (Zwede et al., 2025).

3.2.6 A Contrasting Infrastructural Pattern: Green Electricity Labeling

P6 addresses the same infrastructure-level problem – distributing verification so that a relying party can check an aggregate claim without seeing the underlying data – through a structurally different arrangement, thus sharpening what can be generalized about both. In P6's architecture for green-electricity labeling, a utility holds the operational data and runs the optimization and proving services, while a blockchain serves as a shared verification layer that stores only compact commitments and public proof outputs instead of processing the data itself; stakeholders verify their claims against this neutral, openly readable layer (Principato et al., 2023; Sedlmeir et al., 2022; Zwede, Mertel, et al., 2026).

The two arrangements distribute verification along different axes. P8 distributes it across *organizational roles* – issuer, holder, delegated holder, verifier – bound together by wallets and delegation. P6 distributes it across an *architectural layering* – confidential off-chain processing beneath a public on-chain verification layer – bound together by a neutral ledger. The locus of relocated trust differs accordingly: in P8 it rests on delegated credentials and the issuer that anchors them; in P6 it rests on the shared ledger and the proof system that writes to it. Yet the underlying logic is identical: both relocate trust from the parties one shares data with onto a verifiable mechanism, and both distribute verification so that no relying party need see all the underlying data. That the same infrastructural logic carries across two separate energy use cases as different as flexibility provision and electricity labeling, and across two arrangements as different as role-distributed credentials and layer-distributed ledgers, is what suggests it is a transferable design pattern reaching beyond a single point solution. How P6's proofs actually establish their claims is the subject of Section 3.3;

here P6 serves only to highlight that the infrastructural pattern generalizes beyond P8's particular role configuration.

3.2.7 The Oracle Problem as a Boundary Condition

Neither arrangement removes trust altogether, and locating precisely where it remains is essential to stating the dissertation's contribution honestly. A VC or VP verifies that a claim was correctly issued, delegated, and aggregated; it does not establish that the original real-world fact behind the claim was true. This is the oracle problem, and in the flexibility setting it has two distinct faces that must be kept apart (Babel et al., 2023; Zwede et al., 2025).

The first concerns *master data*: a device credential is only as good as the OEM's attestation of the device's characteristics and prequalification. P8 offers a governance-bounded resolution that is tailored to this exact setting. Because the verifiers are few – grid operators – and can maintain bilateral relationships with the OEMs of relevant devices, the GO can require each OEM to carry out a one-time type prequalification for each device type, after which devices of that type are trusted until prequalification is revoked. Membership of a device on the resulting whitelist can then be proven within a VP without revealing the device's identity to the aggregator (Caldarelli & Ellul, 2021). The second face concerns *transaction data*: the delivered-flexibility proofs in P8, like the accounting proofs in P6, are computed over meter readings either from the internal meters of the FD or the boundary smart-meter or both. Here, a proof over a falsified reading is a valid proof of a false statement. Addressing this requires two things. The mechanisms that render such transaction-data claims verifiable are the subject of Section 3.3; but verifiability of the claim presupposes that the reading was rightfully quantified and credibly introduced into the system in the first place – which, in both P8 and P6, rests on the meter signing its readings and thereby coupling the physical measurement to the verifiable mechanism (Zwede, Mertel, et al., 2026).

This central boundary condition of the dissertation holds for the whole of the remaining chapter. Guaranteeing that the real-world fact behind a signed reading is true – fully solving the oracle problem – is outside the scope of this work. The contribution concerns the verifiability of data *sharing*, not the truth of the data's *source*: the architectures and mechanisms developed here presuppose that only credible data, appropriately captured and attested at the point of measurement, enter them. Everything downstream of that point can be made verifiable; the point of entry itself is assumed, not proven.

Two further residual concerns must be raised at the infrastructure level. First, P8's design does not by itself prevent double-spending *across* aggregators: a single flexibility agent could submit the same offer to several aggregators, a vector that delegation does not close and that would require a privacy-preserving registration of devices to aggregators for each market period – though this could relatively easily be solved with a separate entry in the delegation registry, ensuring that a credential is only delegated once (Bogensperger et al., 2025). Second, the aggregator, while constrained from lying about forwarded claims, becomes a new locus of coordination control, raising governance and market-design questions – collusion, gaming, lock-in, and monopoly

formation – that the architecture cannot settle on its own. P8 is explicit that the GO must define the rule set the aggregated VP is required to prove (for instance, that an aggregated offer cannot exceed the sum of its parts), and that a competitive market with free switching between aggregators is needed to keep the intermediary in check (Amprion et al., 2024). As a result, the aggregator-mediated architecture significantly reduces central direct trust and disclosure requirements while opening a new set of governance questions.

3.2.8 Performance as Feasibility Evidence

Both P8 and P6 supply performance evidence, and read together they support a measured claim about feasibility without overreaching toward deployment. In P8, end-to-end latency is dominated by the aggregator's generation of the ZKP for its aggregated offer; the proof's complexity scales near-linearly with the number of flexibility agents at roughly 55,000 constraints per agent, yielding proving times on the order of nineteen seconds for one hundred agents and permitting on the order of 1,611 FD owners to be served within a five-minute window on a single server instance – megawatt-scale flexibility per instance – while verification stays essentially constant at around ten milliseconds, as expected from the succinctness of the Succinct Non-interactive Argument of Knowledge (zk-SNARK) protocol (Groth, 2016; iden3, 2025; Samardzic et al., 2024; Zwede et al., 2025). P6's prototype exhibits the same qualitative profile in its separate setting: on-chain verification remains approximately constant regardless of system size. Practical testing indicates that a single server can support on the order of a hundred thousand consumer accounts, but only around 19,000 producer accounts – limited by system RAM – since producer-side proofs must additionally verify computationally expensive data signatures. A separate benchmark under an even split with additional system storage shows the system could prove $2^{17} = 131{,}072$ (half producers, half consumers) in roughly nine minutes, remaining within current electricity market timing requirements (Zwede, Mertel, et al., 2026). As such, two independent proof-of-concepts, built on different arrangements, both exhibit constant-time verification and scale linearly to five- or six-figure numbers in accounts under proof-of-concept conditions.

The claim this evidence supports is correspondingly bounded. It demonstrates practical feasibility and promising scalability under field test conditions; it does not demonstrate production scalability, field robustness beyond the small device counts actually tested, security-audited operation, or readiness for the regulatory environment of critical infrastructure. P8 is explicit that scaling materially beyond a few thousand devices per aggregator would depend on communication efficiency, hardware allocation, and distributed proving, and that latency and bandwidth outside the sandbox would matter more than local proving time (Garg et al., 2023). The performance results establish that the infrastructure is buildable and evaluable, not that it is necessarily deployable.

3.2.9 Trustworthy Digital Energy Data Infrastructure – Synthesis

This section has developed the infrastructure layer of the dissertation's design response. Its central claim is that trustworthy digital energy data infrastructure is neither a purely organizational

trust arrangement nor a purely cryptographic proof system, but a role architecture that organizes issuance, holding, delegation, aggregation, and verification so that the trust relocated onto technology in Chapter 2 has somewhere concrete to rest. P8 supplies the central pattern: by Verifiability through Delegation, the trust an operator would otherwise have to place in an aggregator is substituted by a verifiable data lineage the operator can check for itself, and through Mediated Sovereignty, device owners retain control of their data while still contributing verifiable claims. P6 supplies a contrasting arrangement that distributes the same verification across a different architectural layering, and the fact that one infrastructural logic carries across both suggests it is a transferable pattern.

However, the contribution is bounded. P8 is an Action Design Research (ADR) prototype validated in a supervised field test; it offers no evidence on household adoption, incentives, or compensation, leaves cross-aggregator double-spending and aggregator governance open, and does not establish that aggregators are neutral. Above all, both arrangements presuppose that credible data enter them at the point of measurement – the oracle problem that stays outside the dissertation's scope.

What the infrastructure layer establishes is *who* verifies *what*, through which role configuration and under which constraints. What it does not open is *how* a concrete claim is actually rendered checkable: an aggregated flexibility offer, a delivered-flexibility statement, a green-electricity accounting claim, a traceable certificate. Throughout this section, the proofs that carry those claims were treated as black boxes – P8's plausibility and delivered-flexibility ZKPs were described by what they assert, not by how they establish it. P6 has already indicated that this "how" can be opened, since its architecture rests on a defined division between a global accounting proof and local inclusion proofs. Section 3.3 opens these mechanisms, turning from the configuration of roles to the construction of the proofs through which selected claims become verifiable under disclosure constraints.

3.3 Mechanisms for Verifiable Digital Energy Data Sharing

Section 3.2 settled who verifies what, through which role configuration and under which constraints, but it treated the proofs that carry the claims as black boxes: P8's plausibility and delivered-flexibility proofs were described by what they assert, not by how they establish it. This section aims to open those black boxes. To that end, it develops the mechanism layer of the dissertation's design response, asking how a concrete claim – an aggregated offer, a green-electricity accounting statement, a traceable emission certificate – is rendered checkable without disclosing the data behind it. The oracle problem lodged in Section 3.2.7 holds throughout and is not reopened here: the mechanisms below verify what is done with data once admitted into the scope of this dissertation.

A *mechanism for verifiable data sharing* is understood here, more narrowly than the infrastructure of Section 3.2, as a technical procedure – embedded in socio-technical assumptions – that binds a data object or attribute to a claim a relying party can check under specified conditions. Its constituents are proofs, commitments, and credential and claim representations, not role alloca-

tions or governance arrangements. The section develops two such mechanisms and reads them as complementary stages of a single transaction-data lifecycle. P6 secures the step from signed reading to accounting claim: a proof over committed transaction data. P7 secures the step that follows, the certified value in motion: an emission certificate as it is minted, fractionally split, transferred, and prevented from double-use. Each verifies that a claim, once admitted, holds against defined properties. For each, the section states three things in turn – what claim is made, what is actually proven, and what is presupposed.

3.3.1 Abstracting Verifiability from Transparency

Both mechanisms instantiate one logic: sensitive or off-chain data are transformed into commitments and proofs that permit selected checks without exposing the inputs. The motivation is a tension that openness alone cannot resolve. In P6, a blockchain supplies the openness and public verifiability that green-electricity labeling needs, but processing granular smart-meter data on-chain would breach data protection and overwhelm scalability (Sedlmeir et al., 2022; Zwede, Mertel, et al., 2026). In P7, a ledger can prevent the double-use of certificate fractions, yet publishing fine-grained emission and transaction data would expose information that is sensitive in both senses Chapter 2 distinguished: upstream it is commercially confidential business data that competitors could exploit, while at the consumer end it can become personally identifiable and fall under data-protection law (Babel et al., 2022; Principato et al., 2023). The same mechanism hence protects firm-level confidentiality and personal privacy at different points in the data value chain. The mechanism-level contribution is not that blockchains, zero-knowledge proofs, or non-fungible tokens are desirable technologies, but that a verification function can be separated from full disclosure and from replicated raw-data processing.

3.3.2 Securing the Accounting Step: Green Electricity Labeling

P6's claim is that a relying party can confirm green electricity was allocated correctly without receiving the underlying generation and consumption data. The mechanism combines two proofs whose division along specific tasks instantiates the principles DP3 and DP4 abstracted in Section 3.1. A global zk-SNARK proves selected accounting properties over private, off-chain inputs and is verifiable through compact public outputs. Local Merkle inclusion proofs let each stakeholder confirm that its own data object sits in the committed set summarized by a Merkle root. The blockchain functions strictly as a verification layer: it stores the Merkle roots, the public proof outputs, and the verification transaction, while the detailed generation and consumption data remain off-chain with the utility and the stakeholders (Goldwasser et al., 1989; Zwede, Mertel, et al., 2026).

The presented proofs are distinct in their function. The global zk-SNARK proves three properties (Figure 3.5): that no more green electricity is allocated to consumers than was generated by registered generators in the epoch (R1); that the timestamps on the included data fall within the epoch's public start and end times (R2); and that the Merkle roots – necessary for the local

inclusion proof – were correctly computed from the leaves (R3). The local inclusion proof then links a stakeholder's own data object to the globally committed set: each data object is a leaf in a Merkle tree, and by recomputing the hash path from its own leaf up to the publicly published root, a stakeholder can confirm that its data were included in exactly the set the global proof was computed over, without learning any other leaf. Because R3 has already established that the published root faithfully summarizes the committed leaves, a successful inclusion check binds the stakeholder's own data to the globally verified accounting; the root against which it checks is publicly and immutably available on the blockchain. Meanwhile the mechanism deliberately does not verify the optimality of the allocation of generators to consumers. P6 scopes this out by design, because proving optimality would inflate the computational complexity of the proof mechanism substantially while the fraud vector that matters – over-allocating green electricity beyond what was generated – is already closed by R1; suboptimal matching itself is hardly a fraud vector (Zwede, Mertel, et al., 2026).

Global accounting proof (zk-SNARK)

PRIVATE INPUTS: per-generator generation data; per-consumer allocated green consumption; epoch start and end times

PUBLIC OUTPUTS: generator Merkle root; consumer Merkle root; epoch start and end timestamps

PROVING THAT:

(R1) total allocated green consumption $\leq$ total green generation

(R2) all included timestamps lie within the public epoch boundaries

(R3) the Merkle roots are correctly computed from the committed leaves

Local accounting proof (Merkle inclusion)

PROVING THAT: *a stakeholder's own data object is included in the committed set referenced by the globally verified Merkle root*

Figure 3.5: Division of labor in P6's proving scheme: a global zk-SNARK over private inputs establishes aggregate accounting consistency, while local Merkle proofs establish per-stakeholder inclusion (Zwede, Mertel, et al., 2026).

The mechanism assumes that the provided meter readings are signed and credible – the oracle assumption of Section 3.2.7. In doing so, P6 shrinks the trusted surface to a single, well-defined anchor: trust is concentrated at the point of measurement, where readings are signed – in P6's case, by meters whose signing keys could in the future be tied to machine identities by recognized certificate authorities such as the Qualified Trust Service Providers of the eIDAS regulation (Babel et al., 2023). Everything downstream of that signature is verifiable, which is the trust shift in its mechanism-level form: the relying party believes the accounting not because the counterparty asserts it but because the system lets it check everything downstream of a single signed measurement anchor. The boundary remains – a signed but false reading yields a valid proof of a false statement – but it is relocated to one inspectable point instead of diffused across the chain.

3.3.3 Securing the Value in Motion: Shielded Fractionalized NFTs

P7 secures the stage that begins where P6's accounting ends. An emission certificate carries a certified transaction value – a quantity of electricity and its associated carbon factor – so altering, double-using, or fraudulently re-attributing the certificate as it changes hands is a way of falsifying transaction data downstream. P7 makes that lifecycle verifiable while keeping the certificate's contents confidential. It verifies the value as it moves.

The data object is a proof-of-origin certificate – or a fraction thereof – that can be minted, split, transferred, and traced along the accounting or contractual path of electricity (Babel et al., 2022). The certificate is represented as a *shielded, fractional non-fungible token*, with each qualifier adding a substantial capability to the overall mechanism: non-fungibility makes certificate histories distinguishable, so a unit of green electricity can be individually labelled and a corresponding polluter held to its emissions; fractionality lets a certificate be divided across smaller quantities, so a wind turbine's output can be apportioned to individual consumers; and shielding keeps the certificate's contents and the transaction's parties confidential.

P7's contribution to the cryptographic literature is the combination of all three capabilities into a single mechanism, which no prior construction offered comprehensively (Babel et al., 2022). The remaining primitives realize the shielding. A *commitment* – a salted hash of a certificate's pre-image (its certificate hash, quantity, owner public key, and salt) – binds the system to hidden certificate and transaction data. A *nullifier* marks a commitment once it is spent so it cannot be used twice; constructing this nullifier as the hash of the owner's signature over the commitment, $\text{nullifier} = \text{Hash}(\text{Signature}(\text{SK}, \text{commitment}))$, achieves three things at once: only the owner can produce it (it requires the secret key), it provably corresponds to the spent commitment, and it reveals nothing about which commitment was spent. *Merkle structures* support inclusion checks – of commitments in the global set, and of authorized minters' keys on a safelist – so a minter can prove its key is safelisted without disclosing it. Finally, *off-chain bilateral exchange* of certificate pre-images means the fine-grained emission data are shared only between transacting parties, never published – the cryptographic counterpart of the one-up-one-down confinement of disclosure to immediate partners discussed in Section 3.1.5.

The proof scope, again, is highly specialized to the relevant task. A minting proof establishes that the minter's key is on the safelist and that the new commitment's pre-image is well-formed. A transfer proof establishes five properties: that the sender's commitment is a valid member of the committed set; that the transfer conserves value, with the spent amount positive and equal to the sum of the receiver's share and the change (sender $=$ receiver $+$ change); that the nullifier is correctly derived, corresponds to the spent commitment, and has not been published before; and that the receiver and change commitments are both well-formed (Babel et al., 2022). The conservation property is the certificate-lifecycle counterpart of P6's R1: where R1 prevents allocating more green electricity than was generated, the transfer proof prevents a fractional split from creating certificate value out of nothing. What P7 does not trace is the physical path of electricity. It follows the accounting and contractual attribution of emissions, not electrons through

the grid – a property it shares with P6 and with every other electricity accounting system, since physical electron flows are untraceable in a synchronous grid, not a limitation peculiar to this mechanism or particularly relevant to the real world (Babel et al., 2022).

Among several differences, one architectural consequence particularly distinguishes P7 from P6: because P7 keeps all sensitive data off the ledger by construction, it is *blockchain-agnostic*: the ledger need only guarantee integrity and non-censorship, not openness, so the system can run on a public blockchain or, as in P7's prototype, on a central ledger authority trusted for nothing more than those two properties (Babel et al., 2022). P7's exemplary application makes the lifecycle concrete: a wind turbine mints a proof-of-origin certificate for each 15-minute interval of generation, transfers it whole to its electric utility, and the utility fractionally transfers the share corresponding to a vehicle's charged energy to that vehicle – which can then verify the validity of the electricity's certificate back to its source and compute the associated emissions from the certificate's carbon factor, all without any party learning more than its own transaction (Figure 3.6).

3.3.4 The Common Logic behind Two Mechanism Designs

While they differ in the data object they secure, the two mechanisms presented in P6 and P7 share a higher-order logic. Both transform sensitive or off-chain data into commitments and proofs that permit selected disclosure without exposing the entirety of their inputs, demonstrating from two independent constructions that verifiability and disclosure control can be achieved jointly. However, because their data objects differ, they cannot be collapsed into a single working mechanism: P6 proves a computation over a committed dataset, whereas P7 governs a lifecycle over distinguishable, shielded, transferable tokens. Their trust postures toward the ledger differ accordingly. P6 relies on the blockchain's openness as the substrate of public verifiability; P7's ledger – still required to register commitments and published nullifiers – need only be trusted for integrity and non-censorship, not openness, and may as a result be centralized or decentralized. While they cannot be joined into a single mechanism, read along the transaction-data lifecycle the two approaches are highly complementary: P6 secures the passage from signed reading to accounting claim, P7 secures the certified value as it is subsequently split and transferred, and together they make verifiable a longer stretch of that lifecycle than either does alone. Table 3.4 sets out the comparison.

3.3.5 Evidence on Feasibility and Embeddedness

Both mechanisms are evaluated as prototypes, and their evidence supports a claim of feasibility, not of deployment. P7's per-transaction cost is light: a circuit of roughly ten thousand constraints using the Poseidon hash function yields proof creation in about four seconds with default tooling and around 0.23 seconds with optimized proving, a proof under one kilobyte, and verification in the order of milliseconds with optimized libraries – light enough to run on a consumer's mobile device (Babel et al., 2022; Groth, 2016). This is a different scalability claim from the aggregator- and utility-side account counts reported for P8 and P6: it concerns the cost borne by an end user

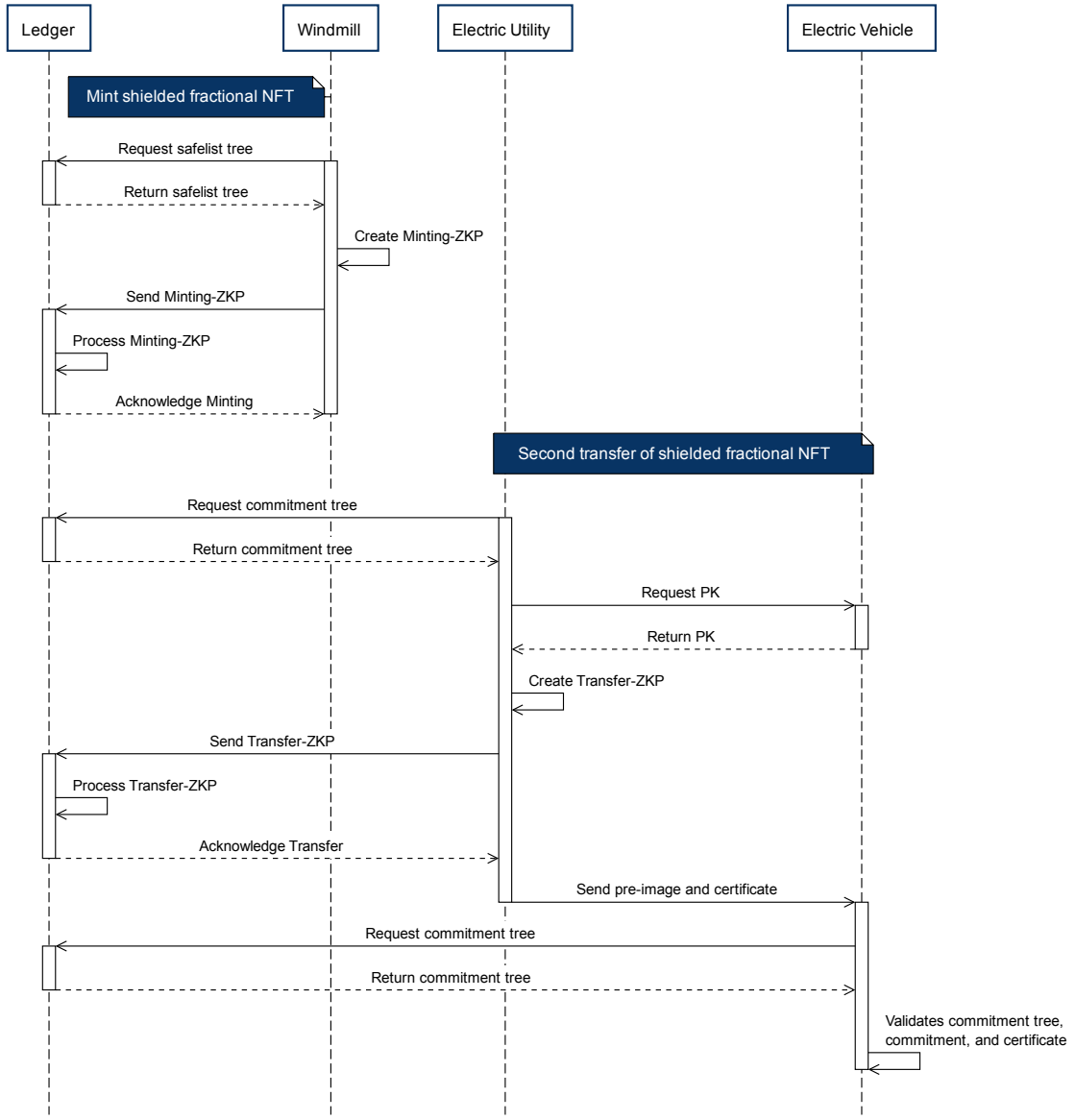


Figure 3.6: Process of minting and transferring shielded fractional proof-of-origin certificates for verifiable carbon-emission tracing (Babel et al., 2022).

per certificate, owing to the user-centric design of the mechanism. What the prototypes do not establish is long-term or large-scale operation, field robustness, or readiness for production, all of which P7 and P6 name as open.

The mechanisms are also embedded in the layers above them. Both share a common dependency at the point of data entry: each presupposes the oracle assumption of Section 3.2.7 – trustworthy, tamper-resistant capture at the sensor and a signed, credibly attested reading, ideally anchored in recognized certificate authorities or equivalent assurance. Beyond that shared foundation, each carries its own governance add-on. P6 additionally depends, across separate implementations, on governance against the double-generation and double-registration of green electricity (dena, 2020; Zwede, Mertel, et al., 2026). P7 additionally depends on safelisted keys at minting, on ledger

Table 3.4: The two mechanism patterns of Section 3.3 compared.

	P6 (Zwede, Mertel, et al., 2026)	**P7** (Babel et al., 2022)
Lifecycle stage	Reading → accounting claim	Certified value in motion (mint, split, transfer)
Data object	Green-electricity accounting over a committed dataset	Distinguishable, shielded, fractional emission certificate
Core mechanism	Global zk-SNARK + local Merkle inclusion proofs	Shielded fractional NFTs with commitments, nullifiers, off-chain exchange
What is verified	Allocation $\leq$ generation; epoch consistency; Merkle-root correctness; stakeholder inclusion	Authorized minting; transfer conservation; commitment membership; nullifier correctness; no double-use
What stays hidden	Detailed generation and consumption data	Certificate contents; emission sources; transacting parties
Ledger role	Open ledger as substrate of public verifiability	Technology-agnostic; ledger trusted only for integrity and non-censorship
Out of proof	Allocation optimality; source-data truth	Physical electron tracing; source-data truth

integrity and non-censorship, and on continued progress in oracle integrity, interoperability, and large-scale performance (Babel et al., 2022). These describe the boundary conditions under which the mechanisms operate; Section 3.4 returns to how the three design levels condition one another.

3.3.6 Mechanisms for Verifiable Digital Energy Data Sharing – Synthesis

This section has highlighted how selected energy- and emission-related claims can be made verifiable without disclosing the data behind them. The mechanism-level contribution is that verifiable digital energy data sharing can be operationalized by binding private or off-chain data to selectively verifiable claims through proofs, commitments, inclusion proofs, and distinguishable certificate representations. P6 demonstrates this for green-electricity accounting by combining a global zk-SNARK with local Merkle inclusion proofs; P7 demonstrates it for emission-certificate tracing of electricity by creating shielded fractional non-fungible tokens leveraging commitments, nullifiers, and off-chain bilateral data sharing; and across the transaction-data lifecycle the two are complementary.

The zk-SNARK recurs across all three design papers – it carries P6's global accounting proof, P7's minting and transfer proofs, and P8's aggregated plausibility and delivery proofs. The zk-SNARK is a fundamental instrument in each artifact, since it is what allows the necessary claims to be proven, specified, and checked succinctly. It is, however, not sufficient on its own. In none of the three artifacts does the proof system carry the design by itself; each also required a set of surrounding decisions – what to prove and what to scope out (P6's DP1), which primitive to select for end-to-end performance (P6's DP2), how to divide global from local proofs (P6's DP4), how to represent and shield the data object (P7), and how to distribute the roles that produce and check the proof (P8). The mechanism-level claim of the dissertation is not that a particular proof system is the answer, but that the design logic – binding a data object to a checkable claim under clearly

defined disclosure constraints – is what carries value, with the proof system as one central but not its only instrument.

The argument of the devised mechanisms is, as throughout this chapter, limited: what a mechanism verifies is the encoded relation among data objects, commitments, proofs, and claims under stated assumptions, with source-data truth, governance, interoperability, and adoption lying outside the proof system, as Section 3.2.7 established. With the mechanism layer in place, the chapter's three levels are complete: the principles that specify what a sharing arrangement must support, the infrastructure that organizes who verifies what, and the mechanisms that render the individual claims checkable. Section 3.4 integrates these levels into the chapter's layered design response and carries it toward the governance and policy conditions of Chapter 4.

3.4 Designing Trustworthy & Verifiable Digital Energy Data Infrastructure – Synthesis

The chapter's contribution demonstrates that three layers of design – design principles, trustworthy architectures, and verifiable mechanisms – must be aligned to enable verifiable and trustworthy digital energy data sharing, and that those levels exhibit the same conceptual trust-shift as previous chapters.

The levels are mutually dependent rather than additive. Design principles specify what a cross-organizational sharing arrangement must support, but they cannot say who holds which responsibility: P5 and P6 establish that data must be timely, interoperable, confidential, traceable, automatable, and incentive-compatible, and that cryptographic verification can reconcile confidentiality with verifiability, without allocating any of this to concrete actors. The infrastructure layer distributes those responsibilities across issuers, holders, delegated holders, and verifiers, but treats the proofs that carry the claims as black boxes: P8's Trust Diamond organizes who verifies what without specifying how. The mechanism layer renders the individual claims checkable, but only by presupposing the requirements and the role configuration above it: P6 and P7 bind data to checkable claims that are meaningful only inside a governance arrangement that has already settled what must be supported and who must verify it. A mechanism without an arrangement to embed it, or an arrangement without principles to satisfy, does not produce verifiable data sharing. This interdependence is what "layered design knowledge" denotes, and it is why the chapter amounts to more than the sum of its embedded papers.

Read this way, the chapter discharges the design-oriented part of the dissertation's research aim. It addresses the three design objectives that the introduction posed in sequence: design principles for cross-organizational energy data sharing (RO2), a trustworthy infrastructure for verifiable and privacy-preserving data sharing (RO3), and mechanisms that make claims verifiable under privacy constraints (RO4). Table 3.5 states the cumulative contribution at each level. P6 appears at all three: developed as a built and evaluated green-electricity labeling system, it contributes artifact-grounded principles (RO2), a ledger-based verification architecture (RO3), and a concrete

proof construction (RO4), and so serves as the connective case that demonstrates the three levels cohering in a single system, while P5, P8, and P7 each anchor a specific level.

Table 3.5: Cumulative contribution of Chapter 3 across its three design levels.

Level	Objective	Embedded papers	Design question	Cumulative contribution
Design principles	RO2	P5, P6	What must a cross-organizational energy data-sharing arrangement support?	Socio-technical requirements for valuable, protected, traceable, automatable, and incentive-compatible data sharing, with cryptographic verification reconciling confidentiality and verifiability
Infrastructure	RO3	P8, P6	How are verification responsibilities distributed across actors?	A role architecture for credential issuance, holding, delegation, aggregation, and verification, in which delegation substitutes verifiable lineage for trust in an intermediary
Mechanisms	RO4	P7, P6	How is a single claim rendered checkable without full disclosure?	Mechanism patterns binding private or off-chain data to selectively verifiable accounting and certificate claims

The central trust shift of the dissertation recurs throughout this chapter. At the principle level, verification moves from an institutional auditor to a cryptographic proof, the supply-side counterpart of the consumer preference P3 documented. At the infrastructure level, the grid operator no longer trusts the aggregator's word but checks a verifiable data lineage the aggregator cannot falsify on the holder's behalf. At the mechanism level, a relying party trusts the verification procedure that lets it check any data downstream of a single signed anchor, instead of its counterparty's assertion. This is the trust shift that Chapter 2 identified at the organizational, data, and user levels, now recurring at the requirement, infrastructure, and mechanism levels of the design response. Its recurrence on both the explanatory and the design side of the argument is what lets the dissertation advance it as a *candidate structural feature* of verifiable data sharing, as opposed to an isolated artifact of any single setting – while acknowledging that a pattern the analysis deliberately traced at each level is thereby illustrated more than independently proven. It is in this qualified sense that the trust shift, and not any one artifact, constitutes the dissertation's integrative contribution.

A second claim cuts across the chapter and qualifies the first. Verifiability and disclosure control are not opposed design goals – P5 and P6 establish this at the principle level, P8 at the infrastructure level, and P6 and P7 at the mechanism level – but every reconciliation is bought at a specific and nameable cost. Upstream aggregation forgoes provenance and peer verification beyond the immediate supplier. Delegation through an aggregator removes a trust requirement but creates a new locus of coordination control, with its attendant governance and market-design questions. Cryptographic scoping verifies selected claims precisely because it does not verify everything: P6 proves accounting consistency but deliberately not allocation optimality, and P7 secures a certificate's lifecycle – authorized minting, conserved value, no double-use – but not the truth of the source reading at issuance, which the oracle boundary places outside the proof. The chapter's answer to the data-sharing dilemma is not that technology resolves it. It is that technology relocates and bounds the dilemma into a designed trade-off – a socio-technical achievement, since

the trade-off can be designed in both, implementation and the governance that lies on an entirely different layer.

This chapter's findings are limited, however. The design knowledge developed here is nascent and prototype-grade: P5 offers expert-evaluated principles without a situated deployment, and P6, P7, and P8 offer proof-of-concept artifacts evaluated in laboratory and small field settings, with no evidence on adoption, incentives, or compensation. The arrangements presuppose, however, that credible data enter them at the point of measurement; solving the oracle problem lies outside the dissertation's scope, as Section 3.2.7 set out. Governance questions remain open at every level – cross-aggregator double-spending, double-generation across separate implementations, and the market design that keeps an aggregator competitive and non-collusive. And the knowledge was first derived from specific use cases: developed for battery emission data, flexibility provision, green-electricity labeling, and emission-certificate tracing, its generalization to further digital energy data sharing instances is argued along the presented data sharing structure and remains to be substantiated by further work.

These contributions land in the three fields the dissertation engages. To Information Systems, the chapter contributes design knowledge for data-sharing arrangements in which trust, control, and disclosure are jointly managed through technical mechanisms rather than relational assurance, demonstrating how the trust that Chapter 2 located on mediating technology can be vested in an infrastructure built to bear it. To Energy Informatics, it contributes concrete verification mechanisms and infrastructure designs for three coordination problems of the decentralized energy system – flexibility provision, green-electricity labeling, and emission-certificate tracing for electricity – each instantiated as an evaluated artifact. To Green IS, it shows how information systems can make sustainability-relevant claims verifiable without assuming unrestricted transparency, so that emission and provenance data can support decarbonization decisions while the confidentiality and privacy of the actors who hold that data are preserved.

The open items enumerated above – the oracle boundary at data entry, the market design that disciplines an aggregator, the cross-implementation governance that prevents double-generation, and the regulatory recognition of verifiable data sharing as compliant – are the conditions which must be actively induced for the artifacts to realize their value potential. Each names a lever that design alone cannot pull: an aggregator architecture needs a market design that prevents collusion, a labeling mechanism needs governance against double-generation, and any of them needs a regulatory environment that admits verifiable data sharing as a compliant substitute for disclosure. These enabling conditions are the territory of the dissertation's final objective, defining the agenda Chapter 4 takes up. Through P9, which assesses the digital capabilities that decentralized electricity systems require and the policy measures that would enable their deployment, the conclusion completes the arc from the value drivers of Chapter 2, through the design knowledge of this chapter, to the governance and policy conditions under which that knowledge can create value.

4 Conclusion

This dissertation set out to develop design-oriented knowledge for verifiable data sharing in decentralized digital energy systems and the trustworthy infrastructure it requires. Chapters 2 and 3 elaborated how verifiable data sharing creates value and how it can be effectively designed for the use case of digital energy data; this chapter steps back from the individual artifacts to their joint contribution and the conditions of its deployment. Section 4.1 synthesizes the cumulative answer to the research question, derives policy implications from P9, and sets out the resulting research and implementation agenda. Section 4.2 then performs the boundary work, clarifying how the mantle text relates to the embedded papers and the research on which it builds. The chapter introduces no new evidence; its contribution is synthetic.

4.1 Summary, Policy Implications & Outlook

The dissertation was guided by one overarching question: how verifiable data sharing and the necessary trustworthy infrastructure can be designed to support value creation in decentralized digital energy systems while addressing privacy concerns and loss-of-control risks. Its cumulative answer demonstrates that this is achievable, but only once verifiability is understood not as a substitute for trust but as a means of *relocating* it – from the counterparties an actor shares data with toward the technologies and infrastructures that mediate the act of data sharing. Trust, the willingness to accept vulnerability under uncertainty and perceived risk (Mayer et al., 1995), and verifiability, the possibility of leveraging information systems to establish the truthfulness of data, claims, or attributes as opposed to accepting them as asserted (Sedlmeir, Smethurst, et al., 2021), are hence closely linked but not interchangeable: verifiability can discharge part of the trust an actor would otherwise need to extend toward its counterpart, yet it neither assumes it to be present nor completely removes it from the interaction. This *trust shift* is the dissertation's overarching finding, and it recurs – as the following synthesis highlights – at every level of both the explanatory and the design argument. The dissertation develops this conclusion along a single arc: from the value drivers that make verifiable data sharing worthwhile (Chapter 2), through the design knowledge that realizes it (Chapter 3), to the governance and policy conditions under which that knowledge can create value at system scale (this chapter).

The explanatory foundation in Chapter 2 established why trust and verifiability drive value, and did so at three levels. At the organizational level, P1 conceptualized technology-enabled data sovereignty as a socio-technical arrangement in which governance structures and privacy-enhancing technologies make control a realizable property of data sharing instead of a promise contingent on a counterpart's goodwill; its model traces how data sovereignty enables control, control lowers perceived risk, and reduced risk raises participants' willingness to share data (Ehaus et al., 2026). Its decisive result is that this arrangement does not raise trust uniformly but relocates it – reducing the reliance actors must place on trust between parties while elevating the role of

trust in the mediating technology and its operators – and that this relocation is what allows data sharing to scale beyond bilaterally negotiated relationships (Ehaus et al., 2026; Söllner et al., 2016). At the data-object level, P2 demonstrated that sustainability-related data create value not through availability but through purpose-fit, with data verification as one of the central characteristics that define the usability and thus value-potential of data within an organization (Zwede, Valett, et al., 2026); P3 sharpened this into a behavioral result, demonstrating in a discrete-choice experiment that digitally verifiable carbon information functions as a credibility signal that raises consumers' willingness to pay and can outweigh third-party certification at the point of choice, most strongly where product involvement and price are high (Geist et al., 2026; Spence, 1973). At the user level, P4 derived a Self-Sovereign Identity Acceptance Model in which the social-influence constructs central to established acceptance models drop out entirely, and identified *comprehensibility* – users' ability to understand what is shared, with whom, and to what end – as the construct doing the main work for the acceptance of sovereign and verifiable data sharing specifically (Guggenberger et al., 2023). Read together, the three levels exhibit the same movement: the object of trust shifts from a counterpart organization to a verification mechanism defined by the software and parties operating it.

The design chapters translated these value drivers into prescriptive knowledge at three cumulative levels. At the level of design principles, P5 derived the requirements a cross-organizational emission-data-sharing arrangement must satisfy in a complex and competitively sensitive battery value chain – common standards, technology-enabled confidentiality, traceability, automation, and explicit participation incentives – and P6 grounded a complementary set of principles in a green-electricity labeling system that was built and evaluated in a realistic field test environment (Babel et al., 2026; Zwede, Mertel, et al., 2026). At the infrastructure level, P8 developed the Trust Diamond and the accompanying Decentralized Flexibility Provision Architecture for market-based redispatch through small-scale devices, in which the flexibility-device owner delegates a revocable credential to one of several competing aggregators and the aggregator proves, through a zk-SNARK-enabled plausibility check, that its aggregated offer satisfies the grid operator's rule set without disclosing sensitive device-level data (Zwede et al., 2025). The architecture's decisive contribution is that delegation substitutes a verifiable data lineage for trust in the intermediary: the grid operator no longer trusts the aggregator's word but checks a lineage the aggregator cannot falsify on the holder's behalf (Zwede et al., 2025). At the mechanism level, P7 introduced shielded, fractional non-fungible tokens combined with off-chain bilateral exchange to harden a carbon certificate's credibility along its lifecycle – authorized issuance, conserved value, and prevention of double-use – at high resolution while keeping the underlying data confidential, and P6 used zk-SNARKs to prove accounting consistency for green-electricity labeling while deliberately not proving allocation optimality (Babel et al., 2022; Zwede, Mertel, et al., 2026).

Two claims cut across this design response. First, verifiability and disclosure control can be understood not as opposed goals – which the data-sharing dilemma would imply – but as co-designable characteristics. Yet, their specific alignment always carries a trade-off: upstream aggregation obscures provenance beyond the immediate supplier, delegation removes a trust requirement but creates a new locus of coordination control, and cryptographic scoping only

verifies precisely selected claims and nothing beyond. The dissertation's answer to the data-sharing dilemma is therefore not that verifiable and trustworthy data sharing resolve it, but that they transform it into a trade-off that can be actively managed. Second, the trust shift identified at the organizational, data, and user levels reappears at the requirement, infrastructure, and mechanism levels of the design: verification moves from an institutional auditor to a cryptographic proof, the grid operator verifies a data lineage rather than trusting an assertion, and a relying party trusts a verification mechanism instead of its counterparty's word. That the same movement recurs at six distinct points across the dissertation, on both the explanatory and the design side of the argument, is what establishes it as the dissertation's contribution beyond any single artifact. Figure 1.1, introduced at the outset of the dissertation, lays out the relationships of the individual claims behind this cumulative argument as a whole; the present chapter substantiates its final layer – the governance and policy conditions under which the argument holds at system scale (Figure 4.1 revisits the conceptual overview introduced at the outset of the dissertation).

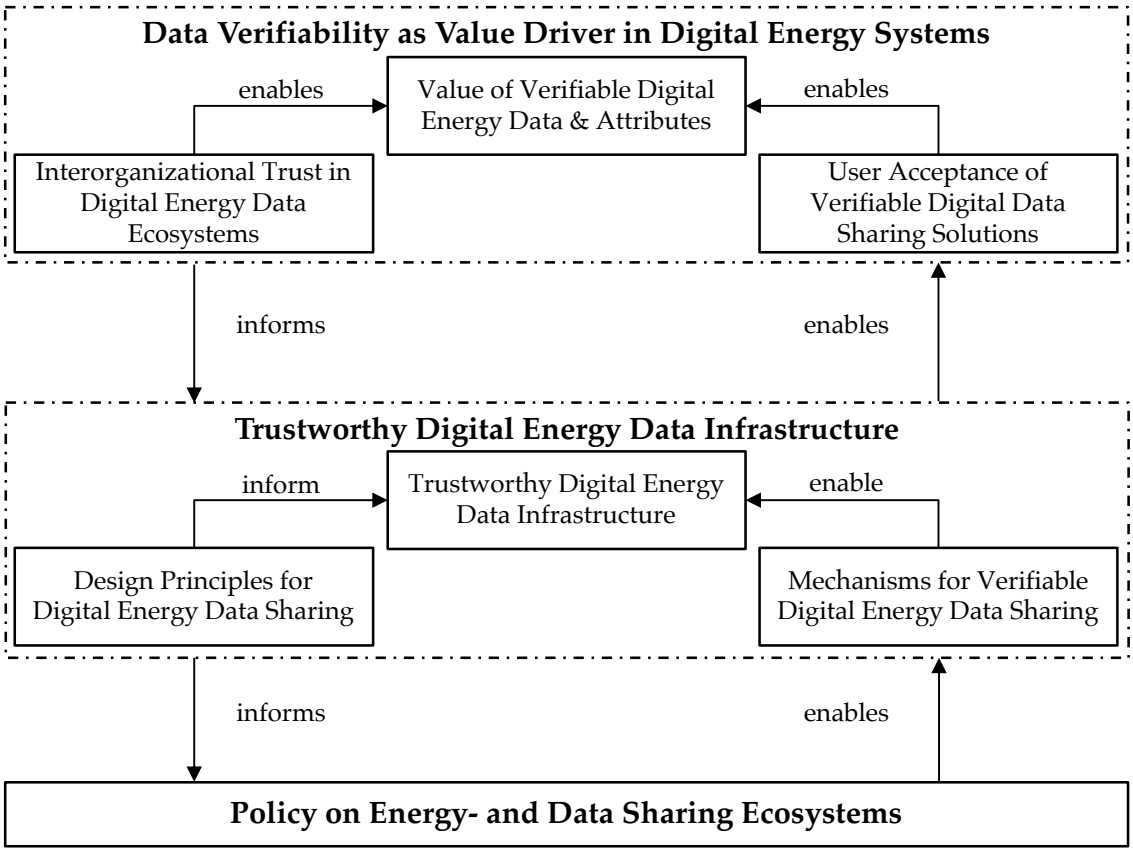


Figure 4.1: Revisited cumulative argument of the dissertation: trust and verifiability as value drivers, design knowledge for trustworthy infrastructure and verifiable mechanisms, and the governance conditions for their deployment – connected by the recurring relocation of trust onto mediating technology.

Design knowledge, however, does not create value in an institutional vacuum. Chapter 3 closed by naming the enabling conditions its artifacts presuppose but cannot themselves supply: a trusted anchor at the point of measurement (the oracle boundary), a market design that keeps an aggregator competitive and non-collusive, cross-implementation governance that prevents

double-generation, and regulatory recognition of verifiable data sharing as a compliant substitute for full disclosure. Establishing these conditions is a matter of governance and policy, and it is here that P9 completes the dissertation's arc. Through a qualitative multi-method study – a review of 92 articles, a workshop with 19 experts, and interviews with 8 practitioners – P9 derives five characteristics of a successful decentralized electricity transition and assesses which digital capabilities support them and which policy measures enable their deployment (Zwede, Heeß, et al., 2026). Its central stance is capability-oriented as opposed to technology-deterministic: policy should not promote specific classes of credentials, ledgers, wallets, or proofs as ends in themselves, but should clarify which forms of coordination, verification, controlled data access, and privacy-preserving exchange should be enabled from a public welfare perspective (Zwede, Heeß, et al., 2026). P9's own diagnosis sharpens why this matters: much of the regulatory environment now in place was written for a centralized electricity system and, left unchanged, actively obstructs the decentralized solutions the energy transition requires, risking a lock-in into centralized digital architectures at the very time decentralized generation, storage, and flexibility are expressing the capabilities to reshape the energy system (Zwede, Heeß, et al., 2026). The measures that follow are derived for the German energy system but transfer to jurisdictions with comparable legislation, notably across Europe (Zwede, Heeß, et al., 2026).

This capability lens is the system-level restatement of the dissertation's trust shift. The capabilities P9 foregrounds – actor and asset identification and authorization, selective disclosure, auditable data sharing, claim verification, and maintenance of trustworthy records among actors that do not fully trust one another – are precisely the functions the embedded artifacts operationalize: digital identities and verifiable credentials instantiate the identification and authorization that P1 and P4 presuppose, distributed ledgers and shared fractionalized NFTs condition the auditable exchange within P6 and P7, and zero-knowledge proofs and self-sovereign identities enable the privacy-preserving claim verification of P6, P7, and P8 (Zwede, Heeß, et al., 2026). In doing so, these technologies can move the anchor of trust from central authorities toward auditable technology on the level of shared public infrastructure governance (Ahmad & Satrovic, 2023; Eaves et al., 2024; Jørgensen et al., 2017; OECD, 2024; Soeiro & Dias, 2020).

Four clusters of policy implications follow. P9 itself groups its seven measures around three underlying tensions – staying technology-neutral while still cultivating a diverse portfolio of technology options, rewriting rules that were written for a centralized grid and now obstruct decentralized alternatives, and choosing resilience over convenience in infrastructure design (Zwede, Heeß, et al., 2026). The clusters below regroup the same measures by policy domain instead, so that each remains visibly linked to the embedded paper whose design knowledge it puts to use; where this regrouping cuts across one of P9's tensions, the text says so.

The first cluster concerns digital infrastructure and standardization. Verifiable data sharing among decentralized actors presupposes interoperable infrastructures, reliable identity and access management, and standards under which data attributes and verification results can be interpreted across organizational boundaries. P9's corresponding measure is the buildup of a shared digital infrastructure – automating asset registration in registries comparable to the German Marktstam-

mdatenregister through digital identities, rolling out digital metering and scalable data flows between households and network operators, and standardizing data formats to raise the "data hygiene" on which downstream use cases depend (Zwede, Heeß, et al., 2026). This operationalizes P5's standards principle at system scale: without common schemas, accountable issuers, and reliable data sources, even a technically verifiable claim remains organizationally unusable (Babel et al., 2026). P9 treats this buildup as inseparable from the resilience argument taken up in the fourth cluster below: a shared digital infrastructure is a central prerequisite to the proposed concept of decentralization-for-resilience. This situates the dissertation's infrastructure argument within the broader notion of digital public infrastructure (DPI) – shared, secure, and interoperable digital systems, such as digital identity and data sharing ecosystems, provided in the public interest at societal scale (Eaves et al., 2024; OECD, 2024). The shared energy-data infrastructure this dissertation aims to contribute to can be read as a sectoral instance of DPI, and the resilience and digital-sovereignty rationale P9 invokes mirrors an argument central to the DPI literature: that publicly governed, interoperable infrastructure tends to be more resilient to lock-in and political-economic dependency than the proprietary, centralized alternatives it often replaces (Eaves et al., 2024).

The second cluster concerns responsible data use, privacy, and regulatory recognition. The dissertation's red thread does not lead to a recommendation for maximum transparency; excessive disclosure reproduces the loss-of-control risks that deter sharing in the first place. P9's measure here is the alignment of data-protection law with decentralized data ownership: instruments such as the GDPR were written for centralized data systems, and it is often unclear whether solutions built on digital identities are compliant, even though they typically afford stronger privacy than the centralized alternatives they replace (Zwede, Heeß, et al., 2026). Resolving this uncertainty is the institutional counterpart to P4's finding that perceived privacy and data protection are direct conditions of user acceptance (Guggenberger et al., 2023): unless selective-disclosure mechanisms such as those of P6, P7, and P8 are recognized in the relevant regulation as a compliant substitute for full disclosure, the very artifacts that reconcile verifiability with confidentiality remain institutionally blocked (Babel et al., 2022; Zwede, Mertel, et al., 2026; Zwede et al., 2025).

The third cluster concerns participation, incentives, and market design. Verifiable infrastructures become practically relevant only where decentralized actors have feasible and incentive-compatible use cases in which to apply them; if the costs of credential management, verification, or compliance exceed the benefits for smaller actors, such infrastructures reinforce participation asymmetries when they should reduce them. To that end, P9 proposes completing the transposition of the RED-II directive on energy communities into national law, enabling adequate electricity pricing that reflects the local grid state, and reforming network-tariff regulation so that operators' costs become recoverable (Zwede, Heeß, et al., 2026). These conditions are what make P8's architecture economically viable: a revocable delegation to a competitive aggregator reinforces a market design that keeps aggregators disciplined and non-collusive, and a redispatch mechanism for small-scale devices presupposes that grid-supporting behavior is remunerated (Zwede et al., 2025).

The fourth cluster concerns technology openness and resilience. Because future technological developments are unpredictable, P9's interviewees consistently favored regulation that stays open to evolving technologies over technology-specific subsidies that quickly become obsolete or even obstructive; the corresponding measures are diversified research funding matched to the heterogeneous readiness levels of emerging technologies, and the deliberate use of technologically open, yet adequate digital architectures that strengthen the resilience and sovereignty of critical energy infrastructure (Zwede, Heeß, et al., 2026). This again supports the notion of recent literature that treats openness, interoperability, and public-interest governance as the very properties that make shared infrastructure resilient and sovereign – properties a convenient, centralized path hampers. In the context of this dissertation, P9's fourth cluster is best read as a single infrastructural choice to enable openness and resilience in DPI (Eaves et al., 2024). This goal of openness and resilience is also consistent with the dissertation's own stance that technologies are to be assessed by the capability they provide, the assumptions they require, and the governance dependencies they introduce, because focusing on outcomes as opposed to technological headlines enables the design of entirely novel and elegant solutions that a technology-deterministic approach might not have developed.

Beyond these policy implications, the dissertation carries implications for research and practice. Its central pattern – treating trust not as something verification removes but as something verifiable design relocates – speaks directly to one of the research directions that Kotlarsky et al. (2023) set out for digital sustainability: the study of *digital sustainability ecosystems* and the governance question of how the heterogeneous actors that develop, deploy, and govern digital sustainability solutions engage, interact, and coordinate. The dissertation contributes an integrated account of how trust, control, risk, and value creation are jointly shaped among such actors in decentralized energy-data ecosystems, and specifies a concrete coordination mechanism – relocating trust vested in verifiable technology in place of the counterparties themselves.

For Green IS, the dissertation responds to two calls specifically. vom Brocke et al. (2013) urge the discipline to move beyond descriptive theory toward designed and evaluated solutions for societal sustainability challenges; the dissertation answers with artifact-grounded design knowledge describing, implementing, and evaluating concrete solutions for making sustainability claims verifiable. Watson et al. (2010) set the agenda of building information systems that render energy use and emissions attributable to specific actors, so that environmental costs can be assigned and acted upon; the dissertation responds to that agenda by supplying the element it leaves implicit – how such attribution is made credible and independently verifiable – and extends it by addressing a tension that typical granularity-maximizing visions of energy data sharing exhibit: that the fine-grained data required for attribution are frequently privacy- and confidentiality-sensitive. The Green IS contribution is a reframing of where value originates: not alone in making sustainability data available, but in also making sustainability claims credible and interpretable under privacy and control constraints, with digital verifiability supplying credibility where institutional reputation is insufficient or not scalable.

For Energy Informatics, it delivers evaluated design knowledge for three concrete coordination problems – flexibility provision, green-electricity labeling, and carbon-emission tracing – drawing upon and extending previous conceptual proposals (Goebel et al., 2014; Schmeck et al., 2022).

For practice, the findings are relevant to specific actors. Grid operators can improve the efficiency of integrating small-scale flexibility by leveraging verifiable data lineage in place of raw device data, using type-level prequalification of devices as the trust anchor and delegated, revocable credentials to preserve a competitive aggregator market – incidentally also reducing their own burden of managing privacy-sensitive personal data (Zwede et al., 2025). Aggregators gain a role that is economically defensible precisely because mediated sovereignty lets them add value without becoming a point of privacy loss or lock-in (Zwede et al., 2025). Certificate issuers, utilities, and supply-chain actors gain mechanism designs that make provenance and emission claims independently checkable without exposing the process data behind them (Babel et al., 2022, 2026; Zwede, Mertel, et al., 2026), an approach that has since been advanced to enable verifiable human-centric digital product passports by Babel, Guthmann, et al. (2025), demonstrating the generalizability of the underlying mechanisms beyond a single specific use case. Providers of consumer-facing verification and digital identity applications learn that artifact acceptance turns less on cryptographic sophistication than on comprehensibility, privacy assurance, and a sufficient breadth of use cases – properties that can be deliberately designed and institutionally supported to improve user adoption (Guggenberger et al., 2023), i.e. in the design of government-issued digital identities. And policymakers gain a capability lens that reframes the question from which technologies to fund to which coordination, verification, and privacy-preserving capabilities to enable (Zwede, Heeß, et al., 2026).

The dissertation develops design- and governance-oriented knowledge, but exhibits several limitations; it does not demonstrate broad adoption, production-grade scalability or security, or proven causal effects. Its design artifacts are prototype-grade: P5 alone offers expert-evaluated principles without practical implementation, and P6, P7, and P8 are proof-of-concept artifacts evaluated in laboratory and small field settings, with adoption, incentive design, and compensation left to future work (Babel et al., 2022, 2026; Zwede, Mertel, et al., 2026; Zwede et al., 2025). Additionally, the proposed solutions and principles presuppose that credible data enter them at the point of measurement; solving this oracle problem lies outside their scope by design and represents a stream of current and future research to solve. P9's policy implications are strongest for Germany and comparable European jurisdictions and should be transferred to others with corresponding care (Zwede, Heeß, et al., 2026). The knowledge was, moreover, first derived from specific use cases – for battery emission data, flexibility provision, green-electricity labeling, and emission-certificate tracing – and its generalization to further digital energy data sharing instances is argued through the shared structure of the sharing problem and not established for each individually or through a joint solution. However, none of these limitations endanger the central claim of this work: trust is not eliminated by digital verification; it is redistributed across mechanisms, infrastructures, organizations, and institutions – and the dissertation shows, concretely and repeatedly, how that redistribution can be designed to alleviate the burden for organizations and arrive at scalable solutions for verifiable and trustworthy digital energy data sharing.

The outlook that follows is an agenda for making data-driven coordination trustworthy, verifiable, privacy-preserving, and institutionally accountable under real-world conditions along the streams connected to this dissertation. The oracle problem – the join between cryptographic validity and real-world inputs – must be addressed through the development of adequate governance mechanisms and technologies such as signed metering and accountable issuance, since a proof about encoded inputs is only as meaningful as the process that produced them. The governance of issuers and verifiers, the usability of credentials and proofs for non-expert actors, and the treatment of verification results in markets and regulation all call for longitudinal and field implementation and iterative evaluation and improvement instead of further conceptual refinement. Above all, the dissertation's infrastructure knowledge should now be used to inform actual developments in decentralized digital energy systems. The decentralized redispatch architecture of P8 may educate Redispatch3.0 solutions currently under development in practice, and its remaining open questions – aggregator market design, compensation, and cross-implementation governance – are more likely to be resolved through iterative development on a running system than through continued theorizing in isolation (Zwede et al., 2025). Here, a capable implementation that operates today, even short of the academic optimum, is worth more to the energy transition than a perfect one deferred: each deployment cycle is likely to surface the incentive, usability, and governance frictions that laboratory evaluation cannot, and feeds them back into the design. Progress on decentralized, verifiable energy data sharing will now come from iterating between deployment and design, not from waiting for a perfect theoretical solution.

What began as a coordination problem in decentralized energy systems thus resolves into a design and governance challenge: not whether these systems should become more data-driven, but how their data-driven coordination can be made automated, trustworthy, and verifiable without forcing those who hold data into undue disclosure. The design-oriented knowledge developed across this dissertation is a step toward that end, and toward the decarbonization it is ultimately meant to serve. The following section clarifies how this cumulative contribution relates to the embedded papers and the research on which it builds.

4.2 Acknowledgement of Previous & Related Work

This section performs the necessary boundary work a cumulative dissertation requires. Due to its cumulative nature, the dissertation's contribution does not rest on the claim that its conceptual insights, empirical observations, design artifacts, verification mechanisms, or policy considerations originate in the mantle text. It rests on the transparent synthesis and positioning of nine embedded papers into a single argument about trustworthy and verifiable digital energy data sharing, while the paper-level contributions remain attributable to the respective papers and their co-author teams (Babel et al., 2022, 2026; Ehaus et al., 2026; Geist et al., 2026; Guggenberger et al., 2023; Zwede, Heeß, et al., 2026; Zwede, Mertel, et al., 2026; Zwede, Valett, et al., 2026; Zwede et al., 2025). The embedded papers are co-authored research outputs; the individual author contributions, and publication status are declared separately in the appendix.

The cumulative contribution is synthetic and positioning-oriented. It connects levels of analysis that the individual papers treat in isolation – interorganizational trust and control, verifiable data attributes, user acceptance, design principles, infrastructure design, governance roles, verification mechanisms, and supporting boundary conditions – into the red thread the dissertation develops: decentralization makes energy-system coordination data-dependent; this dependence produces a data-sharing dilemma; the dilemma is shaped by tensions between trust, control, privacy, and verifiability; and resolving these tensions requires socio-technical design knowledge that remains attentive to institutional embedding. The value of this synthesis lies in preserving each level as a clear contribution within a single integrated argument, while retaining the limits of its paper-level evidence – a division of labor that Table 4.1 makes explicit by stating, for each paper, what it contributes, how the dissertation uses it, and what it must not be read to prove.

Table 4.1: Contribution boundaries between the embedded papers and the dissertation-level synthesis.

Paper(s)	Paper-level contribution	Dissertation-level use
P1 (Ehaus et al., 2026)	Conceptualizes interorganizational trust, control, and perceived risk as technology-enabled data sovereignty in data platform ecosystems.	Grounds the trust–control logic and the relocation of trust from counterparties onto mediating technology.
P2/P3 (Geist et al., 2026; Zwede, Valett, et al., 2026)	Order fragmented ESG data by purpose-fit (P2) and highlight digitally verifiable carbon information outweighing third-party certification in consumer choice (P3).	Establish the data-attribute value driver: credibility and verification status, not mere availability.
P4 (Guggenberger et al., 2023)	Derives an SSI acceptance model in which comprehensibility and trust, not social influence, drive adoption.	Supplies the user-acceptance value driver for verifiable data-sharing applications.
P5 (Babel et al., 2026)	Derives design principles for emission-data sharing in battery value-chain data spaces.	Provides the requirements layer that reconciles confidentiality and verifiability by design.
P8 (Zwede et al., 2025)	Designs and prototypes the Trust Diamond and Decentralized Flexibility Provision Architecture with revocable delegation and zk-SNARK-enabled plausibility checks.	Provides the infrastructure layer in which delegation substitutes verifiable data lineage for trust in the intermediary.
P7/P6 (Babel et al., 2022; Zwede, Mertel, et al., 2026)	Build privacy-preserving, publicly verifiable mechanisms: zk-SNARKs for green-electricity labeling (P6) and shielded fractional NFTs for carbon-emission tracing (P7).	Provide the mechanism layer that makes specific claims checkable under selective disclosure.
P9 (Zwede, Heeß, et al., 2026)	Develops a capability-and-policy perspective on digital technologies for decentralized electricity systems.	Provides the governance layer, positioning technologies as capabilities rather than policy goals.

Beyond its embedded papers, the dissertation is located within a large body of existing knowledge and established research traditions that it builds on. Green IS and Energy Informatics inform its concern with information systems for environmentally sustainable development and with digital coordination in energy systems (Goebel et al., 2014; Schmeck et al., 2022; vom Brocke et al., 2013; Watson et al., 2010). Design Science Research informs its orientation toward artifact-centered development, design principles, and the positioning of design contributions (Gregor & Hevner,

2013; Gregor et al., 2020; Hevner et al., 2004; Peffers et al., 2007). Research on data spaces and data sovereignty informs its treatment of controlled interorganizational data sharing and ecosystem-level infrastructure (Jarke et al., 2019; Kotlarsky et al., 2023). This section does not revisit this literature; it acknowledges it and positions the dissertation's own contribution as their integration in the specific context of verifiable and trustworthy digital energy data sharing.

The dissertation should accordingly be read as a bounded synthesis of design-oriented knowledge in which technologies, artifacts, infrastructures, and policy measures each contribute a complementary, partial response to the data-sharing dilemma in digital energy systems and how to govern its intrinsic trade-offs. Across the embedded papers, verifiability takes several related but non-interchangeable senses – data-attribute credibility (P2, P3), user-facing demonstrability (P4), mechanism-level proof (P6, P7), infrastructure capability (P8), and policy-relevant coordination condition (P9). Trust, likewise, is not replaced by digital verification but redistributed across actors, infrastructures, mechanisms, and institutions toward the technical mechanisms and underlying infrastructures to reduce the need for bilateral trust between actors engaging in data sharing instances. Holding this boundary is what distinguishes the presented synthesis from mere technological solutionism and what keeps its contribution aligned with the research aim: design-oriented knowledge for trustworthy and verifiable data sharing under explicit privacy, control, and governance constraints.

The following part of the dissertation reproduces the embedded research papers on which this synthesis builds. They should be read as the paper-level foundations of the cumulative argument developed above: the mantle has positioned them within a shared dissertation logic, and the papers supply the conceptual, empirical, design-oriented, and policy-oriented detail that substantiates it.

Use of writing assistance *Please note that I have utilized various writing assistance software programs (e.g., ChatGPT, Claude, and DeepL) to enhance the language and readability of this work. The use of these tools was guided by ethical considerations and standards of academic integrity, in accordance with the guidelines of the Executive Committee of the Deutsche Forschungsgemeinschaft (DFG / German Research Foundation) on the influences of generative models of text and image creation on science and the humanities as well as on the DFG's funding activities. Nevertheless, I take full responsibility for its content and have thoroughly reviewed and edited the material as necessary.*

Bibliography

Abbas, A. E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., & de Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets*, *34*(20). https://doi.org/10.1007/s12525-024-00695-2

Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic Markets*, *32*(3), 1577–1602. https://doi.org/10.1007/s12525-022-00572-w

Ahmad, M., & Satrovic, E. (2023). How do fiscal policy, technological innovation, and economic openness expedite environmental sustainability? *Gondwana Research*, *124*, 143–164. https://doi.org/10.1016/j.gr.2023.07.006

Amprion, E-Bridge, E.ON, TenneT, & TransnetBW. (2024). Vorbereitung der pilotierung des komplementären marktbasierten engpassmanagements. https://www.transnetbw.de/%20_Resources/Persistent/1/f/7/6/1f76f3b163788f99a6e03d95e26e1526fdbd7a67/20240514_PKME_Abschlussbericht_final.pdfx

Atkinson, L., & Rosenthal, S. (2014). Signaling the green sell: The influence of eco-label source, argument specificity, and product involvement on consumer trust. *Journal of Advertising*, *43*(1), 33–45. https://doi.org/https://doi.org/10.1080/00913367.2013.834803

Babel, M., Gramlich, V., Guthmann, C., Schober, M., Körner, M.-F., & Strüker, J. (2023). Vertrauen durch digitale identifizierung: Über den beitrag von ssi zur integration von dezentralen oracles in informationssysteme. *HMD Praxis der Wirtschaftsinformatik*, *60*(2), 478–493. https://doi.org/10.1365/s40702-023-00955-3

Babel, M., Gramlich, V., Paetzold, F., & Zwede, T. (2024). On the energy consumption of a decentralized financial sector. In *Decentralization technologies: Financial sector in change* (pp. 247–263). Springer.

Babel, M., Guthmann, C., Körner, M.-F., Kranz, T., & Strüker, J. (2025). Human-centric digital product passports: Enabling verifiable information sharing for sustainable consumption through wallet-based identity management and zero-knowledge proofs. *Hawaii International Conference on System Sciences 2025*. https://doi.org/10.24251/HICSS.2025.527

Babel, M., & Sedlmeir, J. (2023). Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs. *arXiv preprint*. https://doi.org/10.48550/arXiv.2301.00823

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, *35*(1), 1–14. https://doi.org/10.1007/s12525-025-00772-0

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, 1020–1034.

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems*, *8*(4), 211–218. https://doi.org/10.17705/1jais.00126

Bhatia, P., Cummis, C., Brown, A., Draucker, L., Rich, D., & Lahd, H. (2011). *Greenhouse gas protocol: Product life cycle accounting and reporting standard*. World Resources Institute ; World Business Council for Sustainable Development.

Bogensperger, A., Bruckmeier, A., Sprunk, R., Paetzold, F., Förster, F., Babilon, L., & Adamski, I. (2025). Digitale identitäten als vertrauensanker im energiesystem. 03. mehrwerte für die energiewirtschaftlichen anwendungsfälle.

Boiral, O., & Heras-Saizarbitoria, I. (2020). Sustainability reporting assurance: Creating stakeholder accountability through hyperreality? *Journal of Cleaner Production*, *243*.

Brucker, A. D., & Yalman, S. (2022). Confidentiality Enhanced Life-Cycle Assessment. In A. Marrella & B. Weber (Eds.), *Business Process Management Workshops, Bpm 2021* (Vol. 436). Springer International Publishing Ag.

Bühler, F., Müller Holm, F., & Elmegaard, B. (2019). Potentials for the electrification of industrial processes in Denmark. *Proceedings of ECOS 2019: 32nd International Conference on Efficiency, Cost, Optimization, Simulation and Environmental Impact of Energy Systems*. https://orbit.dtu.dk/en/publications/potentials-for-the-electrification-of-industrial-processes-in-den

Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance—a multivocal approach. *Applied Sciences*, *11*(16), 7572. https://doi.org/10.3390/app11167572

Chua, C., Indulska, M., Lukyanenko, R., Maass, W., & Storey, V. C. (2022). Data management – MIS Quarterly research curations.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars. *MIS Quarterly*, *45*(4), 1863–1892. https://doi.org/10.25300/misq/2021/14165

Clark, S., Bleken, F. L., Stier, S., Flores, E., Andersen, C. W., Marcinek, M., Szczesna-Chrzan, A., Gaberscek, M., Palacin, M. R., Uhrin, M., & Friis, J. (2022). Toward a Unified Description of Battery Data. *Advanced Energy Materials*, *12*(17).

Darby, M. R., & Karni, E. (1973). Free competition and the optimal amount of fraud. *The Journal of law and economics*, *16*(1), 67–88.

Das, T. K., & Teng, B.-S. (2001). Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies*, *22*(2), 251–283. https://doi.org/10.1177/0170840601222004

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Doctoral dissertation, Sloan School of Management, Massachusetts Institute of Technology]. https://dspace.mit.edu/handle/1721.1/15192

De Soete, W. (2016). Towards a Multidisciplinary Approach on Creating Value: Sustainability through the Supply Chain and ERP Systems. *Systems*, *4*(1).

dena. (2020). Machine ID ledger. Retrieved July 31, 2021, from https://future-energy-lab.de/piloten/machine-id-ledger/

Dimodugno, M., Hallman, S., Plaisent, M., & Bernard, P. (2021). The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach. *Journal of Physics: Conference Series*, *2090*, 012017. https://doi.org/10.1088/1742-6596/2090/1/012017

Dyer, J. H., & Chu, W. (2003). The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the united states, japan, and korea. *Organization Science*, *14*(1), 57–68. https://doi.org/10.1287/orsc.14.1.57.12806

Eaves, D., Mazzucato, M., & Vasconcellos, B. (2024). Digital public infrastructure and public value: What is 'public' about DPI? (IIPP WP 2024-05). https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05

Edelenbos, J., & Eshuis, J. (2012). The interplay between trust and control in governance processes: A conceptual and empirical investigation. *Administration & Society*, *44*(6), 647–674. https://doi.org/10.1177/0095399711413876

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science*, *31*(2), 134–149. https://doi.org/10.1287/mnsc.31.2.134

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, *14*(1), 57–74. https://doi.org/10.2307/258191

European Commission. (2020a). ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council concerning batteries and waste batteries, repealing Directive 2006/66/ EC and amending Regulation (EU) No 2019/1020. (COM(2020) 798 final).

European Commission. (2020b). Powering a climate-neutral economy: An EU Strategy for Energy System Integration [COM(2020) 299 final, Brussels, Belgium].

European Commission. (2020c). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020.

European Commission. (2022). Digitalising the energy system – EU action plan [COM(2022) 552 final, Strasbourg, France].

European Commission. (2023). What data can we process and under which conditions?

European Commission: Directorate-General for Energy, Lise, W., Ansarin, M., de Haas, V., Bene, C., Gorenstein Dedecca, J., Henriquez, E., Krishnappa, H., Aslanoglou, M., Kavvadias, K., Capros, P., Altmann, M., Diehl, L., Lust, F., vom Scheidt, F., & Böszörmenyi, J. (2024). *Study on promoting energy system integration through the increased role of renewable electricity, decentralised assets and hydrogen: Final report*. Luxembourg, Publications Office of the European Union. https://doi.org/10.2833/560304

European Parliament and Council of the European Union. (2023). Regulation (eu) 2023/2854 of the european parliament and of the council of 13 december 2023 on harmonised rules on fair access to and use of data (data act) [Official Journal of the European Union, L 2023/2854, 22 December 2023].

Evans, J. S. B., & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. *Perspectives on psychological science*, *8*(3), 223–241.

Fassnacht, M., Benz, C., Heinz, D., Leimstoll, J., & Satzger, G. (2023). Barriers to data sharing among private sector organizations. In T. X. Bui (Ed.), *Proceedings of the 56th hawaii international conference on system sciences* (pp. 3695–3704). https://doi.org/10.24251/HICSS.2023.453

Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable cities and society*, *38*, 806–835. https://doi.org/10.1016/j.scs.2017.12.041

Fridgen, G., Keller, R., Körner, M.-F., & Schöpf, M. (2020). A holistic view on sector coupling. *Energy Policy*, *147*. https://doi.org/10.1016/j.enpol.2020.111913

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, *13*(2), 159–190. https://doi.org/10.1046/j.1365-2575.2003.00146.x

Garg, S., Goel, A., Jain, A., Policharla, G., & Sekar, S. (2023). Zksaas: Zero-knowledge snarks as a service. *32nd USENIX Security Symposium*. https://eprint.iacr.org/2023/905

Gebhardt, M., Beck, J., Kopyto, M., & Spieske, A. (2022). Determining requirements and challenges for a sustainable and circular electric vehicle battery supply chain: A mixed-methods approach. *Sustainable Production and Consumption*, *33*.

Gelhaar, J., Bergmann, N., Müller, P., & Dogan, R. (2023). Motives and Incentives for Data Sharing in Industrial Data Ecosystems: An Explorative Single Case Study. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Gelhaar, J., Groß, T., & Otto, B. (2021). A Taxonomy for Data Ecosystems. *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Gelhaar, J., & Otto, B. (2020). Challenges in the emergence of data ecosystems. In K. K. Wei, W. W. Huang, J. K. Lee, D. Xu, J. J. Jiang, & H. Kim (Eds.), *Proceedings of the 23rd pacific asia conference on information systems* (pp. 1–14). https://aisel.aisnet.org/pacis2020/175/

Goebel, C., Jacobsen, H.-A., Del Razo, V., Doblander, C., Rivera, J., Ilg, J., Flath, C., Schmeck, H., Weinhardt, C., Pathmaperuma, D., et al. (2014). Energy informatics. *Business & Information Systems Engineering*, *6*(1), 25–31.

Goedeking, N., & Meckling, J. (2024). Coordinating the energy transition: Electrifying transportation in California and Germany. *Energy Policy*, *195*, 114321. https://doi.org/10.1016/j.enpol.2024.114321

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, *18*(1), 186–208. https://doi.org/10.1145/22145.2217

Gossen, T., Guggenberger, T., Fechtelhoff, M., Hauffe, S., Huber, H., Ismer, R., Jackl, Q., Knipschild, A., Krebs, R., Kühne, D., Maier, C., Meßerschmidt, K., Urbach, N., Völter, F., Wischrop, G., & Zehetmeir, S. (2022). Nessi - nachweisplattform elster self-sovereign identities. https://www.finanzamt.bayern.de/Informationen/Aktuelles/White_Paper_NESSI.pdf

Gramlich, V., Körner, M.-F., Michaelis, A., & Strüker, J. (2023). SSI in the energy sector : A study. *Fraunhofer Institute for Applied Information Technology FIT, Elia Group*.

Gramlich, V., Principato, M., Schellinger, B., Sedlmeir, J., Amend, J., Stramm, J., Zwede, T., Strüker, J., & Urbach, N. (2022). Decentralized finance (defi): Foundations, applications, potentials, and challenges. *Applications, Potentials, and Challenges (July 2022)*.

Gregor, S., Chandra Kruse, L., & Seidel, S. (2020). Research perspectives: The anatomy of a design principle. *Journal of the Association for Information Systems*, *21*(6). https://doi.org/10.17705/1jais.00649

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*.

Groth, J. (2016). On the size of pairing-based non-interactive arguments. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 305–326.

Grover, V., & Kohli, R. (2012). Cocreating it value: New capabilities and metrics for multifirm environments. *Mis Quarterly*.

Haki, K., Blaschke, M., Aier, S., & Winter, R. (2019). A value co-creation perspective on information systems analysis and design. *Business & information systems engineering*, *61*.

Heess, P., Holly, S., Körner, M.-F., Nieße, A., Radtke, M., Schick, L., Stark, S., Strüker, J., & Zwede, T. (2025). A multi-agent approach with verifiable and data-sovereign information flows for decentralizing redispatch in distributed energy systems. *Energy Informatics*, *8*(1), 24.

Heiss, J., Oegel, T., Shakeri, M., & Tai, S. (2023). Verifiable carbon accounting in supply chains. *IEEE Transactions on Services Computing*, *17*(4), 1861–1874.

Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. *Logistics*, *5*(3).

Hellmeier, M., & von Scherenberg, F. (2023). A delimitation of data sovereignty from digital and technological sovereignty. In M. Aanestad, S. Klein, M. Tarafdar, S. Han, S. Laumer, & I. Ramos (Eds.), *Proceedings of the 31st european conference on information systems* (pp. 1–19).

Helms, H., Kämper, C., Biemann, K., Lambrecht, U., Jöhrens, J., & Meyer, K. (2019). *Klimabilanz von Elektroautos* (tech. rep.). Agora Verkehrswende.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hinterstocker, M., Schott, P., & von Roon, S. (2017). Disaggregation of household load profiles. *Internationale Energiewirtschaftstagung, Vienna*, 1–11.

Hirth, L., & Glismann, S. (2018). *Congestion management: From physics to regulatory instruments* (tech. rep.). Kiel, Hamburg, ZBW – Leibniz Information Centre for Economics.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Ibbott, C. J., & O'Keefe, R. M. (2004). Trust, planning and benefits in a global interorganizational system. *Information Systems Journal*, *14*(2), 131–152. https://doi.org/10.1111/j.1365-2575.2004.00167.x

iden3. (2025). Snarkjs [GitHub repository. JavaScript/CLI toolkit for zkSNARKs. Accessed: 2025-08-24].

Ixmeier, A., Wagner, F., & Kranz, J. (2024). Leveraging information systems for environmental sustainability and business value. *MIS Quarterly Executive*, 57–75. https://doi.org/10.17705/2msqe.00090

Jaeger, F. A., Saling, P., Otte, N., Steidle, R., Bollen, J., Golembiewski, B., Dencic, I., Letinois, U., Rehl, T., & Wunderlich, J. (2022). Challenges and requirements of exchanging Product Carbon Footprint information in the supply chain. In S. Albrecht, M. Fischer, C. Scagnetti, M. Barkmeyer, & A. Braune (Eds.), *E3S Web of Conferences* (Vol. 349).

Jarke, M., Otto, B., & Ram, S. (2019). Data sovereignty and data space ecosystems. *Business & Information Systems Engineering*, *61*(5), 549–550. https://doi.org/10.1007/s12599-019-00614-2

Jørgensen, M. S., Jørgensen, U., & Jensen, J. S. (2017). Navigations and governance in the Danish energy transition reflecting changing Arenas of Development, controversies and policy mixes. *Energy Research & Social Science*, *33*, 173–185. https://doi.org/10.1016/j.erss.2017.09.034

Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023). Data Sharing Fundamentals: Definition and Characteristics. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Kaplan, R. S., & Ramanna, K. (2021). Accounting for Climate Change. *Harvard Business Review*.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1).

Kiemel, S., Rietdorf, C., Schutzbach, M., & Miehe, R. (2022). How to Simplify Life Cycle Assessment for Industrial Applications—A Comprehensive Review. *Sustainability*, *14*(23).

Kim, H. C., Wallington, T. J., Arsenault, R., Bae, C., Ahn, S., & Lee, J. (2016). Cradle-to-Gate Emissions from a Commercial Electric Vehicle Li-Ion Battery: A Comparative Analysis. *Environ. Sci. Technol.*, *50*(14).

Kindervag, J., et al. (2010). Build security into your network's dna: The zero trust network architecture. *Forrester Research Inc*, *27*, 1–16.

Kirsch, L. S. (1997). Portfolios of control modes and is project management. *Information Systems Research*, *8*(3), 215–317. https://doi.org/10.1287/isre.8.3.215

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Körner, M.-F., Nolting, L., Babel, M., Ehaus, M., Heeß, P., Lautenschlager, J., Radtke, M., Schick, L., Strüker, J., Wiedemann, S., et al. (2025). A digital infrastructure for integrating decentralized assets into redispatch. decentralized redispatch (deer): Interfaces for providing flexibility.

Körner, M.-F., Nolting, L., Babel, M., Ehaus, M., Heeß, P., Lautenschlager, J., Radtke, M., Schick, L., Strüker, J., Wiedemann, S., & Zwede, T. (2024). A digital infrastructure for integrating decentralized asstes into redispatch. *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik*, 1–22. https://doi.org/10.15495/EPub_UBT_00008184

Körner, M.-F., Sedlmeir, J., Weibelzahl, M., Fridgen, G., Heine, M., & Neumann, C. (2022). Systemic risks in electricity systems: A perspective on the potential of digital technologies. *Energy Policy*, *164*, 112901. https://doi.org/10.1016/j.enpol.2022.112901

Kotlarsky, J., Oshri, I., & Sekulic, N. (2023). Digital sustainability in information systems research: Conceptual foundations and future directions. *Journal of the Association for Information Systems*, *24*(4).

Krasikov, P., & Legner, C. (2023). Introducing a data perspective to sustainability: How companies develop data sourcing practices for sustainability initiatives. *Communications of the Association for Information Systems*, *53*(1).

Kundisch, D., Muntermann, J., Oberländer, A. M., Rau, D., Röglinger, M., Schoormann, T., & Szopinski, D. (2021). An update for taxonomy designers: Methodological guidance from information systems research. *Business & Information Systems Engineering*, 1–19. https://doi.org/10.1007/s12599-021-00723-x

Lacity, M., & Carmel, E. (2022). Implementing self-sovereign identity (ssi) for a digital staff passport at uk nhs. *University of Arkansas*.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? a study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

Lin, X., Li, X., Kulkarni, S., & Zhao, F. (2021). The Application of Blockchain-Based Life Cycle Assessment on an Industrial Supply Chain. *Sustainability*, *13*(23).

Lind, L., Cossent, R., Chaves-Ávila, J. P., & Gómez San Román, T. (2019). Transmission and distribution coordination in power systems with high shares of distributed energy resources providing balancing and congestion management services. *Wiley Interdisciplinary Reviews: Energy and Environment*, *8*(6), e357. https://doi.org/10.1002/wene.357

Loschan, C., Schwabeneder, D., Lettner, G., & Auer, H. (2023). Flexibility potential of aggregated electric vehicle fleets to reduce transmission congestions and redispatch needs: A case study in austria. *International Journal of Electrical Power & Energy Systems*, *146*, 108802. https://doi.org/10.1016/j.ijepes.2022.108802

Maldet, M., Schwabeneder, D., Lettner, G., Loschan, C., Corinaldesi, C., & Auer, H. (2024). Local sustainable communities: Sector coupling and community optimization in decentralized energy systems. *Cleaner Energy Systems*, *7*, 100106. https://doi.org/10.1016/j.cles.2023.100106

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

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), 1–25. https://doi.org/10.1145/1985347.1985353

Meckling, W. H., & Jensen, M. C. (1976). Theory of the firm. *Managerial Behavior, Agency Costs and Ownership Structure*. https://doi.org/10.1007/978-94-009-9257-3_8

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*. Springer International Publishing.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Müller, F., Hofmann, P., Strüker, J., Leinauer, C., & Körner, M.-F. (2023). Digital Decarbonization: Design Principles for an Enterprise-wide Emissions Data Architecture. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Nischak, F., Hanelt, A., & Kolbe, L. M. (2017). Unraveling the interaction of information systems and ecosystems-a comprehensive classification of literature. In Y. J. Kim, R. Agarwal, & J. K. Lee (Eds.), *Proceedings of the 38th international conference on information systems* (pp. 1–21). https://aisel.aisnet.org/icis2017/General/Presentations/20

OECD. (2024). Digital public infrastructure for digital governments. (68). https://doi.org/10.1787/ff525dc8-en

Oliveira, M. I. d. S., Barros Lima, G. d. F., & Farias Lóscio, B. (2019). Investigations into data ecosystems: A systematic mapping study. *Knowledge and Information Systems*, *61*, 589–630. https://doi.org/10.1007/s10115-018-1323-6

Oliveira, M. I. d. S., Oliveira, L. E. R. A., Batista, M. G. R., & Lóscio, B. F. (2018). Towards a metamodel for data ecosystems. In M. Janssen, S. A. Chun, & V. Weerakkody (Eds.), *Proceedings of the 19th annual international conference on digital government research: Governance in the data age* (pp. 1–10). https://doi.org/10.1145/3209281.3209333

Otto, B. (2022). The Evolution of Data Spaces. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces*. Springer International Publishing.

Patchell, J. (2018). Can the implications of the GHG Protocol's scope 3 standard be realized? *Journal of Cleaner Production*, *185*.

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Peiseler, L., Bauer, C., Beuse, M., Wood, V., & Schmidt, T. S. (2022). Toward a European carbon footprint rule for batteries. *Science*, *377*(6613).

Perego, P., & Kolk, A. (2012). Multinationals' accountability on sustainability: The evolution of third-party assurance of sustainability reports. *Journal of business ethics*, *110*.

Perrini, F., Castaldo, S., Misani, N., & Tencati, A. (2010). The impact of corporate social responsibility associations on trust in organic products marketed by mainstream retailers: A

study of italian consumers. *Business Strategy and the Environment*, *19*(8), 512–526. https://doi.org/10.1002/bse.660

Pettenpohl, H., Spiekermann, M., & Both, J. R. (2022). International Data Spaces in a Nutshell. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces*. Springer International Publishing.

Piccoli, G., & Ives, B. (2003). Trust and the unintended effects of behavior control in virtual teams. *MIS Quarterly*, *27*(3), 365–395. https://doi.org/10.2307/30036538

Piétron, D., Stenzel, A., & Teuber, A. (2023). *Designing Digital Product Passports. A Data Commons Approach for a More Sustainable Economy* (tech. rep.). Einstein Center Digital Future, SINE Foundation, Systemiq.

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials* (1st ed.). Manning Publications.

Priesmann, J., Nolting, L., Kockel, C., & Praktiknjo, A. (2021). Time series of useful energy consumption patterns for energy system modeling. *Scientific Data*, *8*(1), 148. https://doi.org/10.1038/s41597-021-00907-w

Principato, M., Babel, M., Guggenberger, T., Kropp, J., & Mertel, S. (2023). Towards solving the blockchain trilemma: An exploration of zero-knowledge proofs. *International Conference on Information Systems*. https://aisel.aisnet.org/icis2023/blockchain/blockchain/5/

Püchel, L., Wang, C., Buhmann, K., Brandt, T., von Schweinitz, F., Edinger-Schons, L. M., vom Brocke, J., Legner, C., Teracino, E., & Mardahl, T. D. (2024). On the pivotal role of data in sustainability transformations. *Business & Information Systems Engineering*, *66*(6), 831–848. https://doi.org/10.1007/s12599-024-00904-4

Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, *6*(1), 3. https://doi.org/10.1038/s41562-021-01243-0

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 1–52.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Samardzic, N., Langowski, S., Devadas, S., & Sanchez, D. (2024). Accelerating zero-knowledge proofs through hardware-algorithm co-design. *Proceedings of the 57th IEEE/ACM International Symposium on Microarchitecture (MICRO)*. https://doi.org/10.1109/MICRO61859.2024.00035

Samuel, J., Kashyap, R., Samuel, Y., & Pelaez, A. (2022). Adaptive cognitive fit: Artificial intelligence augmented management of information facets and representations. *International Journal of Information Management*, *65*, 102505. https://doi.org/10.1016/j.ijinfomgt.2022.102505

Schleimer, A. M., Jahnke, N., & Otto, B. (2023). Architecture Design Options for Federated Data Spaces. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Schmeck, H., Monti, A., & Hagenmeyer, V. (2022). Energy informatics: Key elements for tomorrow's energy system. *Communications of the ACM*, *65*(4), 58–63.

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, *63*(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y

Sedlmeir, J., Völter, F., & Strüker, J. (2021). The next stage of green electricity labeling: Using zero-knowledge proofs for blockchain-based certificates of origin and use. *ACM SIGENERGY Energy Informatics Reviev*, *1*(1), 20–31. https://doi.org/10.1145/3508467.3508470

Seidel, S., Recker, J., & vom Brocke, J. (2013). Sensemaking and sustainable practicing: Functional affordances of information systems in green transformations. *MIS quarterly*.

Sica, D., Esposito, B., Malandrino, O., & Supino, S. (2022). The role of digital technologies for the LCA empowerment towards circular economy goals: A scenario analysis for the agri-food system. *Int J Life Cycle Assess*.

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, *69*(1), 99–118. https://doi.org/10.2307/1884852

Soeiro, S., & Dias, M. F. (2020). Renewable energy community and the European energy market: main motivations. *Heliyon*, *6*(7). https://doi.org/10.1016/j.heliyon.2020.e04511

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. https://doi.org/10.1057/ejis.2015.17

Spence, M. (1973). Job market signaling. In *Uncertainty in economics* (pp. 281–306). Academic Press. https://doi.org/10.1016/B978-0-12-214850-7.50025-5

Stampatori, D., Raimondi, P. P., & Noussan, M. (2020). Li-Ion Batteries: A Review of a Key Technology for Transport Decarbonization. *Energies*, *13*(10).

Stenzel, A., & Waichman, I. (2023). Supply-chain data sharing for scope 3 emissions. *npj Clim. Action*, *2*(1).

Ströher, T., Körner, M.-F., Paetzold, F., & Strüker, J. (2025). Bridging carbon data's organizational boundaries: Toward automated data sharing in sustainable supply chains. *Electronic Markets*, *35*(1), 1–22. https://doi.org/10.1007/s12525-025-00779-7

Strüker, J., Reichert, S., & Brenig, C. (2013). Inter-organizational demand response applications: How to address moral hazard in smart grids. *Proceedings of the Nineteenth Americas Conference on Information Systems*, 15–17.

Thomaßen, G., Kavvadias, K., & Jiménez Navarro, J. P. (2021). The decarbonisation of the EU heating sector through electrification: A parametric analysis. *Energy Policy*, *148*, 111929. https://doi.org/10.1016/j.enpol.2020.111929

Tobin, A., & Reed, D. (2017). *The inevitable rise of self-sovereign identity: A white paper from the sovrin foundation* (T. S. Foundation, Ed.). Retrieved March 30, 2024, from https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Treiblmaier, H., & Garaus, M. (2023). Using blockchain to signal quality in the food supply chain: The impact on consumer purchase intentions and the moderating effect of brand

familiarity. *International Journal of Information Management*, *68*, 102514. https://doi.org/10.1016/j.ijinfomgt.2022.102514

Van den Broek, T., & van Veenstra, A. F. (2015). Modes of governance in inter-organizational data collaborations. In J. Becker, J. vom Brocke, & M. de Marco (Eds.), *Proceedings of the 23rd European Conference on Information Systems*. https://doi.org/10.18151/7217509

Venable, J., Pries-Heje, J., & Baskerville, R. (2014). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1).

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Vogelsang, K., Steinhüser, M., & Hoppe, U. (2013). A qualitative approach to examine technology acceptance. *Proceedings of the International Conference on Information Systems*. https://aisel.aisnet.org/icis2013/proceedings/ResearchMethods/9

Völter, F., Urbach, N., & Padget, J. (2023). Trusting the trust machine: Evaluating trust signals of blockchain applications. *International Journal of Information Management*, *68*, 102429. https://doi.org/10.1016/j.ijinfomgt.2022.102429

vom Brocke, J., Watson, R. T., Dwyer, C., Elliot, S., & Melville, N. (2013). Green information systems: Directives for the IS discipline. *Communications of the association for information systems*, *33*(1), 30.

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets*, *34*(15), 1–11. https://doi.org/10.1007/s12525-024-00693-4

Wang, J., Teracino, E., & Legner, C. (2025). From puzzle pieces to principles for sustainability reporting and disclosure: A design theory. *Proceedings of the 46th International Conference on Information Systems*.

Watson, R. T., Boudreau, M.-C., & Chen, A. J. (2010). Information systems and environmentally sustainable development: Energy informatics and new directions for the is community. *MIS Quarterly*, *34*(1), 23–38. https://doi.org/10.2307/20721413

Xue, Y., & Wang, J. (2022). Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. *Security and Communication Networks*, *2022*, 1–12. https://doi.org/10.1155/2022/5842371

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science*, *9*(2), 141–159. https://doi.org/10.1287/orsc.9.2.141

A Overview of Research Papers

A.1 Research Papers Included in This Dissertation

Research Paper P1: The Impact of Technology-Enabled Data Sovereignty on Trust and Control in Data Platform Ecosystems

Ehaus, M., Zwede, T., Körner, M.-F., & Strüker, J. (2026). The Impact of Technology-Enabled Data Sovereignty on Trust and Control in Data Platform Ecosystems. submitted to *Outlet hidden due to the double-blind review process* (VHB-JQ3[1]: A, VHB-JQ4[2]: A)

Research Paper P2: From Fragments to Conceptual Clarity: A Taxonomy for Effective ESG Data Management

Zwede, T., Valett, L., Körner, M.-F., Schneider, M., & Strüker, J. (2026). From Fragments to Conceptual Clarity: A Taxonomy for Effective ESG Data Management. submitted to *Outlet hidden due to the double-blind review process* (VHB-JQ3: A, VHB-JQ4: A)

Research Paper P3: From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour

Geist, A., Körner, M.-F., Strüker, J., Valett, L., & Zwede, T. (2026). From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour. *Thirty-Fourth European Conference on Information Systems (ECIS), Milan, Italy* (VHB-JQ3: B, VHB-JQ4: A)

Research Paper P4: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications

Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6560–6569 (VHB-JQ3: C, VHB-JQ4: B)

Research Paper P5: Data Spaces for Battery Value Chains: Uncovering Design Principles for Emission Data Sharing

Babel, M., Handke, M., Körner, M.-F., Strüker, J., & Zwede, T. (2026). Data Spaces for Battery Value Chains: Uncovering Design Principles for Emission Data Sharing. In preparation for resubmission to *Outlet hidden due to the double-blind review process* (VHB-JQ3: B, VHB-JQ4: B, SJR[3]: Q1)

Research Paper P6: Designing Practical Blockchain-Based Green Electricity Labeling With Succinct Non-Interactive Zero-Knowledge Proofs

Zwede, T., Mertel, S., Rieger, A., Strüker, J., & Schönrich, J. (2026). Designing Practical Blockchain-Based Green Electricity Labeling With Succinct Non-Interactive Zero-Knowledge Proofs. Submit-

[1]VHB-JQ3: VHB-JOURQUAL3
[2]VHB-JQ4: VHB Publication Media Rating 2024
[3]SJR: Scimago Journal & Country Rank, 2026

ted to *Outlet hidden due to the double-blind review process* (VHB-JQ3: B, VHB-JQ4: B, SJR: Q1, IF[4]: 7.5)

Research Paper P7: Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs
Babel, M., Gramlich, V., Körner, M.-F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs. *Energy Informatics* (VHB-JQ4: C, SJR: Q2)

Research Paper P8: Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision
Zwede, T., Ehaus, M., Babel, M., Heeß, P., Schick, L., Körner, M.-F., & Strüker, J. (2025). Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision. *Energy Informatics*, *8*(1), 143 (VHB-JQ4: C, SJR: Q2)

Research Paper P9: Governing Digital Technologies in Decentralized Energy Systems: A Qualitative Assessment of Capabilities and Policy Implications
Zwede, T., Heeß, P., Körner, M.-F., Parak, D., Schubert, A., & Strüker, J. (2026). Governing Digital Technologies in Decentralized Energy Systems: A Qualitative Assessment of Capabilities and Policy Implications. Submitted to *Outlet hidden due to the double-blind review process* (VHB-JQ3: B, VHB-JQ4: B, SJR: Q1, IF: 9.3)

A.2 Index of Further Papers

Over the course of the dissertation, I also authored and co-authored the following research papers, studies, and reports. These papers are not part of this dissertation.

Gramlich, V., Principato, M., Schellinger, B., Sedlmeir, J., Amend, J., Stramm, J., Zwede, T., Strüker, J., & Urbach, N. (2022). Decentralized finance (defi): Foundations, applications, potentials, and challenges. *Applications, Potentials, and Challenges (July 2022)*

Heess, P., Holly, S., Körner, M.-F., Nieße, A., Radtke, M., Schick, L., Stark, S., Strüker, J., & Zwede, T. (2025). A multi-agent approach with verifiable and data-sovereign information flows for decentralizing redispatch in distributed energy systems. *Energy Informatics*, *8*(1), 24

Körner, M.-F., Nolting, L., Babel, M., Ehaus, M., Heeß, P., Lautenschlager, J., Radtke, M., Schick, L., Strüker, J., Wiedemann, S., et al. (2025). A digital infrastructure for integrating decentralized assets into redispatch. decentralized redispatch (deer): Interfaces for providing flexibility

Babel, M., Gramlich, V., Paetzold, F., & Zwede, T. (2024). On the energy consumption of a decentralized financial sector. In *Decentralization technologies: Financial sector in change* (pp. 247–263). Springer

[4]IF: Impact Factor, 2026

A.3 Individual Contribution to the Included Research Papers

This cumulative dissertation comprises nine research papers, all co-authored with multiple collaborators. This section details the context and outlines my contributions to these papers.

Research Paper P1 entitled "The Impact of Technology-Enabled Data Sovereignty on Trust and Control in Data Platform Ecosystems" (Ehaus et al., 2026, Section B.1) was written by a team of four authors. Together with one co-author, I served as one of the two lead authors of this paper. We jointly developed the conceptual design and the methodological approach, and administered the project. We were both also involved in reviewing and editing the manuscript. The remaining co-authors contributed to the conceptualization, the methodological approach, provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

Research Paper P2 entitled "From Fragments to Conceptual Clarity: A Taxonomy for Effective ESG Data Management" (Zwede, Valett, et al., 2026, Section B.2) was written by a team of five authors. Together with one co-author, I served as one of the two lead authors of this paper. We jointly developed the conceptual design and the methodological approach, conducted the data analysis, wrote the original draft of the manuscript, created the visualizations, and administered the project. We were both also involved in reviewing and editing the manuscript. The remaining co-authors contributed to the conceptualization, the methodological approach, and the formal analysis, provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

Research Paper P3 entitled "From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour" (Geist et al., 2026, Section B.3) was written by a team of five authors. I contributed to this paper in a supervisory capacity. My involvement included supporting the establishment of the research idea, providing continuous feedback on the manuscript throughout the research process, and assisting in the writing of the paper. One of the co-authors was responsible for the primary execution of the research, including the conceptualization, survey development, and the drafting of the manuscript. The remaining co-authors provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

Research Paper P4 entitled "Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications" (Guggenberger et al., 2023, Section B.4) was written by a team of five authors. I contributed to this paper in a reviewing and editing capacity. The involvement of myself and another co-author included providing continuous feedback on the manuscript throughout the research process and assisting in the writing, reviewing and editing of the paper. One of the co-authors was responsible for the primary execution of the research, including the conceptualization, survey development, and the drafting of the manuscript. The remaining co-authors provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

Research Paper P5 entitled "Data Spaces for Battery Value Chains: Uncovering Design Principles for Emission Data Sharing" (Babel et al., 2026, Section B.5) was written by a team of five authors.

Together with two co-authors, I served as one of the three equal authors of this paper. We jointly developed the conceptual design and the methodological approach, and administered the project. We were also involved in writing, reviewing and editing the manuscript. The third equal co-author was additionally involved in data acquisition. The remaining co-authors contributed to the conceptualization, the methodological approach, provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

Research Paper P6 entitled "Designing Practical Blockchain-Based Green Electricity Labeling With Succinct Non-Interactive Zero-Knowledge Proofs" (Zwede, Mertel, et al., 2026, Section B.6) was written by a team of five authors. Together with one co-author, I served as one of the two lead authors of this paper. We jointly developed the methodological approach, conducted the data analysis, wrote the original draft of the manuscript, and created the visualizations. I was also involved in reviewing and editing the manuscript. The remaining co-authors contributed to the conceptualization and, in part, the methodological approach, provided supervision throughout the research process, administered the project, acquired funding, and were involved in reviewing and editing the manuscript.

Research Paper P7 entitled "Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs" (Babel et al., 2022, Section B.7) was written by a team of six authors. Together with three co-authors, I contributed equally to the conceptualization, drafting, and reviewing and editing of the manuscript. The other co-authors contributed through supervision and reviewing and editing of the manuscript.

Research Paper P8 entitled "Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision" (Zwede et al., 2025, Section B.8) was written by a team of seven authors. I served as the lead author of this paper, extending a previous publication, with significant support from two co-authors. Together, we developed the conceptual design and the methodological approach, conducted the investigation, and wrote the original draft of the manuscript. My two supporting co-authors were also involved in the software development, and we were all involved in reviewing and editing the manuscript. I additionally created the visualizations, administered the project, and acquired funding. Two further co-authors contributed to the conceptualization, the methodological approach, and the investigation, contributed to the original draft, and were involved in reviewing and editing the manuscript. The remaining co-authors contributed to the conceptualization and the methodological approach, provided supervision throughout the research process, administered the project, acquired funding, and were involved in reviewing and editing the manuscript.

Research Paper P9 entitled "Governing Digital Technologies in Decentralized Energy Systems: A Qualitative Assessment of Capabilities and Policy Implications" (Zwede, Heeß, et al., 2026, Section B.9) was written by a team of six authors. I served as the lead author of this paper. I contributed to the conceptualization, the methodological approach, and the formal analysis, created the visualizations, provided supervision throughout the research process, and was involved in reviewing and editing the manuscript. Two co-authors were responsible for the data curation, created the visualizations, and wrote parts of the original draft of the manuscript. The remaining

co-authors contributed to the conceptualization and, in part, the methodological approach, provided supervision throughout the research process, and were involved in reviewing and editing the manuscript.

B Research Papers

B.1 Research Paper P1: The Impact of Technology-Enabled Data Sovereignty on Trust and Control in Data Platform Ecosystems

Authors:
M. Ehaus, T. Zwede, M.-F. Körner, and J. Strüker

Submitted to:
Outlet hidden due to the double-blind review process

Extended Abstract[1]:
Interorganizational data sharing enables organizations to improve coordination, develop new services, and create value across organizational boundaries. However, concerns about opportunistic data use, unintended knowledge spillovers, and loss of control continue to impede participation in data platform ecosystems (Fassnacht et al., 2023). Data sovereignty promises to address this tension by allowing organizations to share data with relevant stakeholders while retaining control over their access and use (von Scherenberg et al., 2024). Although emerging data spaces seek to operationalize this approach through technological infrastructures and governance mechanisms, its effects on organizational data-sharing decisions remain insufficiently understood. Established research identifies trust, control, and perceived risk as central determinants of interorganizational collaboration (Das & Teng, 2001; Gallivan & Depledge, 2003), yet offers limited explanation of how technology-enabled data sovereignty reshapes their interplay. This study addresses this gap by developing a conceptual model explaining how technology-enabled data sovereignty shapes trust, control, and perceived risk in interorganizational data sharing within decentralized data platform ecosystems. Following a grounded theory approach (Webster & Watson, 2002; Wolfswinkel et al., 2013), the study combines a review of two focused literature streams with practice-oriented publications from five data sovereignty initiatives: GAIA-X, the International Data Spaces Association, ID-Ideal, NESSI, and DEER. The first stream yielded 22 relevant articles on trust and interorganizational data sharing, supplemented by five publications identified through backward searching. The second stream contributed 14 publications on technology-enabled data sovereignty. Together with 15 practice-oriented documents, the final corpus comprised 56 publications. Open, axial, and selective coding of approximately 600 text passages supported the iterative identification of constructs and relationships as the dataset for theory development. From this dataset, we develop a model that comprises seven core constructs: Technology-enabled Data Sovereignty, Control, Trust between Organizations, Trust in Technology, Perceived Risk, Data Sharing, and Value. Technology-enabled data sovereignty is conceptualized as a socio-technical arrangement in which

[1] At the time of writing, this research paper is under review for acceptance at an academic conference. Therefore, an extended abstract is provided here.

governance structures and digital technologies jointly enable organizations to define, constrain, and verify data access and use across organizational boundaries. Privacy-enhancing technologies, including secure multi-party computation, zero-knowledge proofs, and self-sovereign identity, provide mechanisms for controlled computation, selective disclosure, and verification (Agahari et al., 2022; Xue & Wang, 2022). The model proposes that these arrangements enable control, which helps reduce perceived risk and supports organizations' willingness to share data. Data sharing, in turn, creates opportunities for improved processes, new services, and joint value creation. A central insight is that technology-enabled data sovereignty may shift the focus of trust. Enforceable and verifiable control mechanisms can partially substitute for reliance on positive expectations about the intentions of other organizations, which is particularly relevant in dynamic ecosystems where participants lack established relationships. At the same time, reliance on these mechanisms increases the importance of trust in the technological infrastructure and its governance (Li et al., 2008; Söllner et al., 2016). Trust is therefore redistributed rather than eliminated. This distinction extends the discussion of whether trust and control act as substitutes or complements (Gallivan & Depledge, 2003): technology-enabled control can reduce the need for interorganizational trust while making trust in technology more consequential. Together, control and these differentiated trust relationships shape perceived risk and the conditions for data sharing. The study contributes to Information Systems research in three ways. First, it provides a mechanism-based explanation of how socio-technical arrangements can mitigate barriers to interorganizational data sharing. Second, it refines understanding of trust and control by distinguishing reduced reliance on interorganizational trust from increased reliance on technological infrastructures. Third, it advances data sovereignty research by linking governance and technical capabilities to organizational behavior (Abbas et al., 2024; von Scherenberg et al., 2024). For practitioners, the model highlights the importance of transparent, auditable control mechanisms and credible infrastructure governance. Overall, the study positions technology-enabled data sovereignty as a means of reconfiguring trust, control, and perceived risk to support data sharing and value creation, while providing a conceptual foundation for future empirical validation.

Keywords:
Data Sovereignty; Data Platform Ecosystems; Interorganizational Data Sharing

References

Abbas, A. E., van Velzen, T., Ofe, H., van de Kaa, G., Zuiderwijk, A., & de Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electronic Markets*, *34*(20). https://doi.org/10.1007/s12525-024-00695-2

Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic Markets*, *32*(3), 1577–1602. https://doi.org/10.1007/s12525-022-00572-w

Das, T. K., & Teng, B.-S. (2001). Trust, control, and risk in strategic alliances: An integrated framework. *Organization Studies*, *22*(2), 251–283. https://doi.org/10.1177/0170840601222004

Fassnacht, M., Benz, C., Heinz, D., Leimstoll, J., & Satzger, G. (2023). Barriers to data sharing among private sector organizations. In T. X. Bui (Ed.), *Proceedings of the 56th hawaii international conference on system sciences* (pp. 3695–3704). https://doi.org/10.24251/HICSS.2023.453

Gallivan, M. J., & Depledge, G. (2003). Trust, control and the role of interorganizational systems in electronic partnerships. *Information Systems Journal*, *13*(2), 159–190. https://doi.org/10.1046/j.1365-2575.2003.00146.x

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? a study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, *17*(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. https://doi.org/10.1057/ejis.2015.17

von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets*, *34*(15), 1–11. https://doi.org/10.1007/s12525-024-00693-4

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii. https://doi.org/https://www.jstor.org/stable/4132319

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Xue, Y., & Wang, J. (2022). Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. *Security and Communication Networks*, *2022*, 1–12. https://doi.org/10.1155/2022/5842371

B.2 Research Paper P2: From Fragments to Conceptual Clarity: A Taxonomy for Effective ESG Data Management

Authors:
T. Zwede, L. Valett, M.-F. Körner, M. Schneider, and J. Strüker

Submitted to:
Outlet hidden due to the double-blind review process

Extended Abstract[2]:
Environmental, social, and governance (ESG) data have become increasingly important for organizations seeking to address sustainability requirements, support managerial decision-making, and respond to growing demands for transparency (Kotsantonis & Serafeim, 2019; Püchel et al., 2024). At the same time, their effective management remains challenging because ESG data encompass heterogeneous information that differs in origin, structure, scope, temporal characteristics, and intended use. Regulatory initiatives such as the Corporate Sustainability Reporting Directive (CSRD) and the European Banking Authority's ESG risk management guidelines further increase the variety and volume of data that organizations need to manage (European Banking Authority, 2025; European Parliament and European Council, 2022). Existing Information Systems (IS) research addresses individual aspects of ESG data management, yet provides limited conceptual guidance for systematically distinguishing and structuring ESG data across organizational contexts (Krasikov & Legner, 2023; Wang et al., 2024, 2025). This study addresses this gap by developing a taxonomy that provides a structured conceptual basis for understanding and managing ESG data. Following the taxonomy development method of (Kundisch et al., 2021), which extends the approach of (Nickerson et al., 2013), the taxonomy was developed through an iterative combination of conceptual and empirical-to-conceptual design activities. A structured literature review of 73 relevant publications provided the initial conceptual foundation. This was complemented by 22 semi-structured interviews with practitioners from diverse industries, an expert workshop with six IS experts, and the analysis of 180 ESG data objects originating from academic, regulatory, and organizational contexts. Across four development iterations, the taxonomy was progressively refined against objective and subjective ending conditions. A subsequent evaluation with four additional practitioners, who independently classified ESG data objects from their professional contexts, confirmed the applicability, comprehensiveness, and practical relevance of the resulting taxonomy. The final taxonomy comprises three meta-dimensions - Context, Data Management, and Data Usage - which encompass 17 dimensions and 63 characteristics. The Context meta-dimension captures characteristics such as data classification, source, type, temporality, scope, aggregation, and sector. Data Management describes how ESG information is structured, formatted, collected, processed, analysed, and verified. Finally, Data Usage captures the organizational purposes and stakeholder contexts in which ESG data are employed, including reporting and compliance, performance and optimization, strategy and development, and communication and

[2]At the time of writing, this research paper is under review for acceptance at an academic conference. Therefore, an extended abstract is provided here.

engagement. Together, these dimensions provide a structured representation of ESG data that accounts for both their inherent heterogeneity and their organizational context. The application of the taxonomy to 180 ESG data objects further indicates that the functional purpose of ESG data plays a particularly important role in determining how data are interpreted and managed. For example, operational data used for performance optimization tend to require frequent collection and automated processing, whereas data supporting regulatory reporting place greater emphasis on verification, standardization, and traceability. Data intended for external communication, such as product carbon footprints, additionally require comparability and credible translation of sustainability impacts into stakeholder-relevant information. These findings reinforce the notion that data acquire meaning and organizational value through their context and use (Seidel et al., 2013). The study contributes to IS research in three ways. First, it consolidates fragmented knowledge on ESG data into a systematic conceptual structure, establishing a common vocabulary for future research. Second, it complements process-oriented perspectives on sustainability data management (Chua et al., 2022; Wang et al., 2024) by focusing on the characteristics of the data objects that organizations need to manage. Third, the taxonomy provides a diagnostic basis for data governance, classification, interoperability, and cross-organizational data exchange (Khatri & Brown, 2010; Möller et al., 2024). Overall, the study positions ESG data not merely as reporting inputs but as organizational resources whose characteristics and intended use jointly determine how they can be managed and leveraged for sustainability-related value creation.

Keywords:
ESG Data; Data Management; Taxonomy Development; Sustainability

References

Chua, C., Indulska, M., Lukyanenko, R., Maass, W., & Storey, V. C. (2022). Data management – MIS Quarterly research curations.

European Banking Authority. (2025). Guidelines on the management of environmental, social and governance (ESG) risks. Retrieved April 26, 2026, from https://www.eba.europa.eu/activities/single-rulebook/sustainable-finance/guidelines-management-esg-risks

European Parliament and European Council. (2022). Directive (EU) 2022/2464 amending regulation (EU) no 537/2014, directive 2004/109/EC, directive 2006/43/EC and directive 2013/34/EU, as regards corporate sustainability reporting.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1).

Kotsantonis, S., & Serafeim, G. (2019). Four things no one will tell you about ESG data. *Journal of Applied Corporate Finance*, *31*(2), 50–58. https://doi.org/10.1111/jacf.12346

Krasikov, P., & Legner, C. (2023). Introducing a data perspective to sustainability: How companies develop data sourcing practices for sustainability initiatives. *Communications of the Association for Information Systems*, *53*(1).

Kundisch, D., Muntermann, J., Oberländer, A. M., Rau, D., Röglinger, M., Schoormann, T., & Szopinski, D. (2021). An update for taxonomy designers: Methodological guidance from information systems research. *Business & Information Systems Engineering*, 1–19. https://doi.org/10.1007/s12599-021-00723-x

Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J. C., Gelhaar, J., Guggenberger, T., & Otto, B. (2024). Industrial data ecosystems and data spaces. *Electronic Markets*, *34*(1), 1–17. https://doi.org/10.1007/s12525-024-00724-0

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Püchel, L., Wang, C., Buhmann, K., Brandt, T., von Schweinitz, F., Edinger-Schons, L. M., vom Brocke, J., Legner, C., Teracino, E., & Mardahl, T. D. (2024). On the pivotal role of data in sustainability transformations. *Business & Information Systems Engineering*, *66*(6), 831–848. https://doi.org/10.1007/s12599-024-00904-4

Seidel, S., Recker, J., & vom Brocke, J. (2013). Sensemaking and sustainable practicing: Functional affordances of information systems in green transformations. *MIS quarterly*.

Wang, J., Teracino, E., & Legner, C. (2024). Towards data management for navigating the dynamic landscape of sustainability regulations and standards. *Proceedings of the 45th International Conference on Information Systems*.

Wang, J., Teracino, E., & Legner, C. (2025). From puzzle pieces to principles for sustainability reporting and disclosure: A design theory. *Proceedings of the 46th International Conference on Information Systems*.

B.3 Research Paper P3: From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour

Authors:
A. Geist, M.-F. Körner, J. Strüker, L. Valett, and T. Zwede

Published as:
Geist, A., Körner, M.-F., Strüker, J., Valett, L., & Zwede, T. (2026). From Data to Sustainable Decisions: The Impact of Verifiable Carbon Information on Consumer Behaviour. *Thirty-Fourth European Conference on Information Systems (ECIS), Milan, Italy*

Abstract:
Climate crisis demands credible sustainability communication, yet consumers struggle to assess the reliability of products' environmental claims. This study examines how different verification mechanisms – manufacturer claims, third-party certification, and digital verification – shape consumer decision-making and perceived utility. Drawing on Random Utility Theory, a Best-Worst Scaling experiment with 122 participants compares preferences across two product types. Quantitative results show that digitally verifiable carbon information significantly boosts perceived utility and choice likelihood, with attribute weights favouring digital verification (β=2.02 | 0.81) over manufacturer claims (reference) and third-party certifications (β=-0.9 | -1.86). We also find that price sensitivity (β=-0.21 | -0.41) constrains this impact for low-involvement goods. The study contributes to Information Systems (IS) research on cognition and human behaviour by showing that digital verification acts as a credibility signal, shaping cognitive evaluation and decision-making. It links these insights to Green IS and digital trust, demonstrating how algorithmic verifiability may reduce information asymmetry and enhance credibility in sustainability communication.

Keywords:
Digital Verifiability; Carbon Information; Random Utility Theory; Consumer Behaviour

B.4 Research Paper P4: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications

Authors:
T. Guggenberger, L. Neubauer, J. Stramm, F. Völter, and T. Zwede

Published as:
Guggenberger, T., Neubauer, L., Stramm, J., Völter, F., & Zwede, T. (2023). Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications. *Proceedings of the 56th Hawaii International Conference on System Sciences*, 6560–6569

Abstract:
Self-sovereign identity represents a novel phenomenon aiming to innovate how entities interact with, manage, and prove identity-related information. As with any emerging phenomenon, user acceptance represents a major challenge for the adoption of Self-sovereign identity. Since previous initiatives for digital identity management solutions have not been successfully adopted while at the same time their benefits are largely driven by network effects, user acceptance research is of particular importance for Self-sovereign identity. Therefore, we investigate the user acceptance of Self-sovereign identity by conducting a qualitative interview study. We contribute novel variables to existing theory and offer guidelines for building Self-sovereign identity systems.

Keywords:
Digital identities; adoption; TAM2; theory building

B.5 Research Paper P5: Data Spaces for Battery Value Chains: Uncovering Design Principles for Emission Data Sharing

Authors:
M. Babel, M. Handke, M.-F. Körner, J. Strüker, and T. Zwede

In preparation for resubmission to
Outlet hidden due to the double-blind review process

Extended Abstract[3]**:**
Reliable product carbon footprints (PCFs) are essential for identifying emission sources and supporting decarbonization across product value chains. For complex and long-lived products such as lithium-ion batteries for electric vehicles, however, relevant emission data are fragmented across numerous life cycle stages and organizations (Gebhardt et al., 2022; Stampatori et al., 2020). Current assessments consequently rely heavily on secondary data, industry averages, and assumptions, limiting their ability to differentiate products and inform carbon management decisions (Jaeger et al., 2022; Lin et al., 2021). Data spaces offer a promising approach to sharing data across organizational boundaries (Otto, 2022), yet existing research provides limited prescriptive guidance for their design in the context of value chain carbon accounting. This study addresses this gap by developing design principles for data spaces that support improved PCF assessments, using battery value chains as an illustrative case. Following a design science research approach (Peffers et al., 2007), the study combines a structured literature review with iterative design and expert evaluation. The review covers four search streams addressing data space foundations, data spaces for PCFs, analogous digital systems for carbon footprinting, and data sharing challenges in battery value chains. The resulting set of 47 publications provides the basis for identifying 30 meta-requirements, which are synthesized into six key requirements. Building on established approaches to design principle development (Gregor et al., 2020; Möller et al., 2020), six principles are formulated and refined through three design cycles involving 14 semi-structured expert interviews. The evaluation progresses from formal and conceptual refinement to assessments by specialists in data spaces, system engineering, batteries, and sustainability. The resulting principles cover real timeliness, common standards, technology-enabled confidentiality, traceability, automation, and explicit incentivization. Real timeliness enables dynamic emission inputs, such as electricity-related emissions, to reflect the individuality of a battery's carbon footprint. Common data and interface standards support interoperability across diverse systems and organizations. Confidentiality-preserving technologies safeguard commercially sensitive information, while traceability mechanisms support access to verifiable emission data across upstream value chain stages. Automation increases the efficiency in updating PCFs and supplier master data. Finally, explicit incentives address unevenly distributed participation benefits and encourage the broad adoption needed for value creation. Together, these principles connect technical capabilities with the organizational conditions required for emission data sharing. The expert evaluations

[3]At the time of writing, this research paper is in preparation for submission at an academic journal. Therefore, an extended abstract is provided here.

further reveal a central dilemma between traceability and confidentiality: granular primary data improve carbon accounting but may expose production processes, supplier relationships, and other trade secrets (Babel et al., 2022; Brucker & Yalman, 2022). Upstream aggregation, whereby firms combine their own emissions with footprint information received from immediate suppliers, offers a potential compromise. However, sharing aggregated indicators restricts the identification of supplier-specific emission hotspots and independent verification of underlying data and calculations. The findings therefore highlight the importance of suitable verification mechanisms and confidentiality-preserving technologies such as zero-knowledge proofs and self-sovereign identities. They also indicate that regulatory pressure is perceived as a particularly strong participation incentive, whereas the viability of direct markets for emission data remains contested. The study contributes to Information Systems research in three ways. First, it consolidates fragmented knowledge at the intersection of data spaces, PCF assessment, and battery value chains. Second, it establishes a structured requirements basis for emission data sharing. Third, it translates these requirements into six evaluated design principles, contributing nascent design knowledge to Green IS, Energy Informatics, and digital decarbonization (Müller et al., 2023; Watson et al., 2010). For practice, the principles guide the development of data spaces supporting carbon management and sustainability-related value co-creation across organizations. Their effectiveness in operational settings remains to be assessed through situated implementations and naturalistic evaluation.

Keywords:
Data Sharing; Decarbonization; Cross-organizational collaboration; Green IS; Life cycle assessment; Product carbon footprint

References

Babel, M., Gramlich, V., Körner, M.-F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling end-to-end digital carbon emission tracing with shielded NFTs. *Energy Informatics*, *5*(1).

Brucker, A. D., & Yalman, S. (2022). Confidentiality Enhanced Life-Cycle Assessment. In A. Marrella & B. Weber (Eds.), *Business Process Management Workshops, Bpm 2021* (Vol. 436). Springer International Publishing Ag.

Gebhardt, M., Beck, J., Kopyto, M., & Spieske, A. (2022). Determining requirements and challenges for a sustainable and circular electric vehicle battery supply chain: A mixed-methods approach. *Sustainable Production and Consumption*, *33*.

Gregor, S., Chandra Kruse, L., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*.

Jaeger, F. A., Saling, P., Otte, N., Steidle, R., Bollen, J., Golembiewski, B., Dencic, I., Letinois, U., Rehl, T., & Wunderlich, J. (2022). Challenges and requirements of exchanging Product Carbon Footprint information in the supply chain. In S. Albrecht, M. Fischer, C. Scagnetti, M. Barkmeyer, & A. Braune (Eds.), *E3S Web of Conferences* (Vol. 349).

Lin, X., Li, X., Kulkarni, S., & Zhao, F. (2021). The Application of Blockchain-Based Life Cycle Assessment on an Industrial Supply Chain. *Sustainability*, *13*(23).

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. Springer International Publishing.

Müller, F., Hofmann, P., Strüker, J., Leinauer, C., & Körner, M.-F. (2023). Digital Decarbonization: Design Principles for an Enterprise-wide Emissions Data Architecture. *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Otto, B. (2022). The Evolution of Data Spaces. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces*. Springer International Publishing.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3).

Stampatori, D., Raimondi, P. P., & Noussan, M. (2020). Li-Ion Batteries: A Review of a Key Technology for Transport Decarbonization. *Energies*, *13*(10).

Watson, Boudreau, & Chen. (2010). Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. *MIS Quarterly*, *34*(1).

B.6 Research Paper P6: Designing Practical Blockchain-Based Green Electricity Labeling With Succinct Non-Interactive Zero-Knowledge Proofs

Authors:
T. Zwede, S. Mertel, A. Rieger, J. Strüker, and J. Schönrich

Submitted to:
Outlet hidden due to the double-blind review process

Extended Abstract[4]:
Guarantees of Origin (GOs) support credible renewable electricity claims by certifying the renewable origin of electricity through accounting-based systems (Hamburger, 2019; Leinauer et al., 2025). However, existing systems offer limited temporal resolution and insufficient opportunities for consumers to independently verify the underlying accounting (de Chalendar & Benson, 2019; Winther & Ericson, 2013). Blockchain technology promises open and verifiable provenance tracking, yet its replicated storage and computation introduce scalability constraints and expose sensitive generation and consumption data (Roth et al., 2022; Sedlmeir et al., 2022). Although zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) promise to mitigate these limitations, their application to electricity labeling remains insufficiently specified and evaluated (Sedlmeir et al., 2021). This study addresses this gap by designing and implementing an information system that combines blockchain technology, Merkle proofs, and zk-SNARKs to reconcile verifiable green electricity accounting with data confidentiality and scalability. Following a design science research approach (Peffers et al., 2007), the study combines requirements identification, iterative artifact development, and qualitative and quantitative evaluation. A structured literature review identified 31 relevant publications from an initial set of 9,532 records and informed four design objectives: verifiability, openness, data confidentiality, and scalability. Expert input complemented the requirements analysis and artifact development. Across four design cycles, the architecture was refined to reduce cryptographic complexity and address manipulation risks, including attack vectors such as arithmetic overflows, duplicate accounts, and invalid measurement timestamps. The resulting prototype was evaluated quantitatively through performance tests and qualitatively through ten semi-structured expert interviews. The interviews assessed the architecture against the design objectives, while the performance evaluation examined setup requirements, proof generation, and verification across different configurations and scales of consumers and generators. The resulting architecture separates local verification from global accounting verification. In five-minute epochs, a utility collects metering data and allocates available green electricity to consumers. Separate Merkle trees commit to generator and consumer data, allowing individual stakeholders to verify the inclusion of their own records through local Merkle proofs. A global zk-SNARK establishes that the committed data satisfy the accounting constraints, including that allocated green electricity does not exceed authenticated generation. Compact

[4]At the time of writing, this research paper is under review for acceptance at an academic journal. Therefore, an extended abstract is provided here.

commitments and proof verification results are recorded on-chain, while detailed operational data remain off-chain. Consumers can therefore verify their allocation without accessing other participants' data or managing tradable electricity tokens. The prototype uses a permissioned Ethereum network with public read access; deployment on a public permissionless network is architecturally feasible but was not demonstrated. The evaluation indicates that cryptographic design choices substantially affect practical feasibility. Replacing SHA-256 with the proof-friendly Poseidon hash function reduced circuit complexity by 99.2% in the corresponding design cycle (Grassi et al., 2021). The largest tested integrated configuration comprised 2,048 consumers and 512 generators, while on-chain proof verification remained below one second across the evaluated scenarios. Scalability was primarily constrained by trusted setup requirements and proof generation resources, particularly the cost of verifying generator signatures. Experts underlined the relevance of the four design objectives and regarded the combination of confidential processing and publicly verifiable accounting as promising. Nevertheless, the artifact remains a proof of concept: deployment requires further auditing, performance improvements, trustworthy metering inputs, and governance arrangements preventing duplicate registration across systems (Babel et al., 2023). The study contributes to Information Systems research in three ways. First, it provides an implemented architecture for green electricity labeling that connects individual inclusion checks with publicly verifiable aggregate accounting. Second, it extends conceptual work on privacy-preserving electricity labeling through empirical evidence on implementation choices, performance constraints, and expert assessments (Sedlmeir et al., 2021). Third, it derives four nascent design principles: scope proofs according to actor-specific incentives and attack surfaces; select cryptographic primitives based on their performance across the complete architecture; use blockchains as immutable verification layers for off-chain processing; and combine local inclusion proofs with global consistency proofs. Together, these contributions show how information systems can provide selective transparency and verifiable collective outcomes without requiring full disclosure or replicated processing of sensitive operational data.

Keywords:
Distributed ledger technology; energy transition; green IS; guarantee of origin; privacy; scalability; zk-SNARK

References

Babel, M., Gramlich, V., Guthmann, C., Schober, M., Körner, M.-F., & Strüker, J. (2023). Vertrauen durch digitale identifizierung: Über den beitrag von ssi zur integration von dezentralen oracles in informationssysteme. *HMD Praxis der Wirtschaftsinformatik*, *60*(2), 478–493. https://doi.org/10.1365/s40702-023-00955-3

de Chalendar, J. A., & Benson, S. M. (2019). Why 100 % renewable energy is not enough. *Joule*, *3*(6), 1389–1393. https://doi.org/https://doi.org/10.1016/j.joule.2019.05.002

Grassi, L., Khovratovich, D., Rechberger, C., Roy, A., & Schofnegger, M. (2021). Poseidon: A new hash function for zero-knowledge proof systems. *30th USENIX Security Symposium*. Retrieved July 31, 2021, from https://www.usenix.org/conference/usenixsecurity21/presentation/grassi

Hamburger, Á. (2019). Is guarantee of origin really an effective energy policy tool in europe? A critical approach. *Society and Economy*, *41*(4), 487–507. https://doi.org/https://doi.org/10.1556/204.2019.41.4.6

Leinauer, C., Körner, M.-F., Ströher, T., & Strüker, J. (2025). Digital measuring, reporting, and verification (dMRV). *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-025-00953-3

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Roth, T., Utz, M., Baumgarte, F., Rieger, A., Sedlmeir, J., & Strüker, J. (2022). Electricity powered by blockchain: A review with a European perspective. *Applied Energy*. https://doi.org/10.1016/j.apenergy.2022.119799

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir, J., Völter, F., & Strüker, J. (2021). The next stage of green electricity labeling: Using zero-knowledge proofs for blockchain-based certificates of origin and use. *ACM SIGENERGY Energy Informatics Reviev*, *1*(1), 20–31. https://doi.org/10.1145/3508467.3508470

Winther, T., & Ericson, T. (2013). Matching policy and people? Household responses to the promotion of renewable electricity. *Energy Efficiency*, *6*(2), 369–385. https://doi.org/https://doi.org/10.1007/s12053-012-9170-x

B.7 Research Paper P7: Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs

Authors:
M. Babel, V. Gramlich, M.-F. Körner, J. Sedlmeir, J. Strüker, and T. Zwede

Published as:
Babel, M., Gramlich, V., Körner, M.-F., Sedlmeir, J., Strüker, J., & Zwede, T. (2022). Enabling End-To-End Digital Carbon Emission Tracing with Shielded NFTs. *Energy Informatics*

Abstract:
In the energy transition, there is an urgent need for decreasing overall carbon emissions. Against this background, the purposeful and verifiable tracing of emissions in the energy system is a crucial key element for promoting the deep decarbonization towards a net zero emission economy with a market-based approach. Such an effective tracing system requires end-to-end information flows that link carbon sources and sinks while keeping end consumers' and businesses' sensitive data confidential. In this paper, we illustrate how non-fungible tokens with fractional ownership can help to enable such a system, and how zero-knowledge proofs can address the related privacy issues associated with the fine-granular recording of stakeholders' emission data. Thus, we contribute to designing a carbon emission tracing system that satisfies verifiability, distinguishability, fractional ownership, and privacy requirements. We implement a proof-of-concept for our approach and discuss its advantages compared to alternative centralized or decentralized architectures that have been proposed in the past. Based on a technical, data privacy, and economic analysis, we conclude that our approach is a more suitable technical backbone for end-to-end digital carbon emission tracing than previously suggested solutions.

Keywords:
Blockchain; Certificate; Decarbonization; Distributed Ledger Technology; Electric Vehicle; Guarantee of Origin; Personal Carbon Tracing; Privacy; Non-Fungible Token; Sustainability; Zero-Knowledge Proof

B.8 Research Paper P8: Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision

Authors:
T. Zwede, M. Ehaus, M. Babel, P. Heeß, L. Schick, M.-F. Körner, and J. Strüker

Published as:
Zwede, T., Ehaus, M., Babel, M., Heeß, P., Schick, L., Körner, M.-F., & Strüker, J. (2025). Designing and Implementing the Trust Diamond for Verifiable and Privacy-Preserving Data Sharing: Engineering Energy Flexibility Provision. *Energy Informatics*, *8*(1), 143

Abstract:
While data sharing in a digitalized world is increasingly important, its inherent tension between data verifiability and privacy limits stakeholders' engagement. In the course of the sustainable energy transition, this tension also hinders the integration of small-scale flexibility devices in electricity grids: Grid operators must rely on verifiable data for secure operations, while device owners often seek to ensure data protection and thus privacy. Applying an Action Design Research Approach, we design and implement the Flexibility Provision Data Flow and the digital Trust Diamond that leverages wallet-based identity management for ensuring verifiability and privacy-preserving data sharing. To that end, we also derive two fundamental design principles for systems that leverage the Trust Diamond, namely Verifiability through Delegation and Mediated Sovereignty, and show their applicability for optimized grid operations. Our research further results in proposing a Decentralized Flexibility Provision Architecture that operationalizes these findings in a laboratory and field test environment. Performance tests indicate the solution's practical scalability. This study highlights the importance of Information Systems-based solutions to enhance data sharing and address trust concerns between stakeholders. Moreover, it provides an actionable design to realize wallet-based data sharing to enable a decentralized flexibility provision for Redispatch measures.

Keywords:
Decentralized Redispatch; Small-scale Flexibility; Data-Sovereignty

B.9 Research Paper P9: Governing Digital Technologies in Decentralized Energy Systems: A Qualitative Assessment of Capabilities and Policy Implications

Authors:
T. Zwede, P. Heeß, M.-F. Körner, D. Parak, A. Schubert, and J. Strüker

Submitted to:
Outlet hidden due to the double-blind review process

Extended Abstract[5]**:**
The renewable energy transition is transforming electricity systems towards increasingly distributed generation, heterogeneous ownership, and growing sectoral coupling between electricity, mobility, heating, and industry. This decentralization creates coordination and governance challenges that extend beyond the technical operation of individual assets (Körner et al., 2022). Digital technologies promise diverse mechanisms for coordinating distributed actors, verifying information, and enabling local market participation. However, existing research predominantly examines individual technologies and applications, leaving their combined contribution to system-level requirements insufficiently understood (Andoni et al., 2019). Regulatory barriers further complicate the implementation of decentralized solutions (Campos et al., 2020; Horstink et al., 2021). This study addresses this gap by investigating how digital technologies can support the coordination and governance of decentralized electricity systems and which policy measures can enable their responsible deployment. The study follows a qualitative multi-method research design combining a literature review, an expert workshop, and semi-structured interviews. A thematic synthesis of 92 peer-reviewed publications provides the foundation for identifying characteristics of a successful transition towards a sustainable, decentralized electricity system. These characteristics are reviewed and mapped to relevant digital technologies and use cases in a workshop with 19 academic experts. Subsequently, eight interviews with professionals from energy companies, technology providers, consulting, and applied research refine the technology–characteristic mapping and inform the derivation of policy implications. The interviews last 61 minutes on average and are analysed through iterative open and axial coding. This process yields 55 unique statements linking digital technologies to transition characteristics, with the final two interviews generating no additional codes. The resulting framework comprises five overarching characteristics: reliable and open electricity markets; energy inclusivity and local participation; an economically efficient electricity transition; security of supply; and technology openness and responsible data usage. The framework distinguishes coordination concepts, such as local energy communities and virtual power plants, from enabling digital technologies, including peer-to-peer networks, distributed ledgers, digital identities, verifiable credentials, self-sovereign identity, and zero-knowledge proofs. This distinction clarifies how organizational and market arrangements depend on complementary digital capabilities for identification, authorization, transaction coor-

[5]At the time of writing, this research paper is under review for acceptance at an academic journal. Therefore, an extended abstract is provided here.

dination, information verification, and controlled data disclosure. The mapping indicates that digital identities provide a foundation for registering distributed assets, authenticating participants, and assigning market rights and obligations. Peer-to-peer networks can facilitate local trading and participation by smaller actors, while virtual power plants aggregate distributed resources for flexibility provision. Distributed ledgers can support shared records and automated settlement, whereas verifiable credentials enable the verification of eligibility, asset attributes, and energy-related claims. Self-sovereign identity and zero-knowledge proofs complement these functions by strengthening user control and enabling verification without unnecessary disclosure of sensitive information (Berentsen et al., 2023; Miyamae et al., 2023; Podgorelec et al., 2022). Their potential benefits depend on appropriate institutional conditions: technical capabilities alone do not ensure fair participation, economic efficiency, or trustworthy governance (Milchram et al., 2018). The study contributes an integrated framework connecting previously fragmented technology-specific insights with the governance requirements of decentralized electricity systems. It also provides a capability-oriented basis for policy design, shifting attention towards the coordination, verification, participation, and privacy functions that regulation should enable. The policy implications address three tensions: steering innovation without selecting individual technological winners; adapting rules designed for centralized electricity systems; and building resilient digital infrastructure despite greater implementation demands. Proposed measures include diversified research funding, clarification of data-protection requirements for decentralized identity architectures, implementation of energy-community provisions, stronger dynamic pricing incentives, recognition of digital operating costs in network tariffs, and interoperable infrastructure for asset registration and data exchange. Derived primarily from the German context, these recommendations offer guidance for jurisdictions with comparable institutional arrangements. Overall, the study positions digital technologies as complementary governance enablers whose contribution to the renewable electricity transition depends on supportive regulatory, market, and data-governance conditions.

Keywords:
Decentralized electricity systems; digital coordination; digital technologies; energy system governance; renewable energy transition

References

Andoni, M., et al. (2019). DLT technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

Berentsen, A., Lenzi, J., & Nyffenegger, R. (2023). An Introduction to Zero-Knowledge Proofs in DLTs and Economics. *Federal Reserve Bank of St. Louis Review*, *105*(4). https://doi.org/10.20955/r.105.280-94

Campos, I., Pontes Luz, G., Marín-González, E., Gährs, S., Hall, S., & Holstenkamp, L. (2020). Regulatory challenges and opportunities for collective renewable energy prosumers in the EU. *Energy Policy*, *138*, 111212. https://doi.org/10.1016/j.enpol.2019.111212

Horstink, L., Wittmayer, J. M., & Ng, K. (2021). Pluralising the European energy landscape: Collective renewable energy prosumers and the EU's clean energy vision. *Energy Policy*, *153*, 112262. https://doi.org/10.1016/j.enpol.2021.112262

Körner, M.-F., Sedlmeir, J., Weibelzahl, M., Fridgen, G., Heine, M., & Neumann, C. (2022). Systemic risks in electricity systems: A perspective on the potential of digital technologies. *Energy Policy*, *164*, 112901. https://doi.org/10.1016/j.enpol.2022.112901

Milchram, C., Hillerbrand, R., de Kaa, G. v., Doorn, N., & Künneke, R. (2018). Energy Justice and Smart Grid Systems: Evidence from the Netherlands and the United Kingdom. *Applied Energy*, *229*, 1244–1259. https://doi.org/10.1016/j.apenergy.2018.08.053

Miyamae, T., Kozakura, F., Nakamura, M., & Morinaga, M. (2023). Zgridbc: Zero-knowledge proof based scalable and privacy-enhanced blockchain platform for electricity tracking. *IEICE TRANSACTIONS on Information and Systems*, *106*(7), 1219–1229. https://doi.org/10.1587/transinf.2023EDP7043

Podgorelec, B., Alber, L., & Zefferer, T. (2022). What is a (Digital) Identity Wallet? A Systematic Literature Review. *Proceedings 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022*, 809–818.