UNIVERSITÄT
BAYREUTH

Reconciling Data Verifiability and Sovereignty in Digital Sustainability Infrastructures

Dissertation

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

vorgelegt
von

Matthias-Maximilian Gerhard Babel
aus
Fürth

Dekan:	Prof. Dr. Claas Christian Germelmann
Erstberichterstatter:	Prof. Dr. Jens Strüker
Zweitberichterstatter:	Prof. Dr. Nils Urbach
Tag der mündlichen Prüfung:	09. Juli 2025

If you see a turtle on a fence post,
you know it didn't get there by itself.

Acknowledgments

With this thesis, I reflect on a defining phase of my academic journey, shaped by an environment that challenged, supported, and inspired me to grow both personally and professionally. I am deeply grateful to all those who accompanied me along the way and helped make this work possible.

I would like to thank my supervisors and mentors. Jens Strüker, thank you not only for your academic guidance, but also for your humanity and constant personal engagement. You created a foundation on which I was able to grow professionally, intellectually, and personally. You placed great trust in me, encouraged my independent development, and entrusted me with significant responsibility while always remaining a reliable source of support during critical phases. Your guidance extended far beyond academic matters, and I am deeply grateful for your lasting commitment. Nils Urbach, thank you for your constructive feedback and continuous encouragement throughout this journey. From the beginning, you paved the way for my entry into this field of research, creating a reliable, trust-based environment that consistently supported my academic and personal development. Marc-Fabian Körner, thank you for your steady mentorship and for the approachable and grounded way in which you accompanied me throughout my doctoral journey. Your support was a valuable anchor during this formative phase.

I would also like to extend my heartfelt thanks to my colleagues and co-authors at Branch Business & Information Systems Engineering (Fraunhofer FIT), the Research Center for Information Management (FIM), and the University of Bayreuth. Thank you for your collaboration, inspiration, and friendship.

My deepest gratitude goes to my wife, Isabell. Your unconditional support, love, and understanding made this journey possible. You carried the weight of this time with me, and I cannot thank you enough.

Finally, I would like to thank my parents for their lifelong encouragement and support. You gave me everything you had, and I dedicate this thesis to you.

Copyright Statement

Some parts of the following sections include content taken from the published research papers included in this thesis. To maintain the readability of the text, I omit the standard labeling of these citations.

Abstract

Digital technologies have become pervasive, permeating nearly every aspect of the modern world. The ongoing process of datafication, which can be defined as the conversion of real-world activities into digital representations, is a major phenomenon in contemporary society and industry. In light of the pressing environmental challenges that currently exist, the growing availability of data has significant potential to support transformative sustainability efforts. Consequently, the nascent discipline of Digital Sustainability explores the potential of information systems to support environmental, economic, and social sustainability objectives. In this context, digital infrastructures play a crucial role in enabling the exchange of sustainability-related information across diverse actors, sectors, and geopolitical boundaries. The significance of this paradigm shift is underscored by concrete applications, including the need for proof-of-origin for electricity, decentralized redispatch of flexible energy assets, and the adoption of digital product passports for circular supply chains. However, the implementation of such applications exposes a fundamental structural deficiency. While they are contingent on verifiable data, which refers to the capacity to independently validate its authenticity, integrity, and context for effective decision-making, transparency, and regulatory compliance, a cohesive and integrated infrastructure to support such verifiability remains deficient. To address this limitation, data sovereignty, which describes the ability to control, manage, and share one's own data, emerges as a pivotal enabler. While verifiable data frequently exists, it often remains isolated within proprietary databases or subject to unilateral access controls, impeding its utilization and integration across diverse platforms and applications. The concept of data sovereignty has been identified as a significant solution to this challenge, as it facilitates the equitable and transparent dissemination of data across various use cases, particularly in contexts where environmental objectives are at stake. Consequently, the design of digital infrastructures must prioritize the promotion of verifiability and sovereignty. The application of data is contingent upon its reliability and fairness, both of which are contingent upon the presence of these qualities. This dual objective will serve as a foundational framework for promoting environmental, economic, and social sustainability in an integrated and equitable manner.

This thesis explores the design of digital infrastructures that collectively support data verifiability and data sovereignty in sustainability-related use cases. The development of these patterns draws upon emerging technologies from the Web3 ecosystem, including

self-sovereign identity, zero-knowledge proofs, blockchain, and token-based data representations. The result is a set of architectural patterns that facilitate trustworthy, privacy-preserving, and decentralized data sharing. The research is founded on a design-oriented Information Systems perspective and synthesizes insights from seven research papers. Across a range of use cases, including proof-of-origin for electricity, decentralized redispatch, and digital product passports, the thesis demonstrates the potential for verifiability and sovereignty to be realized in tandem. This approach contributes to a more comprehensive understanding of digital infrastructures as socio-technical foundations of sustainability transitions. Instead of regarding sovereignty as a compromise to verifiability, this work asserts that both sovereignty and verifiability are indispensable for inclusive, reliable, and forward-thinking digital ecosystems.

Table of Contents

List of Figures and Tables

1 Introduction

1.1 Motivation

"On the Internet, nobody knows you're a heat pump". This updated riff on Peter Steiner's iconic 1993 cartoon[1] "On the Internet, nobody knows you're a dog" captures the growing trust challenges on digital identity in an increasingly connected world. Originally a commentary on online anonymity, the phrase now reflects a deeper and more systemic issue: the absence of reliable, interoperable infrastructures for identity and data that span both humans and machines. This challenge extends far beyond individual users to include devices, organizations, and complex networks of actors embedded in digital ecosystems (Research Paper 1, 3, 4, 5, and 7).

Thirty years following Steiner's cartoons, the Internet has undergone a profound transformation from a human-centered medium for information exchange into a foundational infrastructure that underlies nearly every facet of modern society. In the contemporary era, the Internet, and more broadly, information systems, have emerged as pivotal catalysts of systemic transformation across various sectors, including those at the vanguard of addressing global sustainability challenges. They play an increasingly pivotal role in initiatives that accelerate decarbonization, enhance energy efficiency, promote circular resource utilization, and foster transparent and accountable supply chains (Fridgen et al., 2016; Watson et al., 2010; Watson et al., 2022). Building on this evolving role, the field of Digital Sustainability seeks to harness digital technologies and artifacts to address the intertwined goals of environmental, economic, and social sustainability goals (Kotlarsky et al., 2023; Schoormann et al., 2025).

In alignment swith the United Nations' 2030 Agenda for Sustainable Development (Nations, 2015), this thesis contributes to two key Sustainable Development Goals: #12 (responsible consumption and production) and #13 (climate action). These global objectives call for new kinds of digital infrastructure capable of providing sustainability-related information across diverse actors, sectors, and geopolitical boundaries. Concrete applications underscore this need. Proof-of-origin for electricity (Research Papers 1 and 3), decentralized redispatch of flexible energy assets (Research Paper 4), and digital product

[1] https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_a_dog

passports for circular supply chains (Research Paper 7) all rely on the availability of robust data infrastructures to operate effectively at scale and drive meaningful climate impact.

The implementation of such applications has exposed a pivotal vulnerability in the realm of digital sustainability: the inability to verify data due to the absence of a cohesive and profoundly interconnected identity and data framework. Verifiability, defined as the ability to confirm the authenticity, integrity, and context of data, is imperative for effective decision-making, accountability, and regulatory compliance (Research Papers 1, 3, 4 and 7). In the contemporary digital landscape, centralized entities, such as technology providers, platforms, and certification authorities, frequently confine verifiable data to proprietary silos, impeding access irrespective of the data owner's intentions. Attempts to achieve verifiability outside these silos depend on costly, opaque certification processes or on other proprietary systems that reinforce dependencies between data providers and consumers (Krasikov and Legner, 2023, Research Papers 1 and 5). In both cases, the capacity of data to engender value and propel sustainability remains predominantly unexploited (Jarke et al., 2019; Verhulst, 2023).

The enforcement of data sovereignty, defined as the ability to control, manage, and share one's own data, is a strategic measure that can be employed to facilitate access to verifiable data. Absent this concept, incumbent organizations leverage their informational advantage to fortify their market dominance, thereby impeding the autonomy of data originators. This hinders the originators' capability to disseminate data with smaller stakeholders, curtailing prospects for innovation, fair competition, and informed decision-making (Verhulst, 2023). In contrast to the promotion of inclusive engagement, centralized yet verifiable infrastructures have the tendency to concentrate power among established actors, thereby undermining the societal and environmental objectives of Digital Sustainability initiatives (Research Paper 7). This deficiency poses a significant threat to critical use cases, including but not limited to: circular supply chains, low-carbon product tracking, and decentralized energy coordination. The functionality of these use cases is contingent upon the availability of open, verifiable, and controlled data (Scherenberg et al., 2024; Verhulst, 2023, Research Papers 1, 3, 4, and 7). Digital infrastructures, therefore, must break open existing silos and guarantee data sovereignty for all participants. This bottom-up approach has the potential to establish the foundation for the seamless sharing of data, thereby supporting environmental, social, and economic sustainability (Jarke et al., 2019, Research Paper 7). In instances where verifiable data is applicable to digital

sustainability use cases, there is an urgent need for data infrastructures that respect data sovereignty. Failure to do so could potentially undermine data owners, neglecting social and economic sustainability.

This thesis explores the design of digital infrastructures that support both data verifiability and data sovereignty. Drawing on emerging technologies from the Web3 ecosystem, including self-sovereign identity (Research Paper 4 and 5), zero-knowledge proofs (Research Paper 1, 2, and 6), and token-based representations (Research Paper 1 and 7), is a salient feature of this study. The thesis develops and evaluates architectural principles and technical patterns that enable verifiable while sovereign information sharing across organizations, individuals, and devices. This development is especially relevant for the sake of Digital Sustainability in the applications of proof-of-origin for electricity (Research Paper 1 and 3), decentralized redispatch of flexible energy assets (Research Paper 4), and digital product passports for circular supply chains (Research Paper 7).

This research posits that data sovereignty is not merely a normative ideal, but rather a functional necessity for the sustenance of sustainable digital ecosystems. It fosters equitable participation, prevents extractive data practices, and ensures that sustainability-driven innovation remains open, trustworthy, and inclusive. Consequently, sovereignty must be regarded not as a trade-off to verifiability, but rather as a co-requirement and precondition for durable, trustworthy infrastructures that serve both people and the planet.

1.2 Structure of the Thesis and Overview of Embedded Research Papers

This cumulative thesis explores the design of digital infrastructures that enable verifiable and sovereign data ecosystems for sustainability-related use cases. It adopts a design-oriented information system research approach and synthesizes insights from seven research papers.

Section 2 provides both the conceptual groundwork and original theoretical contributions that underpin this thesis. It synthesizes key challenges and terminology at the intersection of verifiability and data sovereignty in Digital Sustainability and introduces a structured framing of technologies and design tensions that inform the subsequent artifact designs. Starting with section 2.1, which frames the central challenge: while Digital Sustainability applications increasingly rely on fine-grained, multilateral data sharing, today's

infrastructures lack mechanisms to exchange data verifiably without undermining data sovereignty. Three representative domains of Digital Sustainability and Green IS are used to exemplify this challenge: greenhouse gas trading and tracing in section 2.1.1 (Research Paper 1), decentralized redispatch in section 2.1.2 (Research Paper 4), and digital product passports for a circular economy in section 2.1.3 (Research Paper 7). Section 2.1.1 is further elaborated through a taxonomy developed in Research Paper 3, which draws on a structured literature review (Webster and Watson, 2002) and semi-structured interviews (Nickerson et al., 2013) to analyze existing GHG tracking and trading systems. Section 2.2 introduces the foundational concepts of trust (section 2.2.1), data verifiability (section 2.2.2), and data sovereignty (section 2.2.3), which emerge from the application challenges identified earlier. This section defines key terminology and unpacks how verifiability can help close trust gaps, while simultaneously creating new tensions with data sovereignty. Building on this conceptual grounding, section 2.3 introduces relevant technological paradigms for implementing verifiable data infrastructures: blockchain (section 2.3.1), zero-knowledge proofs (section 2.3.2) (Research Paper 2), and self-sovereign identity (section 2.3.3) (Research Paper 5). Research Paper 2 presents findings from a multivocal structured literature review (Garousi et al., 2016) examining the interplay between blockchain and zero-knowledge proofs. This review incorporates both academic and grey literature to reflect the fast-moving nature of the field. Research Paper 5 draws from seven applied research projects and a structured literature review to synthesize the value propositions and architectural implications of self-sovereign identity. While Reserach Paper 6 presents an implementation-oriented proposal for integrating generic-zero-knowledge proofs into self-sovereign identity systems, thereby enhancing data verifiability and strengthening privacy and sovereignty guarantees. Together, these foundational chapters do more than frame the thesis's scope, as they develop a coherent theoretical perspective and introduce key analytical constructs that directly inform and shape the subsequent design contributions.

Section 3 presents the design contributions of the thesis across four thematic areas building up on each other, each anchored in real-world use cases and supported by concrete design artifacts. Section 3.1 synthesizes insights from Research Papers 1, 3, 4, and 5 to highlight the foundational role of verifiable identity infrastructures in establishing trustworthy and reusable data ecosystems. It demonstrates how self-sovereign identity-based architectures can provide robust master and operational layers for sustainability-oriented applications, including proof-of-origin origin tracking and decentralized redispatch. Sec-

tion 3.2 explores the use of zero-knowledge proofs to reconcile data verifiability with data sovereignty, drawing primarily from Research Paper 4. The research follows the Action Design Research (ADR) approach (Sein et al., 2011) and includes iterative artifact development in collaboration with industry stakeholders. It received the Best Paper Award in the Decision Analytics and Service Science track at the 58th Hawaii International Conference on System Sciences (HICSS). The artifact developed in Research Paper 4 demonstrates how zero-knowledge proofs enable aggregators to present verifiable, privacy-preserving flexibility data to grid operators without disclosing individual asset data. Section 3.3 focuses on the findings of Research Paper 1 and introduces shielded fractionalized non-fungible tokens (SFNFTs) as a novel solution for tracing single-sourced goods like electricity. The artifact was developed in the context of a publicly funded research project, with extensive engagement through interviews and workshops. Research Paper 1 demonstrates how combining fractionalized non-fungible tokens (NFTs) with zero-knowledge proofs can produce tamper-proof, privacy-compliant proof-of-origin infrastructures. The result is a mechanism for creating verifiable provenance information for energy-related value creation steps without exposing sensitive data.

The research journey between Research Paper 1 and Research Paper 7 reflects a substantial evolution in both the scope and ambition of the artifact design, structured along three major design iterations. Anchored in the design science research paradigm (Gregor and Hevner, 2013; Peffers et al., 2007; Venable et al., 2016), the process began with a narrowly scoped objective in the energy sector: enabling tamper-resistant, privacy-preserving provenance information for electricity using SFNFTs. However, the findings of Research Paper 1 pointed to broader applicability in domains requiring fine-grained, sovereign data sharing. Responding to the rising momentum of European regulatory frameworks for digital product passports, the artifact was extended to support multi-sourced and domain-agnostic traceability use cases. This second iteration, consolidated in Babel et al., 2025, introduced a nested and composable infrastructure, addressing the complexity of multi-tiered value chains and highlighting remaining gaps related to long-term data custodianship. In a final design cycle, these insights were used to refocus the artifact on user-side data control and verifiability through wallet-based architectures. Research Paper 7 formalizes this third iteration by presenting a decentralized, sovereign, and transferable digital product passport infrastructure. Section 3.4 consolidates these contributions and presents the design iterations that culminated in Research Paper 7. It demonstrates how the final artifact supports composability across multiple value chain layers, aligns with emerging

circular economy requirements, and empowers end-users to manage and control product-related data throughout the lifecycle. The approaches outlined in Research Papers 1, 4, 6, and 7 are grounded in theoretical design and have been validated through prototypical implementation and testing.

The section 4 offers a comprehensive summary of the core findings and contributions. The bibliography is provided in the subsequent section. Additional supporting information is included in section 6, which offers detailed insights into the integrated research articles, including their abstracts or extended abstracts. The supplementary material includes the full texts of all seven research papers (not for publication).

2 Trust and Sovereignty in Digital Sustainability

Digital Sustainability increasingly relies on accurate, trustworthy data and robust digital infrastructures to achieve meaningful impacts, particularly in the context of addressing global challenges such as climate change and sustainable resource management. This section explores the interlinked concepts of trust, verifiability, and sovereignty, emphasizing their centrality to the effectiveness of Digital Sustainability initiatives.

Initially, the section focuses on the pivotal role of *Digital Sustainability*, highlighting three crucial application domains: *Emission Tracing and Trading*, *Decentralized Redispatch*, and *Digital Product Passports for a Circular Economy*. Each section emphasizes the necessity of detailed, reliable data for informed decision-making and accountability, illustrating the current shortcomings in data granularity and trustworthiness, as well as outlining opportunities to improve these practices.

Subsequently, the foundations required to support these Digital Sustainability efforts are explored through the lenses of trust (section 2.2.1), data verifiability (section 2.2.2), and data sovereignty (section 2.2.3). The trust section addresses the gaps emerging from digital ecosystems, where increasingly complex, multi-party interactions demand stronger mechanisms for trust. Data verifiability then builds on this by outlining how accurate, authenticated data can mitigate these trust gaps. Data sovereignty further expands upon the critical need for maintaining individual and organizational autonomy over data, particularly as data-sharing grows more prevalent and essential.

Finally, the analysis turns to emergent Web3 technologies in section 2.3, particularly blockchain and token-based representations (section 2.3.1), zero-knowledge proofs (section 2.3.2), and self-sovereign identity (section 2.3.3), which offer promising solutions to balance and enhance trust, verifiability, and sovereignty. By leveraging decentralization, transparency, and advanced cryptographic techniques, these technologies provide powerful frameworks that support secure, trustworthy data ecosystems essential for effective Digital Sustainability practices.

Together, these sections articulate a comprehensive perspective on establishing trust and sovereignty as foundational elements in pursuing sustainable digital transformations.

2.1 Relevance of Trustworthy Data Infrastructures in Digital Sustainability

Green IS is the branch of Information System (IS) scholarship that examines how digital technologies and data can be designed, deployed, and governed to advance environmental sustainability objectives (Dedrick, 2010; Jenkin et al., 2011; Watson et al., 2008). It investigates IT artifacts and managerial practices that reduce energy and resource consumption, minimise emissions, and enable circular material flows at the levels of products, organisations, and entire value networks (Jenkin et al., 2011; Watson et al., 2008). In addition to exploring how digital systems can support sustainability goals, Green IS also considers the environmental implications of the information systems themselves. Research topics range from energy-aware software and sensor-based monitoring infrastructures to analytics-driven supply chain optimisation and product lifecycle management. By embedding robust environmental metrics into decision processes, Green IS seeks to align organisational behaviour with ecological thresholds and regulatory requirements (Gholami et al., 2016; Melville, 2010; Sarkis et al., 2013; Watson et al., 2010).

Yet sustainability is inherently multi-dimensional. The triple-bottom-line view positions environmental, social, and economic objectives as interdependent rather than isolated (Norman and MacDonald, 2004). As these technological interventions aimed at environmental benefits mostly interact with social justice (e.g., privacy, fairness) and economic resilience (e.g., data-driven business models, value distribution). Neglecting these interdependencies risks shifting burdens from one dimension to another and thus undermining long-term sustainability (Hahn et al., 2015; Schoormann et al., 2025). This has triggered a conceptual broadening within the IS community. *Digital Sustainability* has emerged as an umbrella term that captures how digital resources and digital artifacts can be designed and governed to advance environmental, social, and economic goals concurrently (Kotlarsky et al., 2023; Pan et al., 2022). As Kotlarsky et al. (2023) argue, the shift from Green IS to Digital Sustainability reflects an ontological reversal: digital phenomena increasingly shape physical realities, requiring scholars to move beyond efficiency-oriented "greening" towards systemic, cross-sector transformation under conditions of high technological complexity.

In practical terms, this paradigm shift foregrounds social and economic values, such as verifiability, trust, and data sovereignty, as critical infrastructure conditions for sustainable digital ecosystems (Scherenberg et al., 2024; Schoormann et al., 2025; Verhulst, 2023).

For example, initiatives such as digital product passports illustrate how environmental objectives (e.g., circularity) depend on transparent and trustworthy data exchanges across supply-chain actors, which raise issues of economic value capture and individual agency over data (Ducuing and Reich, 2023). Consequently, addressing environmental problems in isolation is insufficient; sociotechnical tensions must be anticipated, described, and managed throughout the design and use of digital technologies (Kotlarsky et al., 2023; Schoormann et al., 2025).

2.1.1 Emission Tracing and Trading

A central concern of Green IS research is the reduction of greenhouse gas emissions, particularly the carbon dioxid (CO_2)-intensity associated with electricity, as a means of addressing climate change (Dedrick, 2010; Nations, 1998; Sarkis et al., 2013). Despite this promise, precise measurement of environmental impacts remains difficult. Emissions data is often incomplete or outdated, and supply chain structures introduce considerable complexity (Ahi and Searcy, 2015; Björklund et al., 2012; Hervani et al., 2005; Lehtinen and Ahola, 2010; Strüker et al., 2021, Research Paper 1). These limitations persist even in regulated contexts. Policy instruments such as Emission Trading Systems (ETS), Personal Carbon Trading (PCT), and Voluntary Carbon Markets (VCM) aim to incentivize decarbonization (Hepburn, 2007; Icap, 2021), but often lack the granularity and transparency needed for meaningful operational steering (Hamburger, 2019; Sedlmeir et al., 2021b). Likewise, consumer-facing measures such as green electricity tariffs rely on generalized averages rather than precise, traceable data. Although international frameworks like the Kyoto Protocol introduced mechanisms such as emissions trading and Joint Implementation (Nations, 1998), implementation challenges remain – chief among them the continued dependence on estimates, manual reporting, and third-party verifications (Research Paper 1 and 3).

Research Paper 3 develops a taxonomy to systematically compare existing greenhouse gas tracking and trading mechanisms. As illustrated in Figure 1, it identifies ten key dimensions, such as emissions type (e.g., CO_2, CH_4), scope (direct vs. indirect), assignment of responsibility (upstream vs. downstream), voluntary vs. mandatory participation, incentive and regulation mechanisms, sectoral coverage, spatial scale, governance structures, and actor roles. This framework reveals a highly fragmented landscape that impedes interoperability, comparability, and shared understanding. By structuring this

Dimension	Characteristics							Description
Tracked/Traded Emission	CO_2	CH_4	N_2O	HFCs	PFCs	SF_6	NF_3	Which emissions are tracked or traded?
Scope of Emissions	Direct				Indirect			Which scope of emissions does the system consider?
Compensation Responsibility	Upstream				Downstream			Who is responsible for the compensation of emissions?
Commitment	Mandatory				Voluntary			Why do participants use the system?
Incentive Mechanism	Market-Based				Command & Control			Which kind of incentive mechanism is used?
Regulation Mechanism	Budgeting of GHGs				Pricing of GHGs			Which kind of regulation mechanism is used?
Energy Consuming Sectors Covered	Residential		Commercial		Industry		Transport	Which energy consuming sectors does the system cover?
Spatial Scale	International			National			Sub-National	On which spatial scale is the system implemented?
Active System Participants	Individuals			Enterprises			Other Institutions	Who actively participates in the system?
Governance	Centralized			Semi-Decentralized			Decentralized	Who controls the system?

Figure 1: Taxonomy on the design and implementation of GHG tracking and trading approaches; Source: Research Paper 3

complexity, the taxonomy offers guidance to both enterprises and policymakers. It helps companies identify systems aligned with their decarbonization goals, and supports policymakers in refining instruments for broader adoption and greater effectiveness. It also reinforces a critical insight: meaningful climate action depends on the availability of granular, trustworthy emissions data. Given the volatility of electricity generation and consumption, coarse annual averages obscure actual emissions patterns and render CO_2-adaptive decision-making ineffective.

These constraints hinder efforts by enterprises to pursue verifiable, deep decarbonization (Luers et al., 2022). Enterprises are central to this landscape, as they must increasingly demonstrate transparent and accountable CO_2 management in response to demands from investors, consumers, and regulators (Schoormann et al., 2021). Achieving this requires new tracking methods that generate real-time, trustworthy insights by leveraging advances in digital technologies and information system (Fuso Nerini et al., 2021). Only with fine-grained, verifiable emissions data can enterprises and individuals align their decisions with actual environmental impact, closing the transparency gaps that weaken existing approaches (Research Paper 1 and 3).

Digital technologies play an increasingly vital role in the effort to enable data-driven, CO_2-adaptive decision-making (Fiorini and Aiello, 2018; Lima et al., 2021; Zampou et al., 2022). High-resolution, time- and location-specific emissions data for electricity is seen as critical to these applications (Pina et al., 2012; Strüker et al., 2021). Both literature

and interviews in Research Paper 3 stress the importance of verifiable data that is temporally and spatially precise, interoperable across supply chains, and privacy-preserving. Without such data, risks of greenwashing persist, and efforts to create effective regulation or steer behavior remain blunt. Addressing these gaps is essential to empower enterprises and individuals to make informed contributions to climate mitigation (Jarke et al., 2019; Verhulst, 2023, Research Paper 1 and 3).

2.1.2 Decentralized Redispatch

To reduce greenhouse gas emissions from electricity production, the electricity system is undergoing a fundamental transformation, from centralized, fossil-fuel-based structures toward decentralized renewable generation. Unlike conventional power plants, renewable technologies such as photovoltaic panels and wind turbines are inherently more distributed and volatile (Shrestha et al., 2018). This shift imposes new demands on electricity systems, particularly in coping with the variability of renewable supply. Consequently, grid operators now face increased complexity in congestion management, as renewable volatility challenges conventional grid operations (Hirth and Glismann, 2018; Lind et al., 2019, Research Paper 4).

In parallel, low-greenhouse gas electricity enables cross-sectoral decarbonization in heating, mobility, and industry through widespread electrification (Fridgen et al., 2020; Ramsebner et al., 2021). This not only increases overall electricity demand but also decentralizes it, as small-scale, flexible assets, such as electric vehicles, heat pumps, and battery storage, are increasingly deployed (Michaelis et al., 2024a; Priesmann et al., 2021, Research Paper 4). Such devices can contribute to distributed load management and enhance system stability by enabling the decentralized redispatch (Michaelis et al., 2024b; Nieße et al., 2018). To harness this potential for grid balancing and congestion mitigation, grid operators increasingly depend on the responsiveness of these assets (Research Paper 4).

Tapping into the flexibility of small-scale assets requires trustworthy, near real-time data (Fridgen et al., 2022). Accordingly, seamless and secure sharing of trustworthy data between distributed assets and grid operators is essential. Yet several barriers remain. Most devices are located behind household-level smart meters, which limit the real-time visibility of grid operators and restrict direct access to operational data. Since the smart meter marks the system boundary, grid operators must rely on third-party mechanisms to ensure data quality and validate the availability of flexibility. Furthermore, without proper

inspection and qualification of devices, grid operators face considerable uncertainty regarding promised flexibility contributions (Parag and Sovacool, 2016). Managing device-level data across millions of endpoints would create excessive operational overhead. To address these challenges, recent conceptual approaches propose delegating the communication and coordination of flexibility to independent intermediaries, commonly referred to as aggregators (Brandt et al., 2022; Ross and Mathieu, 2020). Aggregators act as interfaces between grid operators and distributed resources, coordinating flexibility offers on behalf of device owners (Research Paper 4).

However, even with aggregators, grid operators must ensure that aggregated flexibility is traceable and verifiable. A fundamental requirement remains the ability to validate offers for flexibility potentials and reduce operational risk. Unverified or unreliable flexibility may compromise grid stability (Parag and Sovacool, 2016). Thus, the integration of distributed flexibility into grid operations requires not only digital infrastructure for real-time data exchange but also mechanisms to ensure the trustworthiness of flexibility, specifically its availability, reliability, and settlement. Without such mechanisms, the benefits of decentralized flexibility remain largely inaccessible, limiting the effectiveness of efforts to stabilize the grid and decarbonize the energy system (Faquir et al., 2021, Research Paper 4).

2.1.3 Digital Product Passports for a Circular Economy

A sustainable future demands a fundamental shift in how resources are consumed and managed. Unlike the linear ”cradle-to-grave” trajectory, where products are discarded after use. The circular economy model establishes regenerative loops to minimize waste and maximize resource efficiency (Jensen et al., 2023; Zeiss et al., 2021). It subverts traditional economic logic by promoting the continual use and reintegration of materials, thereby reducing the depletion of environmental resources (Geissdoerfer et al., 2017; Kirchherr et al., 2017). Central to the circular economy are the strategies of narrowing, slowing, and closing material loops, which guide economic actors to prolong product lifespans, optimize material use, and reintegrate waste into value chains (Geissdoerfer et al., 2017; Kirchherr et al., 2017; Potting et al., 2017, Research Paper 7).

Realizing this vision requires a systemic transformation that aligns economic actors, policy frameworks, and technological infrastructures. In this context, stakeholders must closely interact with information systems to enable a socio-economic shift that is criti-

cal for the implementation of circular practices (Reich et al., 2025; Zeiss et al., 2021). One of the main barriers to this transition, however, is the persistent information gap among stakeholders across product and material value chains (Heeß et al., 2024; Rizos and Bryhn, 2022; Vermunt et al., 2019). These gaps hinder effective decision-making regarding repairability, recyclability, and reuse, ultimately slowing the adoption of circular business models. To overcome these challenges, stakeholders, including manufacturers, retailers, recyclers, and consumers, require access to comprehensive, reliable data on material composition, usage history, and end-of-life options (Serna-Guerrero et al., 2022). Only with this information can products be kept in circulation for as long as possible (Research Paper 7).

A key enabler in this context are digital product passports. As inter-organizational data-sharing mechanisms, digital product passports serve as structured repositories of product lifecycle information. They ensure the availability of essential sustainability data throughout the value chain, supporting informed decisions and bridging information gaps that otherwise impede value creation in circular systems (Chaudhuri et al., 2024; Gieß and Möller, 2025; Jensen et al., 2023; Neramballi et al., 2024). Information Systems research has extensively examined the conceptual foundations of digital product passports and their role in enabling material reuse within specific product domains (Adisorn et al., 2021; Plociennik et al., 2022; Walden et al., 2021). However, integrating heterogeneous data sources into a single, trustworthy digital product passport remains a key challenge, especially in globally distributed value networks. Without shared trust in the validity and provenance of such data, circular strategies remain fragmented, constraining the full potential for optimized reuse, repair, and recycling (Gieß and Möller, 2025; Jäger-Roschko and Petersen, 2022, Research Paper 7).

2.2 Interdependence of Trust, Verifiable Data, and Sovereignty

2.2.1 Trust Gaps in Digital Infrastructures

Achieving digital decarbonization through the fields of greenhouse gas reduction (see section 2.1.1), decentralized redispatch (see section 2.1.2), and sustainable consumption (see section 2.1.3) necessitates a foundation of mutual trust among involved stakeholders, particularly on the data that underpin these processes. Rousseau et al. (1998, p. 395) define trust as “a psychological state comprising the intention to accept vulnerability based upon

positive expectations of the intentions or behavior of another". Consequently, trust is a fundamental prerequisite for effective and efficient human interactions and increasingly critical in facilitating collaboration between machines and digital systems.

Traditionally, trust has underpinned business transactions and personal exchanges in face-to-face environments, ensuring smooth and predictable interactions. Yet, the rise of digitalization has significantly altered the trust landscape. Digital communication and online commerce introduce substantial gaps in trust, as these interactions frequently occur between anonymous or unfamiliar parties. Individuals increasingly rely on digital platforms to compare offers and make decisions based primarily on convenience, immediacy, and efficiency, rather than established relationships or reputations. Through this anonymous match making, users often place considerable trust in unfamiliar entities without sufficient reasoning or assurance, creating what Yan and Holtmanns (2008) describe as a trust gap (Babel and Körner, 2025). More broadly, this phenomenon aligns with the principal-agent theory. Meckling and Jensen (1976, p. 4) defines the agency relationship as "a contract under which one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision-making authority to the agent". Given both parties are typically utility maximizers, the agent might not always act in the principal's best interest, further exacerbating the trust gap.

In parallel, digital ecosystems, especially for addressing environmental, social, and economic sustainability, are rapidly becoming more interconnected, fundamentally reshaping how individuals and organizations interact. Instead of maintaining isolated and trusted relationships, entities now engage within extensive networks of stakeholders spanning multiple sectors and geographical regions. This introduces considerable complexity regarding trust management, secure data sharing, and operational reliability. In today's globalized economy, maintaining competitiveness demands that businesses leverage comprehensive data from diverse stakeholders, such as suppliers, service providers, distributors, and even customers, to optimize their operations and support sustainability initiatives (Heeß et al., 2024). Consequently, organizations increasingly rely on extensive data flows within these ecosystems (Babel and Körner, 2025).

The necessity of data sharing within these ecosystems creates a network of interdependent relationships, tying businesses to the trustworthiness and data security practices of their partners, often indirectly. Even entities without direct interactions can become vulnerable, as security breaches or trust failures in any part of the interconnected ecosystem can prop-

agate widely. These unintended dependencies pose substantial risks, including challenges related to privacy, consent, data ownership, and overall ecosystem security. Without explicit trust frameworks and clearly defined agreements governing these relationships, interconnected digital ecosystems risk undermining the foundational trust required for their effective functioning. Stakeholders might question the integrity and security of the entire network, potentially jeopardizing its stability and long-term viability (Babel and Körner, 2025).

As previously outlined, trustworthy data is paramount for Digital Sustainability initiatives (Research Papers 1, 3, and 7). To enable these initiatives at scale, data infrastructures must be designed to bridge existing trust gaps between consumers, enterprises, and regulators. Developing reliable trust frameworks in digital environments is therefore not merely a technological challenge, but a a critical enabler for advancing global sustainability efforts.

2.2.2 Data Verifiability Closing Trust Gaps

Data verifiability is crucial to address the trust gaps that arise within today's increasingly interconnected digital ecosystems, especially in the context of sustainability. Efforts aimed at reducing greenhouse gas emissions, for instance, require reliable data sourced from multiple stakeholders across extensive value chains. These data include detailed information about greenhouse gas emissions categorized into three scopes: scope one, representing direct emissions from owned or controlled sources; scope two, covering indirect emissions resulting from purchased electricity and heat; and scope three, comprising all other indirect emissions occurring in the broader value chain. Given the indirect and multi-step nature of data transmission in these ecosystems, trust gaps about the integrity and provenance of such data naturally emerge. A key mechanism for establishing the necessary trust frameworks for addressing trust gaps is data verifiability.

We define data verifiability as the assurance that data maintains integrity and authenticity throughout its lifecycle. Integrity implies that the data remains unaltered during transmission, while authenticity ensures that data originates from a reliable and trusted source (Research Paper 5). Verifiable data significantly mitigates trust gaps by enabling stakeholders to confidently use the data even when direct trust in every intermediary is not established.

The necessity of data verifiability can be further explained through agency theory, which highlights issues arising from information asymmetry. According to (Meckling and Jensen, 1976), agency relationships inherently involve the delegation of tasks, creating a situation where the agent may not always act in the principal's best interests, resulting in potential trust issues. Similarly, in sustainability contexts such as emissions tracking and reporting, stakeholders frequently face uncertainty regarding the accuracy and reliability of shared data (Research Paper 1 and 3).

Hence, ensuring data verifiability does not remove the requirement for trust but shifts it strategically (Babel and Körner, 2025). Stakeholders do not necessarily need to trust every intermediary involved in data transmission, but they must trust the original issuer of the data (Research Paper 1, 4, and 5). By clearly establishing the source and integrity of the data, verifiability provides a foundational element essential for maintaining accountability, credibility, and ultimately, effective sustainability measures (Research Paper 1, 4, and 7).

2.2.3 The Role of Data Sovereignty in Digital Infrastructure

Since trustworthy data is essential for Digital Sustainability use cases, its availability is a fundamental prerequisite. The concept of datafication refers to the transformation of diverse aspects of the world, such as human behavior, social interactions, and machine operations, into quantifiable digital data (Verhulst, 2023). This transformation enables new forms of control, optimization, automation, and value creation across a wide range of domains, from industrial processes to everyday digital services (Jarke et al., 2019; Mejias and Couldry, 2019). Although datafication holds significant promise for addressing sustainability challenges through information systems, its practical implementation often falls short. In many cases, data remains fragmented, siloed, or inaccessible. It is often "hidden from public view or use, thus limiting the capacity of policymakers, researchers, or other actors to leverage its potential" (Verhulst, 2023, p. 3). A key reason for this disconnect lies in persistent information asymmetries. These arise when data holders, such as companies or organizations, do not fully disclose what data exist or how they are handled. Data subjects and potential data users are left unaware of valuable data resources and their provenance. This lack of transparency can undermine trust, reinforce power imbalances, and ultimately prevent the use of data in ways that could support informed decision-making or societal benefit. To fully realize the potential of datafication

for sustainability, it is therefore essential to reduce information asymmetries and promote transparent, equitable access to data across all stakeholders (Verhulst, 2023).

In today's digital ecosystems a common distinction is made between the data subject, the identifiable entity the data refers to, and the data holder, the entity that collects, controls, or administers the data (European Commission, 2023). Historically, large technology platforms have significantly undermined users' digital self-determination (Jarke et al., 2019). This principle is defined as "the principle of respecting, embedding, and enforcing people's and peoples' agency, rights, interests, preferences, and expectations throughout the digital data life cycle in a mutually beneficial manner for all parties involved" (Verhulst, 2023, p. 6). In response to this erosion of agency, the European Union has introduced regulatory frameworks such as the general data protection regulation (GDPR) (European Commission, 2016) and the Data Act (European Commission, 2023), which aim to strengthen the rights of data subjects, reduce informational asymmetries, and promote fair and responsible data-sharing practices. These frameworks also help dismantle data silos and support the reuse of data for sustainable digital applications.

Within this context, the concept of data sovereignty gains particular importance. Nagel and Lycklama (2021, p. 27) defines data sovereignty as "the capability of a natural person or corporate entity for exclusive self-determination over its economic data goods". It extends beyond privacy and consent by emphasizing a more comprehensive understanding of control, transparency, and value attribution. The principle suggests that the economic benefits derived from data should be aligned with the rights and interests of those to whom the data refers. Ideally, data subjects should also act as data holders, or at minimum be fully informed, actively involved, and not disadvantaged by structural or informational imbalances (Jarke et al., 2019; Verhulst, 2023). Ideally, data owners should benefit directly from the economic value of their data.

Furthermore, verifiable data, meaning data whose origin, context, and integrity can be proven, holds significantly higher economic value than unverifiable data. Its reliability enables confident use across stakeholders and scenarios. Embedding verifiability and sovereignty into digital infrastructures is therefore essential to establish trust, ensure accountability, and enable responsible data reuse in support of sustainability goals.

In the context of sustainable digitalization, which encompasses not only environmental but also social and economic sustainability, protecting the data sovereignty of individuals and organizations is a foundational requirement. Data sharing must be fostered in a

way that does not undermine personal rights or create economic disadvantages for those who contribute data. Sustainability efforts that disregard digital agency risk reinforcing existing power asymmetries or introducing new forms of digital exploitation.

2.3 Web3 as a Backbone for Sustainable Digital Infrastructures

In light of the tension of data verifiability and data sovereignty in information systems, particularly within the context of Digital Sustainability, the emergence of new technological paradigms is both timely and necessary. Web3 technologies, in particular, have been developed with the goal of addressing these challenges by creating mutual trust and reinforcing sovereignty on the Internet.

The Internet began as a stateless, read-only network, primarily operated by institutions and digital experts. Due to the limited availability of content, widespread adoption remained constrained (Murray et al., 2023). The introduction of cookies and the rise of platforms for user-generated content marked a shift toward a stateful, interactive web. This transition to Web2 enabled basic read-write capabilities, but control and ownership of user data remained in the hands of the platforms that hosted the content (Wan et al., 2024). Social media service provider such as Alphabet and Meta facilitated user participation and content creation, fueling strong network effects and resulting in the dominance of a few major platforms (Jullien and Sand-Zantman, 2021; Tafesse and Dayan, 2023). These platforms also centralized identity management by implementing federated login systems such as Single Sign-On (Research Paper 5). This growing concentration of control, coupled with the pervasive datafication of everyday life through the proliferation of internet of things devices, has raised serious concerns about user autonomy and data sovereignty (Constantinides et al., 2018).

Web3 offers a response by seeking to re-establish decentralized control structures and restore agency to individual users. It introduces the “read-write-own” paradigm, in which users are no longer mere visitors, as in Web2, but can actively co-design and control digital infrastructures. Through technologies such as crypto wallets, self-sovereign identity, and privacy enhancing technologies, it promotes user ownership, decentralized trust frameworks, and self-managed digital identities (Sunyaev et al., 2021; Wan et al., 2024). By enabling users to participate in infrastructure governance and data control, Web3 chal-

lenges centralized models and reinforces data sovereignty as a foundational principle (Research Paper 7).

2.3.1 The Role of Blockchain in Trust Ecosystems

In 2008, Nakamoto (2008) introduced Bitcoin, proposing a decentralized electronic payment system maintained by its users rather than a central intermediary, such as a bank. This innovation effectively addressed the double-spending problem of digital goods without intermediaries (Schär, 2021; Sunyaev et al., 2021). Thereby Nakamoto (2008) layed the foundation for a whole ecosystem of distributed ledger technologies focusing on reaching decentralized consensus, from which blockchain technology represents a subgroup. Blockchain is built upon a peer-to-peer network architecture, where each participant (node) can directly interact with others without centralized intermediaries. Consensus nodes validate these transactions initiated in the network, bundle them into blocks, and cryptographically link them together into an immutable and chronological chain, creating the term "blockchain". Every node maintains an identical copy of the blockchain, ensuring transparency, security, and decentralization, as the entire transaction history is publicly visible to all network participants (Zheng et al., 2017, Research Paper 1 and 7).

The landscape of blockchain technology expanded considerably with the introduction of Ethereum and smart contracts in 2015. This innovation not only broadened the application spectrum of decentralized finance but also laid the foundation for decentralized platforms that empower users to reclaim control over their digital assets (Buterin et al., 2014; Schär, 2021). One of the key developments emerging from this shift is the massive tokenization of both physical and digital assets, enabling value exchange on the Internet – an environment that had previously been limited to information exchange (Schär, 2021; Sunyaev et al., 2021). This transition contributed significantly to shaping the foundational principles of Web3 (Research Paper 7).

Blockchain networks differ fundamentally in terms of openness and governance (Zheng et al., 2017), see also Table 1:

- *Public vs. Private:* Public blockchains are open to everyone, allowing unrestricted participation and visibility, while private blockchains restrict access and visibility to approved participants only.

Network Type	Visibility / Access	Validators
Public, permissionless	Open to all	Anyone can validate
Public, permissioned	Open visibility & access	Pre-selected validators
Private, permissioned	Restricted access & visibility	Pre-selected validators

Table 1: Comparison of Network Types in Distributed Ledger Systems

- *Permissioned vs. Permissionless:* Permissionless blockchains allow any participant to join the network and participate in consensus processes freely. Permissioned blockchains restrict this access.

Various consensus mechanisms, commonly referred to as "Proof of X", are employed to achieve agreement on the state of the ledger (Zheng et al., 2017):

- *Proof of Work (PoW):* A public, permissionless mechanism known for high security and decentralization but lower efficiency and higher energy consumption, as it requires computational resources to solve complex cryptographic puzzles.
- *Proof of Stake (PoS):* Also public and permissionless, PoS improves efficiency and scalability by selecting validators based on economic stakes rather than computational effort, substantially reducing energy consumption.
- *Proof of Authority (PoA):* A private, permissioned mechanism utilizing pre-approved, trusted validators, resulting in higher efficiency and lower decentralization, suitable for consortium and enterprise contexts.
- *Delegated Proof of Authority (DPoA):* Public and permissioned, DPoA balances transparency and efficiency by delegating validation rights to a limited set of selected authorities, achieving quicker transaction processing and controlled decentralization.

A fundamental distinction among consensus mechanisms lies in whether they ensure byzantin fault tolerance (BFT) or merely crash fault tolerance (CFT). While CFT protects against benign failures such as crashes or disconnections, BFT additionally safeguards the network against malicious actors and adversarial behavior (Lamport et al., 1982). This distinction is crucial for determining the trust model and resilience of a distributed system. Blockchains enable participants to trust the integrity and origin of data

without having to trust all individual nodes. This trust is established through the consensus mechanism, which ensures that all valid transactions are agreed upon by the network and are cryptographically verifiable (Cachin and Vukolić, 2017; Zheng et al., 2017). As a result, blockchains offer verifiability of the data processing to all participants (Babel and Körner, 2025). The degree of trust among network participants directly influences the required strength of the consensus protocol. In public blockchains such as Ethereum, where the network is open to any participant, strong guarantees provided by BFT are necessary to maintain integrity in the presence of potentially malicious actors. In contrast, consortium blockchains like Hyperledger Fabric operate in a permissioned environment with identifiable participants who share a baseline of mutual trust. In such settings, more lightweight consensus protocols that provide CFT may suffice, enabling higher efficiency and lower overhead (Babel and Körner, 2025; Cachin and Vukolić, 2017; Ekparinya et al., 2019; Zheng et al., 2017).

Trust in the platform's infrastructure does not inherently imply trust in the data it processes. Where external, off-chain data is integrated, such as in greenhouse gas trading and tracing. There is a critical need for reliable oracles to ensure data accuracy (Babel et al., 2023). This requirement reintroduces trust dependencies outside the blockchain's inherent guarantees, necessitating either trustworthy intermediaries or tamper-proof hardware, both of which establish new trust relationships. This challenge, commonly referred to as the "oracle problem", highlights the difficulty of ensuring the correctness of data at the point of entry into the blockchain, or more fundamentally in the information system (Babel and Körner, 2025; Caldarelli, 2020, Research Paper 1).

Blockchains provide a foundational infrastructure for trust ecosystems by enabling transparent, immutable, and decentralized governance without the need for central authorities (Babel and Körner, 2025; Cachin and Vukolić, 2017). While private blockchains offer stronger access control for sensitive data, they often face a bootstrapping problem due to their limited scope and purpose-specific deployment. In contrast, public blockchains play a crucial role by offering an already available, highly decentralized infrastructure that can be leveraged across diverse use cases, even in scenarios where no intermediaries currently exist (Research Paper 7).

Smart contracts enhance decentralized governance models by seamlessly allowing their implementation for automated rule enforcement (Cachin and Vukolić, 2017). They embed governance logic directly into code, ensuring transparent and tamper-proof execution.

Building on this principle, ecentralized autonomous organisation implement decentralized decision-making processes on blockchain protocols, operating without hierarchical structures.

Overall, blockchain contributes to user sovereignty through its openness, transparency, and participatory structure. Users are free to engage deeply with the infrastructure that governs their data. Furthermore, tokenization enables individuals to claim and manage ownership over digital assets, supporting fine-grained control and accountability (Babel and Körner, 2025, Research Paper 7).

2.3.2 Zero-Knowledge Proofs For Upholding Sovereignty in Data Verifiability

A central theoretical concept to describe the design trade-offs in blockchain systems is the blockchain trilemma, which highlights the inherent tension between decentralization, security, and scalability (Hafid et al., 2020). Public, permissionless blockchains like Bitcoin exemplify strong decentralization and BFT-level security through the use of proof of work (Nakamoto, 2008), but struggle with limited scalability, leading to slower transactions and higher fees under heavy load (Zhou et al., 2020). In contrast, private, permissioned blockchains such as Hyperledger Fabric restrict participation and rely on lighter CFT-based mechanisms like proof of authority. This enhances scalability through higher throughput and lower latency but comes at the cost of reduced decentralization and resilience (Guggenberger et al., 2022). These examples illustrate the core dilemma: blockchain systems can typically optimize for two of the three properties, but not all simultaneously (Research Paper 2).

Privacy has also emerged as a critical concern in blockchain systems, yet it remains largely unresolved within the constraints of the blockchain trilemma (Bernabe et al., 2019). A seemingly straightforward approach is to encrypt sensitive data. However, this hinders consensus, as nodes can no longer verify transaction validity or reach deterministic agreement on the blockchain's state, thereby weakening security (Cachin and Vukolić, 2017). Private blockchains attempt to address privacy by restricting ledger access, but this typically comes at the cost of decentralization. Achieving robust privacy while maintaining decentralization, security, and scalability continues to be an challenge (Research Paper 2).

Against this backdrop, recent developments in the blockchain space have turned toward a cryptographic technique known as zero-knowledge proofs, suggesting that they may

help overcome the limitations posed by the blockchain trilemma (Buterin, 2021b). Originally introduced in the seminal work by Goldwasser et al. (1989), zero-knowledge proofs emerged from theoretical computer science as a novel form of interactive proof systems. A zero-knowledge proof enables one party (the prover) to convince another party (the verifier) that a given statement is true, without disclosing any further information beyond the validity of the statement itself (Research Paper 2). Formally, a zero-knowledge proof satisfies three key properties:

- *Completeness:* If the statement is true, an honest verifier will be convinced by an honest prover.
- *Soundness:* If the statement is false, no dishonest prover can convince an honest verifier, except with negligible probability.
- *Zero-knowledge:* The verifier learns nothing beyond the fact that the statement is true.

The transformation of zero-knowledge proofs into non-interactive forms has significantly broadened their practical applicability (Wu and Wang, 2014). As a result, recent research has largely focused on advancing non-interactive general-purpose zero-knowledge proof schemes, leading to the development of several prominent protocols, including zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) (Bitansky et al., 2012), Bulletproofs (Bünz et al., 2020), and zero-knowledge scalable transparent arguments of knowledge (zk-STARKs) (Ben-Sasson et al., 2018). While the implementation of zero-knowledge proofs was traditionally limited to cryptographic experts, the emergence of domain-specific language such as Circom (Iden3, 2022) and ZoKrates (Eberhardt and Tai, 2018) has made it possible for developers without deep cryptographic expertise to build zero-knowledge proof-based applications. Nevertheless, deploying these systems at scale still demands rigorous security audits to ensure their reliability and correctness (Research Paper 2 and 6).

Amid the blockchain trilemma, recent industry developments have increasingly focused on scalability. A notable example is Ethereum's shift toward "Danksharding," which integrates zero-knowledge proofs to enhance scalability without sacrificing decentralization or security (Buterin, 2022). This effort is part of a broader trend, with platforms like Polygon, Starkware, Loopring, and others also adopting zero-knowledge proofs to overcome performance bottlenecks. A key outcome of this movement is the rise of rollups, which

are scaling solutions that aggregate transactions off-chain and submit a single proof of the updated state to the main chain. Rollups come in two main forms: optimistic rollups, which rely on fraud proofs and game-theoretic assumptions, and zk-rollups, which use validity proofs based on Merkle trees and zero-knowledge proofs. Rollups are categorized as Layer 2 solutions, as they operate a top existing Layer 1 blockchains while preserving their security models (Buterin, 2021a, Research Paper 2).

While Layer 2 solutions are commonly associated with public blockchains, their architectural principles can also be applied to less decentralized infrastructures, including private blockchains and even centralized ledgers. Depending on the specific design of a zk-rollup, transaction data may remain entirely hidden from both third-party participants and even rollup or ledger validators. As a result, the trust placed in validators is limited to ensuring fair and non-discriminatory access. In this way, zk-rollups offer a powerful mechanism for achieving data verifiability without compromising data sovereignty. They enable prevention of double-spending without requiring the disclosure of sensitive data at any point in the process (Research Paper 1, 2, and 7).

On blockchains, verifiability is typically ensured through transparency, as all participants can observe the correct execution of processes. In contrast, zero-knowledge proofs enable the reduction of transparency while preserving verifiability. This allows sensitive data to remain confidential, since the exact process execution is no longer visible, yet still provably correct. This is made possible by the three core properties of zero-knowledge proofs, which together ensure that a statement can be verified without revealing the underlying data. By minimizing the amount of data that must be shared, zero-knowledge proofs help to improve user sovereignty. Whenever data is disclosed, sovereignty diminishes, because the data owner loses control over how third parties process or use the data, often leading to information asymmetries. Although originally developed in the context of blockchain systems, this concept can be generalized to all types of information systems. Whenever data owners are required to share data, zero-knowledge proofs improve data sovereignty by making it possible to prove properties about the data without actually disclosing it, while still ensuring its correctness can be verified.

2.3.3 Self-Sovereign Identity Unlocking Verifiable Data

Current federated identity management solutions, like single-sign-on services, provided by major tech companies centralize control over digital identities, limiting users' data

sovereignty despite nominal portability across platforms (Vapen et al., 2016). This dependency becomes increasingly problematic in the evolving machine-to-machine economy, where billions of connected devices will autonomously engage in business transactions (Braud et al., 2021; Jöhnk et al., 2021; Körner et al., 2022; Schweizer et al., 2020, Research Paper 1). In such a scenario, relying on third parties to manage machine identities risks undermining strategic autonomy. A unified identity management approach is needed to resolve fragmented identity processes and support verifiable, sovereign transactions, particularly in contexts of Digital Sustainability, where reducing information asymmetry is essential (Allen, 2016; Preukschat and Reed, 2021; Schoormann et al., 2025, Research Paper 3, 5, and 7).

Rooted in Web3 principles, self-sovereign identity offers a decentralized identity management approach, allowing individuals to manage their identity data independently. Through verifiable credentials, which are digitally signed by trusted issuers, self-sovereign identity enables machine-verifiable authenticity and integrity using public private key infrastructure and asymmetric encryption (Mühle et al., 2018). These credentials encapsulate claims such as identity attributes, relationships, or entitlements (Preukschat and Reed, 2021; Sartor et al., 2022; Sporny et al., 2022), and are managed by holders in digital wallets, which can create verifiable presentations to share selected information with verifiers (Čučko and Turkanović, 2021; Davie et al., 2019). A digital wallet typically runs on a user's edge device, such as a smartphone (Naik and Jenkins, 2020), and empowers the holder to manage, store, and selectively disclose verifiable credentials (Research Paper 3, 5, and 6). Figure 2 illustrates this interaction.

The concept of the "trust triangle" eliminates the need for verifiers to place direct trust in the identity holder presenting claims. Instead, it relies on trusted issuers who vouch for the validity of those claims, thereby addressing the inherent trust gap between holder and verifier (Mühle et al., 2018). Self-sovereign identity creates verifiability, therefore it does not eliminate the need for trust but shifts it to trust anchors, as outlined in Sections 2.2.1 and 2.2.2. For instance, rather than trusting a holder's claim like "I am allowed to drive", a verifier trusts the issuer, such as a licensing authority, to have issued that claim appropriately. This infrastructure allows for both the reinforcement of existing trust structures and the creation of new ones, as verifiers can decide which issuers they deem credible. The clear separation of roles and decentralized management of identity attributes makes it essential that stakeholders can establish trustworthy connections. Verifiers must reliably

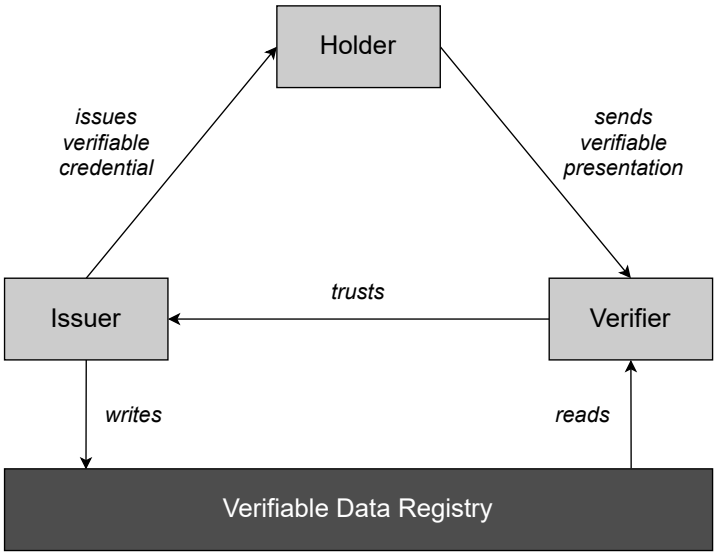

Figure 2: Trust triangle in the context of self-sovereign identity-based interactions; Source: Research Paper 5

associate digital signatures with known issuers, and holders must be protected against verifiers lacking a legitimate basis to process disclosed data (Research Paper 5). To support this, self-sovereign identity utilizes publicly accessible infrastructures, such as trusted (distributed) ledgers, to publish cryptographic key material and metadata about issuers and verifiers, including public institutions (Schmidt et al., 2021). These verifiable data registries form the backbone for associating credentials with issuers and establishing trust within the trust triangle (Research Paper 5).

Importantly, verifiable credentials are not limited to natural persons (Bartolomeu et al., 2019; Kulabukhova et al., 2019). They may also refer to organizations or machines. Furthermore, the holder of a credential need not be its subject, for example, a machine's credential may be held by its owner, or a company's credential by its legal representative (Research Paper 5).

The European Commission introduced the *eIDAS 2.0* regulation and the proposed the regulation around the European Digital Identity Wallet, aiming to create a secure, interoperable digital identity framework across the EU strongly relying on the foundations of the paradigm of self-sovereign identity. This initiative seeks to empower citizens with a unified and trustworthy digital identity system while supporting both public and private services (Bochnia et al., 2023; Degen and Teubner, 2024). At the same time, it strives to

reinforce data sovereignty and level the playing field within the EU's digital single market (Codagnone and Weigl, 2023; Ernstberger et al., 2023; Rieger et al., 2022, Research Paper 5). Traditional identity verification methods, such as document scans or digital signatures in PDFs, typically require disclosing all embedded information, resulting in unnecessary data exposure. Self-sovereign identity mitigates this by enabling selective disclosure and data minimization, using techniques like zero-knowledge proofs. Perifiable credentials contain claims, such as age, status, or entitlements, attested by trusted issuers and managed in digital wallets. These credentials can be transformed into verifiable presentations that reveal only relevant information (Čučko and Turkanović, 2021; Davie et al., 2019). In many cases, a predicate like "over 21" is sufficient rather than the exact birthdate (Glöckler et al., 2023, Research Paper 6).

Advanced cryptographic methods, such as Boneh-Boyen-Shachum (BBS) (Looker et al., 2022) and Camenisch-Lysyanskaya (CL) (Camenisch and Lysyanskaya, 2002) signatures, reduce metadata linkability and empower holders to share only what is strictly necessary, thus enhancing privacy and reducing risks like identity theft. While these techniques offer basic data minimization, general-purpose zero-knowledge proofs (e.g., zk-SNARKs) go further by enabling anonymous credentials to fulfill critical requirements such as scalable revocation, programmable accountability, or designated verifier presentations (Feulner et al., 2022; Hardman, 2020; Schellinger et al., 2022; Schlatt et al., 2022; Sedlmeir et al., 2022; Young, 2022). These features are often absent in even advanced identity systems like Hyperledger Aries cloudagent in Python (ACA-Py), but can be implemented efficiently using zk-SNARKs (Research Paper 6).

Research Paper 6 describes the implementation of such credentials in detail and highlights their potential. Consider two examples to illustrate their benefits:

First, complex predicates across multiple credentials become feasible. During the COVID-19 pandemic, individuals were often required to present both vaccination certificates and identity documents. Verifying that both documents matched and fulfilled the requirements involved manual checks, leading to errors and oversharing of unrelated information (e.g., gender, residence, other vaccinations). With a zk-SNARK-based approach, a single verifiable presentation could confirm: (1) both credentials belong to the same person, and (2) the required vaccination is recorded, without disclosing any additional information. This also streamlines the process, enabling efficient, privacy-preserving checks (Research Paper 6).

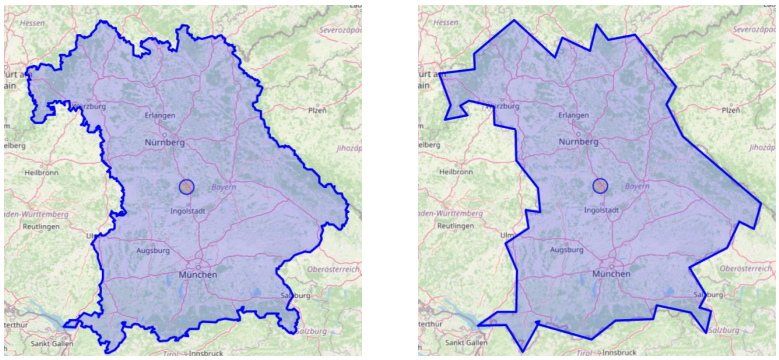

Figure 3: Approximating the boundary of Bavaria such that a location can be efficiently verified with a ZKP; Source: Research Paper 6

Second, general-purpose zero-knowledge proofs allow for computations over credential data. For example, if a distributed energy ressource must prove it operates within a specific region, disclosing its exact geolocation may compromise privacy. Instead, a polygon-bound proof algorithm can verify whether coordinates (latitude/longitude) lie within a defined area. A zero-knowledge proof-based verifiable presentation could thus reveal only a yes/no answer to the question "Is the asset within region X, described through polgyon Y?" without exposing the exact location. Research Paper 6 includes an implementation using a region approximated by 50 vertices representing Bavaria (Figure 3) (Research Paper 6).

By introducing wallet-based identity management, self-sovereign identity emphasizes data sovereignty for holders and verifiability for verifiers. Holders manage identity attributes through verifiable credentials stored in digital wallets, placing users at the center rather than the edge of identity management (Sartor et al., 2022; Weigl et al., 2022). This approach also aims for reforcing user's consciousness in the usage of their identity data addressing the privacy paradox, where users often disclose more information online than intended (Gimpel et al., 2018; Norberg et al., 2007). Traditional methods require disclosure of entire documents, often resulting in over-sharing of information, while self-sovereign identity supports selective disclosure and advanced data minimization techniques like zero-knowledge proofs, limiting the exposure to necessary information (Glöckler et al., 2023, Research Paper 6). By enabling predicate disclosures rather than exact data, and by using advanced cryptographic signatures to prevent unnecessary linkability (Camenisch and Lysyanskaya, 2002; Looker et al., 2022), holders gain granular control over their data sharing, significantly enhancing privacy and reducing risks like identity theft (Research Paper 5 and 6).

Self-attested identity data is vulnerable to fraud and poor quality, while traditional verification processes are costly and inefficient (Lacity and Carmel, 2022; Sedlmeir et al., 2021a). In contrast, self-sovereign identity promotes an open ecosystem based on trusted relationships between issuers and verifiers, leveraging machine-verifiable credentials to assure authenticity and integrity, thus providing an infrastructure for veriable data (Mühle et al., 2018). This reduces costs for verifiers, lowers entry barriers, and supports broad adoption (Schlatt et al., 2022). Verifiability in self-sovereign identity systems involves confirming data integrity and authenticity, including checks for validity, expiration, and revocation (Preukschat and Reed, 2021; Sedlmeir et al., 2021a). Verifiable data registries securely link issuer identities and public keys, enhancing trust and facilitating decision-making by verifiers. Although many self-sovereign identity initiatives initially focused on decentralized registries using distributed ledger technology, future implementations might favor broader decentralized ecosystems beyond specific technologies (Koens and Meijer, 2018; Mühle et al., 2018, Research Paper 5).

In summary, self-sovereign identity presents a foundational approach to digital identity management that addresses key challenges of verifiability, data sovereignty, and privacy. By empowering users through wallet-based identity management and advanced cryptographic techniques, self-sovereign identity reduces information asymmetries and strengthens trust between stakeholders. These capabilities are particularly vital in sustainability-related digital ecosystems, such as greenhouse gas tracing or digital product passports, where trustworthy and verifiable data exchange is essential for coordination and accountability. More generally, self-sovereign identity inherently aims to address the conflict verifiability poses to sovereignty by enabling selective disclosure and minimizing unnecessary data exposure. In doing so, it not only supports a more secure and user-centric digital identity landscape but also acts as a key enabler for broader sustainability objectives in the digital economy (Research Papers 1, 3, 4, 5, 6, and 7).

3 Designing Digital Sustainability Infrastructures

Sustainable digital infrastructures must balance at least two critical requirements: data verifiability and data sovereignty. Emerging use cases across climate and resource governance, such as verifiable greenhouse gas tracking, decentralized redispatch, or the implementation of digital product passports for circularity, rely on fine-granular, trustworthy data. At the same time, they must ensure that data holders retain control over their digital assets. This tension challenges the design of open, cross-sectoral infrastructures that can support verifiable, sovereign data exchange at scale.

This chapter presents a set of technical design results that respond to this challenge by proposing modular, decentralized infrastructure components grounded in Web3 technologies. These components are designed to facilitate machine-verifiable trust relationships across organizational boundaries while safeguarding user autonomy and limiting information asymmetry.

This section is structured as follows: section 3.1 focuses on the binding of master and operational data in sustainability contexts. Building on the concept of verifiable credentials and digital wallets from the self-sovereign identity paradigm, this section proposes an infrastructure for machine-verifiable data exchange that can function in environments, where trust gaps exist, while reducing onboarding friction and enabling cross-sectoral reuse of Digital Sustainability data. Section 3.2 explores how generic zero-knowledge proofs can be used to reconcile the inherent trade-offs between verifiability and sovereignty. It shows how zero-knowledge proofs enable data minimization and predicate-based disclosure, thus allowing actors to verify claims about data without seeing the data itself thereby making shared data both private and verifiable. Section 3.3 introduces shielded fractionalized non-fungible tokens (SFNFTs), a novel token-based design for tracing single-sourced goods like electricity or hydrogen. By combining fractionalized ownership with privacy-preserving rollups, this approach ensures that environmental attributes of digital goods remain verifiable without disclosing sensitive production or consumption details. Section 3.4 builds upon the SFNFT infrastructure to design a decentralized architecture for digital product passports. It extends the model to represent complex, multi-sourced products across modular value chains. The proposed architecture supports verifiable, issuer-independent transfer of product lifecycle data, thereby enabling regulatory compliance, circular economy practices, and greater user agency over digital product information.

Together, the results present a coherent technical vision for how verifiability and sovereignty can be embedded directly into the architecture of digital infrastructures for sustainability closing critical trust gaps. By leveraging verifiable credentials, decentralized identifiers, privacy-preserving proofs, and token-based asset representations, these designs contribute to the creation of resilient, scalable, and ethically grounded data ecosystems.

3.1 Implementing Verifiable Master and Operational Data

While the amount of data and the number of actors in data ecosystems continue to grow, access remains constrained. For instance, Germany's public smart meter infrastructure rollout for its electricity system is still in progress resulting in blind data spots (Bundesnetzagentur, 2025). Private infrastructure, like already exsting data energy management systems, could potentially fill this gap. However, even though modern devices generate both operational and master data, this information is often siloed by original equipment manufacturers (OEMs) or service providers. Although the European Data Act promotes fair data access (European Commission, 2023), implementing interoperable infrastructures remains difficult, and data silos continue to reinforce platform lock-ins (Verhulst, 2023).

Generally, data can be separated into master and operational data (Research Paper 1). Operational data – dynamic data documenting or predicting the behavior of assets – serves as the fuel of digital ecosystems and is vital for any Digital Sustainability use case. However, to generate value from operational data through sharing, it must be combined with the corresponding master data – static information that defines identity properties and may include identifiers of the asset producing the data (Research Papers 1 and 3).

This combination enables labeling of operational data, which is crucial for use cases such as proof-of-origin. For instance, metering data alone has limited value unless linked to master data, such as information about the renewable energy source generating it. While current infrastructures address this to some extent, master and operational data are often managed separately. Information systems typically construct contextual links internally, but when data is shared beyond system boundaries, especially in untrusted environments, its original context and associated value may be lost (Research Paper 3). Hence, verifiably binding operational to master data becomes essential.

Establishing a robust master data infrastructure is therefore fundamental. Findings from Research Papers 1, 3, 4, and 6 suggest that infrastructures based on the paradigm of self-sovereign identity can support sustainability-related use cases by promoting data verifiability and sovereignty, enabling cross-sector data reuse. Digital wallets holding verifiable credentials from trusted issuers (e.g., OEMs) streamline verification, reduce onboarding costs, and make small-scale sustainability solutions economically viable (Research Papers 1, 3, 4, and 5).

Equipping end users or their devices with such wallets also mitigates lock-in effects and lowers the barriers to data sharing (Research Papers 4, 5, and 7). Building private, trusted infrastructures is costly, particularly in the absence of trust between service providers and users. Verifiable credentials minimize the need for repeated verification and support efficient, trustworthy data flows.

Nonetheless, binding operational and master data is non-trivial and faces the oracle problem (Babel et al., 2023). Research Papers 1, 5, and 7 highlight two main approaches to address this challenge. One involves leveraging existing trust structures, such as trusted parties, who already generate certified reports and could act as public trusted issuers within an self-sovereign identity-based ecosystem. Another approach is using trusted metering devices equipped with digital wallets. By storing master data bound to a securely held cryptographic key in, for example an hardware secure module, and signing operational data, devices can cryptographically prove both the authenticity and the source of data. While this requires sufficient edge computing and Internet access, hybrid solutions such as edge-cloud architectures offer viable alternatives (Babel et al., 2023; Deutsche Energie-Agentur (dena), 2024, Research Paper 1).

To illustrate, a private customer's photovoltaic system could be equipped with a digital wallet. The entirety of the information pertaining to the system is securely stored within the designated wallet. All measured values are recorded in real time via trusted hardware and cryptographically linked with the identity data from the digital wallet. Consequently, the proprietor of the facility is able to assign precise, quantifiable values to the electricity generated, values that are associated with the identity data of the facility, including such characteristics as geographical location and sustainability metrics. These values can be stored for the purpose of internal reporting or transferred within the context of sale.

As relying on blockchain infrastructure for establishing trust between issuers and verifiers is not mandatory, its use can nevertheless support seamless onboarding of new issuers

and encourage cross-sectoral adoption of identity infrastructures. Due to its decentralized governance mechanisms, blockchain may also help prevent unwanted centralization of control, thus reinforcing the principles of sovereignty and openness (Research Paper 5).

Despite the promise of self-sovereign identity, several barriers remain. Its decentralized architecture still relies on foundational infrastructure developed by initial stakeholders. To date, no cross-sectoral agreement on unified architectures or standards exists (Research Paper 5). Initiatives like eIDAS 2.0 are promising but limited; they focus on individuals and organizations, excluding machine identities, and lack a diverse network of credential issuers. Moreover, self-sovereign identity shifts control from issuers to data holders, disincentivizing participation by organizations unless regulatory or economic incentives are introduced. Without such measures, crucial data may remain siloed, hindering the development of sustainable digital infrastructures.

3.2 Zero-Knowledge Proofs to Mediate Between Data Verifiability and Sovereignty

In today's digital markets, particularly regarding Digital Sustainability, data is often multilaterally shared: Data often does not remain solely with its subject or initial holder but is shared among various data consumers and providers, and moved across multiple data infrastructures. This can occur directly or indirectly between parties that may not trust one another (Babel and Körner, 2025; Scherenberg et al., 2024). Consequently, maintaining data sovereignty for data subjects, even with the best intentions, proves to be a considerable challenge.

Verifiability of shared data creates constraints that can further endanger data sovereignty. Firstly, verifiability requires validation of data origin from a source that is deemed trustworthy by the data consumer. This requirement may lead to the introduction of new participants such as trusted third parties, who might assume the role of data holders. As a result, data subjects could lose control over their data and their ability to share it, thereby jeopardizing their data sovereignty. Secondly, the need to maintain data verifiability often conflicts with the use of privacy-enhancing methods. Sharing aggregated data from multiple data subjects, which could afford herd privacy for individual data assets, becomes impractical as it compromises the verifiability of each asset. Third, verifiability dramatically enhances the value of data. Data pertaining to subjects is initially just a claim and,

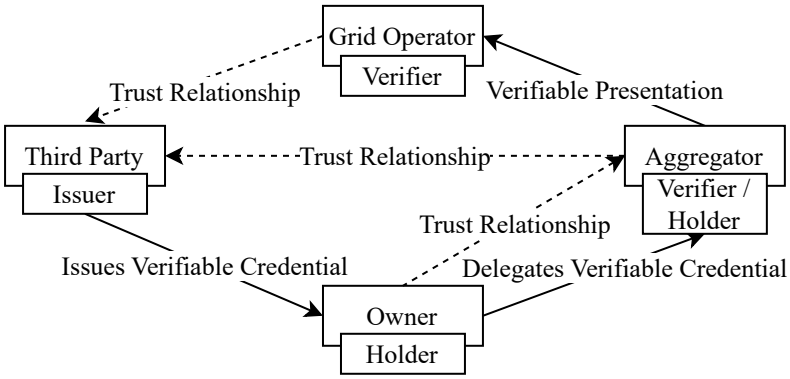

Figure 4: Trust Diamond; Source Research Paper 4

therefore, inherently questionable. Once data is rendered verifiable, its accuracy and association with the data subject are established with greater reliability. Sharing verifiable data thus poses a significant threat to the distinctive sovereignty of data subjects (Research Paper 1, 3, and 4).

As soon as data is shared, data sovereignty is threatend. Therefore, keeping shared data to a minimum is essential. In the context of self-sovereign identity, the distinction between verifiable credentials and verifiable presentations plays a central role in preserving data sovereignty by limiting data exposure. Generic zero-knowledge proofs support this goal by enabling application-specific predicates that uphold the verifiability of data while minimizing the information actually shared (Research Paper 6).

For example, in the use case of *Decentralized Redispatch*, the aggregator collects data from its flexibility pool and must present it to the grid operator (see figure 4), a presentation of data the asset owner may not intent, thus loosing sovereignty. As the grid operator does not require individual asset data, which may be sensitive for asset owners, the grid operator does require assurance of predicates about this data. Zero-knowledge proofs enable the aggregator to prove statements, for example, about the aggregated flexibility potential of its assets without disclosing individual data points. Thereby the aggregator respects data owner's data sovereignty through the application of zero-knowledge proofs (Research Paper 4). In this way, the application of zero-knowledge proofs helps to reconcile the tension between data verifiability and data sovereignty in data sharing environments. Nonetheless, Research Paper 4 describes this data sovereignty as derived sovereignty, as it depends on fair behaviour of another party (aggregator) in the multilateral data sharing chain.

3.3 Tracability of Single-Sourced Goods Through Shielded Fractional Non-Fungible Tokens

Blockchain digitally solves the double-spending problem without the need for a trusted intermediary. “A token is a sequence of characters that serves as an identifier for a specific asset (e.g., a personalized usage right) or asset type (e.g., a cryptocurrency). The abilities to represent assets in form of digital tokens on a decentralized digital platform and to assign ownership of these assets to agents in a fraud-resistant way can help to reduce drawbacks related to TTPs [trusted third parties] (e.g., the presence of single points of failures) and enable a new type of economy: the token economy” (Sunyaev et al., 2021, p. 1).

Tokens can be categorized in multiple ways, including utility, security, native, or governance tokens (Voshmgir, 2019). This work focuses on the use of tokens to claim and transfer ownership of assets. Tokens can broadly be classified as fungible (e.g., represented by the ERC-20 standard) or non-fungible (e.g., ERC-721). Non-fungible tokens (NFTs) represent heterogeneous goods such as art or real estate. In contrast, fungible tokens represent homogeneous goods, such as money or electricity. However, in the context of greenhouse gas trading and tracing, it becomes increasingly important to distinguish electricity by its attributes. Rather than tracing physical electricity flows – a complex and ongoing research challenge – this work limits to balance sheet-based system.

Research Paper 1 proposes a hybrid approach that represents electricity as fractionalizable NFTs. The master data of the generating asset forms the base-attributes of the NFT, which is minted at regular intervals. This enables fine-granular labelling of electricity based on the characteristics of its generation. As one production interval may serve multiple consumers, each NFT is fractionalized, and the corresponding shares are transferred proportionally to the actual electricity consumption. This representation of NFTs as fractionalized tokens actively prevents double spending of green electricity, as labeled electricity can only have one owner. Such a mechanism relies on a highly digitalized infrastructure, ideally with digital wallets at the edge and secure metering systems.

Electricity production and consumption data may include sensitive information. If recorded on a public blockchain, this data is accessible to all participants. While using a private blockchain limits access, it also compromises decentralization. To address this trade-off, Research Paper 1 adopts a zk-rollup approach (see section 2.3.2) to ensure pri-

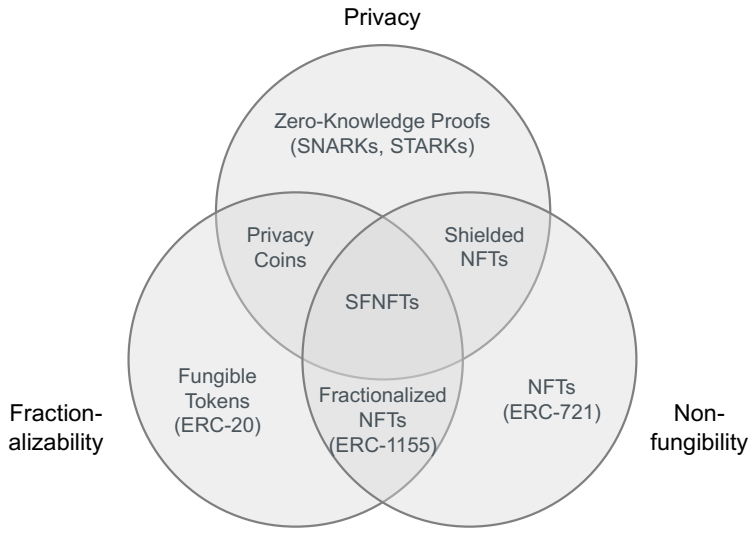

Figure 5: Combining fractionalisability, non-fungibility, and privacy; Source: Research Paper 1

vacy. Figure 5 presents the intersections between the concepts of fungible, non-fungible and shielded tokens. With zk-rollups, transaction details remain completely private: only the sender and recipient know the transaction, while zero-knowledge proofs ensure correctness and prevent double spending. This enables anchoring on either public or private blockchains – or even a centralized ledger – without disclosing transactional data. The only requirements for the network are availability and non-discrimination, ensuring that no transaction is refused or modified post-submission.

Combining NFTs with fractionalizability and zero-knowledge proofs, Research Paper 1 introduces shielded fractionalized non-fungible tokens (SFNFTs) as a mechanism for verifiably and sovereignly labeling electricity. This approach contributes to the field of greenhouse gas trading and tracing by enabling verifiable, fine-granular proofs-of-origins while maintaining data sovereignty for all participants. By providing high-resolution data, SFNFTs empower consumers to make greenhouse gas-adaptive decisions (Research Paper 1 and 3). Beyond electricity, the concept is applicable as digital product passport to other single-sourced goods like flow-based or fungible goods that benefit from fine-grained, traceable labeling, such as hydrogen or synthetic fuels, where verifiability and sovereignty are equally critical in ensuring transparency and trust across supply chains.

However, this approach also entails two major limitations. First, regarding data sovereignty: although transaction details remain visible only to sender and receiver, the primary data embedded in the NFT travels along the entire electricity supply chain. This compromises the sovereignty of the original asset holder who minted the token, which

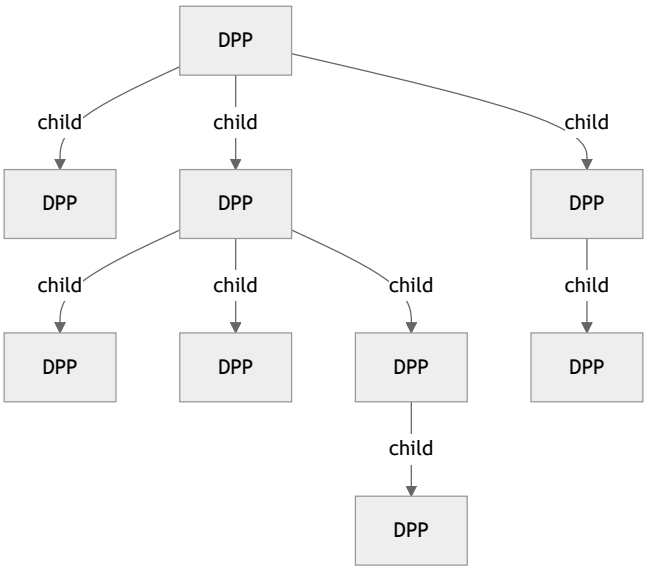

Figure 6: Example of a nested digital product passport; Source: Research Paper 7

poses an unavoidable trade-off as long as primary data remains necessary. Second, while rollups are designed to address blockchain scalability issues, the practical scalability of this approach remains to be demonstrated in the field. The fine-granular metering and transfer of energy data may result in substantial data volumes. Moreover, using zero-knowledge proofs for privacy adds computational overhead, potentially exceeding that of more lightweight solutions like optimistic rollups (Research Paper 2).

This implementation illustrates how token-based representations combined with zero-knowledge proofs can address the challenge of missing fine-granular, verifiable data required for CO_2-aware decision making, thereby supporting decarbonization as a key objective within Digital Sustainability. At the same time, it preserves the privacy of electricity consumption patterns of individuals and organizations, contributing to socially and economically responsible data handling and promoting sovereignty in digital energy infrastructures.

3.4 Implementing Verifiability and Sovereignty in a Digital Product Passport Infrastructure

The infrastructure the preceding section presents demonstrates strong potential for labeling single-sourced goods, such as electricity, along their supply chains. However, the

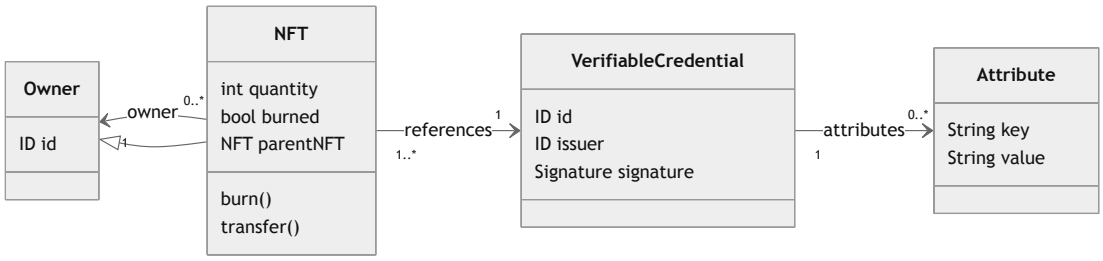

Figure 7: Class Diagram of a DPP; Source: Research Paper 7

restriction to single-source provenance constitutes a significant limitation, as most goods in today's globalized economy are manufactured within multi-layered value chains. To overcome this limitation and enhance applicability to generic goods, Research Paper 7 extends the SFNFT concept by introducing a nested digital product passport structure. This structure aggregates individual credentials from various stages of value creation into an unbalanced tree, as illustrated in Figure 6. It thereby enables a domain-agnostic representation of complex supply chains (Babel et al., 2025, Research Paper 1 and 7).

Figure 7 provides an overview of the technical implementation that combines SFNFTs with verifiable credentials to realize digital product passports and their nesting. Each individual digital product passport consists of a verifiable credential encapsulating static value creation data, and a corresponding NFT that manages dynamic states and ownership. In contrast to traditional verifiable credentials, the holder identity field is omitted. Ownership is instead governed by the linked NFT, which eliminates the need for issuer involvement in each transfer and thereby preserves user autonomy across the product lifecycle (Research Paper 1, 5 and 7).

The *quantity* attribute specifies the fractional share of the credential owned via NFTs, with the underlying infrastructure preventing double spending and ensuring that fractions sum to the original value. The *burned* attribute marks credentials as consumed or transformed (e.g., electricity consumed (Research Paper 1)). The *parentNFT* field links digital product passports in nested structures. In such cases, the parent NFT inherits ownership, allowing recursive representation of products and subcomponents. Each end-user manages these assets via a digital wallet (Research Paper 1 and 5), which stores key pairs, NFTs, verifiable credentials, and supports the creation of verifiable presentations (Research Paper 6). This setup empowers users as custodians of their product information thus enhancing their data sovereignty (Research Paper 1 and 7).

Digital product passports have gained traction in the information system domain as inter-organizational data carriers for transparently documenting product lifecycle information across value chains. To advance their practical applicability, Research Paper 7 proposes a decentralized, modular, and transferable digital product passport infrastructure that ensures verifiability and supports data sovereignty for all participants. Building on the concept of SFNFTs (Research Paper 1), the proposed design addresses limitations of centralized systems by enabling issuer-independent digital product passport that remain verifiable and transferable across organizational boundaries and product ownership transitions. This is achieved by decoupling data authenticity, ensured through digitally signed verifiable credentials, from ownership, managed through NFTs, which allows data subjects to retain long-term control without ongoing dependency on original issuers (Sunyaev et al., 2021, Research Paper 2, 5, and 7).

The architecture supports nested digital product passports, enabling parent-child hierarchies that reflect the modular composition of physical goods. Each module is represented by a discrete verifiable credential, linked via fractionalized NFTs. Since all digital product passports remain intact, this approach facilitates traceability across multi-tiered supply chains. It allows product data to be independently verified and transferred at the component level, enabling granular documentation of value creation in multi-sourced goods (Research Paper 7). The implementation also introduces data sovereignty techniques that ensure product data persists beyond the control of manufacturers. Verifiable credentials remain anchored to the product owner and can be transferred alongside ownership, while mechanisms such as strong double-spending prevention safeguard against fraud, such as using the same digital product passport for multiple goods. Additionally, long-term data availability is independend from issuers exit the market or digital services cease to exist (Research Paper 7).

These architectural decisions lay the foundation for a verifiable and sovereign digital product passport infrastructure that centers the product owner in the circular economy. This not only preserves the digital self-determination of individuals and organizations regarding their product data, but also contributes to a more dynamic and open circular economy. Full control about the digital product passport for the owner of the corresponding good allows a holistic, independent of central service providers such as OEMs, management of the good. Ultimately, this supports extended product lifetimes, strengthens user auton-

omy, and enables the emergence of new service-oriented business models (Human et al., 2022; Human and Cech, 2020; Li et al., 2024, Research Paper 7).

4 Conclusion

Datafication holds tremendous potential to enable data-driven Digital Sustainability. Vast amounts of data on products, processes, and behaviors are theoretically available, offering the foundation to optimise material flows, reduce emissions, and foster circular value creation. However, this potential remains largely untapped, as relevant data is often confined to intentional and structural silos, inaccessible to those who need it for sustainability-related decision-making. Unlocking these silos is essential to fully leverage data for environmental, social, and economic sustainability. This requires data infrastructures that facilitate large-scale exchange of both master and operational data, while ensuring the trustworthiness of the information being shared. Data verifiability is not a luxury – it is a prerequisite for meaningful and value-adding utilisation. Yet collecting verifiable data through centralised, top-down approaches, such as rigid regulatory reporting, risks undermining the autonomy of those who generate and own the data. Even if such measures aim to serve environmental goals, they may neglect the social and economic dimensions of sustainability. Ensuring data sovereignty, that is, giving data owners control over access, usage, and disclosure, is therefore equally important. Data infrastructures can only truly support Digital Sustainability in a comprehensive and equitable manner when verifiability and sovereignty are addressed in tandem.

This cumulative thesis investigates how digital infrastructures can be designed to enable verifiable and sovereign data ecosystems for sustainability-related use cases. Drawing on a design-oriented Information Systems research approach, it synthesizes insights from seven research papers. The conceptual foundation is developed in the early chapters, introducing key challenges at the intersection of verifiability and data sovereignty in the context of Digital Sustainability. Relevant technologies such as blockchain, zero-knowledge proofs, and self-sovereign identity are introduced and critically assessed on their potential to solve these challenges. The core design contributions are presented across four interrelated areas. First, the thesis outlines how self-sovereign identity-based architectures establish reusable and trustworthy identity and data infrastructures. Second, it demonstrates how zero-knowledge proofs can reconcile the need for data verifiability with the principle of data sovereignty. Third, it introduces SFNFTs as a mechanism to trace single-source goods like electricity while preserving privacy. Finally, the artifact design evolves into a human-centric infrastructure for decentralized and composable digital product passports, enabling fine-grained control over multi-sourced product data. At a more fundamental

level, this thesis contributes to a growing recognition that sustainability is not only a question of material systems but also of digital infrastructures. As societies increasingly rely on data to govern energy, mobility, and consumption, the way this data is structured, verified, and shared becomes a critical determinant of whether digitalization serves the common good or entrenches new forms of control and exclusion. In this light, sovereign and verifiable infrastructures are not merely technological artifacts, but essential building blocks for a more equitable, accountable, and sustainable digital future. The thesis contributes theoretical constructs, technical designs, and practical insights to advance the development of sovereign, verifiable, and sustainability-oriented data ecosystems. It argues that data sovereignty is not merely a normative goal but a functional requirement for equitable, trustworthy, and durable digital infrastructures. Rather than opposing verifiability, sovereignty must be understood as a complementary condition for sustainable innovation that serves both people and the planet.

Notwithstanding the contributions of this thesis, there are several limitations to consider. First, the implementation of infrastructures that preserve verifiability and sovereignty is dependent on the broader adoption of enabling technologies, including digital wallets and trustworthy metering devices. The implementation of such infrastructure at a large scale necessitates considerable expenses, a substantial investment of time, and meticulous coordination efforts. From a technological perspective, the majority of Web3 components examined in this thesis are still in the nascent stages of development. While the presented approaches demonstrate conceptual and prototypical viability, they are not yet prepared for large-scale, production-grade implementation. Furthermore, the artifacts developed in this thesis were validated in controlled, laboratory settings. Further empirical research is necessary to assess their scalability, resilience, and auditability in real-world environments. Current ecosystems continue to experience challenges related to interoperability and standardization for digital data infrastructures, particularly in the absence of regulatory clarity or supportive market mechanisms. This encompasses the resolution of bootstrapping challenges and the establishment of governance models and incentive structures that facilitate equitable participation, thereby ensuring that end users and prominent technology providers can interact on a level playing field. This is particularly salient in contexts where existing infrastructures are lacking, as it can result in the emergence of fragmented and centralized data platforms rather than a shared, interoperable infrastructure. Such fragmentation has the potential to exclude smaller actors or niche use cases, thereby hindering inclusive innovation in sustainability-oriented data sharing. However,

the extent to which users will adopt sovereignty-preserving technologies remains uncertain. The privacy paradox posits that even if digital systems are designed to protect user rights, factors such as skepticism, inertia, or convenience may lead individuals to adopt alternatives that are less aligned with user sovereignty. Furthermore, the advent of decentralized data infrastructures, predicated on the principles of profound data sovereignty and a proclivity for self-sovereign agency, has led to the logical expectation of active engagement and responsibility from users. However, the extent to which the general public is willing to engage in data sharing, particularly in the context of sustainability, is not guaranteed. This creates a tension between individual data control and collective sustainability goals. Consequently, it is imperative to investigate the triad of digital sustainability, comprising environmental, social, and economic sustainability, in an integrated manner. This approach ensures that no single aspect is structurally disadvantaged, thereby aiming for a mutually beneficial outcome.

5 References

Adisorn, T., L. Tholen, and T. Götz (2021). "Towards a Digital Product Passport Fit for Contributing to a Circular Economy". In: *Energies* 14.8, p. 2289. DOI: 10.3390/en14082289.

Ahi, P. and C. Searcy (2015). "An analysis of metrics used to measure performance in green and sustainable supply chains". In: *Journal of Cleaner Production* 86, pp. 360–377.

Allen, C. (2016). *The Path to Self-Sovereign Identity*. Life With Alacrity. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 01/30/2023).

Babel, M., V. Gramlich, C. Guthmann, M. Schober, M.-F. Körner, and J. Strüker (2023). "Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme". In: *HMD Praxis der Wirtschaftsinformatik* 60.2, pp. 478–493. ISSN: 2198-2775. DOI: 10.1365/s40702-023-00955-3.

Babel, M., C. Guthmann, M.-F. Körner, T. Kranz, and J. Strüker (2025). "Human-Centric Digital Product Passports: Enabling Verifiable Information Sharing for Sustainable Consumption through Wallet-Based Identity Management and Zero-Knowledge Proofs". In: *Proceedings of the Annual Hawaii International Conference on System Sciences*. URL: https://api.semanticscholar.org/CorpusID:276216280.

Babel, M. and M.-F. Körner (2025). "Trust". In: *Elgar Encyclopedia Of Cryptocurrencies, Blockchain, And Dlt*. Ed. by R. Beck. Edward Elgar Publishing Ltd.

Bartolomeu, P. C., E. Vieira, S. M. Hosseini, and J. Ferreira (2019). "Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT". In: *24th IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 1173–1180. DOI: 10.1109/etfa.2019.8869262.

Ben-Sasson, E., I. Bentov, Y. Horesh, and M. Riabzev (2018). "Scalable, transparent, and post-quantum secure computational integrity". In: *Cryptology ePrint Archive*.

Bernabe, J. B., J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta (2019). "Privacy-preserving solutions for blockchain: Review and challenges". In: *Ieee Access* 7, pp. 164908–164940.

Bitansky, N., R. Canetti, A. Chiesa, and E. Tromer (2012). "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again". In: *Pro-*

ceedings of the 3rd innovations in theoretical computer science conference, pp. 326–349.

Björklund, M., U. Martinsen, and M. Abrahamsson (2012). "Performance measurements in the greening of supply chains". In: *Supply Chain Management: An International Journal* 17.1. Ed. by F. Cucchiella and L. Koh, pp. 29–39. ISSN: 1359-8546.

Bochnia, R., D. Richter, and J. Anke (2023). "Self-Sovereign Identity for Organizations: Requirements for Enterprise Software". In: *IEEE Access* 12, pp. 7637–7660. DOI: 10.1109/access.2023.3349095.

Brandt, J., E. Frost, S. Ferenz, P. H. Tiemann, A. Bensmann, R. Hanke-Rauschenbach, and A. Nieße (2022). "Choosing the right model for unified flexibility modeling". In: *Energy Informatics* 5.1, pp. 1–10.

Braud, A., G. Fromentoux, B. Radier, and O. L. Grand (2021). "The Road to European Digital Sovereignty with Gaia-X and IDSA". In: *IEEE Network* 35.2, pp. 4–5. DOI: 10.1109/mnet.2021.9387709.

Bundesnetzagentur (2025). *Roll-out Intelligente Messsysteme: Quartalsweise Erhebungen*. https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/NetzzugangMesswesen/Mess-undZaehlwesen/iMSys/artikel.html. (Visited on 05/26/2025).

Bünz, B., S. Agrawal, M. Zamani, and D. Boneh (2020). "Zether: Towards privacy in a smart contract world". In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 423–443.

Buterin, V. (2021a). *An Incomplete Guide to Rollups*. https://vitalik.eth.limo/general/2021/01/05/rollup.html. (Visited on 05/16/2025).

Buterin, V. (2021b). *The Limits to Blockchain Scalability*. https://vitalik.eth.limo/general/2021/05/23/scaling.html. (Visited on 05/16/2025).

Buterin, V. (2022). "Proto-danksharding faq". In: *HackMD. July* 30.

Buterin, V. et al. (2014). *A next-generation smart contract and decentralized application platform*.

Cachin, C. and M. Vukolić (2017). *Blockchain consensus protocols in the wild*. URL: https://arxiv.org/abs/1707.01873 (visited on 04/22/2022).

Caldarelli, G. (2020). "Real-World Blockchain Applications under the Lens of the Oracle Problem. A Systematic Literature Review". In: *2020 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*. Marrakech, Morocco: Ieee, pp. 1–6. ISBN: 978-1-7281-5950-8. DOI: 10.1109/ictmod49425.2020.9380598.

Camenisch, J. and A. Lysyanskaya (2002). “A signature scheme with efficient protocols”. In: *International Conference on Security in Communication Networks*. Springer, pp. 268–289. DOI: 10.1007/3-540-36413-7_20.

Chaudhuri, A., B. V. Wæhrens, H. Treiblmaier, and S. F. Jensen (2024). “Impact Pathways: Digital Product Passport for Embedding Circularity in Electronics Supply Chains”. In: *International Journal of Operations & Production Management*. ISSN: 0144-3577. DOI: 10.1108/ijopm-01-2024-0012.

Codagnone, C. and L. Weigl (2023). “Leading the charge on digital regulation: The more, the better, or policy bubble?” In: *Digital Society* 2.1, p. 4. DOI: 10.1007/s44206-023-00033-7.

Constantinides, P., O. Henfridsson, and G. G. Parker (2018). “Introduction - platforms and infrastructures in the digital age”. In: *Information systems research* 29.2, pp. 381–400.

Čučko, Š. and M. Turkanović (2021). “Decentralized and Self-Sovereign Identity: Systematic Mapping Study”. In: *IEEE Access* 9, pp. 139009–139027. DOI: 10.1109/access.2021.3117588.

Davie, M., D. Gisolfi, D. Hardman, J. Jordan, D. O’Donnell, and D. Reed (2019). “The trust over IP stack”. In: *IEEE Communications Standards Magazine* 3.4, pp. 46–51. DOI: 10.1109/mcomstd.001.1900029.

Dedrick, J. (2010). “Green IS: Concepts and Issues for Information Systems Research”. In: *Communications of the Association for Information Systems* 27.Article 11, pp. 173–184. DOI: 10.17705/1cais.02711.

Degen, K. and T. Teubner (2024). “Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective”. In: *Electronic Markets* 34.1, p. 50. DOI: 10.1007/s12525-024-00731-1.

Deutsche Energie-Agentur (dena) (2024). *EnerComputing – Cloud- und Edge-Technologien für ein dezentrales Energiesystem*. Berlin.

Ducuing, C. and R. H. Reich (2023). “Data governance: Digital product passports as a case study”. en. In: *Competition and Regulation in Network Industries* 24.1. Publisher: SAGE Publications Ltd STM, pp. 3–23. ISSN: 1783-5917. DOI: 10.1177/17835917231152799. URL: https://doi.org/10.1177/17835917231152799 (visited on 03/05/2025).

Eberhardt, J. and S. Tai (2018). “Zokrates – scalable privacy-preserving off-chain computations”. In: *International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data*. Ieee, pp. 1084–1091. DOI: 10.1109/Cybermatics_2018.2018.00199.

Ekparinya, P., V. Gramoli, and G. Jourjon (2019). “The attack of the clones against proof-of-authority”. In: *arXiv preprint arXiv:1902.10244*.

Ernstberger, J., J. Lauinger, F. Elsheimy, L. Zhou, S. Steinhorst, R. Canetti, A. Miller, A. Gervais, and D. Song (2023). “SoK: Data Sovereignty”. In: *8th European Symposium on Security and Privacy*. Ieee. Ieee, pp. 122–143. DOI: 10.1109/EuroSP57164.2023.00017.

European Commission (2016). “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): (Text with EEA relevance)”. In: *Official Journal of the European Union*. Ed. by Publications Office of the European Union. URL: https://op.europa.eu/de/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en (visited on 07/26/2022).

European Commission (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*. https://eur-lex.europa.eu/eli/reg/2023/2854/oj. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

Faquir, D., N. Chouliaras, V. Sofia, K. Olga, and L. Maglaras (2021). “Cybersecurity in smart grids, challenges and solutions”. In: *AIMS Electronics and Electrical Engineering* 5.1, pp. 24–37.

Feulner, S., J. Sedlmeir, V. Schlatt, and N. Urbach (2022). “Exploring the use of self-sovereign identity for event ticketing systems”. In: *Electronic Markets* 32, pp. 1759–1777. DOI: 10.1007/s12525-022-00573-9.

Fiorini, L. and M. Aiello (2018). “Household CO_2-efficient energy management”. In: *Energy Informatics* 1.1, pp. 21–34.

Fridgen, G., L. Häfner, C. König, and T. Sachs (2016). “Providing utility to utilities: the value of information systems enabled flexibility in electricity consumption”. In: *Journal of the Association for Information Systems* 17.8.

Fridgen, G., S. Halbrügge, M.-F. Körner, A. Michaelis, and M. Weibelzahl (2022). “Artificial Intelligence in Energy Demand Response: A Taxonomy of Input Data Requirements”. In: *Proceedings of the 17th International Conference on Wirtschaftsinformatik*. URL: https://aisel.aisnet.org/wi2022/sustainable\%5Fit/sustainable\%5Fit/4.

Fridgen, G., R. Keller, M.-F. Körner, and M. Schöpf (2020). “A holistic view on sector coupling”. In: *Energy Policy* 147.

Fuso Nerini, F., T. Fawcett, Y. Parag, and P. Ekins (2021). “Personal carbon allowances revisited”. In: *Nature Sustainability* 4.12, pp. 1025–1031.

Garousi, V., M. Felderer, and M. V. Mäntylä (2016). “The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature”. In: *Proceedings of the 20th international conference on evaluation and assessment in software engineering*, pp. 1–6.

Geissdoerfer, M., P. Savaget, N. M. Bocken, and E. J. Hultink (2017). “The Circular Economy – A New Sustainability Paradigm?” In: *Journal of Cleaner Production* 143, pp. 757–768. ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2016.12.048.

Gholami, R., R. T. Watson, H. Hasan, A. Molla, and N. Bjorn-Andersen (2016). “Information systems solutions for environmental sustainability: How can we do more?” In: *Journal of the Association for Information Systems* 17.8, p. 2.

Gieß, A. and F. Möller (2025). “Exploring the value ecosystem of digital product passports”. In: *Journal of Industrial Ecology*.

Gimpel, H., D. Kleindienst, and D. Waldmann (2018). “The disclosure of private data: measuring the privacy paradox in digital services”. In: *Electronic Markets* 28.4, pp. 475–490. DOI: 10.1007/s12525-018-0303-8.

Glöckler, J., J. Sedlmeir, M. Frank, and G. Fridgen (2023). “A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity”. In: *Business & Information Systems Engineering*. DOI: 10.1007/s12599-023-00830-x.

Goldwasser, S., S. Micali, and C. Rackoff (1989). “The Knowledge Complexity of Interactive Proof Systems”. In: *SIAM Journal on Computing* 18.1, pp. 186–208.

Gregor, S. and A. R. Hevner (2013). “Positioning and presenting design science research for maximum impact”. In: *MIS quarterly*, pp. 337–355.

Guggenberger, T., J. Sedlmeir, G. Fridgen, and A. Luckow (2022). “An in-depth investigation of the performance characteristics of Hyperledger Fabric”. In: *Computers & Industrial Engineering* 173, p. 108716.

Hafid, A., A. S. Hafid, and M. Samih (2020). “Scaling blockchains: A comprehensive survey”. In: *IEEE access* 8, pp. 125244–125262.

Hahn, T., L. Preuss, J. Pinkse, and F. Figge (2015). “Tensions in Corporate Sustainability: Toward an Integrative Framework”. In: *Journal of Business Ethics* 127.2, pp. 297–316. DOI: 10.1007/s10551-014-2047-5.

Hamburger, Á. (2019). "Is guarantee of origin really an effective energy policy tool in Europe? A critical approach". In: *Society and Economy* 41.4, pp. 487–507. ISSN: 1588-9726. DOI: 10.1556/204.2019.41.4.6.

Hardman, D. (2020). *No paradox here: ZKPs deliver savvy trust*. Evernym. URL: https://www.evernym.com/blog/no-paradox-here-zkps-deliver-savvy-trust/ (visited on 12/29/2022).

Heeß, P., J. Rockstuhl, M.-F. Körner, and J. Strüker (2024). "Enhancing Trust in Global Supply Chains: Conceptualizing Digital Product Passports for a Low-Carbon Hydrogen Market". In: *Electronic Markets* 34.1, pp. 1–20. ISSN: 1019-6781. DOI: 10.1007/s12525-024-00690-7.

Hepburn, C. (2007). "Carbon Trading: A Review of the Kyoto Mechanisms". In: *Annual Review of Environment and Resources* 32.1, pp. 375–393. ISSN: 1543-5938. DOI: 10.1146/annurev.energy.32.053006.141203.

Hervani, A. A., M. M. Helms, and J. Sarkis (2005). "Performance measurement for green supply chain management". In: *Benchmarking: An International Journal*.

Hirth, L. and S. Glismann (2018). *Congestion Management: From Physics to Regulatory Instruments*. eng. Tech. rep. Kiel, Hamburg.

Human, S., R. Alt, H. Habibnia, and G. Neumann (2022). "Human-Centric Personal Data Protection and Consenting Assistant Systems: Towards a Sustainable Digital Economy". In: *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*.

Human, S. and F. Cech (2020). "A Human-centric Perspective on Digital Consenting: The Case of GAFAM". In: *Huma centred intelligent systems 2020*.

Icap (2021). *Emissions Trading Worldwide: Status Report 2021*. Berlin. URL: https://icapcarbonaction.com/en/publications/emissions-trading-worldwide-icap-status-report-2021 (visited on 07/26/2022).

Iden3 (2022). *Circom documentation*. URL: https://docs.circom.io/ (visited on 12/29/2022).

Jäger-Roschko, M. and M. Petersen (2022). "Advancing the Circular Economy through Information Sharing: A Systematic Literature Review". In: *Journal Of Cleaner Production* 369, p. 133210. ISSN: 1879-1786. DOI: 10.1016/j.jclepro.2022.133210.

Jarke, M., B. Otto, and S. Ram (2019). "Data sovereignty and data space ecosystems". In: *Business & Information Systems Engineering* 61, pp. 549–550.

Jenkin, T. A., J. Webster, and L. McShane (2011). "An agenda for 'Green' information technology and systems research". In: *Information and organization* 21.1, pp. 17–40.

Jensen, S. F., J. H. Kristensen, S. Adamsen, A. Christensen, and B. V. Waehrens (2023). "Digital Product Passports for a Circular Economy: Data Needs for Product Life Cycle Decision-Making". In: *Sustainable Production and Consumption* 37, pp. 242–255. ISSN: 23525509. DOI: 10.1016/j.spc.2023.02.021.

Jöhnk, J., T. Albrecht, L. Arnold, T. M. Guggenberger, L. Lämmermann, A. Schweizer, and N. Urbach (2021). "The Rise of the Machines: Conceptualizing the Machine Economy". In: *Proceedings of the 25th Pacific Asia Conference on Information Systems*. URL: https://aisel.aisnet.org/pacis2021/54.

Jullien, B. and W. Sand-Zantman (2021). "The Economics of Platforms: A Theory Guide for Competition Policy". In: *Information Economics and Policy* 54, p. 100880. DOI: 10.1016/j.infoecopol.2020.100880. URL: https://scispace.com/papers/the-economics-of-platforms-a-theory-guide-for-competition-552sygjczz?utm\%5Fsource=chatgpt.

Kirchherr, J., D. Reike, and M. Hekkert (2017). "Conceptualizing the Circular Economy: An Analysis of 114 Definitions". In: *Resources, Conservation and Recycling* 127, pp. 221–232. DOI: 10.1016/j.resconrec.2017.09.005.

Koens, T. and S. Meijer (2018). "Matching Identity Management Solutions to Self-Sovereign Identity Principles". URL: https://www.slideshare.net/TommyKoens/matching-identity-management-solutions-to-selfsovereign-identity-principles/1 (visited on 01/30/2023).

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

Kotlarsky, J., I. Oshri, and N. Sekulic (2023). "Digital Sustainability in Information Systems Research: Conceptual Foundations and Future Directions". In: *Journal of the Association for Information Systems* 24.4, pp. 936–952. DOI: 10.17705/1jais.00825.

Krasikov, P. and C. Legner (2023). "Introducing a data perspective to sustainability: How companies develop data sourcing practices for sustainability initiatives". In: *Communications of the Association for Information Systems* 53.1, pp. 162–188.

Kulabukhova, N., A. Ivashchenko, I. Tipikin, and I. Minin (2019). "Self-Sovereign Identity for IoT Devices". In: *International Conference on Computational Science and Its Applications*. Springer, pp. 472–484. DOI: 10.1007/978-3-030-24296-1_37.

Lacity, M. and E. Carmel (2022). “Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet”. In: *MIS Quarterly Executive* 21.3. URL: https://aisel.aisnet.org/misqe/vol21/iss3/6.

Lamport, L., R. Shostak, and M. Pease (1982). “The Byzantine Generals Problem”. In: *ACM Trans. Program. Lang. Syst.* 4.3, 382–401. ISSN: 0164-0925. DOI: 10.1145/357172.357176. URL: https://doi.org/10.1145/357172.357176.

Lehtinen, J. and T. Ahola (2010). “Is performance measurement suitable for an extended enterprise?” In: *International Journal of Operations & Production Management*.

Li, X., B. Li, and Z. Yang (2024). “The Dark Side of Voluntary Data Sharing”. In: *Mis Q.* 49, pp. 155–178. URL: https://api.semanticscholar.org/CorpusID:271776769.

Lima, T. D. de, J. F. Franco, F. Lezama, J. Soares, and Z. Vale (2021). “Joint Optimal Allocation of Electric Vehicle Charging Stations and Renewable Energy Sources Including CO_2 Emissions”. In: *Energy Informatics* 4.2.

Lind, L., R. Cossent, J. P. Chaves-Ávila, and T. Gómez San Román (2019). “Transmission and distribution coordination in power systems with high shares of distributed energy resources providing balancing and congestion management services”. In: *Wiley Interdisciplinary Reviews: Energy and Environment* 8.6, e357.

Looker, T., V. Kalos, A. Whitehead, and M. Lodder (2022). *The BBS signature scheme*. URL: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html (visited on 01/30/2023).

Luers, A., L. Yona, C. B. Field, R. B. Jackson, K. J. Mach, B. W. Cashore, C. Elliott, L. Gifford, C. Honigsberg, L. Klaassen, H. D. Matthews, A. Peng, C. Stoll, M. van Pelt, R. A. Virginia, and L. Joppa (2022). “Make greenhouse-gas accounting reliable - build interoperable systems”. In: *Nature* 607.7920, pp. 653–656. ISSN: 0028-0836. DOI: 10.1038/d41586-022-02033-y.

Meckling, W. H. and M. C. Jensen (1976). “Theory of the Firm”. In: *Managerial Behavior, Agency Costs and Ownership Structure*.

Mejias, U. A. and N. Couldry (2019). “Datafication”. In: *Internet policy review* 8.4.

Melville, N. (2010). “Information Systems Innovation for Environmental Sustainability”. In: *MIS Quarterly* 34, pp. 1–21. ISSN: 02767783. DOI: 10.2307/20721412. JSTOR: 20721412.

Michaelis, A., L. Hanny, M.-F. Körner, J. Strüker, and M. Weibelzahl (2024a). “Consumer-centric electricity markets: Six design principles”. In: *Renewable and Sustainable Energy Reviews* 191, p. 113817.

Michaelis, A., L. Hanny, M.-F. Körner, J. Strüker, and M. Weibelzahl (2024b). "Consumer-centric electricity markets: Six design principles". In: *Renewable and Sustainable Energy Reviews* 191, pp. 1–11.

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

Murray, A., D. Kim, and J. Combs (2023). "The Promise of a Decentralized Internet: What Is web3 and How Can Firms Prepare?" In: *Business Horizons* 66.2, pp. 191–202. ISSN: 00076813. DOI: 10.1016/j.bushor.2022.06.002. (Visited on 11/26/2024).

Nagel, L. and D. Lycklama (2021). *Design Principles for Data Spaces*. Tech. rep. Zenodo. DOI: 10.5281/zenodo.5244997. (Visited on 03/10/2025).

Naik, N. and P. Jenkins (2020). "Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology". In: *8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*. Ieee, pp. 90–95. DOI: 10.1109/MobileCloud48802.2020.00021.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Nations, U. (1998). "Kyoto protocol to the united nations framework convention on climate change". In.

Nations, U. (2015). *Transforming our world: the 2030 Agenda for Sustainable Development*. https://sdgs.un.org/2030agenda. A/res/70/1.

Neramballi, A., L. Milios, T. Sakao, and J. Matschewsky (2024). "Toward a Policy Landscape to Support the Product–as–a–Service Design Process for a Circular Economy". In: *Journal of Industrial Ecology* 28.5, pp. 1045–1059. ISSN: 1088-1980. DOI: 10.1111/jiec.13535.

Nickerson, R. C., U. Varshney, and J. Muntermann (2013). "A method for taxonomy development and its application in information systems". In: *European Journal of Information Systems* 22.3, pp. 336–359. ISSN: 0960-085x. DOI: 10.1057/ejis.2012.26.

Nieße, A., N. Ihle, S. Balduin, M. Postina, M. Tröschel, and S. Lehnhoff (2018). "Distributed ledger technology for fully automated congestion management". In: *Energy Informatics* 1.Suppl 1, p. 22.

Norberg, P. A., D. R. Horne, and D. A. Horne (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors". In: *Journal of Consumer Affairs* 41.1, pp. 100–126. DOI: 10.1111/j.1745-6606.2006.00070.x.

Norman, W. and C. MacDonald (2004). “Getting to the bottom of “triple bottom line””. In: *Business ethics quarterly* 14.2, pp. 243–262.

Pan, S. L., L. Carter, Y. Tim, and M. S. Sandeep (2022). “Digital Sustainability, Climate Change, and Information Systems Solutions: Opportunities for Future Research”. In: *International Journal of Information Management* 63, p. 102444. DOI: 10.1016/j.ijinfomgt.2021.102444.

Parag, Y. and B. K. Sovacool (2016). “Electricity market design for the prosumer era”. In: *Nature energy* 1.4, pp. 1–6.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee (2007). “A design science research methodology for information systems research”. In: *Journal of management information systems* 24.3, pp. 45–77.

Pina, A., C. Silva, and P. Ferrão (2012). “The impact of demand side management strategies in the penetration of renewable electricity”. In: *Energy* 41.1, pp. 128–137.

Plociennik, C., M. Pourjafarian, S. Saleh, T. Hagedorn, A. do Carmo Precci Lopes, M. Vogelgesang, J. Baehr, B. Kellerer, M. Jansen, H. Berg, M. Ruskowski, L. Schebek, and A. Ciroth (2022). *Requirements for a Digital Product Passport to Boost the Circular Economy*. DOI: 10.18420/inf2022_127.

Potting, J., M. P. Hekkert, E. Worrell, A. Hanemaaijer, et al. (2017). “Circular economy: measuring innovation in the product chain”. In: *Planbureau voor de Leefomgeving* 2544.

Preukschat, A. and D. Reed (2021). *Self-sovereign identity*.

Priesmann, J., L. Nolting, C. Kockel, and A. Praktiknjo (2021). “Time series of useful energy consumption patterns for energy system modeling”. In: *Scientific Data* 8.1, p. 148.

Ramsebner, J., R. Haas, A. Ajanovic, and M. Wietschel (2021). “The sector coupling concept: A critical review”. In: *Wiley interdisciplinary reviews: energy and environment* 10.4, e396.

Reich, R., E. Prieto, M. Pauwels, L. Alaerts, and K. van Acker (2025). “Discovering the Circular Economy as a Problem Space for IS Research”. In: *Proceedings of the 58th Hawwaii International Conference on System Sciences*.

Rieger, A., T. Roth, J. Sedlmeir, L. Weigl, and G. Fridgen (2022). “Not yet another digital identity”. In: *Nature Human Behaviour* 6 (1), pp. 3–3. DOI: 10.1038/s41562-021-01243-0.

Rizos, V. and J. Bryhn (2022). “Implementation of Circular Economy Approaches in the Electrical and Electronic Equipment (EEE) Sector: Barriers, Enablers and Policy Insights”. In: *Journal of Cleaner Production* 338, p. 130617. ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2022.130617.

Ross, S. C. and J. L. Mathieu (2020). “A method for ensuring a load aggregator’s power deviations are safe for distribution networks”. In: *Electric Power Systems Research* 189, pp. 1–7.

Rousseau, D. M., S. B. Sitkin, R. S. Burt, and C. Camerer (1998). “Not so different after all: A cross-discipline view of trust”. In: *Academy of management review* 23.3, pp. 393–404.

Sarkis, J., C. Koo, and R. T. Watson (2013). “Green information systems & technologies–this generation and beyond: Introduction to the special issue”. In: *Information Systems Frontiers* 15, pp. 695–704.

Sartor, S., J. Sedlmeir, A. Rieger, and T. Roth (2022). “Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets”. In: *Proceedings of the 30th European Conference on Information Systems*. URL: https://aisel.aisnet.org/ecis2022\%5Frp/46.

Schär, F. (2021). “Decentralized finance: on blockchain and smart contract-based financial markets”. In: *Review of the Federal Reserve Bank of St Louis* 103.2, pp. 153–174.

Schellinger, B., J. Sedlmeir, L. Willburger, J. Strüker, and N. Urbach (2022). “Mythbusting Self-Sovereign Identity (SSI). Discussion paper on portable digital identities”. In: URL: https://www.fim-rc.de/wp-content/uploads/2022/06/Whitepaper\%5FSSI\%5FMythbusting\%5FEnglish\%5Fversion\%5Fcompressed.pdf (visited on 01/30/2023).

Scherenberg, F., M. Hellmeier, and B. Otto (2024). “Data Sovereignty in Information Systems”. In: *Electronic Markets* 34.1, p. 15. ISSN: 1019-6781. DOI: 10.1007/s12525-024-00693-4. (Visited on 02/11/2025).

Schlatt, V., J. Sedlmeir, S. Feulner, and N. Urbach (2022). “Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity”. In: *Information & Management* 59, p. 103553. DOI: https://doi.org/10.1016/j.im.2021.103553.

Schmidt, K., A. Mühle, A. Grüner, and C. Meinel (2021). “Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members”. In: *18th International Conference on Privacy, Security and Trust*. Ieee. DOI: 10.1109/pst52912.2021.9647797.

Schoormann, T., F. Möller, C. Hoppe, and J. vom Brocke (2025). “Digital Sustainability”. In: *Business & Information Systems Engineering*, pp. 1–10.

Schoormann, T., M. Stadtländer, and R. Knackstedt (2021). “Designing business model development tools for sustainability—a design science study”. In: *Electronic Markets*, pp. 1–23. ISSN: 1422-8890.

Schweizer, A., P. Knoll, N. Urbach, H. A. von der Gracht, and T. Hardjono (2020). “To What Extent Will Blockchain Drive the Machine Economy? Perspectives From a Prospective Study”. In: *IEEE Transactions on Engineering Management* 67.4, pp. 1169–1183. DOI: 10.1109/tem.2020.2979286.

Sedlmeir, J., J. Huber, T. J. Barbereau, L. Weigl, and T. Roth (2022). “Transition Pathways towards Design Principles of Self-Sovereign Identity”. In: *Proceedings of the 43rd International Conference on Information Systems*. Ais. URL: https://aisel.aisnet.org/icis2022/is\%5Fimplement/is\%5Fimplement/4.

Sedlmeir, J., R. Smethurst, A. Rieger, and G. Fridgen (2021a). “Digital identities and verifiable credentials”. In: *Business & Information Systems Engineering* 63.5, pp. 603–613. DOI: 10.1007/s12599-021-00722-y.

Sedlmeir, J., F. Völter, and J. Strüker (2021b). “The next stage of green electricity labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use”. In: *ACM SIGENERGY Energy Informatics Review* 1.1, pp. 20–31.

Sein, M. K., O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren (2011). “Action Design Research”. In: *MIS Quarterly* 35.1, pp. 37–56.

Serna-Guerrero, R., S. Ikonen, O. Kallela, and E. Hakanen (2022). “Overcoming Data Gaps for an Efficient Circular Economy: A Case Study on the Battery Materials Ecosystem”. In: *Journal Of Cleaner Production* 374. ISSN: 1879-1786. DOI: 10.1016/j.jclepro.2022.133984.

Shrestha, P., A. Shrestha, and B. Adhikary (2018). “Comparative analysis of grid integration on distributed energy system”. In: *5th International Conference on the Developments in Renewable Energy Technology*, pp. 1–5.

Sporny, M., D. Longley, and D. Chadwick (2022). *Verifiable Credentials Data Model v1.1*. URL: https://www.w3.org/TR/did-core/ (visited on 01/30/2023).

Strüker, J., M. Weibelzahl, M.-F. Körner, A. Kießling, A. Franke-Sluijk, and M. Hermann (2021). *Decarbonisation through digitalisation: Proposals for transforming the energy sector*. Ed. by University of Bayreuth. DOI: 10.15495/EPub{\textunderscore

}UBT{\textunderscore}00005762. URL: https://epub.uni-bayreuth.de/5762/ (visited on 04/22/2022).

Sunyaev, A., N. Kannengießer, R. Beck, H. Treiblmaier, M. Lacity, J. Kranz, G. Fridgen, U. Spankowski, and A. Luckow (2021). "Token Economy". In: *Business & Information Systems Engineering* 63.4, pp. 457–478. DOI: 10.1007/s12599-021-00684-1.

Tafesse, W. and M. Dayan (2023). "Content creators' participation in the creator economy: Examining the effect of creators' content sharing frequency on user engagement behavior on digital platforms". In: *Journal of Retailing and Consumer Services* 73, p. 103357.

Vapen, A., N. Carlsson, A. Mahanti, and N. Shahmehri (2016). "A Look at the Third-Party Identity Management Landscape". In: *IEEE Internet Computing* 20, pp. 18–25. DOI: 10.1109/mic.2016.38.

Venable, J., J. Pries-Heje, and R. Baskerville (2016). "FEDS: A Framework for Evaluation in Design Science Research". In: *European Journal of Information Systems* 25.1, pp. 77–89. DOI: 10.1057/ejis.2014.36.

Verhulst, S. G. (2023). "Operationalizing digital self-determination". In: *Data & Policy* 5, e14.

Vermunt, D. A., S. O. Negro, P. A. Verweij, D. V. Kuppens, and M. P. Hekkert (2019). "Exploring Barriers to Implementing Different Circular Business Models". In: *Journal of Cleaner Production* 222, pp. 891–902. ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2019.03.052.

Voshmgir, S. (2019). "Token economy: How blockchains and smart contracts revolutionize the economy". In: *(No Title)*.

Walden, J., A. Steinbrecher, and M. Marinkovic (2021). "Digital Product Passports as Enabler of the Circular Economy". In: *Chemie Ingenieur Technik* 93.11, pp. 1717–1727. ISSN: 0009-286x. DOI: 10.1002/cite.202100121.

Wan, S., H. Lin, W. Gan, J. Chen, and P. S. Yu (2024). "web3: The Next Internet Revolution". In: *IEEE Internet of Things Journal* 11.21, pp. 34811–34825. ISSN: 2327-4662. DOI: 10.1109/jiot.2024.3432116. (Visited on 11/30/2024).

Watson, R. T., M.-C. Boudreau, A. Chen, and M. Huber (2008). "Green IS: Building sustainable business practices". In: *Information systems* 17, p. 17.

Watson, R. T., M.-C. Boudreau, and A. J. Chen (2010). "Information systems and environmentally sustainable development: energy informatics and new directions for the IS community". In: *MIS Quarterly*, pp. 23–38.

Watson, R. T., W. Ketter, J. Recker, and S. Seidel (2022). “Sustainable energy transition: Intermittency policy based on digital mirror actions”. In: *Journal of the Association for Information Systems* 23.3, pp. 631–638.

Webster, J. and R. Watson (2002). “Analyzing the past to prepare for the future: Writing a literature review”. In: *MIS Quarterly* 26.2, pp. 13–23. URL: https://www.jstor.org/stable/4132319.

Weigl, L., T. J. Barbereau, A. Rieger, and G. Fridgen (2022). “The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility”. In: *Proceedings of the 55th Hawaii International Conference on System Sciences*. URL: https://scholarspace.manoa.hawaii.edu/items/17d400d6-5230-4fc8-a569-7b30b0ef3e82.

Wu, H. and F. Wang (2014). “A survey of noninteractive zero knowledge proof system and its applications”. In: *The scientific world journal* 2014.1, p. 560484.

Yan, Z. and S. Holtmanns (2008). “Trust modeling and management: from social trust to digital trust”. In: *Computer security, privacy and politics: current issues, challenges and solutions*. IGI Global Scientific Publishing, pp. 290–323.

Young, K. (2022). *Being “real” about Hyperledger Indy & Aries / Anoncreds*. URL: https://identitywoman.net/being-real-about-hyperledger-indy-aries-anoncreds/ (visited on 12/29/2022).

Zampou, E., I. Mourtos, K. Pramatari, and S. Seidel (2022). “A design theory for energy and carbon management systems in the supply chain”. In: *Journal of the Association for Information Systems* 23.1, pp. 329–371.

Zeiss, R., A. Ixmeier, J. Recker, and J. Kranz (2021). “Mobilising Information Systems Scholarship for a Circular Economy: Review, Synthesis, and Directions for Future Research”. In: *Information Systems Journal* 31.1, pp. 148–183. ISSN: 1365-2575. DOI: 10.1111/isj.12305.

Zheng, Z., S. Xie, H. Dai, X. Chen, and H. Wang (2017). “An overview of blockchain technology: Architecture, consensus, and future trends”. In: *2017 IEEE international congress on big data (BigData congress)*. Ieee, pp. 557–564.

Zhou, Q., H. Huang, Z. Zheng, and J. Bian (2020). “Solutions to scalability of blockchain: A survey”. In: *Ieee Access* 8, pp. 16440–16455.

6 Appendix

6.1 Research Papers Relevant to This Thesis

Research Paper 1 Babel, Matthias; Gramlich, Vincent; Körner, Marc-Fabian; Sedlmeir, Johannes; Strüker, Jens; Zwede, Till (2022):

Enabling end-to-end digital carbon emission tracing with shielded NFTs.

In: Energy Informatics.
DOI: 10.1186/s42162-022-00199-3.

VHB Jourqual 4: Category C, CiteScore: 5.5, SJR 2024: 0.685, SNIP 2023: 0.76 /67th percentile.

Research Paper 2 Principato, Marc; Babel, Matthias; Guggenberger, Tobias; Kropp, Julius; Mertel, Simon (2023).

Towards solving the blockchain trilemma: An exploration of zero-knowledge proofs.

In: Proceedings of the 44th International Conference on Information Systems (ICIS).

VHB Jourqual 4: Category A, Nominee Best Paper.

Research Paper 3 Babel, Matthias; Körner, Marc-Fabian; Ströher, Tobias; Strüker Jens (2024).

Accelerating Decarbonization Digitally: Status Quo and Potentials of Greenhouse Gas Emission Tracking and Trading.

In: Journal of Cleaner Production.
DOI: 10.1016/j.jclepro.2024.143125

VHB Jourqual 4: Category B, CiteScore: 20.4, SJR 2024: 2.174, SNIP 2023: 2.236 /98th percentile.

Research Paper 4 Babel, Matthias; Ehaus, Marvin; Heeß, Paula; Körner, Marc-Fabian; Schick, Leo; Strüker, Jens (2025). Introducing the Trust Diamond for Energy Flexibility Provision : On the Tension of Data Verifiability and Privacy

In: Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS).

VHB Jourqual 4: B, Best Paper Award in the Decisions Analytics and Service Science track.

Research Paper 5 Babel, Matthias; Willburger, Lukas; Völter, Fabiane; Lautenschlager, Jonathan; Guggenberger, Tobias; Körner, Marc-Fabian; Sedlmeir, Johannes; Strüker, Jens; Urbach, Nils (2025).

Self-Sovereign Identity: A Paradigm for Wallet-Based Identity Management.

In: Electronic Markets.
DOI: 10.1007/s12525-025-00772-0

VHB Jourqual 4: B, CiteScore: 14.8, SJR 2024: 2.325, SNIP 2023: 2.29, /97th percentile.

Research Paper 6 Babel, Matthias; Sedlmeir, Johannes (2025).

Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs.

In: ArXiv.
DOI: 10.48550/arXiv.2301.00823

Research Paper 7 Babel, Matthias; Guthmann, Claus; Körner, Marc-Fabian, Kranz, Tobias; Strüker Jens.

Don't Throw the End-Consumer From the Edge of the Information System: About Human-Centricity in Circular Economy.

submitted

During my PhD, I also contributed to a number of other publications, which are listed below. These publications are not part of the dissertation.

- Babel, Matthias; Guthmann, Claus; Körner, Marc-Fabian; Kranz, Tobias; Strüker, Jens (2025). Human-Centric Digital Product Passports: Enabling Verifiable Information Sharing for Sustainable Consumption through Wallet-Based Identity Management and Zero-Knowledge Proofs. In: *Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS)*, S. 4387–4396.

- Urbach, Nils; Guggenberger, Tobias; Pfaff, Hendrik; Stoetzer, Jens-Christian; Feulner, Simon; Babel, Matthias; Principato, Marc; Lautenschlager, Jonathan (2024). EU Digital Identity Wallet: Anwendungsfälle, Nutzungspotenziale und Herausforderungen für Unternehmen. Frankfurt am Main: Fraunhofer-Institut für Angewandte Informationstechnik FIT.

- Babel, Matthias; Gramlich, Vincent; Paetzold, Felix; Zwede, Till (2024). On the Energy Consumption of a Decentralized Financial Sector. In: Fridgen, G.; Guggenberger, T.; Sedlmeir, J.; Urbach, N. (Hrsg.): *Decentralization Technologies: Financial Sector in Change*. Cham: Springer, S. 247–263.

- Körner, Marc-Fabian; Nolting, Lars; Babel, Matthias; Ehaus, Marvin; Heeß, Paula; Lautenschlager, Jonathan; Radtke, Malin; Schick, Leo; Strüker, Jens; Wiedemann, Stefanie; Zwede, Till (2024). A Digital Infrastructure for Integrating Decentralized Assets Into Redispatch: Decentralized Redispatch (DEER): Interfaces for Providing Flexibility. In: *Bayreuther Arbeitspapiere zur Wirtschaftsinformatik*, Nr. 70. Bayreuth: Universität Bayreuth.

- Babel, Matthias; Gramlich, Vincent; Guthmann, Claus; Schober, Marcus; Körner, Marc-Fabian; Strüker, Jens (2023). Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme. In: *HMD Praxis der Wirtschaftsinformatik*, 60(2), S. 478–493.

- Babel, Matthias; Körner, Marc-Fabian; Zwede, Till (2022). The Potential of Data Sharing for Accelerating Decarbonization: A Research Agenda for IS Scholars. In: *SIGGreen Pre-ICIS Workshop 2022*.

- Munilla Garrido, Gonzalo; Babel, Matthias; Sedlmeir, Johannes (2022). Towards Verifiable Differentially-Private Polling. In: *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022)*, S. 1–11.
- Groß, Jonas; Sedlmeir, Johannes; Babel, Matthias; Bechtel, Alexander; Schellinger, Benjamin (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. In: *SSRN Electronic Journal*.
- Babel, Matthias; Danninger, Nadja; Ehresmann, Andreas; Guggenberger, Tobias; Urbach, Nils; Völter, Fabiane; Wachter, Martin (2020). Digitalisierung in der Justiz – Vertrauen in digitale Dokumente durch Blockchain-Technologie. In: *Wirtschaftsinformatik & Management*, 12(4), S. 18–25.

6.2 Declaration of Co-authorship and Individual Contribution

This doctoral thesis is cumulative and comprises seven research papers. All of them were written in collaboration with multiple co-authors. In this section, I will describe my individual contribution to each of the seven papers.

Research Paper 1 was written by six co-authors. All authors contributed significantly to the paper. Together with three co-authors, I conceptualized and co-developed the research project. In particular, I contributed by analyzing the theoretical and technical foundations of the paper, developing the concept of the solution artifact, implementing the prototype, and elaborating major parts of the text. Moreover, I participated in research discussions and provided feedback on the paper's content and structure. Two additional co-authors supported the research by contributing to the theoretical framing, providing continuous feedback, and mentoring the project throughout. One of them also contributed to the textual elaboration. While two co-author acted in a mentoring and supervisory role and one co-author subordinately contributed to the research. The other three co-authors and I acted as lead authors of the paper.

Research Paper 2 was written by six co-authors. All authors contributed significantly to the paper. Together with four co-authors, I co-initiated and co-developed the research project. In particular, I contributed by developing the paper's theoretical foundation, analyzing the results of the literature review, and elaborating the theoretical contribution. I also engaged in textual elaboration, especially in the introduction, conceptual background,

method, discussion, and conclusion sections. Moreover, I participated in research discussions and provided feedback on the paper's content and structure. Three of the co-authors, including myself, acted as lead authors throughout the entire research process. The other three co-authors contributed on subordinately, supporting the conceptual development, writing process, and feedback cycles in a collaborative manner.

Research Paper 3 was written by four co-authors. Together with one co-author, I initiated and coordinated the research project. I also contributed substantially to the writing, conceptual development, and overall supervision of the work. One co-author authored the major share of the manuscript and collaborated with me on the paper's conceptual framing and revisions. Consequently, that co-author and I acted as the lead authors of the paper. The remaining two co-authors concentrated on supervising the project and giving continuous scientific feedback. Their contributions are therefore considered subordinate.

Research Paper 4 was written by six co-authors. Together with three co-authors, I participated equally in every stage of the research – from conceptualization through writing, revision, and finalization. Within this group of four lead authors, two co-authors focused chiefly on coordinating project management, while I oversaw the conceptual framing and shaped the final contribution. The remaining two co-authors served in a supervisory capacity, providing guidance and feedback throughout the process; their contributions are considered subordinate. Accordingly, the remainding four co-authors, including myself, acted as lead authors.

Research Paper 5 was written by nine co-authors. All authors contributed to the paper. Together with one co-author, I conceptualized and co-developed the research project. In particular, we worked out the paper's theoretical foundation, structured its content, wrote the major share of the text, and led the revisions during peer review. Accordingly, these two co-authors, including myself, acted as lead authors across all phases of the project. Two additional co-authors supported the textual elaboration, helped collect the data, and assisted in the peer-review revisions. Their contributions are considered secondary. The remaining five co-authors provided supervision and scientific mentorship throughout the project and offered feedback to refine the manuscript. Their contributions are likewise considered secondary.

Research Paper 6 was written by two co-authors. Both authors contributed significantly to the paper. Together with the other co-author, I conceptualized the study, developed the software, performed the validation and investigation, and contributed to the visualizations.

I also focused on the writing during the review and editing phases. The other co-author likewise participated in the conceptualization, software development, validation, investigation, and visualization. In addition, that co-author curated the data and supervised the project. Accordingly, both authors acted as lead authors of the research paper.

Research Paper 7 was written by five co-authors. I initiated and coordinated the research project and acted as a single lead author. My contribution spanned all phases of the work, including conceptualization, software development, writing, and overall project management. One co-author focused primarily on coding the artifact and supported the conceptualization. Another co-author contributed mainly to the structuring, research on background, and writing, thus contributed along most research stages, except for the main artifact development. The remaining two co-authors provided supervision and scientific guidance, offering feedback that helped refine the manuscript throughout the process. Accordingly, I served as the lead author, while the other four co-authors contributed as subordinate authors.

6.3 Research Paper 1 – Enabling end-to-end digital carbon emission tracing with shielded NFTs

Authors:
Matthias Babel, Vincent Gramlich, Marc-Fabian Körner, Johannes Sedlmeir, Jens Strüker, Till Zwede

Published in:
Energy Informatics (doi: 0.1186/s42162-022-00199-3)

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.

6.4 Research Paper 2 – Towards Solving the Blockchain Trilemma: An Exploration of Zero-Knowledge Proofs

Authors:
Marc Principato, Matthias Babel, Tobias Guggenberger, Julius Kropp, Simon Mertel

Published in:
Proceedings of the 44th International Conference on Information Systems (ICIS)

Abstract:
Research on blockchain has found that the technology is no silver bullet compared to traditional data structures due to limitations regarding decentralization, security, and scalability. These limitations are summarized in the blockchain trilemma, which today represents the greatest barrier to blockchain adoption and applicability. To address these limitations, recent advancements by blockchain businesses have focused on a new cryptographic technique called" Zero-knowledge proofs". While these primitives have been around for some time and despite their potential significance on blockchains, not much is known in information systems research about them and their potential effects. Therefore, we employ a multivocal literature review to explore this new tool and find that although it has the potential to resolve the trilemma, it currently only solves it in certain dimensions, which necessitates further attention and research.

6.5 Research Paper 3 – Accelerating decarbonization digitally: Status quo and potentials of greenhouse gas emission tracking and trading

Authors:
Matthias Babel, Marc-Fabian Körner, Tobias Ströher, Jens Strüker

Published in:
Journal of Cleaner Production (doi: 10.1016/j.jclepro.2024.143125)

Extended Abstract:
To effectively mitigate climate change, policymakers worldwide established various GHG tracking and trading systems. In the light of ambitious climate goals, stricter regulations, and increasing demand for climate action, various groups such as researchers and governmental institutions suggested additional approaches. This paper addresses the complexity that arises from the breadth of suggested approaches and implemented systems for GHG tracking and trading. By doing so, it synthesizes relevant dimensions in a way that is understandable to enterprises and policymakers, enabling them to design meaningful systems incorporating the reduction of GHG emissions and advance cleaner production. Therefore, this paper presents a first-of-its-kind taxonomy of GHG tracking and trading approaches through a systematic literature review. It illustrates ten main design and implementation dimensions with 30 corresponding characteristics. To accelerate decarbonization, this paper sets impulses for future GHG tracking in the electricity sector based on semi-structured expert interviews. Consecutively, it provides policy directions for CO2-adaptive decision-making for enterprises, formulated as a Call for Action with seven prospective questions. These include, for example, questions concerning technical aspects like data management, legal issues like the sufficiency of existing data security and privacy regulations, as well as economic topics like the calculation of an appropriate local and temporal granularity.

6.6 Research Paper 4 – Introducing the Trust Diamond for Energy Flexibility Provision: On the Tension of Data Verifiability and Privacy

Authors:
Matthias Babel, Marvin Ehaus, Paula Heess, Marc-Fabian Körner, Leo Schick, Jens Strüker

Published in:
Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS)

Abstract:
Data sharing in a digitalized world is increasingly important, but its inherent tension between data verfiability and privacy limits stakeholders engagement. Data consumers need to confirm the data's authenticity while providers fear privacy breaches. 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 seek to ensure data protection and thus privacy. Based on Action Design Research, we develop a Flexibility Provision Data Flow and propose a conceptual Trust Diamond that leverages wallet-based identity management to ensure verifiability and privacy-preserving data sharing. We derive the design principles of Verifiability through Delegation and Derived Sovereignty and show their applicability for optimized grid operations. This study highlights the importance of Information Systems-based solutions to enhance data sharing and address trust concerns between stakeholders.

6.7 Research Paper 5 – Self-Sovereign Identity: A Paradigm for Wallet-Based Identity Management

Authors:
Matthias Babel, Lukas Willburger, Jonathan Lautenschlager, Fabiane Völter, Tobias Guggenberger, Marc-Fabian Körner, Johannes Sedlmeir, Jens Strüker, Nils Urbach

Published in:
Electronic Markets (doi: 10.1007/s12525-025-00772-0)

Abstract:
Current approaches to managing digital identities struggle to meet the demands of ongoing digital transformation. They either create fragmented identities tied to specific online services, making it difficult for users to manage, or they raise concerns about being locked into corporate identity providers and data protection issues. Additionally, they provide limited support for machine-verifiable identity attributes. This reliance on third parties for managing machine identities can put companies at a market disadvantage. Therefore, there is a pressing need for a unified identity management solution that allows for the portable and interoperable use of verifiable identity data across services. The recently announced European Digital Identity Wallet marks a significant step forward in digital identity management. This initiative aims to provide EU citizens with a unified, secure, and convenient way to access both public and private online services, thereby enhancing the efficiency and security of digital interactions and prioritizing user needs. Self-sovereign identity (SSI) forms the basis for such a wallet-based identity ecosystem that supports electronic market growth. However, as a relatively new concept, SSI still lacks a unified theoretical analysis and a thorough exploration of its value propositions for digital ecosystems and networked businesses.

6.8 Research Paper 6 – Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs

Authors:
Matthias Babel, Johannes Sedlmeir

Published in:
ArXiv (doi 10.48550/arXiv.2301.00823)

Abstract:
Today, digital identity management for individuals is either inconvenient and error-prone or creates undesirable lock-in effects and violates privacy expectations. These shortcomings inhibit the digital transformation in general and also make existing digital identity management approaches incompatible with emerging blockchain-based applications. "Decentralized" or "self-sovereign" identity aims to offer a solution by providing individuals with convenient digital wallet applications to manage cryptographic keys and machine-verifiable attestations on their edge devices. However, when presented to relying parties, these attestations typically reveal more identity attributes than required and allow for the tracking of end users' activities through unique cryptographic identifiers. Several proposals from academic research and practical solutions exist to reduce or avoid such excessive information disclosure; ranging from simple selective disclosure techniques to data-minimizing anonymous credentials constructed with zero-knowledge proofs. In this paper, we first demonstrate that currently deployed privacy-oriented self-sovereign identity solutions based on anonymous credentials still lack essential features for large-scale deployment in regulated environments. In particular, we argue that data-minimizing certificate chaining, integration with secure elements without involving a "super cookie", and revocation with a sufficiently large anonymity set represent essential privacy requirements that have thus far not been implemented in large-scale pilots. We then propose to address these pressing challenges by designing anonymous credentials based on general-purpose zero-knowledge proofs in the form of zero-knowledge non-interactive arguments of knowledge (zk-SNARKs). We describe our implementation and conduct performance tests on different edge devices to illustrate that the performance of our construction is already practical. We also discuss further advantages general-purpose zero-knowledge proofs can easily provide for reducing privacy risks; e.g., by facilitating customizable

predicates, data-minimized credential issuance, and “designated verifier presentations” that avoid the risk of breaches of verifiable personal information by relying parties.

6.9 Research Paper 7 – Don't Throw the End-Consumer From the Edge of the Information System: About Human-Centricity in Circular Economy

Authors:
Matthias Babel, Claus Guthmann, Marc-Fabian Körner, Tobias Kranz, Jens Strüker

Submitted

Extended Abstract:
The environmental crisis necessitates a fundamental shift from linear to circular economic models, aiming to extend product lifecycles through reuse, repair, and recycling (Geissdoerfer et al., 2017; Parliament, 2023). Reliable, detailed product-related data is critical for this transition, yet such information remains scarce and challenging to access for consumers (Legner and Schemm, 2008; Morseletto, 2020). To bridge this information gap, digital product passports (DPPs) have emerged, facilitating structured and verifiable data exchange across supply chains, enhancing transparency, accountability, and informed decision-making (Gieß and Möller, 2025; Reich et al., 2025; Zeiss et al., 2021).

However, current DPP designs primarily cater to business-to-business (B2B) contexts, granting consumers limited access and participation. This limited involvement is problematic as consumers increasingly engage in lifecycle-extending activities, such as reuse and repair, and as products often outlive their original manufacturers, leading to potential loss of critical lifecycle data (Ducuing and Reich, 2023; Lefebvre et al., 2025). To ensure continuity and resilience in circular economy (CE) practices, addressing the sovereignty and transferability of product-related data beyond corporate boundaries becomes essential.

Grounded in the concept of *data sovereignty* – the self-determined control over one's economic data goods (Nagel and Lycklama, 2021) – this study asks: *How can DPP infrastructures be designed to ensure sovereign and long-lasting data access for end consumers?* Adopting the design science research (DSR) paradigm (Hevner et al., 2004; Peffers et al., 2007), we pursued a design- and development-centered entry point that commenced with a domain-specific use case in the energy sector and iteratively gener-

alized toward a cross-domain architecture for human-centric DPPs. Our proposed artifact employs verifiable credentials (VCs) and non-fungible tokens (NFTs) to decouple data authenticity from ownership, allowing issuer-independent, dynamic, and secure data management across multiple ownership transitions. On the example of an electric vehicle, we demonstrate that our artifact effectively empowers consumers by enabling sustained, autonomous access to product data, significantly enhancing the practicality of human-centric DPPs.

We introduce four generalizable design principles from our research, enriching the knowledge base for human-centric DPPs infrastructure. Our findings emphasize the potential of decentralized, consumer-empowering data structures to foster active participation in the circular economy, thereby counteracting centralization trends in digital infrastructures. Ultimately, this study contributes to advancing both theoretical and practical dimensions of human-centricity within information systems (IS) and the broader pursuit of sustainable, circular economic practices.

The resulting artifact operationalizes web3 principles by combining self-sovereign identity (SSI) wallets with two complementary token types: VCs encapsulate verifiable product facts, while NFTs represent transferable ownership claims. This novel design pattern *decouples data authenticity from ownership*, thereby enabling issuer-independent validation of product information even after multiple ownership transitions or producer market exits. A wallet-based governance layer affords consumers fine-grained control over disclosure and sharing, embedding sovereignty directly into the technical fabric of the DPP. Performance benchmarking confirms that credential issuance and ownership transfer remain within acceptable latency for interactive consumer scenarios (Babel et al., 2025).

References

Babel, M., C. Guthmann, M.-F. Körner, T. Kranz, and J. Strüker (2025). “Human-Centric Digital Product Passports: Enabling Verifiable Information Sharing for Sustainable Consumption through Wallet-Based Identity Management and Zero-Knowledge Proofs”. In: *Proceedings of the Annual Hawaii International Conference on System Sciences*. URL: https://api.semanticscholar.org/CorpusID:276216280.

Ducuing, C. and R. H. Reich (2023). “Data governance: Digital product passports as a case study”. en. In: *Competition and Regulation in Network Industries* 24.1. Publisher:

SAGE Publications Ltd STM, pp. 3–23. ISSN: 1783-5917. DOI: 10.1177/1783591723 1152799. URL: https://doi.org/10.1177/17835917231152799 (visited on 03/05/2025).

Geissdoerfer, M., P. Savaget, N. M. Bocken, and E. J. Hultink (2017). "The Circular Economy – A New Sustainability Paradigm?" In: *Journal of Cleaner Production* 143, pp. 757–768. ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2016.12.048.

Gieß, A. and F. Möller (2025). "Exploring the value ecosystem of digital product passports". In: *Journal of Industrial Ecology*.

Hevner, A. R., S. T. March, J. Park, and S. Ram (2004). "Design Science in Information Systems Research". In: *MIS Quaterly*.

Lefebvre, H., P. Krasikov, C. Legner, and G. Flourac (2025). "Data management as a joint value proposition–A design theory for horizontal data sharing communities". en. In: *Electronic Markets* 35.1, p. 21. ISSN: 1019-6781, 1422-8890. DOI: 10.1007/s12525-025-00755-1. URL: https://link.springer.com/10.1007/s12525-025-00755-1 (visited on 03/15/2025).

Legner, C. and J. Schemm (2008). "Toward the Inter-organizational Product Information Supply Chain – Evidence from the Retail and Consumer Goods Industries". In: *Journal of the Association for Information Systems* 9.4, pp. 119–150. ISSN: 15369323. DOI: 10.17705/1jais.00156. URL: https://aisel.aisnet.org/jais/vol9/iss4/10/ (visited on 03/15/2025).

Morseletto, P. (2020). "Targets for a circular economy". en. In: *Resources, Conservation and Recycling* 153, p. 104553. ISSN: 09213449. DOI: 10.1016/j.resconrec.2019.104 553. URL: https://linkinghub.elsevier.com/retrieve/pii/S0921344919304598 (visited on 03/15/2025).

Nagel, L. and D. Lycklama (2021). *Design Principles for Data Spaces*. Tech. rep. Zenodo. DOI: 10.5281/zenodo.5244997. (Visited on 03/10/2025).

Parliament, E. (2023). *Circular economy: definition, importance and benefits*. URL: https ://www.europarl.europa.eu/topics/en/article/20151201STO05603/circular-economy-definition-importance-and-benefits.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee (2007). "A design science research methodology for information systems research". In: *Journal of management information systems* 24.3, pp. 45–77.

Reich, R., E. Prieto, M. Pauwels, L. Alaerts, and K. van Acker (2025). "Discovering the Circular Economy as a Problem Space for IS Research". In: *Proceedings of the 58th Hawwaii International Conference on System Sciences*.

Zeiss, R., A. Ixmeier, J. Recker, and J. Kranz (2021). “Mobilising Information Systems Scholarship for a Circular Economy: Review, Synthesis, and Directions for Future Research”. In: *Information Systems Journal* 31.1, pp. 148–183. ISSN: 1365-2575. DOI: 10.1111/isj.12305.