

*Decentralized Information Systems for
Verifiable and Confidentiality-Preserving
Interorganizational Information Sharing*

Dissertation

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

Vorgelegt

von

Jan Robert Stramm

aus

Wachenheim an der Weinstraße

Dekan:	Prof. Dr. Claas Christian Germelmann
Erstberichterstatter:	Prof. Dr. Nils Urbach
Zweitberichterstatter:	Prof. Dr. Jens Strüker
Tag der mündlichen Prüfung:	16.09.2026

*Whereas most technologies tend to automate work(ers) on the periphery
doing menial tasks, blockchains automate away the center.*

Vitalik Buterin

Acknowledgments

Many people contributed to making this dissertation possible and the journey far more bearable. I am deeply grateful for the support, trust, encouragement, and companionship I received, and I sincerely thank all of you.

I thank my doctoral advisor, Prof. Dr. Nils Urbach, for the academic freedom and trust he placed in me, as well as for his intellectual guidance and personal mentorship. His support shaped not only this dissertation but also my development as a person and researcher. I also thank Prof. Dr. Jens Strüker for serving as my co-supervisor and for his valuable guidance and perspectives. My gratitude extends to the University of Bayreuth, the FIM Research Center, and Fraunhofer FIT for enabling a unique setup that was challenging but equally rewarding.

To the 069 Boiz & Girlz office crew, Joni, Simon, Alex, Valeriya, and Vincent, as well as the Bayreuth OGs, Timo, Till, Lynne, Matze, Tobi(es), Marc, and everyone else who accompanied me along the way: thank you for your friendship and for making both everyday work and the road to the doctorate much more rewarding. Each of you, in your own way, showed me the value of pragmatism, well-timed opportunism, compelling storytelling, actually submitting a paper, and creating a supportive and welcoming (work) environment. You also gave me countless padel sessions, memes, becoming work husbands, roles we grew into together, and the confidence of knowing that someone always had my back. To all the student assistants I've had the privilege to coach or work with, I hope you gained as much from me as I gained from you!

To my friends from home (IHE) and Die Bayreuth Gang, thank you for providing balance, distraction, and perspective. You kept me grounded precisely because the “details” of academia were neither fully understood nor particularly important to you.

My heartfelt gratitude goes to my family. Mama, Marianne, thank you for your unconditional support and for always believing in me without ever creating pressure,

including when I decided to stay “at university” for several more years, and my explanations of what I was actually doing there all day became increasingly difficult to follow. Papa, Piet, thank you for supporting me with everything I needed, exactly when I needed it. To both of you, thank you for showing me, long before I had a name for it, what academic rigor means, while also raising me with just the right amount of hippie spirit. You never pushed me in any particular direction. Instead, you taught me to analyze and question the status quo until I understood where I wanted to go, what I wanted to change, and what I needed to do to get there, for myself rather than for anyone else. To my sisters, Anna and Julia, and your families: look, your stupid little brother (and uncle) actually made it ;).

I also want to acknowledge my Oma’s and Opa’s. Although I never had the chance to know you as an adult, even as a child, I sensed the work ethic, perseverance, and outlook on life that I hope I inherited from you. You had to work hard, with your hands, to provide for your family while striving to ensure that the next generation could build on it with their brains. You succeeded: your children attended high school and university, the family prospered, and, one generation later, a doctorate was completed. This journey forms part of a family trajectory that I believe would have made you proud.

Finally, my deepest gratitude goes to Annika. You have been part of this journey from the initial decision in Bayreuth through rejections, endless paper sessions, late nights, and working weekends. You listened to unfinished ideas, shared the disappointments, and accepted that papers and deadlines too often occupied our evenings and weekends. Whenever academia made me question the process or lose sight of what truly matters, you restored my perspective and gave me the confidence to keep going. You celebrated every success with me and made even the most difficult phases easier to endure. Your love, patience, honesty, and unwavering support made this journey possible, and I am deeply grateful to have shared it with you.

Mannheim, August 2026

Jan Stramm

Dissertation Abstract

Interorganizational coordination and decision-making are increasingly dependent on information generated or maintained outside the deciding actor's direct control. These dependencies create information problems involving hidden attributes, limited observability, divergent interests, and legitimate restrictions on disclosure. Decision-relevant information must therefore be verifiable, although unrestricted transparency or the concentration of verification and information access in a single intermediary may undermine confidentiality, organizational autonomy, or legitimate institutional authority. This cumulative dissertation investigates how decentralized information systems can enable verifiable, confidentiality-preserving information sharing. It conceptualizes them as contingent socio-technical arrangements whose suitability depends on the underlying information problem and on how verification, control, and information access are governed.

Accordingly, the dissertation pursues two complementary research goals across six Research Papers. Research Goal 1 develops design knowledge on how decentralized infrastructures can enable verifiable and confidentiality-preserving information sharing. Research Goal 2 conceptualizes what information and properties can be made verifiable through digital representations while limiting disclosure, and under which conditions these representations become effective in interorganizational interactions. The methodological portfolio comprises four design science research studies, phenomenon-based theorizing, and an exploratory qualitative acceptance study. The studies combine artifact development and technical assessment with evidence from literature reviews, project workshops, expert interviews, user interviews, and observational and archival material. The infrastructure-focused findings show that decentralization should be configured rather than maximized. Granular access controls and privacy-enhancing arrangements can reconcile shared process execution with legitimate confidentiality, while layered architectures can combine a publicly verifiable trust anchor with confidential and scalable transaction processing. These technical configurations remain dependent on governance arrangements that define participation, rule-setting, system changes, and accountability. The representation-focused findings distinguish between attestable claims and stateful entitlements. Verifiable credentials preserve the provenance and integrity of claims and make issuer and credential validity verifiable,

allowing forged, altered, revoked, or otherwise invalid evidence to be excluded before it informs consequential decisions. Tokenized representations can preserve the uniqueness and lifecycle of entitlements, while smart contracts can constrain duplicate or unauthorized exercise where the underlying rules are sufficiently formalizable. Zero-knowledge proofs complement both forms of representation by enabling selected properties to be verified without disclosing the underlying information. Their practical effectiveness further depends on institutional recognition and on whether users understand, trust, and accept the corresponding interactions.

The cumulative contribution is a dual-level conceptualization of decentralized information systems that connects verification infrastructures with verifiable digital representations. The findings show that decentralized and cryptographic mechanisms can reconfigure when and by whom information problems are addressed, supporting verification before decisions, ex-ante technical constraints, or stronger ex-post oversight. Verifiable and confidentiality-preserving interorganizational information sharing ultimately requires the problem-specific alignment of infrastructure and representation, embedded in appropriate institutional governance and conditions for effective use.

Keywords: Decentralized Information Systems, Interorganizational Information Sharing, Information Problems, Signaling Theory, Principal–Agent Theory, Design Science Research, Verifiability, Confidentiality, Blockchain, Verifiable Credentials

Abbreviations

AD	Aggregate Dimension	KYC	Know Your Customer
AI	Artificial Intelligence	L1	Layer 1
AML	Anti-Money Laundering	L2	Layer 2
API	Application Programming Interface	MiCAR	Markets in Crypto-Assets Regulation
B2B	Business-to-Business	MR	Meta-Requirement
BIM	Building Information Modeling	PAT	Principal-Agent Theory
CFT	Countering the Financing of Terrorism	PEOU	Perceived Ease of Use
CRM	Customer Relationship Management	PET	Privacy-Enhancing Technology
DID	Decentralized Identifier	PKI	Public Key Infrastructure
DLT	Distributed Ledger Technology	PLONK	Permutations over Lagrange-Bases for Oecumenical Noninteractive Arguments of Knowledge
DO	Design Objective	PU	Perceived Usefulness
DP	Design Principle	PXE	Private Execution Environment
DSR	Design Science Research	QR	Quick Response
EDI	Electronic Data Interchange	RG	Research Goal
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport	RP	Research Paper
eID	Electronic Identification	RQ	Research Question
eIDAS	Electronic Identification, Authentica- tion and Trust Services	SCM	Supply Chain Management
EOA	Externally Owned Account	SLR	Systematic Literature Review
ERC-20	Ethereum Request for Comments 20	SME	Small and Medium-Sized Enterprise
ERP	Enterprise Resource Planning	SOT	Second-Order Theme
EU	European Union	SSI	Self-Sovereign Identity
EVM	Ethereum Virtual Machine	SSO	Single Sign-On
FEDS	Framework for Evaluation in Design Science Research	STARK	Scalable Transparent Argument of Knowledge
FI	Financial Institution	TAM	Technology Acceptance Model
FOC	First-Order Concept	TAM2	Technology Acceptance Model 2
GDPR	General Data Protection Regulation	TPS	Transactions per Second
GPS	Global Positioning System	VC	Verifiable Credential
IdM	Identity Management	VDR	Verifiable Data Registry
IoT	Internet of Things	VHB	Verband der Hochschullehrerinnen und Hochschullehrer für Betriebswirtschaft
IS	Information System	VP	Verifiable Presentation
IT	Information Technology	WTA	Winner-Takes-All
ITC	Income Tax Certificate	ZK	Zero-Knowledge
IU	Intention to Use	zk-	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
JQ4	JOURQUAL 4	SNARK	
		ZKP	Zero-Knowledge Proof

Dissertation Table of Contents

Introduction	1
Research Paper 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management.....	85
Research Paper 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry	87
Research Paper 3: Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy	89
Research Paper 4: From Documents to Verifiable Credentials: How Digital Signal-Carriers Reconfigure Decision-Making in Buyer–Supplier Relationship Formation	91
Research Paper 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control	93
Research Paper 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications	95

Introduction to Decentralized Information Systems for Verifiable and Confidentiality-Preserving Interorganizational Information Sharing

Introduction Abstract

Interorganizational coordination and decision-making are increasingly dependent on information generated or maintained outside the deciding actor's direct control. The resulting information problems require actors to infer hidden attributes and monitor actions or states they cannot fully observe, while divergent interests and legitimate confidentiality requirements constrain information sharing. Decision-relevant information must therefore be verifiable without unrestricted disclosure or concentration in a single intermediary that may undermine organizational autonomy or legitimate institutional authority. This cumulative dissertation investigates how decentralized information systems can enable verifiable, confidentiality-preserving information sharing. It conceptualizes them as contingent socio-technical arrangements whose suitability depends on the underlying information problem and on how verification, control, and information access are governed. The dissertation is organized around two interdependent dimensions and corresponding research goals. Research Goal 1 addresses the infrastructural dimension by examining how verification and control can be allocated while reconciling transparency with confidentiality and technical performance with security and governance requirements. Research Goal 2 addresses the representational dimension by examining what information can be made verifiable through digital representations while limiting disclosure and identifying the conditions required for effective use. The dissertation comprises six research papers, of which four are design science research studies, complemented by phenomenon-based theorizing and exploratory qualitative acceptance research. The findings show that decentralized and cryptographic mechanisms reconfigure how credibility, monitoring, and selective verification are achieved. Their effectiveness depends on aligning infrastructures and digital representations with appropriate governance and conditions for effective use.

Keywords: Decentralized Information Systems, Interorganizational Information Sharing, Information Problems, Verifiability, Confidentiality, Blockchain

Introduction Table of Contents

1 Motivation	4
2 Background	8
2.1 Interorganizational Information Sharing and Coordination Problems	8
2.2 Decentralized Information Systems and Blockchain-Based Infrastructures.	10
2.3 Verifiable Digital Representations and Privacy-Preserving Verification	13
3 Deriving the Research Goals, Gaps, and Questions	16
3.1 RG 1: Develop design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing.....	19
3.2 RG 2: Conceptualize verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing.	23
4 Research Designs	28
5 Summary of the Results.....	34
6 Discussion and Conclusion	47
6.1 Summary.....	47
6.2 Contributions to Theory and Implications for Practice.....	48
6.3 Limitations.....	54
6.4 Potential Avenues for Future Research	57
Introduction References	62
Appendices.....	77
Appendix A: Declarations of Co-Authorship and the Individual Contributions	77
Appendix B: Other Publications by the Author	84

List of Figures

Figure 1: Layered structure of the research goals and cumulative contribution.....	17
Figure 2: Blockchain-based prototype architecture for digital delivery invoice processing developed in RP 2	36
Figure 3: Layered blockchain-based architecture and communication flow presented in RP 3	39
Figure 4: Extension of signaling theory through verifiable digital signal-carriers resulting from RP 4	41
Figure 5: Self-Sovereign Identity acceptance model developed in RP 6	45

List of Tables

Table 1: Overview of the research papers addressing the identified research goals ...	18
Table 2: Overview of the research papers' methodological approaches.....	29
Table 3: Overview of other publications by the author.....	84

1 Motivation

Organizations increasingly create value and make consequential decisions based on information generated, maintained, or controlled by other actors (Constantinides et al., 2018; Möller et al., 2025; Tilson et al., 2010). Industrial data ecosystems and data spaces in supply chains illustrate this development: manufacturers, suppliers, logistics providers, authorities, and other ecosystem participants combine data from multiple sources to coordinate operations, demonstrate regulatory compliance, and develop data-driven products and services, while the underlying information remains distributed across organizations with partly divergent interests (Jussen et al., 2024; Möller et al., 2024; Möller et al., 2025). Because relevant events and states emerge across these distributed processes, actors depend on information beyond their direct control, making it critical to establish its credibility and decision-relevant properties (Abdelkafi et al., 2019; Große et al., 2024; Guggenberger et al., 2020; Gulati et al., 2012). Theoretical perspectives on information problems, for example, signaling and principal–agent theory, formalize distinct manifestations of this dependence. When actors infer hidden attributes from evidence supplied by another party, decision quality depends on whether that evidence constitutes a credible rather than deceptive signal (Connelly et al., 2025; Steigenberger, 2024). When one actor delegates activities to another whose actions cannot be fully observed and whose interests may diverge, information asymmetry may create a principal–agent problem and associated agency costs (Eisenhardt, 1989; Jensen & Meckling, 1976; Ross, 1973). Together, these perspectives show that reliable interorganizational decision-making depends not only on access to externally generated or maintained information but also on mechanisms that make its decision-relevant properties verifiable.

Information systems (IS) can support such verification through different arrangements for integrating information and allocating verification and control functions. A centralized arrangement assigns these functions to a common platform usually provided by an intermediary, which can consolidate information, standardize access procedures, and establish a shared reference point for participating actors (Constantinides et al., 2018; Möller et al., 2025; Schweihoff et al., 2024). Such centralization may be effective when participating actors can appropriately entrust the intermediary with the relevant information, verification functions, and control (Wüst & Gervais, 2018).

Where this condition is not met, the actors face a coordination dilemma. Leaving information fragmented across organizational systems can create reconciliation efforts and verification gaps (Guggenberger et al., 2020; Jussen et al., 2024). Such gaps can allow inconsistent records, deceptive signals, or opportunistic behavior to remain undetected (Bergh et al., 2019; Bossler et al., 2024; Steigenberger, 2024). Concentrating information and associated functions within an intermediary's centralized system may create dependencies in information access, verification procedures, and governing rules (Beck et al., 2018; Gleiss et al., 2023; Guggenberger et al., 2020).

This coordination dilemma becomes particularly consequential when the information required for verification is sensitive, and its holders have legitimate confidentiality concerns about disclosing it in full. In machine leasing, for example, a lessor may need to verify a machine's actual wear, while the lessee seeks to withhold detailed usage information that could reveal its products and production processes (Bossler et al., 2024). Greater transparency could facilitate verification but may simultaneously expose commercially sensitive or otherwise protected information. Conversely, restricting access can protect legitimate confidentiality interests while making it more difficult for other actors to verify the decision-relevant information they depend on (Babel, Ehaus, et al., 2025; Schlatt et al., 2021; Sedlmeir et al., 2022; Sternberg et al., 2021). Coopetition theory provides a valuable perspective on this structural tension: organizations cooperate to create joint value while continuing to compete over its appropriation, making information exchange and the protection of strategically sensitive information legitimate and interdependent requirements (Bengtsson & Kock, 2000; Fernandez & Chiambaretto, 2016). The central problem is therefore not how to eliminate information asymmetries through unrestricted transparency, but how to make inter-organizational, decision-relevant information verifiable while preserving its confidentiality by limiting disclosure of the underlying data.

Where concentrating the required information, verification functions, and control in a single intermediary is inappropriate, decentralized IS offer one alternative by distributing selected functions across participating actors and technical components (Beck et al., 2018; Pedersen et al., 2019; Wüst & Gervais, 2018). Blockchain-based infrastructures, for example, can implement such an allocation through tamper-evident shared records, distributed validation, and programmable rules, without requiring a single organization to control the entire information infrastructure (Babich & Hilary, 2020;

Butijn et al., 2021; Nofer et al., 2017). Yet in highly decentralized architectures, governance functions such as participant admission, rule-setting, system updates, exception handling, and accountability must be deliberately embedded within appropriate technical and institutional governance arrangements (Beck et al., 2018; Ellinger et al., 2024; Rossi et al., 2019; Sternberg et al., 2021). Additionally, verifiability is usually derived from replicated or broadly inspectable system states, creating a structural tension between transparent validation and the protection of sensitive information (Bossler et al., 2024; Sedlmeir et al., 2022). Cryptographic primitives and layered architectural mechanisms create new possibilities for verifying selected information while limiting disclosure. However, their integration introduces technical trade-offs concerning system complexity, scalability, and security (Babel & Sedlmeir, 2023; Guggenberger et al., 2022; Pedersen et al., 2019; Principato et al., 2023), as well as socio-technical challenges concerning governance and effective use (Babel, Willburger, et al., 2025; Richter & Anke, 2026; Schellinger et al., 2022; Schlatt et al., 2021; Schwiderowski et al., 2024). Accordingly, this dissertation examines decentralized IS as contingent design options for settings in which decision-relevant information is generated or maintained across organizational boundaries, concentrating verification and control in a single intermediary is inappropriate, and in which the potential benefits of distributing functions to achieve verifiability justify the associated technical and organizational complexity (Pedersen et al., 2019; Wüst & Gervais, 2018).

Within this scope, decentralized IS can be examined along two interdependent dimensions. The infrastructural dimension concerns *how* to technically enable verification and allocate control over validation, information access, and system rules without undermining confidentiality or legitimate institutional authority (Beck et al., 2018; Mishra et al., 2021; Pedersen et al., 2019; Rossi et al., 2019). The representational dimension concerns *what* information can be represented through claims, transactions, credentials, or entitlements so that relevant properties are verifiable while disclosure of the underlying data is limited. For example, verifiable credentials (VCs) and tokenized representations might be used to encode different types of claims and entitlements (Schwiderowski et al., 2024; Sedlmeir et al., 2021), while cryptographic (zero-knowledge) proofs can make selected properties verifiable without disclosing all underlying information (Babel & Sedlmeir, 2023; Ben Sasson et al., 2014; Bencic et al., 2019; Goldwasser et al., 1989; Principato et al., 2023). Neither dimension can be considered independently. A tamper-evident infrastructure can preserve a recorded state

without establishing whether the information represented by that state is legitimate or decision-relevant (Caldarelli, 2020; Hassan et al., 2023). Conversely, a technically verifiable representation depends on arrangements that determine how it is verified and whether its issuer, state, or associated claim is recognized as legitimate (Babel, Willburger, et al., 2025; Richter & Anke, 2026). Practical effectiveness further depends on whether the actors involved understand and enact the corresponding interactions (Ellinger et al., 2024; Sartor et al., 2022). Verifiable and confidentiality-preserving interorganizational information sharing therefore requires alignment between decentralized infrastructures and the digital representations processed through them, complemented by institutional governance and conditions for effective use.

Against this background, this dissertation investigates the following overarching research question:

How can decentralized information systems enable verifiable and confidentiality-preserving interorganizational information sharing?

To answer this question, the dissertation pursues two complementary research goals (RGs). RG 1 develops design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing. RG 2 conceptualizes verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing. Together, the RGs structure the cumulative investigation around these two interdependent dimensions.

The remainder of this introduction is structured as follows. Section 2 outlines the conceptual and technical foundations of interorganizational information sharing, decentralized IS, and privacy-preserving verification. Section 3 derives the RGs, research gaps, and research questions addressed across the six Research Papers (RPs). Section 4 presents the applied research designs. Section 5 summarizes the results of the six RPs. Section 6 concludes by discussing the dissertation's contributions to theory and practice, its limitations, and potential avenues for future research.

2 Background

This section establishes the conceptual and technical foundations for examining how decentralized IS can enable verifiable and confidentiality-preserving interorganizational information sharing. Section 2.1 conceptualizes interorganizational information sharing as a socio-technical coordination problem and draws on signaling theory, principal-agent theory, and coopetition research to explain why verifiability and legitimate confidentiality become interdependent requirements across organizational boundaries. Section 2.2 introduces decentralized IS and blockchain-based infrastructures as potential coordination mechanisms and examines how different allocations of validation and control create architectural trade-offs. Section 2.3 turns to verifiable digital representations and privacy-preserving verification, explaining how claims and entitlements can become verifiable without requiring unrestricted disclosure and why their effectiveness additionally depends on institutional governance and effective use. These perspectives provide the conceptual foundation for the dissertation's two RGs.

2.1 Interorganizational Information Sharing and Coordination Problems

Interorganizational information sharing constitutes a foundational mechanism through which legally independent actors coordinate activities and govern economic exchange across organizational boundaries. As digital infrastructures become increasingly interconnected, organizations no longer rely solely on internally bounded IS but participate in broader socio-technical networks connecting heterogeneous actors, systems, and institutional settings (Bostrom & Heinen, 1977; Constantinides et al., 2018; Tilson et al., 2010). In such environments, the IS structure determines how information is exchanged, interpreted, verified, and acted upon. Reliable information sharing is therefore central to coordination and decision-making among actors that are interdependent but not governed by a single organizational hierarchy (Große et al., 2024; Guggenberger et al., 2020).

Interorganizational information sharing nevertheless remains difficult because relevant information is distributed across organizations with separate systems, records, and governance responsibilities. This fragmentation can produce inconsistent records, media discontinuities, duplicated documentation, and costly reconciliation efforts

(Guggenberger et al., 2020). More fundamentally, actors frequently depend on information whose origin, accuracy, or strategic presentation they cannot assess directly. The resulting problem is therefore not merely one of transmitting information across organizational boundaries, but of establishing whether information can provide a reliable basis for decisions when actors have limited visibility into one another's characteristics, actions, and processes.

These problems can be understood through complementary theoretical perspectives on information asymmetry. Signaling theory focuses on situations in which one actor possesses hidden qualities or capabilities that another actor must infer from observable signals (Connelly et al., 2011; Spence, 1973). Certifications, audit reports, or credentials can reduce such uncertainty, but only when recipients can assess whether the communicated signal is credible and has not been imitated, distorted, or deceptively presented (Connelly et al., 2011; Steigenberger, 2024). The corresponding verification problem concerns whether observable evidence reliably represents an otherwise hidden attribute. Principal–agent theory addresses a related but distinct situation in which responsibilities are delegated between actors whose interests may diverge. When principals cannot adequately observe the information or actions of agents, agents may exploit this informational advantage, while monitoring and verification create additional agency costs (Eisenhardt, 1989; Jensen & Meckling, 1976; Mahoney, 1995). Here, the verification problem concerns whether delegated actions and resulting states can be reliably observed and assessed. Despite these differences, both perspectives highlight the importance of credible evidence for reducing consequential information asymmetries.

Coopetition research adds an important strategic qualification to this reasoning. Organizations may simultaneously cooperate to create joint value and compete to appropriate individual value (Bengtsson & Kock, 2000; Gnyawali & Park, 2011). Information sharing can support coordination and process integration in such relationships, while excessive disclosure may expose commercially sensitive information and weaken participating organizations' competitive positions. The integration principle of coopetition therefore suggests that cooperative and competitive requirements must be managed jointly rather than optimizing one at the expense of the other (Fernandez & Chiambarretto, 2016). This distinction is important for interorganizational information sharing because not every difference in information access represents a dysfunction that

should be eliminated through greater transparency. Unverifiable claims or hidden opportunistic actions may undermine coordination, whereas withholding information can also serve legitimate strategic, legal, or privacy-related interests (Bossler et al., 2024; Sedlmeir et al., 2022).

Taken together, these perspectives locate the central coordination problem at the intersection of verifiability, confidentiality, and control. Verifiability concerns whether actors can establish the relevant properties of information on which they depend. Confidentiality concerns whether sensitive underlying information can remain protected from actors that do not require access. Throughout this dissertation, confidentiality serves as the overarching term for this requirement to limit the disclosure of sensitive information. Privacy terminology is retained where it reflects the specific focus of the underlying literature, individual RPs, or established technical concepts such as privacy-preserving verification. Control concerns how rights and responsibilities over shared information and its verification are allocated among participating actors. These requirements are interdependent: greater visibility may facilitate verification but expose information that should remain confidential, whereas stronger restrictions may protect legitimate interests while reducing shared visibility or increasing dependence on the actors controlling access (Beck et al., 2018; Bossler et al., 2024). Interorganizational information sharing is, therefore, a socio-technical coordination problem rather than merely a question of data availability. The following section examines decentralized IS and blockchain-based infrastructures as one possible means of distributing verification and control functions across organizational boundaries.

2.2 Decentralized Information Systems and Blockchain-Based Infrastructures

Decentralized IS offer an alternative infrastructural approach for coordinating digital interactions among interdependent actors that are not subordinated to a single organizational authority. Whereas centralized systems concentrate data storage, processing, validation, access control, and governance authority within one organization or platform operator, decentralized systems distribute these functions across multiple actors or technical components. Decentralization should therefore not be understood as a binary distinction between systems with and without central authority, but as a multidimensional design property concerning how control and responsibility are allocated

(Beck et al., 2018; Guggenberger et al., 2020; Rossi et al., 2019). A system may, for example, distribute validation while retaining centralized control over participant admission or protocol updates. This distinction is particularly important in regulated and interorganizational settings, where certain responsibilities must remain assigned to identifiable and accountable actors.

Blockchain technology represents one of the most prominent technological foundations for decentralized IS. Originally introduced as the infrastructure underlying Bitcoin (Nakamoto, 2008), blockchain has evolved into a broader class of distributed ledger technologies that enable tamper-evident record keeping without relying on a central database administrator. At its core, a blockchain stores transactions in blocks that are cryptographically linked to previous blocks, thereby creating an append-only data structure. Copies of the ledger are maintained by a network of nodes, while consensus mechanisms establish agreement on the valid ordering and state of recorded transactions (Beck et al., 2017; Butijn et al., 2021; Wüst & Gervais, 2018). Through cryptographic linking, distributed replication, and consensus-based validation, blockchain-based infrastructures can provide a shared and verifiable transaction history among actors who do not necessarily share the same organizational authority.

In interorganizational settings, such a shared record can address coordination problems arising from fragmented and inconsistent information infrastructures. Instead of each actor relying exclusively on separate and potentially conflicting records, blockchain-based IS can provide a common reference point for relevant process events and transactions (Große et al., 2024; Guggenberger et al., 2020). Participating actors can verify whether information has been altered or whether a transaction has occurred, while smart contracts can execute predefined rules once specified conditions are met (Buterin, 2014). They can thereby shift selected coordination activities from retrospective reconciliation toward shared validation and rule-based execution. Blockchain can, however, not preserve the integrity of recorded information without independently establishing whether externally supplied information was correct when entered, reflecting the underlying oracle problem (Caldarelli, 2020; Hassan et al., 2023). Technical verification therefore remains dependent on reliable inputs and appropriate governance.

Blockchain-based infrastructures differ substantially in their degree of openness, participation, and governance. Public blockchains make ledger information broadly

accessible, whereas private blockchains restrict access to authorized actors. Permissionless blockchains allow actors to participate in transaction validation without prior authorization, while permissioned blockchains limit this function to an approved set of participants (Rossi et al., 2019; Wüst & Gervais, 2018). These configurations allocate visibility, validation rights, and governance authority differently. Public permissionless systems can support open verifiability and reduce reliance on a predefined operator, whereas permissioned configurations facilitate stronger control over participation and access but may reintroduce concentrated control and governance dependencies (Beck et al., 2018). The relevant design question is therefore not which configuration is generally preferable, but which allocation of verification and control fits the interorganizational problem being addressed.

The design of blockchain-based infrastructures is further shaped by fundamental trade-offs. The blockchain trilemma describes the difficulty of simultaneously maximizing decentralization, scalability, and security. Broad participation and distributed validation can strengthen decentralization and resilience but increase coordination and computational overhead (Principato et al., 2023). Conversely, architectures that improve throughput by restricting validation or concentrating specific functions may weaken decentralization and introduce additional control points (Wüst & Gervais, 2018). In enterprise and interorganizational contexts, confidentiality adds a further design dimension because shared records may contain commercially sensitive, personal, or otherwise protected information (Bossler et al., 2024; Sedlmeir et al., 2022). Highly transparent infrastructures can support auditability and shared verification but may reveal information that participating organizations cannot legitimately disclose. Blockchain-based infrastructures must therefore reconcile decentralization, scalability, security, and confidentiality through architectural choices rather than maximize any single property in isolation.

These trade-offs demonstrate that decentralized IS do not eliminate trust or governance requirements. Rather, they reconfigure how trust is established and where governance authority is located. Cryptographic integrity, distributed validation, and programmable rules can reduce reliance on a central intermediary, while organizational and institutional governance remains necessary to define legitimate participation, responsibilities, and changes to system rules (Beck et al., 2018; Ellinger et al., 2024). The effectiveness of decentralized infrastructures consequently depends not only on their

technical properties but also on their alignment with interorganizational incentives, regulatory requirements, and legitimate allocations of authority.

For this dissertation, decentralized IS and blockchain-based infrastructures provide the technological foundation for examining how information can become verifiable across organizational boundaries without relying exclusively on centralized control. They establish *how* verification is technically performed and how validation and control are distributed across participating actors and technical components.

2.3 Verifiable Digital Representations and Privacy-Preserving Verification

Building on the infrastructural perspective developed above, interorganizational information sharing also depends on *what* can be verified about the information exchanged and how much underlying information must be disclosed. Actors frequently require evidence that information is authentic, valid, or consistent with predefined rules while the underlying data remain commercially sensitive, personal, or legally protected. Verifiable and confidentiality-preserving information sharing therefore depends on the digital representations through which information is conveyed and the mechanisms through which their relevant properties can be assessed.

Zero-knowledge proofs (ZKPs) provide one mechanism for separating verification from disclosure. A ZKP allows one party to prove the correctness of a statement or computation without revealing the underlying information used to generate the proof (Goldwasser et al., 1989). Rather than granting access to a complete dataset, an actor can demonstrate that a specified condition is fulfilled, such as the validity of a transaction or the existence of an entitlement. ZKPs thereby shift information exchange from disclosing data toward disclosing cryptographic evidence about data. In decentralized IS, they can preserve shared verifiability while reducing the amount of sensitive information that must be stored, transmitted, or made visible to other participants (Schellinger et al., 2022; Sedlmeir et al., 2022). Their implementation nevertheless introduces additional computational and integration complexity, meaning that their use must remain proportionate to the confidentiality and verification requirements of the respective application.

VCs address the representation of attestable claims about actors, objects, or organizations. Within the self-sovereign identity (SSI) paradigm, an authorized issuer creates a

digitally signed credential and provides it to a holder, who can subsequently present it to a verifier (Babel, Willburger, et al., 2025; Richter & Anke, 2026). Cryptographic signatures and supporting registries allow the verifier to assess the credential's issuer, integrity, and validity without relying on an easily manipulated document or repeated bilateral confirmation with the issuer (Ehrlich et al., 2021; Preukschat & Reed, 2021). Where selective disclosure or complementary cryptographic proofs are supported, holders can additionally reveal only the information required for a particular interaction (Sedlmeir et al., 2021). VCs can therefore preserve verification-relevant properties such as provenance and integrity while limiting disclosure to the information required for a particular interaction. Technical validity alone, however, does not establish whether a credential provides meaningful evidence: its informational value also depends on whether the issuer is authorized and trustworthy and whether the represented claim is relevant to the decision at hand.

Tokenization addresses a different representational problem. Whereas credentials primarily attest to claims, tokens can represent assets, rights, or entitlements whose uniqueness and state must be preserved throughout a lifecycle. Blockchain-based tokens can be issued, transferred, restricted, and redeemed according to predefined rules, while their state changes remain traceable through the underlying ledger (Hanneke et al., 2024; Schwiderowski et al., 2024). This is particularly relevant where conflicting or duplicate claims must be prevented or where several actors require a consistent representation of an entitlement across organizational boundaries. Smart contracts complement such representations by encoding the rules governing their interaction. They can restrict critical functions to authorized actors, enforce predefined conditions, and make certain invalid state transitions technically infeasible (Beck et al., 2018; Buterin, 2014). Their applicability is nevertheless limited to conditions that can be specified sufficiently clearly and evaluated on the basis of reliable information. Decisions requiring interpretation, discretion, or legal adjudication continue to depend on organizational and institutional authority.

Across these representation and verification mechanisms, governance connects technical validity with institutional meaning. Cryptographic verification can establish that a formally specified condition has been satisfied, but it cannot independently determine whether an issuer is legitimate, whether a particular representation should be recognized, or whether the verified information has the intended organizational or

legal significance. Governance arrangements therefore define authoritative issuers and roles, establish acceptable representations and verification procedures, and allocate responsibility for exceptional cases or disputes (Beck et al., 2018). Without such institutional anchoring, a proof may be mathematically correct while the underlying claim, entitlement, or process remains irrelevant or illegitimate in the respective context.

Technical validity and institutional legitimacy alone are not sufficient for verifiable digital representations to become effective in practice. The actors interacting with them must be able to understand and enact the corresponding processes and perceive sufficient value in doing so. Technology acceptance research emphasizes perceived usefulness and ease of use as important conditions of system use, while research on SSI additionally highlights the relevance of trust in the technical and institutional arrangements surrounding holder-centered interactions (Davis, 1985; Rieger et al., 2022; Sartor et al., 2022; Venkatesh & Davis, 2000). Effective use is therefore not treated as a separate analytical level in this dissertation, but as a condition under which technically valid and institutionally governed representations become practically enacted.

Taken together, these mechanisms support complementary forms of verifiability. ZKPs enable properties to be verified while limiting disclosure of the underlying data. VCs provide verifiable representations of attestable claims and their provenance, whereas tokens are suited to rights or entitlements whose uniqueness and state must remain consistent over time. Smart contracts can govern permissible interactions with such representations where relevant rules can be formalized. Their suitability consequently depends on the underlying information problem rather than on the technology alone. This representation-centered perspective complements the infrastructural perspective developed in Section 2.2: decentralized infrastructures determine how and under whose control verification occurs, while digital representations and verification mechanisms determine what can be verified and what information must be disclosed to do so. Their practical realization further depends on institutional governance and effective use. Together, these dimensions provide the conceptual foundation for the two RGs derived in the following section.

3 Deriving the Research Goals, Gaps, and Questions

The preceding sections establish verifiable and confidentiality-preserving interorganizational information sharing as a problem that spans two interdependent analytical levels within decentralized IS. At the infrastructural level, the design problem concerns how decentralized IS distribute verification and control across organizational boundaries, that is, how verification is technically enabled and under whose control it occurs. At the representation level, the design problem concerns what can be verified about the information exchanged through these infrastructures and how much underlying information must be disclosed to do so. Put differently, decentralized infrastructures determine the allocation of verification and control, whereas digital representations determine the properties of information that remain verifiable under confidentiality constraints. These levels are analytically distinct but mutually dependent: a decentralized infrastructure can provide shared and tamper-evident states without by itself ensuring that the information represented through them is legitimate or decision-relevant, while a verifiable representation depends on technical and institutional arrangements that establish who may issue, verify, and act on it. The practical realization of representation-based interactions further depends on their effective use, which this dissertation treats as a condition of the representation level. Building on this distinction, the overarching research question introduced in Section 1 provides the point of departure for the cumulative research endeavor:

How can decentralized information systems enable verifiable and confidentiality-preserving interorganizational information sharing?

Answering this question requires knowledge at both analytical levels. The dissertation therefore pursues two complementary RGs:

RG 1: *Develop design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing.*

RG 1 addresses the infrastructural design problem within the problem structure established in Section 1. It investigates how verification and control can be allocated across decentralized infrastructures when participating organizations simultaneously require shared process information and legitimate confidentiality. The resulting knowledge concerns the design of infrastructures that distribute verification without reproducing excessive transparency, concentrating verification and information access in a single

intermediary, or relying on technically infeasible configurations.

RG 2: *Conceptualize verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing.*

RG 2 addresses the complementary representation-level design problem. Even a suitable infrastructure does not ensure that the information exchanged through it carries the properties required for meaningful verification. RG 2 therefore investigates how different forms of information can be represented so that relevant properties remain verifiable while disclosure is limited to what is necessary for verification. It further considers the conditions under which representation-based interactions become effective in practice, without treating effective use as a separate analytical level.

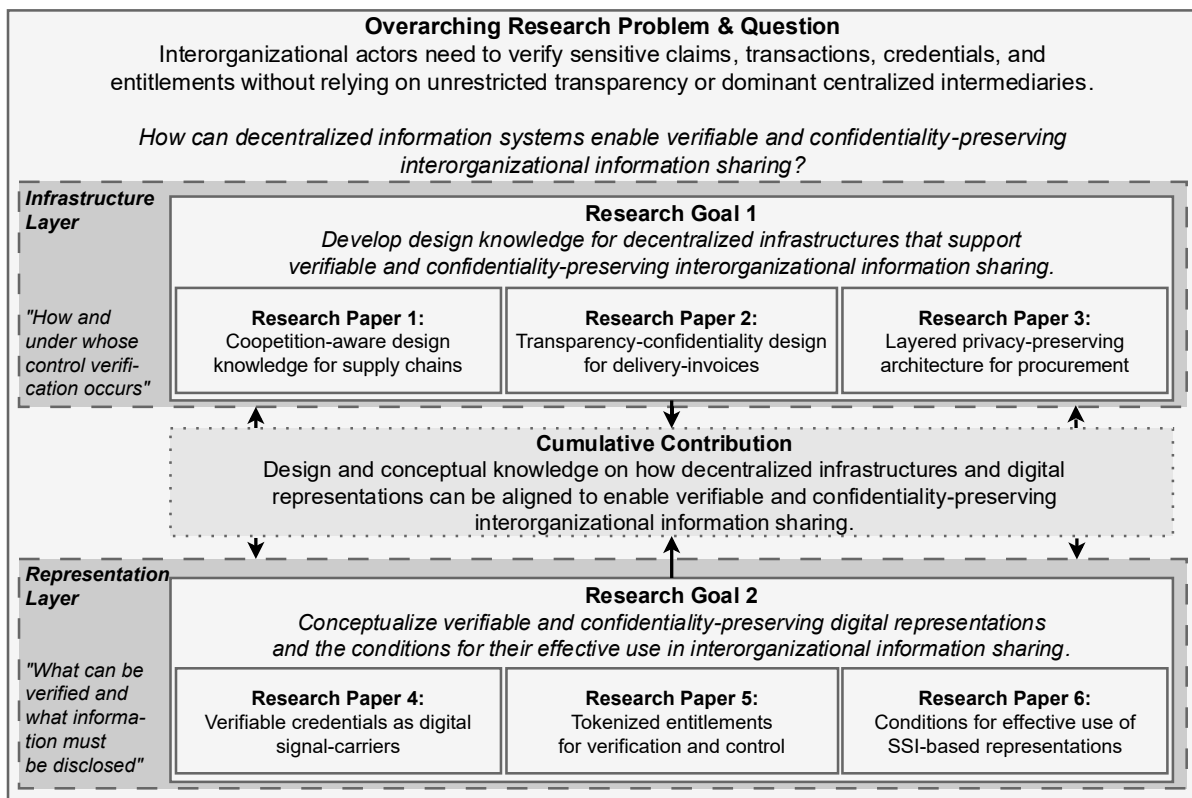


Figure 1: Layered structure of the research goals and cumulative contribution

Figure 1 summarizes how the two RGs combine in the cumulative contribution of this dissertation. RG 1 develops design knowledge concerning the allocation of verification and control at the infrastructure level, while RG 2 develops conceptual knowledge concerning verifiable digital representations and the conditions for their effective use. Their cumulative contribution lies in explaining how decentralized

infrastructures and digital representations can be aligned to enable verifiable and confidentiality-preserving interorganizational information sharing. The figure further maps the six RPs to their respective RGs.

To accomplish these RGs, the following subsections derive the specific research gaps addressed across the six RPs and position their individual research questions within the cumulative research endeavor. Table 1 provides an overview of the RPs, their publication outlets and status, and their assignment to the two RGs.

Title	Publication outlet	VHB JQ4 ranking	Publication status
RG 1: Develop design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing			
RP 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management	Electronic Markets	B	Published
RP 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry	International Conference on Wirtschaftsinformatik Proceedings	B	Published
RP 3: Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy	Information Systems	B	Published
RG 2: Conceptualize verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing			
RP 4: From Documents to Verifiable Credentials: How Digital Signal-Carriers Reconfigure Decision-Making in Buyer–Supplier Relationship Formation	Electronic Markets	B	Under Review Major Revision Round 2
RP 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control	Business & Information Systems Engineering	B	Under Review Minor Revision Round 3
RP 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications	Hawaii International Conference on System Sciences Proceedings	B	Published

Table 1: Overview of the research papers addressing the identified research goals

3.1 RG 1: Develop design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing.

RG 1 addresses a prescriptive knowledge gap at the infrastructural level. Prior research has established blockchain as a potential foundation for shared, tamper-evident, and programmable coordination across organizational boundaries and has particularly emphasized benefits such as transparency, traceability, and reduced reliance on centralized intermediaries (Azzi et al., 2019; Babich & Hilary, 2020; Butijn et al., 2021; Guggenberger et al., 2020; Sternberg et al., 2021). Yet these properties do not prescribe how decentralized infrastructures should be configured when organizations simultaneously require shared verification, confidentiality, and continued control over strategically relevant information. This problem is particularly pronounced in interorganizational settings, as actors that benefit from coordination may also compete, operate separate information systems, or have legitimate reasons not to transfer sensitive information and control over its verification to a common platform operator (Bossler et al., 2024; Sedlmeir et al., 2022). RG 1, therefore, investigates how decentralized infrastructures can support shared verification without requiring unrestricted transparency or concentrating information access and verification in a single intermediary.

A first research gap concerns this tension between cooperation-enabling information sharing and legitimate confidentiality. Supply chain research has extensively discussed blockchain as a means of increasing visibility, traceability, and trust across organizational boundaries (Babich & Hilary, 2020; Beck et al., 2017; Beck et al., 2018; Nofer et al., 2017). However, greater transparency is not unambiguously beneficial when the information exchanged contains commercially sensitive information and participating firms remain competitors (Alt, 2020; Bossler et al., 2024; Guggenberger et al., 2020; Sedlmeir et al., 2022). Coopetition research captures this structural tension by conceptualizing interorganizational relationships in which organizations cooperate to create joint value while simultaneously competing to appropriate individual value (Bengtsson & Kock, 2000; Gnyawali & Park, 2011; Nalebuff & Brandenburger, 1997). What remains insufficiently developed is prescriptive knowledge that translates this cooperation–competition duality into the design of decentralized IS. In particular, decentralized infrastructures must enable sufficient information sharing for process coordination and verification while preventing sensitive information from becoming visible to

actors that do not require access.

RP 1 addresses this gap from a theory-informed infrastructure perspective. Applying coopetition theory, the study conceptualizes cooperation and competition as interdependent design concerns rather than treating confidentiality as an isolated technical requirement. The resulting challenge is to configure decentralized infrastructures so that shared process execution, accountability, and verification remain possible without exposing strategically sensitive information or creating new dependencies on dominant platform actors (Fernandez & Chiambaretto, 2016; Gleiss et al., 2023; Hoess et al., 2025; Loertscher & Marx, 2020). RP 1 therefore investigates how the integration principle of coopetition can be translated into architecture and implementation knowledge for decentralized supply networks and asks:

How to design a blockchain-based information system to facilitate coopetition in supply networks by fostering cooperative interactions while ensuring data confidentiality?

RP 2 complements this broader perspective by examining how the same underlying tension materializes in a concrete interorganizational process. Delivery-invoice processes in construction supply chains involve multiple organizations that must exchange consistent information about deliveries and subsequent processing. Yet these processes have traditionally relied on paper-based or fragmented digital information exchange, resulting in media discontinuities, manual processing, limited automation, and reconciliation efforts (Bajpai & Misra, 2024; Demirkesen & Tezel, 2021; Prebanić & Vukomanović, 2021). Existing electronic data interchange and standardized digital solutions can alleviate some of these inefficiencies but have not established a universally accepted infrastructure across the fragmented construction market (Samuelson & Björk, 2014; Wiehager, 2021). Centralized or provider-specific solutions may additionally create dependencies by concentrating data and decision rights in a platform operator (Gleiss et al., 2023).

The problem is intensified by the coopetitive nature of the setting. Digital process integration requires organizations to share information to realize coordination and automation benefits, while the same actors may compete and therefore have legitimate reasons to restrict access to commercially sensitive data (Hoffmann et al., 2018; Li et al., 2019). In delivery-invoice processing, this includes bilateral transaction information that should not become visible to unauthorized third parties, also because

confidentiality and competition-related requirements constrain unrestricted information sharing (Agdas & Ellis, 2010; Anumba & Ruikar, 2002). A decentralized infrastructure may provide a shared coordination layer for such processes, but its implementation must therefore reconcile process-level transparency with legitimate confidentiality. RP 2 investigates this concrete data-transparency trade-off and asks:

How can blockchain technology help to digitize the process of handling delivery invoices in the construction industry supply chain while addressing the challenges associated with the coopetition trade-off?

RPs 1 and 2 originate from the same overarching design science research (DSR) project and share their empirical and artifact-development basis. Their contributions should therefore not be interpreted as independent empirical validations. Rather, they represent cumulatively related perspectives on the same infrastructural design problem. RP 2 constitutes the earlier process-specific design and evaluation of the blockchain-based delivery-invoice system, whereas RP 1 subsequently reanalyzes and abstracts this foundation through an explicit coopetition lens to derive broader architecture- and implementation-oriented knowledge. Within the cumulative dissertation, RP 1 is presented first because it articulates the broader theoretical and infrastructural problem, while RP 2 demonstrates how this problem materializes in a concrete interorganizational process. Together, the two RPs show that confidentiality must be actively incorporated into decentralized infrastructure design rather than treated as an external constraint on otherwise transparent systems.

A second research gap concerns the broader architectural consequences of preserving confidentiality in decentralized infrastructures. Restricting access through permissioned blockchain architectures can improve confidentiality and performance, but may simultaneously concentrate validation and governance rights and thereby weaken the decentralization and open verifiability that motivate blockchain adoption in the first place (Beck et al., 2018; Rossi et al., 2019; Wüst & Gervais, 2018). Conversely, public permissionless infrastructures provide stronger decentralization and independently verifiable integrity but face limitations regarding transaction throughput and the processing of commercially sensitive information. This reflects the broader blockchain trilemma among decentralization, scalability, and security, which becomes an extended design problem when confidentiality is required in enterprise and interorganizational

contexts (Principato et al., 2023; Sedlmeir et al., 2022). Existing blockchain-based procurement systems frequently address these requirements only partially, particularly by relying on permissioned configurations to obtain privacy and performance at the cost of additional control points (Kim & Kim, 2024; Mishunin, 2024; Nodehi et al., 2022; Wüst & Gervais, 2018; Yang et al., 2022).

RP 3 addresses this gap by investigating how these requirements can be reconciled through architectural allocation rather than by maximizing one property or resolving confidentiality primarily through restricted participation. The study examines procurement processes as an information-intensive interorganizational setting and develops a layered architecture in which a public permissionless blockchain provides a publicly verifiable trust anchor while a privacy-preserving Layer 2 enables confidential and scalable process execution. It thereby investigates whether different infrastructural requirements can be assigned to components suited to fulfilling them while preserving their interaction within an overall decentralized IS. Accordingly, RP 3 asks:

How to design a blockchain-based information system for procurement processes that balances decentralization, scalability, and security while maintaining privacy?

Together, the three RPs develop complementary design knowledge for the infrastructural level of verifiable and confidentiality-preserving interorganizational information sharing. RPs 1 and 2 explain how decentralized infrastructures can reconcile shared coordination with legitimate confidentiality in cooperative networks, combining broader theory-informed design knowledge with its process-specific manifestation. RP 3 extends this reasoning by examining how confidentiality can be reconciled with decentralization, scalability, and security through layered architectural design. RG 1 therefore conceptualizes decentralized infrastructures not as systems of unrestricted transparency, but as configurable socio-technical arrangements in which verification and control are deliberately allocated while access to sensitive information is restricted according to the underlying interorganizational problem structure.

3.2 RG 2: Conceptualize verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing.

RG 2 addresses a complementary knowledge gap at the representation level. Decentralized infrastructures can provide tamper-evident records, distributed validation, and programmable coordination, but infrastructure alone does not ensure that the information objects exchanged through it preserve the properties required for meaningful verification. Claims may be transmitted through manipulable carriers, while rights or entitlements may be duplicated, transferred without authorization, or exercised more than once. Moreover, the effectiveness of technically valid and institutionally governed representations also depends on whether the actors interacting with them understand and enact the corresponding processes. RG 2 therefore examines how different forms of sensitive information can be represented so that relevant properties remain verifiable while disclosure is limited to what is necessary for verification, and under which conditions such representation-based interactions become effective in practice.

A first research gap concerns the credibility of digitally represented claims in interorganizational decision-making. Buyers frequently face substantial information asymmetries when selecting suppliers because they cannot directly observe prospective partners' capabilities, compliance, or operational quality before entering a contractual relationship (Akerlof, 1978; Beer et al., 2018). They consequently rely on observable signals such as certifications, audit reports, or compliance documentation to infer otherwise hidden supplier attributes. Signaling theory explains how costly and observable signals can enable high-quality actors to differentiate themselves from lower-quality competitors and thereby reduce adverse selection (Connelly et al., 2011; Spence, 1973). Digitally mediated interactions, however, complicate this mechanism because signals are increasingly transmitted through documents, platforms, or other digital artifacts rather than observed directly. Such artifacts may be copied, altered, or selectively presented while retaining the appearance of an authentic signal, potentially decoupling the integrity of the transmitted evidence from the effort required to obtain the underlying certification (Steigenberger, 2024).

Although signaling theory considers signal costliness, observability, and sender characteristics, it has devoted comparatively less attention to the properties of the medium through which signal information is transmitted (Connelly et al., 2011; Connelly et al., 2025). The theory acknowledges distortion when the transmission medium reduces signal observability, but the carrier itself has rarely been conceptualized as an explicit analytical element. This limits the ability to explain why substantively similar claims can differ in credibility depending on how they are conveyed and why digital mediation may create additional opportunities for deceptive signaling (Steigenberger, 2024). VCs provide a potential response because cryptographic signatures and supporting verification infrastructures allow recipients to assess properties such as provenance, integrity, issuer, and validity. Existing research has primarily examined VCs and SSI in relation to identity management, privacy, interoperability, and digital trust infrastructures (Babel, Willburger, et al., 2025; Ehrlich et al., 2021; Richter & Anke, 2026; Sedlmeir et al., 2021). What remains insufficiently understood is how VCs alter signaling mechanisms and organizational decision-making when they function as the carrier through which suppliers communicate hidden attributes. RP 4 addresses this gap by asking:

How can verifiable credentials function as digital signal-carriers during pre-contractual decision-making in buyer–supplier relationship formation?

A second research gap concerns information objects for which credibility alone is insufficient because their uniqueness and lifecycle must also remain verifiable across organizational and institutional boundaries. Whereas credentials primarily attest to claims, digital representations of rights or entitlements may need to support controlled creation, authorized reassignment, restriction, and redemption while ensuring that the same underlying entitlement cannot be exercised more than once. Fragmented records and discontinuities between participating IS can make it difficult to establish whether such an entitlement was legitimately created, who currently controls it, and whether it has already been consumed. This becomes particularly consequential where actors possess conflicting incentives and one party cannot fully observe or verify another party's actions.

Principal–agent theory conceptualizes such settings as relationships in which information asymmetries and goal incongruence create opportunities for opportunistic

behavior and impose monitoring or agency costs on the principal (Eisenhardt, 1989; Fama & Jensen, 1983; Jensen & Meckling, 1976). In taxation, taxpayers determine and report tax-relevant information, while tax authorities can verify correct behavior only through monitoring and auditing that entail corresponding costs (Alm et al., 1990; Crocker & Slemrod, 2005; Reinganum & Wilde, 1985). Dividend-stripping arrangements such as Cum-Ex illustrate how information asymmetries and fragmented institutional processes can be exploited to support multiple tax-refund claims based on a single tax payment (Buettner et al., 2020; Schubert, 2021; Spengel, 2021a, 2021b).

Prior taxation research has primarily examined audit optimization, sanctions, and incentive design as mechanisms for addressing such principal–agent problems (Aruoba, 2021; Bazart & Pickhardt, 2011; Crocker & Slemrod, 2005; Pickhardt & Prinz, 2014; Reinganum & Wilde, 1985). These approaches provide limited guidance on how IS could reduce the underlying verification and agency costs by changing how tax-related entitlements themselves are represented and controlled. Only a small number of studies have considered blockchain-based mechanisms for taxation. Existing contributions either remain at a comparatively high level of abstraction or focus on specific cross-border arrangements without fully addressing domestic processes, privacy, regulatory compliance, stakeholder responsibilities, and practical feasibility (Ainsworth & Todorov, 2018; EY, 2021; Faccia & Mosteanu, 2019; Hyvärinen et al., 2017; Yent, 2020). At the same time, blockchain-based IS have been discussed more broadly as mechanisms for reducing information asymmetries through traceability, immutable state histories, and programmable rule enforcement (Beck et al., 2018; Bossler et al., 2024; Carvalho & Karimi, 2021; Ellinger et al., 2024; Große et al., 2024; Treiblmaier, 2018).

The remaining challenge is therefore not simply to make tax transactions more transparent, particularly because tax and financial information is highly sensitive. Instead, the existence and lifecycle of an entitlement must become verifiable while the underlying shareholder and transaction information remains protected. Tokenization offers a means of representing an entitlement as a unique digital object whose creation, authorized reassignment, and redemption can be governed through smart contracts, while privacy-preserving proofs can separate the verification of relevant conditions from disclosure of the underlying data (Schwiderowski et al., 2024; Sedlmeir et al., 2022). What remains underexplored is how these mechanisms can be combined into an IS that constrains duplicate or unauthorized claims, reduces detrimental

information asymmetries, and remains practically feasible within a federated tax system. RP 5 addresses this gap by investigating how a blockchain-based IS can maintain an authoritative and privacy-preserving entitlement state across the organizations involved in withholding-tax administration. It asks:

How can a blockchain-based information system be designed to control duplicate withholding-tax refund claims in a federated tax-administration setting?

RPs 4 and 5 thus address two different representational requirements. RP 4 concerns attestable claims whose credibility depends on properties such as provenance, integrity, issuer authority, and current validity. RP 5 concerns legally and financially consequential entitlements whose reliability additionally depends on uniqueness, authorized creation, controlled lifecycle transitions, and irreversible redemption. The distinction illustrates why the appropriate form of a verifiable digital representation depends on the underlying information problem rather than on a single technological solution.

A third, complementary research gap concerns the effective use of such representations. This issue is particularly visible in SSI-based credential systems because holders actively manage and present identity-related information within issuer–holder–verifier relationships (Babel, Willburger, et al., 2025; Mühle et al., 2018; Preukschat & Reed, 2021). This holder-centered model can increase control over identity information and enable privacy-preserving disclosure, but it also requires users to understand and interact with unfamiliar credential-management processes. Previous digital-identity initiatives illustrate that technical availability alone does not ensure widespread use, particularly when users perceive limited benefits, insufficient use cases, or excessive complexity (Felden et al., 2020; Rederer et al., 2021).

Technology acceptance research provides established explanations for such behavior, particularly through perceived usefulness and perceived ease of use (Davis, 1985; Venkatesh & Davis, 2000). Yet generic acceptance models may not fully capture characteristics that become salient in SSI, where users manage sensitive credentials, authorize disclosures, and depend on both technical and institutional trust. Technology acceptance research has also relied predominantly on quantitative studies using predefined constructs, which can make it difficult to identify acceptance conditions specific to an emerging technology (Benbasat & Barki, 2007; Vogelsang et al., 2013; Wu, 2012).

Although initial studies have examined the acceptance of digital identity and SSI solutions, knowledge about the attributes, features, and characteristics that shape the acceptance of SSI applications remains limited (Cabinakova et al., 2019; Rieger et al., 2022; Sartor et al., 2022).

RP 6 addresses this gap through an exploratory qualitative study of potential users interacting with an SSI demonstrator. Although its focal unit of analysis is the individual user, the demonstrated credential interaction spans an issuer, holder, and verifier and thereby represents the user-facing enactment of interorganizational information sharing. The RP identifies conditions that may influence whether such holder-centered interactions are understood, trusted, and effectively used and asks:

Which attributes, features, and characteristics of Self-Sovereign Identity Systems influence the acceptance of the Identity System?

Together, RPs 4–6 conceptualize complementary aspects of verifiable and confidentiality-preserving digital representations and their effective use. RP 4 examines how the integrity of a digital carrier affects the credibility of attestable claims. RP 5 examines how tokenized representations can preserve the uniqueness and lifecycle of entitlements while enabling privacy-preserving verification. RP 6 complements these representation-centered contributions by examining conditions under which users are willing to interact with holder-centered credential systems. RG 2 therefore extends beyond the technical validity of digital information objects without turning acceptance into a separate analytical level. Across these contributions, RG 2 shows that verifiability depends not only on the technical integrity of a digital representation, but also on whether it preserves the properties relevant to the underlying information problem, carries institutional meaning, and can be effectively used by the actors involved. Together with RG 1, this representation-centered knowledge explains what information must remain verifiable within decentralized IS and under which conditions such verification can support interorganizational information sharing in practice.

4 Research Designs

To answer the overarching research question, the six RPs employ research designs aligned with their respective research questions and intended knowledge contributions. RPs 1, 2, 3, and 5 follow design science research (DSR) to develop and evaluate artifacts and derive prescriptive design knowledge for decentralized infrastructures and verifiable digital representations (Hevner et al., 2004; Peffers et al., 2007; Tuunainen et al., 2024). RP 4 adopts phenomenon-based theorizing to explain how VCs reconfigure signaling mechanisms in buyer–supplier relationship formation (Fisher et al., 2021; Gregory & Henfridsson, 2021). RP 6 uses an exploratory qualitative design informed by the Technology Acceptance Model 2 (TAM2) to identify acceptance conditions that may not be adequately captured by established technology acceptance constructs (Davis, 1985; Venkatesh & Davis, 2000). The methodological portfolio thus combines prescriptive artifact design, explanation of an insufficiently conceptualized mechanism, and exploration of conditions for effective use. Table 2 summarizes the individual research designs.

RP 1 employs a DSR approach to develop architecture- and implementation-oriented design knowledge for blockchain-based IS in coopetitive supply networks (Peffers et al., 2007). To identify the problem domain and derive design objectives, the study conducts a systematic literature review that yields 23 academic publications, which are analyzed through open, axial, and selective coding (Brereton et al., 2007; Corbin & Strauss, 1990; Saldaña, 2013; Webster & Watson, 2002). Coopetition theory structures the interpretation of the underlying cooperation–competition tension and informs the derivation of meta-requirements (Bengtsson & Kock, 2000). Based on the resulting design objectives, the study develops a conceptual blockchain architecture for coopetitive information sharing, using digital delivery-invoice exchange in the construction industry as its unit of analysis. The artifact is represented through Kruchten (1995) 4+1 view model and evaluated within the FEDS framework through nine qualitative ex-post interviews with experts in distributed technologies and the construction industry (Sonnenberg & vom Brocke, 2012; Venable et al., 2016).

Title	Research Design
RG 1: Develop design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing.	
RP 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management	Design science research • SLR-based derivation of design objectives; final set of 23 academic items coded through open, axial, and selective coding. • Coopetition lens used to structure the cooperation–competition trade-off and inform meta-requirements. • Prototype developed and represented through 4+1 view model (Kruchten, 1995); evaluated via FEDS and nine ex-post expert interviews (Venable et al., 2016).
RP 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry	Design science research • DSR-based design of a decentralized infrastructure for digital delivery invoices. • Design objectives derived from literature research and project workshops with construction and IT partners. • Blockchain-based prototype developed and evaluated through nine ex-post expert interviews.
RP 3: Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy	Design science research • SLR- and expert-based derivation of problem statement and design objectives addressing the extended blockchain trilemma. • Layered prototype developed with public permissionless Layer 1 as trust anchor and privacy-preserving Layer 2 for confidential execution. • Evaluation through technical verification, quantitative viability assessment, and 16 semi-structured expert interviews.
RG 2: Conceptualize verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing.	
RP 4: From Documents to Verifiable Credentials: How Digital Signal-Carriers Reconfigure Decision-Making in Buyer–Supplier Relationship Formation	Phenomenon-based theorizing • Exploratory qualitative design using signaling theory as a sensitizing lens. • Primary data collected through 17 semi-structured expert interviews and complemented by observational and archival data. • Iterative analysis to theorize how VCs function as digital signal-carriers.
RP 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control	Design science research • DSR structured along relevance, rigor, and design cycles (Hevner, 2007). • Problem understanding, requirements derivation, and artifact development informed by literature and documentary analysis, and six interdisciplinary consortium working sessions. • Conceptual artifact subsequently assessed through ten semi-structured expert interviews and analytical evaluation of modeled transaction workloads and selected recurring technical costs.
RP 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications	Qualitative exploratory acceptance study • TAM2-informed qualitative design using an SSI income-tax-certificate demonstrator. • Data collected through 13 semi-structured interviews with potential SSI users. • Deductive–inductive content analysis used to develop an extended acceptance model and hypotheses.

Table 2: Overview of the research papers' methodological approaches

RP 2 constitutes the initial conference publication emerging from the underlying DSR project. It focuses on the process-specific design, development, and evaluation of a blockchain-based delivery-invoice system for the construction industry. It also follows a DSR approach to design, develop, and evaluate a decentralized infrastructure for processing digital delivery invoices in the construction industry (Peffer et al., 2007). The research is grounded in a consortium project with construction-industry and technology partners, which allowed the authors to iteratively develop a prototype addressing real-world application challenges. The research design combines literature-based problem analysis, project workshops, prototype development, and expert evaluation. Following Peffer et al. (2007), the artifact addresses a relevant business need by proposing a decentralized solution for a process that remains affected by paper-based procedures, media discontinuities, and limited interoperability. The evaluation relies on nine ex-post expert interviews with distributed technology and construction industry experts, thereby incorporating both technical and domain-specific perspectives (Sonnenberg & vom Brocke, 2012; Venable et al., 2016). The insights from artifact development and expert evaluation are synthesized into design principles for secure data exchange in distributed supply chain environments (Gregor & Hevner, 2013).

RPs 1 and 2 originate from the same overarching research project and draw on the same empirical and artifact-development basis. RP 2 represents the earlier conference publication and presents the process-specific design and evaluation of a blockchain-based delivery-invoice system for the construction industry. RP 1 subsequently extends this work for journal publication by broadening the theoretical framing, level of abstraction, and resulting design knowledge. It uses coopetition as its central theoretical lens and develops a more comprehensive architecture and implementation guidance for blockchain-based information sharing in supply networks characterized by simultaneous cooperation and competition (Bengtsson & Kock, 2000; Gnyawali & Park, 2011; Nalebuff & Brandenburger, 1997). Accordingly, the two RPs should not be interpreted as independent empirical studies or as providing separate empirical validations of the same artifact. Their contribution lies instead in the cumulative refinement and abstraction of the underlying research. RP 2 demonstrates how the transparency trade-off can be addressed in a specific interorganizational process, whereas RP 1 generalizes the insights toward architecture-level and theory-oriented design knowledge for managing confidentiality in coopetitive supply networks.

RP 3 extends the infrastructure-oriented design perspective by focusing on procurement processes and the extended blockchain trilemma (Principato et al., 2023). The RP follows the DSR paradigm because it seeks to design a blockchain-based IS that reconciles decentralization, scalability, security, and privacy under real-world technical, regulatory, and organizational constraints (Hevner et al., 2004; Peffers et al., 2007). The study begins with a structured literature review following Webster and Watson (2002), which is used to synthesize a problem statement and derive preliminary design objectives. These objectives are refined through expert feedback and guide the development of a layered prototype. The artifact design draws on the 4+1 architectural view model and combines a public permissionless blockchain as trust anchor with a privacy-preserving Layer 2 architecture (Kruchten, 1995). The evaluation combines formative and summative elements in line with FEDS (Venable et al., 2016). It includes technical verification, quantitative viability assessment, and 16 semi-structured expert interviews. The interview data are analyzed using structured qualitative coding against predefined design objectives, enabling the RP to assess how the artifact addresses the extended trilemma and to derive transferable design principles (Corbin & Strauss, 2015; Gioia et al., 2013; Gregor et al., 2020).

RP 4 adopts a qualitative, exploratory research design rather than a DSR approach. It investigates how VCs within the SSI paradigm function as digital signal-carriers in pre-contractual buyer–supplier relationship formation. Given the emerging nature of this phenomenon, phenomenon-based theorizing provides an appropriate methodological approach for examining mechanisms that are not yet sufficiently captured by existing theory (Fisher et al., 2021; Gregory & Henfridsson, 2021; Krogh et al., 2012). The research design draws on signaling theory as a sensitizing theoretical lens, using concepts such as observability, signal costliness, and information asymmetry to guide the empirical inquiry without imposing a rigid coding structure (Blumer, 1954; Bowen, 2006). Primary data were collected through 17 semi-structured expert interviews with actors from different parts of the VC and supply chain ecosystem. These interviews were complemented by observational and archival data from SSI initiatives and implementation contexts, which contextualized the interview material and enabled emerging interpretations to be compared across data sources. Data analysis proceeded iteratively, relating empirical observations to signaling theory to theorize how VCs reshape credibility, transmission, and evaluation of supplier signals (Gioia et al., 2013; Saldaña, 2013).

RP 5 returns to a DSR approach and develops a blockchain-based IS to address principal–agent problems in dividend taxation. The research design follows the three-cycle view of DSR, comprising a relevance cycle, a rigor cycle, and a design cycle (Hevner, 2007). The relevance cycle is grounded in the real-world problem of dividend-stripping schemes such as Cum-Ex and incorporates six interdisciplinary consortium working sessions with stakeholders from tax administration, financial infrastructure, and related domains. Due to the sensitivity of the topic, the working sessions were not recorded. The study instead relied on notes produced by the researchers during the working sessions and subsequently refined through collaborative discussion, together with the prepared session presentations, to inform the problem analysis and requirements derivation (Elo & Kyngäs, 2008; Flick et al., 2010). The rigor cycle integrates principal–agent theory with blockchain and taxation literature to derive meta-requirements and design objectives. The design cycle iteratively develops the blockchain-based artifact, including tokenization, smart contracts, and ZKPs. The evaluation follows FEDS and combines a conceptual expert evaluation with an analytical assessment of modeled transaction workloads and selected recurring technical costs (Venable et al., 2016). The analytical evaluation estimates transaction workloads, assesses their feasibility relative to reported permissioned-blockchain capacities, and approximates selected recurring node-operation and proof-processing costs under explicitly stated assumptions. It does not constitute a complete assessment of implementation costs or cost-effectiveness. The qualitative evaluation comprises ten semi-structured expert interviews with experts from IS, economics, law, and tax consultancy, who assessed the artifact’s problem–solution fit, governance implications, and privacy safeguards. Based on these evaluations, the RP derives design principles for blockchain-based IS addressing principal–agent problems (Gregor et al., 2020).

RP 6 adopts an exploratory qualitative research design to investigate the acceptance of SSI systems. Qualitative inquiry is appropriate because SSI represents an emerging phenomenon whose specific acceptance conditions may not be fully captured by predefined constructs from established technology acceptance models. The study follows the approach proposed by Vogelsang et al. (2013), using the TAM2 as a theoretical foundation while retaining sufficient analytical openness for the identification of previously unknown constructs (Venkatesh & Davis, 2000). To provide participants with a common understanding of the investigated system, the interviews incorporated an SSI demonstrator. The empirical data comprise 13 semi-structured interviews with

potential end users who possessed a basic understanding of SSI. Purposeful sampling was used because the study required participants who could both assume the role of prospective users and provide informed reflections on an emerging identity-management concept. The data were analyzed using qualitative content analysis supported by MAXQDA (Corbin & Strauss, 1990; Flick et al., 2010; Mayring, 2014). TAM2 variables initially provided a deductively derived category system (Venkatesh & Davis, 2000). Each category was defined through coding rules and anchor examples to support consistent interpretation. Because the study sought to identify SSI-specific acceptance conditions, the deductive analysis was complemented by inductive category development. The resulting categories were synthesized into an extended acceptance model and corresponding hypotheses. These hypotheses represent theoretically informed propositions derived from qualitative evidence rather than quantitatively validated causal relationships (Vogelsang et al., 2013).

Across the six RPs, the dissertation employs complementary research designs to generate prescriptive, explanatory, and theory-elaborating knowledge. RPs 1, 2, 3, and 5 apply DSR to develop and evaluate architectures, prototypes, technical mechanisms, and design principles for decentralized infrastructures and verifiable digital representations. RPs 1 and 2 provide distinct but cumulatively related outputs from a shared DSR project rather than independent empirical validations. RP 4 complements the prescriptive perspective through phenomenon-based theorizing, explaining how VCs reconfigure the transmission and evaluation of supplier signals. RP 6 adds a user-oriented perspective through TAM2-informed qualitative content analysis, identifying the conditions under which actors accept and use SSI-based representations. Methodologically, the dissertation combines systematic and structured literature reviews, project workshops, expert and user interviews, artifact design and demonstration, observational and archival data, deductive and inductive qualitative coding, expert-based evaluation, and technical feasibility assessment. The coherence of this methodological portfolio does not arise from applying a uniform research design, but from aligning each design with the respective research question and intended knowledge contribution. This combination is appropriate for studying decentralized IS because their effectiveness depends simultaneously on technical design, organizational and institutional governance, the properties of digital representations, and their acceptance and enactment by the involved actors.

5 Summary of the Results

This section summarizes the results of the six RPs included in this cumulative dissertation. The summaries follow the structure of the overarching RGs derived in Section 3. RPs 1–3 contribute to RG 1 by developing design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing. RPs 4 and 5 contribute to RG 2 by conceptualizing verifiable and confidentiality-preserving digital representations, while RP 6 identifies conditions for their effective use in interorganizational information sharing. The following subsections outline the main results of each RP and clarify their contribution to the cumulative research endeavor of this dissertation.

RP 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management

RP 1 applies a DSR approach to develop design knowledge for blockchain-based IS in coopetitive supply chain settings (Peffer et al., 2007). The study addresses a defining tension of digitally integrated supply networks. Shared information infrastructures can enable coordination, automation, and traceability, while participating firms must simultaneously protect strategically sensitive information from competitors or dominant platform operators. This tension is particularly salient in coopetitive relationships, where firms cooperate to create joint value but continue to compete over its individual appropriation (Bengtsson & Kock, 2000; Gnyawali & Park, 2011; Nalebuff & Brandenburger, 1997). Accordingly, RP 1 investigates how blockchain-based IS can facilitate cooperative interactions in supply networks while ensuring data confidentiality.

At the requirements level, the systematic literature review yields eight design objectives for coopetition-aware blockchain-based IS: data protection, accountability, decentralization, performance, interoperability, traceability, transparency, and automation. The study structures these objectives through the integration principle of coopetition theory, according to which cooperation and competition should be addressed as interdependent rather than separate or mutually exclusive design concerns (Bengtsson & Kock, 2000; Fernandez & Chiambaretto, 2016). Decentralized infrastructures for supply-chain automation should therefore not be designed merely to maximize

transparency. Instead, their configuration must enable cooperative process execution while preserving competitive autonomy and protecting sensitive information.

These objectives inform a conceptual blockchain architecture for cooperative supply networks. The architecture combines a permissioned Hyperledger Fabric network with identity management, endorsement policies, channels, and private data collections to establish a shared and traceable process state while restricting confidential business information to authorized participants. Applied to digital delivery-invoice processing as the unit of analysis, this configuration demonstrates how common validation and process automation can be combined with differentiated information access. The artifact thereby translates the cooperation–competition tension into concrete architectural allocations of validation, visibility, and control.

Reflection on the artifact and its evaluation is consolidated into three implementation guidelines for blockchain-based IS in cooperative supply networks:

Implementation Guideline 1: *Opt for a decentralized solution when the benefits of leveraging network effects in a cooperative market surpass the complexities and challenges of its implementation.*

Implementation Guideline 2: *Utilize private data collections and private channels to protect interorganizational data exchanges from unauthorized third-party access.*

Implementation Guideline 3: *Enhance private data collections and channels with additional privacy-preserving technologies to ensure complete data confidentiality.*

Collectively, the design objectives, architecture, and implementation guidelines contribute to RG 1 by integrating cooperation theory with blockchain-based system design. RP 1 shows how shared validation, traceability, and automation can be combined with differentiated access to confidential information, enabling cooperative process execution without requiring unrestricted visibility into competitively sensitive data.

RP 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry

Where RP 1 abstracts broader design knowledge from the shared DSR project, RP 2 provides its earlier, process-specific contribution. The study develops and evaluates a

blockchain-based delivery-invoice system for the construction industry, treating digital delivery-invoice handling as a concrete interorganizational coordination problem (Hevner et al., 2004; Peffers et al., 2007). Construction firms increasingly seek to digitalize paper-based processes to improve efficiency and automation, yet available digital solutions often remain fragmented, centralized, or insufficiently accepted across heterogeneous supply-chain actors (Bajpai & Misra, 2024; Demirkesen & Tezel, 2021; Prebanić & Vukomanović, 2021). RP 2 therefore examines how blockchain technology can support digital delivery-invoice processing while addressing the data-transparency trade-off that arises in cooperative supply chains.

The process analysis translates this trade-off into three design objectives. *Secure data exchange* concerns the confidentiality, integrity, availability, and authenticity of delivery-invoice data. *Collaboration* requires the integration of heterogeneous stakeholders and existing systems into a shared decentralized infrastructure. *Competition* captures the need to protect sensitive business information from unauthorized actors while enabling sufficient information sharing for invoice processing and verification (Lacity & van Hoek, 2021). Together, these objectives establish the requirements against which the artifact is designed and assessed.

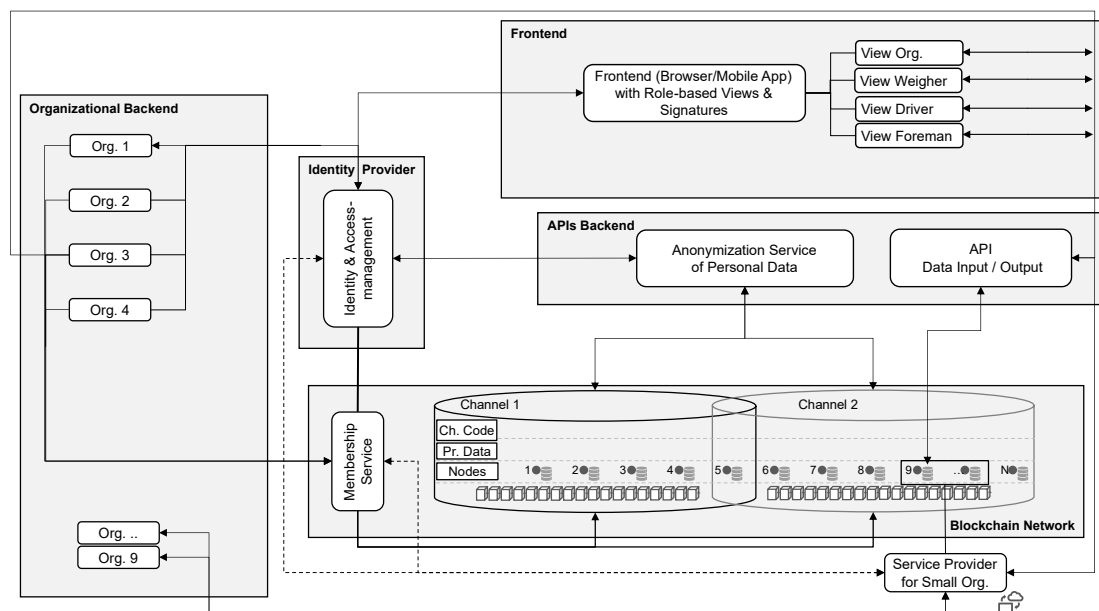


Figure 2: Blockchain-based prototype architecture for digital delivery invoice processing developed in RP 2

Figure 2 presents the resulting blockchain-based prototype for digital delivery-invoice processing. Its architecture comprises backend, frontend, and blockchain layers and incorporates an identity provider to implement company-level roles and access rights.

The underlying Hyperledger Fabric configuration uses a permissioned network, channels, endorsement policies, and private data collections to manage access to confidential information. The prototype supports the creation, transfer, acceptance, rejection, commenting, and status tracking of digital delivery invoices. It thereby demonstrates how process information can be synchronized across supply-chain actors without making every invoice detail visible to all network participants.

Evaluation through nine ex-post expert interviews assesses the prototype and informs three design principles for decentralized delivery-invoice systems (Sonnenberg & vom Brocke, 2012; Venable et al., 2016). The resulting principles condition the use of a decentralized infrastructure on whether its network benefits outweigh its implementation complexity, recommend private data collections and channels for restricting unauthorized access, and identify the need for complementary privacy-preserving technologies, such as ZKPs or multiparty computation, where these native mechanisms provide insufficient confidentiality (Sedlmeir et al., 2022).

By connecting process-specific requirements, an instantiated prototype, and evaluated design principles, RP 2 contributes to RG 1 through a concrete implementation of verifiable and confidentiality-preserving interorganizational information sharing. The study shows that shared process visibility, traceability, and automation depend on deliberately differentiated information access rather than indiscriminate transparency.

RP 3: Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy

RP 3 applies a DSR approach to develop and evaluate a blockchain-based IS for procurement processes (Hevner et al., 2004; Peffers et al., 2007). While RPs 1 and 2 focus on cooperative supply chain settings and delivery invoice processing, RP 3 addresses a broader infrastructural challenge: how blockchain-based procurement systems can reconcile decentralization, scalability, security, and privacy. The paper starts from the observation that procurement processes are characterized by fragmented system landscapes, media discontinuities, isolated records, manual reconciliation, and trust deficits between organizations. Blockchain technology promises a shared, tamper-evident, and programmable coordination layer for such settings (Beck et al., 2017; Butijn et al.,

2021; Wüst & Gervais, 2018). However, existing blockchain-based procurement artifacts often rely on permissioned architectures that improve privacy and performance but weaken decentralization and open verifiability. Against this background, RP 3 investigates how blockchain-based IS can be designed to balance the extended blockchain trilemma in procurement contexts.

A central outcome of the study is the development and evaluation of five design objectives that translate procurement challenges and blockchain-specific tensions into actionable requirements. The artifact should enable enterprises to integrate their enterprise resource planning systems with publicly accessible and interoperable blockchain infrastructure, embed stable and regulation-compliant payment processing into procurement workflows, strengthen trust in dispute resolution without undermining trust in the underlying infrastructure, scale with growing transaction volumes and users, and preserve privacy while maintaining the auditability of blockchain records. These objectives are derived from a structured literature review and refined through expert feedback, thereby connecting procurement-specific information exchange problems with infrastructural design requirements (Venable et al., 2016; Webster & Watson, 2002). The findings suggest that blockchain-based procurement systems should not be viewed merely as process automation tools. Instead, they must address a broader set of interdependent infrastructural requirements that shape the viability of decentralized information sharing.

To operationalize these objectives, the paper proposes a layered blockchain architecture that distributes responsibilities across different infrastructural layers. As Figure 3 shows, the artifact combines a public permissionless Layer 1 blockchain as a trust anchor with a privacy-preserving Layer 2 infrastructure for confidential process execution. The Layer 1 provides standardization, open verifiability, auditability, and security, while the Layer 2 addresses scalability and privacy requirements by processing high-volume, sensitive procurement interactions off-chain and settling proofs on the base layer. ZKPs are used to verify the correctness of relevant computations without revealing underlying sensitive data, thereby allowing procurement information to remain confidential while preserving verifiability. Rather than expecting a single blockchain layer to satisfy all requirements simultaneously, the architecture illustrates how decentralization, scalability, security, and privacy can be addressed through a complementary layering approach.

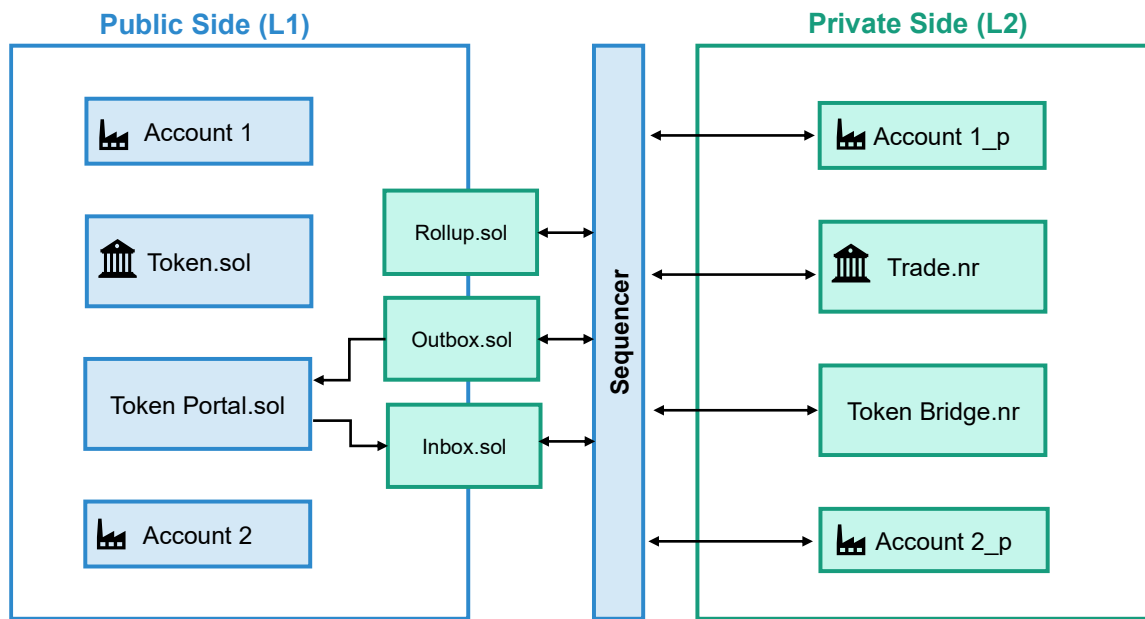


Figure 3: Layered blockchain-based architecture and communication flow presented in RP 3

The proposed artifact is assessed through technical verification, a quantitative viability assessment, and 16 semi-structured expert interviews. The evaluation indicates that the layered architecture provides a feasible approach for balancing the competing demands of decentralization, scalability, security, and privacy in procurement-related interorganizational IS. At the same time, the expert feedback emphasizes that this balance depends on several critical design decisions, including decentralized inter-layer communication, the maturity of roll-up infrastructures, the selection of efficient and resilient ZKP protocols, and the reduction of centralized control mechanisms. Based on these insights, the paper formulates two design principles (Gregor et al., 2020). The first advocates *combining a public Layer 1 as trust anchor with a Layer 2 for scalability and decentralized communication between layers to address the blockchain trilemma*. The second emphasizes the *use of efficient and resilient cryptographic mechanisms alongside minimized control structures to preserve privacy without compromising the overall architectural balance*.

Beyond the specific procurement setting, RP 3 contributes to RG 1 by extending the discussion from individual process applications to the design of decentralized digital infrastructures. The study provides an empirically grounded problem statement, a set of evaluated design objectives, a layered prototype architecture, and prescriptive design principles for blockchain-based procurement systems. Its findings indicate that achieving privacy and scalability does not necessarily require a shift toward

permissioned or centrally governed architectures. Instead, open verifiability and auditability can be maintained when public blockchain layers, privacy-preserving scaling solutions, and cryptographic verification mechanisms are integrated into a coherent architectural design.

RP 4: From Documents to Verifiable Credentials: How Digital Signal-Carriers Reconfigure Decision-Making in Buyer–Supplier Relationship Formation

RP 4 investigates how VCs within the SSI paradigm reshape decision-making in buyer–supplier relationship formation. In contrast to RPs 1–3, which primarily develop design knowledge for decentralized infrastructures, RP 4 adopts a qualitative phenomenon-based theorizing approach to examine how supplier claims can become digitally verifiable before contractual relationships are formed (Fisher et al., 2021; Gregory & Henfridsson, 2021; Krogh et al., 2012). The paper starts from the observation that buyers frequently face information asymmetries when assessing suppliers, as they cannot directly observe a supplier’s capabilities, compliance, or operational quality prior to contracting (Akerlof, 1978; Beer et al., 2018). Signaling theory explains how observable and costly signals can reduce such information asymmetries (Connelly et al., 2011; Riley, 2001; Spence, 1973). However, in digitally mediated environments, signals are often transmitted through documents, platforms, or digital artifacts whose integrity cannot be assumed. Against this background, RP 4 examines how VCs can function as digital signal-carriers in pre-contractual buyer–supplier decision-making.

One central contribution of the paper is the conceptualization of the digital signal-carrier as an explicit analytical construct. Existing signaling research has primarily focused on signal content, signal costliness, and signal observability, while treating the medium through which signals are transmitted as largely neutral (Connelly et al., 2011; Connelly et al., 2025). RP 4 challenges this assumption by showing that digitally mediated signaling depends not only on what is claimed, but also on how the claim is carried, preserved, and verified. Conventional digital documents can often be copied, altered, or selectively presented at low cost, thereby weakening the relationship between signal production and signal observability. By contrast, VCs embed cryptographic verification into the signal carrier itself. This allows buyers to assess whether a supplier-related credential is authentic, unaltered, issued by the claimed authority,

and still valid. The paper therefore extends signaling theory by demonstrating that the credibility of digital signals is partly determined by the structural integrity of their carrier.

Building on this insight, the paper develops an empirically grounded process model comprising three interrelated dimensions: verifiable signal-carrier infrastructure, digital signal credibilization, and digital signal-informed selection. Within this broader process, credible digital signaling depends on a dual-layer mechanism, shown in Figure 4, through which VCs mitigate deceptive signaling. The first layer, technical signal-carrier verification, refers to the ability to verify a credential's provenance, integrity, and validity through cryptographic signatures and supporting verification infrastructure. Technical signal-carrier verification limits the ability to use manipulated credentials successfully because altered, falsified, revoked, or expired credentials can be detected before they inform supplier selection. The second layer, signal-information evaluation, concerns whether the credential was issued by a trusted and contextually relevant issuer, whether the credential type is appropriate, and whether the represented claim provides meaningful evidence of supplier quality. The mechanism therefore combines cryptographic validity with institutional assessment, linking the structural integrity of the digital carrier to the credibility of the underlying supplier signal (Ehrlich et al., 2021; Preukschat & Reed, 2021; Sedlmeir et al., 2021).

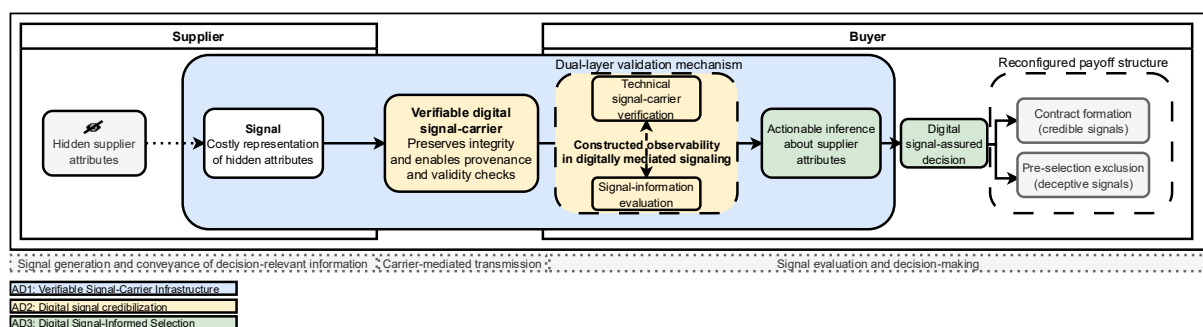


Figure 4: Extension of signaling theory through verifiable digital signal-carriers resulting from RP 4

Another insight concerns the temporal dynamics of signaling in buyer–supplier relationship formation. In conventional document-based processes, deceptive or invalid signals may be detected only after a contract has been concluded, for example, through audits, disputes, or operational failure. VCs move part of this verification to the pre-selection stage: buyers can assess the provenance, integrity, issuer, and validity of a credential before incorporating the corresponding claim into their decision (cf. Figure 4). Forged, altered, revoked, or otherwise invalid credentials can therefore be excluded

before they influence supplier selection. This earlier screening can reduce the expected payoff of deceptive signaling and the risk of adverse selection by restoring signal observability at the point of decision.

Overall, RP 4 contributes to RG 2 by conceptualizing VCs as verifiable digital representations of supplier claims and by explaining how their technical and institutional properties shape the credibility of those claims. The paper demonstrates that verifiability in interorganizational information sharing is not only an infrastructural property but also depends on how exchanged information is represented and interpreted. By theorizing digital signal-carriers, RP 4 shows how buyers can assess decision-relevant supplier claims without requiring direct access to all underlying supplier information. It thereby clarifies how representation design can reduce information asymmetries and deceptive signaling while limiting the information that must be disclosed for pre-contractual decision-making.

RP 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control

The fifth RP examines how a blockchain-based IS can control duplicate withholding-tax refund claims in a federated tax-administration setting. Using the historical German Cum-Ex mechanism as its focal case, the paper identifies an IS problem arising from the fragmentation of tax remittance, securities custody, certification, and refund processing across organizational boundaries. This fragmentation enabled multiple documentary claims to become detached from the single tax payment and substantive entitlement on which a legitimate refund depended (Buettner et al., 2020; Schubert, 2021; Spengel, 2021a, 2021b). Drawing on principal-agent theory (PAT), the study conceptualizes the resulting problem in terms of goal divergence, information asymmetry, and costly monitoring among tax authorities, taxpayers, custodians, and other financial intermediaries (Crocker & Slemrod, 2005; Jensen & Meckling, 1976; Reinganum & Wilde, 1985).

The paper translates this problem into two meta-requirements (MRs) and six corresponding design objectives (DOs). MR1, effectiveness of control, requires reducing opportunistic refund claims arising from harmful information asymmetries. It is primarily operationalized through DOs concerning the prevention of duplicate exercise and

the verifiability of the entitlement lifecycle. MR2, proportionality of control, requires limiting the direct and indirect agency costs induced by stronger control. Its corresponding DOs address privacy-preserving verification, interoperability with financial and tax infrastructures, scalability and availability, and implementation and operating costs (Allingham & Sandmo, 1972; Crocker & Slemrod, 2005; Gurbaxani & Whang, 1991; Jensen & Meckling, 1976; Keen & Slemrod, 2017; Reinganum & Wilde, 1985). This distinction shifts the focus from maximizing transparency or control toward establishing an effective but proportionate control arrangement.

The conceptual artifact combines a private, permissioned consortium blockchain with governed entitlement states, smart-contract-based constraints, and ZKPs. A tax entitlement is represented as an event-specific digital state anchored to a withholding-tax payment recognized by the competent tax authority rather than as a freely transferable cryptoasset or an independent source of legal entitlement (Hanneke et al., 2024; Schwiderowski et al., 2024). For each withholding-tax event and authorized custodian, the tax authority authorizes a maximum entitlement value corresponding to the tax amount recognized as remitted. Custodians can create beneficiary-specific entitlement commitments within this authorization. A legally recognized reassignment replaces rather than duplicates the preceding state, while redemption consumes the current entitlement so that it cannot be exercised again. ZKPs enable the conditions governing authorization, creation, reassignment, and redemption to be verified while concealing beneficiary and transaction information that is not required for the respective control decision (Goldwasser et al., 1989; Sedlmeir et al., 2022). The digital representation does not itself establish legal entitlement or the substantive correctness of the authoritative off-chain information on which the lifecycle depends.

The evaluation combines ten semi-structured expert interviews with an analytical assessment of modeled transaction workloads and selected recurring technical costs. The interviews support the conceptual plausibility of the core entitlement-control logic while identifying boundary conditions concerning formalizability, governance, confidentiality, institutional integration, operational resilience, and economic viability. Under the stated assumptions, the modeled aggregate workloads appear technically manageable, and the estimated recurring blockchain- and proof-related expenses are unlikely to constitute the principal implementation barrier. The evaluation does not, however, establish realized prevention of duplicate claims, reductions in harmful

information asymmetry or agency costs, production reliability, or total cost-effectiveness.

Building on the artifact and its evaluation, RP 5 derives three design principles for regulated interorganizational IS following Gregor et al. (2020):

Design Principle 1: *To constrain formalizable opportunistic actions ex ante in principal–agent settings, design the IS so that only actions satisfying the principal’s objectively specifiable rules can be executed.*

Design Principle 2: *To prevent duplicated or inconsistent claims in fragmented interorganizational processes, bind governed entitlements to authoritative originating events and preserve a unique, conserved state across authorized transitions.*

Design Principle 3: *To reduce decision-relevant information asymmetries while protecting sensitive information, design the IS so that authorized actors can verify only the properties required for their respective control decisions, while underlying information not required for those decisions remains concealed.*

Together, these principles decompose the artifact into complementary mechanisms concerning action admissibility, entitlement-state conservation, and selective verifiability. They show that blockchain-based control does not replace institutional monitoring and authority but can shift selected controls from ex-post detection toward ex-ante restriction where relevant actions are formalizable and authoritative inputs are available. RP 5 thereby contributes to RG 2 by showing how tokenized representations can preserve the uniqueness and lifecycle of legally and financially consequential entitlements while supporting proportionate and confidentiality-preserving control across organizational boundaries.

RP 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications

RP 6 investigates which attributes, features, and characteristics of SSI systems influence user acceptance. SSI aims to provide portable digital identities and VCs that remain under the control of their holders (Babel, Willburger, et al., 2025; Preukschat & Reed, 2021). However, previous digital identity initiatives demonstrate that technical availability alone does not ensure adoption, particularly when systems are perceived

as difficult to use or offer only a limited range of use cases (Felden et al., 2020; Rederer et al., 2021). The paper examines this challenge through an SSI demonstrator in which an income-tax certificate is issued as a VC and selectively presented to a financial institution during a loan-application process. As Figure 5 shows, the analysis identifies 14 acceptance categories: five originate from TAM2, and nine are developed inductively from the interview material. These categories are organized into three overarching groups: framework conditions, software characteristics, and user characteristics. At the center of the resulting model are perceived usefulness, perceived ease of use, and trust, which are proposed as direct determinants of users' intention to use the SSI system. Perceived usefulness and perceived ease of use build on established technology acceptance research (Davis, 1985; Venkatesh & Davis, 2000), while trust extends the original TAM2 structure and reflects the importance of confidence in both the technical system and the institutions involved in its operation (Benbasat et al., 2010; McKnight et al., 2011).

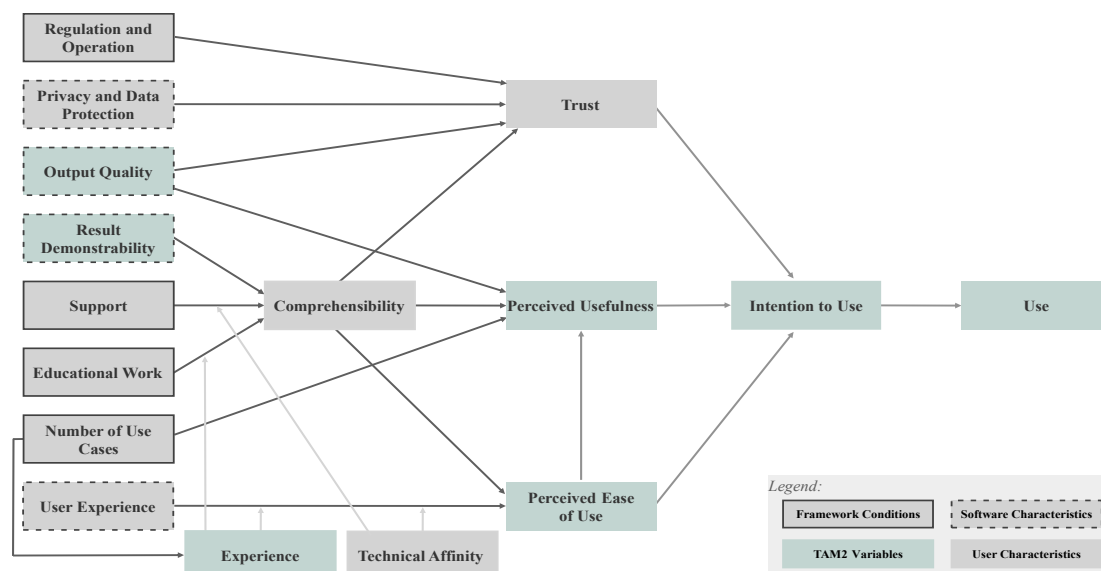


Figure 5: Self-Sovereign Identity acceptance model developed in RP 6

The model proposes that trust is influenced by regulation and operation, privacy and data protection, output quality, and comprehensibility. Privacy is particularly relevant because SSI enables credential holders to control which identity attributes they disclose (Preukschat & Reed, 2021). Comprehensibility further connects technical and institutional system characteristics with users' perceptions: when users understand the system's benefits and process steps, they are more likely to perceive it as useful, easy to use, and trustworthy. Educational measures and user support facilitate this

understanding before and during system use. The paper also identifies the number of available use cases and the user experience as important software-related conditions. A broader range of use cases increases perceived usefulness and allows users to gain experience with SSI, highlighting the importance of network effects. Intuitive interfaces, limited media discontinuities, device independence, and adequate performance support perceived ease of use. The paper further proposes specific moderating roles for technical affinity and prior SSI experience in the relationships among educational measures, user support, user experience, comprehensibility, and perceived ease of use (Franke et al., 2019). The resulting model extends TAM2 with nine inductively derived acceptance categories identified as relevant in the SSI context, including trust, privacy and data protection, comprehensibility, institutional operation, ecosystem reach, and individual technical characteristics. As the proposed relationships are derived from qualitative evidence, they constitute hypotheses for subsequent empirical validation rather than statistically tested causal effects. For practice, the findings indicate that the effective use of SSI systems depends not only on their technical properties but also on tangible user benefits, understandable and low-effort interactions, trustworthy institutional arrangements, adequate support, and a sufficiently broad range of use cases.

RP 6 contributes to RG 2 by conceptualizing the conditions under which verifiable and confidentiality-preserving digital representations become effective in use. Whereas RPs 4 and 5 explain how credentials and tokens preserve verification-relevant properties of claims and entitlements, RP 6 identifies conditions that shape whether the corresponding holder-centered interactions are understood, trusted, and accepted by users.

6 Discussion and Conclusion

This final section summarizes the cumulative findings of the dissertation, discusses their contributions to theory and implications for practice, reflects on the limitations of the research, and outlines avenues for future research.

6.1 Summary

This dissertation investigates how decentralized IS can enable verifiable and confidentiality-preserving interorganizational information sharing. To address this overarching research question, it pursues two complementary RGs. RG 1 develops design knowledge for decentralized infrastructures that support verifiable and confidentiality-preserving interorganizational information sharing. RG 2 conceptualizes verifiable and confidentiality-preserving digital representations and the conditions for their effective use in interorganizational information sharing. The six RPs examine the corresponding research questions through complementary prescriptive and qualitative research designs, combining DSR with phenomenon-based theorizing and exploratory acceptance research.

RPs 1–3 address RG 1 by developing design knowledge for the infrastructure level. RP 1 develops architecture-level and implementation-oriented design knowledge for blockchain-based IS in cooperative supply networks, while RP 2 provides the process-specific design and evaluation of a blockchain-based delivery-invoice system for the construction industry. RP 3 extends this infrastructural perspective by proposing and evaluating a layered blockchain architecture that balances decentralization, scalability, security, and privacy in procurement processes. Together, RPs 1–3 show that supporting verifiable and confidentiality-preserving interorganizational information sharing does not require maximizing decentralization or transparency. Rather, decentralized infrastructures must allocate verification, visibility, and control in accordance with the underlying coordination problem while preserving legitimate confidentiality and governance requirements.

RPs 4–6 address RG 2 by examining how information becomes meaningfully verifiable through digital representations and under which conditions representation-based interactions become effective in use. RP 4 conceptualizes VCs as digital signal-carriers that make the provenance, integrity, issuer, and validity of supplier credentials

verifiable before they inform supplier-selection decisions. RP 5 develops tokenized tax entitlements whose creation, authorized reassignment, and redemption can be governed and verified across organizational boundaries to mitigate principal–agent problems in dividend taxation. RP 6 complements these representation mechanisms by identifying the conditions under which users understand, trust, and accept SSI-based interactions involving VCs. Together, RPs 4–6 show that verifiable digital representations must preserve the properties required to assess claims or entitlements while limiting unnecessary disclosure and must be embedded in governance and interaction conditions that support their effective use.

Taken together, the dissertation answers the overarching research question by showing that decentralized IS can enable verifiable and confidentiality-preserving interorganizational information sharing when selected verification and control functions are distributed at the infrastructure level in accordance with the underlying coordination problem and the exchanged information is represented in forms that preserve verification-relevant properties while limiting disclosure to what is required. Institutional governance determines which actors, representations, and verification procedures are legitimate, while effective use determines whether the resulting interactions are understood and enacted in practice.

6.2 Contributions to Theory and Implications for Practice

Across the six RPs, this dissertation develops a cumulative understanding of how decentralized IS can enable verifiable and confidentiality-preserving information sharing across organizational boundaries. The findings yield three interrelated theoretical contributions. They show that verifiability does not require unrestricted transparency, develop a contingency logic for the timing and form of IS-enabled verification and control, and conceptualize decentralized IS through the alignment of verification infrastructures and verifiable digital representations. Together, these contributions characterize decentralized IS not as infrastructures that eliminate authority or maximize transparency, but as socio-technical arrangements in which verification, disclosure, and control are deliberately allocated across actors and technical components (Beck et al., 2018; Ellinger et al., 2024).

Contributions to Theory

At the intersection of verifiability and confidentiality, the dissertation shows that *verifiability does not require unrestricted transparency*. Blockchain research has frequently emphasized shared visibility and transparency as mechanisms for supporting trust, accountability, and coordination. In interorganizational settings, however, greater visibility can simultaneously expose commercially sensitive, personal, or financial information and thereby conflict with legitimate confidentiality requirements (Bossler et al., 2024; Sedlmeir et al., 2022). RPs 1 and 2 demonstrate this tension in coopetitive supply networks, where organizations depend on shared information for coordination while retaining legitimate reasons to restrict access to strategically sensitive information. By translating the integration principle of coopetition into IS design, the papers show that cooperation and competition can be addressed jointly through differentiated visibility, access control, and privacy-preserving mechanisms rather than by maximizing information disclosure (Bengtsson & Kock, 2000; Fernandez & Chiambaretto, 2016). RP 3 extends this reasoning at the architectural level. Its layered architecture shows that confidentiality does not necessarily require retreating to a fully permissioned or centrally controlled infrastructure (Beck et al., 2018; Wüst & Gervais, 2018). A public Layer 1 can provide a decentralized trust anchor, while confidential and scalable execution is allocated to a privacy-preserving Layer 2. In the terminology of RP 3, privacy therefore becomes an interdependent fourth dimension of the extended blockchain trilemma alongside decentralization, scalability, and security, requiring architectural allocation and cryptographic enforcement rather than treatment as an isolated requirement.

RPs 4 and 5 carry this reasoning from infrastructures to the information objects being verified. VCs allow recipients to assess verification-relevant properties of attestable claims, including provenance, integrity, issuer, and validity, without requiring unrestricted access to all underlying information. Tokenized entitlements similarly enable creation, authorized reassignment, lifecycle continuity, and redemption to become verifiable while sensitive shareholder and transaction information remains protected. Cryptographic mechanisms such as ZKPs provide a direct technical means of separating evidence about a relevant property from disclosure of the underlying data (Babel & Sedlmeir, 2023; Principato et al., 2023; Schellinger et al., 2022; Sedlmeir et al., 2022). They complement access restrictions, verifiable representations, and institutional

governance rather than replacing them. Taken together, these findings establish verification and disclosure as related but distinct design dimensions. Decentralized IS can reduce harmful information asymmetries by making decision-relevant properties verifiable while maintaining strategically, economically, or legally justified confidentiality. The contribution therefore qualifies transparency-centered conceptions of blockchain-based coordination: the objective is not maximum transparency, but sufficient and appropriately governed verifiability under confidentiality constraints.

Extending this insight, the dissertation develops *a contingency logic for the timing and form of IS-enabled verification and control*. This builds upon prior research that has emphasized immutable records, distributed consensus, and smart contracts as mechanisms for reducing uncertainty, supporting monitoring, and coordinating behavior (Beck et al., 2017; Catalini & Gans, 2016; Ellinger et al., 2024). The cumulative findings of this dissertation distinguish three points of intervention: pre-decision verification, ex-ante technical constraint, and ex-post monitoring and adjudication, which are aligned with theoretical observations from principal–agent theory and broader agency-theoretic research (Pavlou et al., 2007; Ross, 1973). Which mechanism is appropriate depends on when relevant evidence becomes verifiable and whether legitimate actions and system states can be formalized.

RP 4 illustrates pre-decision verification in the context of signaling. Signaling theory primarily explains how signal costliness, observability, and sender characteristics enable recipients to infer otherwise hidden qualities, while the medium through which a signal is transmitted has received comparatively less explicit attention (Connelly et al., 2011; Connelly et al., 2025; Spence, 1973). By conceptualizing the digital signal-carrier as an explicit analytical element, RP 4 shows how VCs can restore observability at the point at which a consequential decision is made. Buyers can verify the provenance, integrity, issuer, and validity of a supplier credential before incorporating the signal into supplier selection. This shifts the identification of forged, altered, revoked, or otherwise invalid evidence from later audits and disputes toward the pre-contractual decision stage. Verification therefore changes not only the reliability of information but also when deceptive signals can be excluded from the decision process.

RP 5 identifies a complementary mechanism in principal–agent settings. Principal–agent theory commonly addresses information asymmetries and goal incongruence

through monitoring, incentive alignment, and sanctions (Jensen & Meckling, 1976; Mahoney, 1995). Where permissible actions and system states can be specified sufficiently clearly and verified objectively, smart contracts and tokenized representations allow parts of this governance to shift from ex-post detection toward ex-ante technical constraint (Beck et al., 2018; Carvalho & Karimi, 2021). In the dividend-taxation artifact, linking entitlement creation to a withholding-tax payment recognized by the competent authority and consuming the corresponding entitlement upon redemption constrains the same represented entitlement from supporting multiple refund claims. This mechanism, however, is contingent on the formalizability of the underlying rule. Where decisions require interpretation, discretionary judgment, or authoritative assessment of facts outside the system, technical constraints cannot substitute for institutional decision-making. In such cases, tamper-evident records and cryptographic evidence primarily strengthen ex-post monitoring and adjudication. The theoretical contribution therefore lies not simply in identifying three governance mechanisms, but in establishing a contingency logic between the verifiability and formalizability of an information problem and the point at which IS-enabled governance can intervene. Decentralized IS can move governance toward earlier intervention where evidence or rules permit it, while settings that remain interpretative or discretionary continue to require ex-post institutional oversight.

Bringing these mechanisms together, the dissertation *conceptualizes decentralized IS at two interdependent levels: verification infrastructures and verifiable digital representations*. RG 1 develops prescriptive knowledge about the infrastructure level through mechanisms such as granular access controls, private data collections, public blockchain trust anchors, privacy-preserving scaling architectures, and cryptographic verification. The resulting design objectives, architectures, implementation guidelines, and design principles contribute knowledge about how verification is technically enabled and under whose control it occurs in interorganizational IS (Gregor & Hevner, 2013; Gregor et al., 2020; Hevner et al., 2004). RPs contributing to RG 2 demonstrate that this infrastructural perspective is necessary but insufficient. The information exchanged through an infrastructure must itself preserve the properties required for meaningful verification. RP 4 shows that the credibility of an attestable claim depends on the integrity and provenance of its carrier, while RP 5 shows that legally and

financially consequential entitlements additionally depend on uniqueness, controlled lifecycle transitions, and irreversible redemption. Although VCs and tokens address different information problems, both embed verification-relevant properties into digital representations (Schwiderowski et al., 2024; Sedlmeir et al., 2021).

This distinction clarifies why neither level is sufficient in isolation. A decentralized infrastructure can preserve the integrity and ordering of recorded states without independently ensuring that externally supplied or represented information is correct, legitimate, or decision-relevant (Azzi et al., 2019; Nofer et al., 2017). Conversely, a cryptographically verifiable credential or token requires a supporting technical and governance environment through which issuer authority, validity information, communication, permissible state transitions, and institutional recognition can be established. RP 6 adds an additional condition to this relationship by showing that technically valid and institutionally governed representations do not automatically become effective in use. Holder-centered interactions must also be understood, trusted, and accepted by the actors expected to enact them. Its findings extend established technology acceptance research by identifying conditions that are particularly relevant to SSI-based interactions, including privacy and data protection, institutional operation, user support, perceived benefits, and the availability of relevant use cases (Davis, 1985; Venkatesh & Davis, 2000). Effective use, therefore, does not constitute a third analytical level, but a condition under which representation-based verification becomes practically enacted. The dual-level conceptualization consequently extends research beyond isolated blockchain architectures or representation technologies by showing that verifiable and confidentiality-preserving interorganizational information sharing emerges from the alignment of infrastructural allocation and representational properties, complemented by institutional governance and effective use.

Implications for Practice

For practitioners, the design process should begin by diagnosing where distributed verification and control create value. Decentralized IS are particularly relevant when process-relevant information and responsibilities are distributed across organizations, unrestricted disclosure is unacceptable, and concentrating verification or governance functions in a single intermediary would create undesirable dependencies or be unacceptable to participating actors. Organizations can use these characteristics to compare the expected benefits of shared verification, reduced reconciliation, organizational autonomy, and more balanced control with the costs of integration, governance, cryptographic mechanisms, and ecosystem coordination. Where a trusted intermediary can appropriately provide the required information and verification functions, a conventional architecture may remain preferable (Lacity & van Hoek, 2021; Pedersen et al., 2019; Sternberg et al., 2021; Wüst & Gervais, 2018). The implication for practice is therefore not a blanket recommendation for decentralization, but a structured basis for selecting it where it fits the coordination problem.

Once the architectural scope has been established, organizations should determine where verification should intervene in the respective process. Where evidence can be authenticated before a consequential decision, verification can be moved to the decision point, as illustrated by VC-supported supplier selection. Where legitimate actions and state transitions can be formalized and reliably evaluated, organizations can consider ex-ante technical constraints that prevent invalid represented states from being accepted by the system. Where interpretation, discretionary judgment, or external facts remain essential, decentralized infrastructures should instead be used to strengthen traceability, evidence quality, and ex-post oversight rather than attempting to replace institutional adjudication. This distinction helps organizations avoid both underusing decentralized verification as a passive audit trail and overestimating the extent to which organizational or legal decisions can be automated.

Building on this process perspective, infrastructure, representation, confidentiality mechanisms, and governance responsibilities must be designed jointly whenever a decentralized solution is appropriate. The representational form should correspond to the underlying information problem. VCs are particularly suitable for attestable claims whose issuer, provenance, integrity, and validity must be established, whereas tokenized representations are appropriate where rights or entitlements must remain

unique and undergo controlled creation, authorized reassignment, lifecycle continuity, and redemption (Schwiderowski et al., 2024; Sedlmeir et al., 2021). Cryptographic mechanisms should then be selected according to the properties that must become verifiable and the information that must remain confidential. In parallel, organizations must specify who may participate, issue representations, access information, modify rules, authorize exceptional actions, and resolve disputes. Decentralization does not remove governance responsibilities, it changes where and how they are exercised.

Technical soundness alone is insufficient, successful implementation also depends on conditions for effective use. Holder-centered credential systems require tangible user benefits, understandable and low-effort interactions, trustworthy institutional arrangements, adequate support, and sufficiently relevant use cases. Incremental pilots, modular architectures, standardized interfaces, and quantitative assessments of scalability, latency, costs, process benefits, and user acceptance can reduce implementation risks and expose misalignments before large-scale deployment. Overall, the findings show that verifiable and confidentiality-preserving interorganizational information sharing cannot be achieved merely by transferring existing documents and processes onto a blockchain or another decentralized infrastructure. It requires a problem-specific alignment of infrastructure, representation, verification, confidentiality, governance, and effective use.

6.3 Limitations

Investigating decentralized IS for verifiable and confidentiality-preserving interorganizational information sharing involves substantial socio-technical complexity. The technologies examined in this dissertation are embedded in organizational processes, institutional responsibilities, regulatory environments, and interdependent actor networks whose characteristics cannot be fully reproduced in individual studies or prototype evaluations. While the six RPs discuss respective study-specific boundaries in detail, several overarching limitations delimit the cumulative findings of this dissertation.

The methodological portfolio primarily supports context-sensitive, analytical approaches rather than statistical or causal inference. Literature reviews, workshops, expert and user interviews, artifact development, qualitative analysis, and expert-based evaluation were deliberately selected because they support the context-sensitive investigation of emerging socio-technical phenomena and the development of theoretically

grounded design and conceptual knowledge (Gioia et al., 2013; Hevner, 2007; Mayring, 2014; Peffers et al., 2007; Venable et al., 2016; Webster & Watson, 2002). Nevertheless, the resulting evidence primarily supports analytical rather than statistical generalization and does not provide causal validation of the identified mechanisms across broader populations. RPs 1–3 evaluate implemented or prototypical artifacts through expert feedback and technical or prototype-based assessments, whereas RP 5 evaluates a conceptual artifact through expert-based validation and modeled analyses of technical feasibility and selected recurring costs. They can therefore establish problem–solution fit, technical plausibility, and, where quantitatively assessed, feasibility, as well as perceived practical relevance, but cannot comprehensively determine sustained performance, organizational effects, governance conflicts, or total implementation and operating costs. RP 4 develops theoretical mechanisms from qualitative phenomenon-based inquiry rather than testing their causal effects, while the relationships identified in RP 6 constitute theoretically informed hypotheses derived from qualitative evidence rather than statistically validated relationships. Accordingly, the three cumulative theoretical contributions developed in Section 6.2 should likewise be understood as an integrative synthesis across complementary studies rather than as a unified theoretical model that has itself been independently tested across contexts. Moreover, RPs 1 and 2 originate from the same underlying DSR project and share their empirical material and artifact-development process. Their cumulative value lies in the subsequent refinement and abstraction of the resulting design knowledge, not in independent empirical replication.

The transferability of the findings is further bounded by the dissertation’s concentration on selected interorganizational settings, predominantly in Germany and Europe. The studies investigate construction supply networks, procurement processes, buyer–supplier relationship formation, dividend taxation, and an SSI-based income-tax credential use case. These contexts are particularly informative for the overarching research problem because they combine distributed information and responsibilities with sensitive data, heterogeneous actors, and substantial coordination or compliance requirements. At the same time, they reflect particular regulatory frameworks, competitive structures, institutional responsibilities, technological infrastructures, and user expectations. Several studies additionally rely on purposively selected experts or informed prospective users because the investigated technologies and processes require substantial domain knowledge. This strengthens the ability to obtain informed

assessments but limits representativeness for broader organizational and user populations. The transferability of the resulting design principles, theoretical mechanisms, and acceptance conditions to other industries, jurisdictions, network structures, and user groups therefore requires further empirical examination.

A separate limitation concerns the comparative value of decentralized arrangements relative to centralized alternatives. The individual RPs evaluate whether decentralized artifacts and mechanisms can address their respective design objectives and information problems, but they do not systematically compare decentralized and centralized architectures under equivalent operational conditions. The findings consequently support a contingency perspective on decentralization rather than a universal efficiency or performance claim. They indicate how verification and control can be distributed where the underlying problem warrants such an arrangement, but they do not establish the precise conditions under which the additional complexity of decentralization outweighs the benefits of a trusted intermediary or conventional shared infrastructure. This boundary is particularly important because several proposed artifacts continue to depend on authoritative external actors and reliable information inputs. The tax artifact, for example, requires custodians and tax authorities to provide and authorize process-relevant information, and its evaluation explicitly acknowledges that existing financial-market infrastructures limit how far blockchain-based verification can reduce information asymmetries. Similarly, the procurement architecture depends on the maturity and governance of Layer 2 infrastructures, ZKP technologies, and reliable connections between infrastructural layers. Decentralization therefore redistributes selected verification and control functions but does not remove dependencies on trustworthy inputs, legitimate institutional authority, or the surrounding socio-technical ecosystem.

The findings are also bounded by the evolving technological landscape and the absence of longitudinal evidence on sustained organizational use. Blockchain platforms, Layer 2 architectures, cryptographic protocols, SSI implementations, VC standards, and corresponding regulatory frameworks continue to evolve. Changes in scalability, interoperability, security, governance, usability, or regulation may affect the suitability of specific technical components and implementation choices. Abstracting artifact-specific observations into design objectives, design principles, theoretical mechanisms, and acceptance conditions reduces this technological dependency but cannot eliminate it.

More fundamentally, the dissertation does not provide a longitudinal account of how decentralized IS are adopted, institutionalized, and used once they become embedded in mature organizational environments. Although RP 6 explicitly examines conditions for effective use, its evidence concerns prospective users, perceptions, and intention to use rather than sustained behavioral use. The broader dissertation similarly captures expert assessments, implementation expectations, and designed governance arrangements rather than their evolution over extended periods. Organizational readiness, ecosystem formation, changing incentive structures, power asymmetries, governance disputes, workarounds, and emergent uses are therefore not investigated systematically across the RPs. The findings should consequently be understood as context-sensitive design and conceptual knowledge about how decentralized infrastructures and digital representations can support verifiable and confidentiality-preserving interorganizational information sharing and under which conditions their practical realization appears plausible, rather than as a comprehensive explanation of their adoption, diffusion, and long-term organizational effects.

6.4 Potential Avenues for Future Research

The limitations discussed above, together with the study-specific avenues identified in the individual RPs, provide several opportunities to validate, refine, and extend the findings of this dissertation. Future research should move beyond the design, conceptualization, and bounded evaluation of individual decentralized IS and investigate the boundary conditions under which their design principles and theoretical mechanisms produce sustained value in organizational practice. Building on the cumulative contributions developed in this dissertation, three broader research directions appear particularly promising.

Comparative validation of the boundary conditions for decentralized verification and IS-enabled governance represents a central next step. The findings of this dissertation support a contingency perspective according to which decentralization is not inherently preferable to centralized coordination. Rather, its value depends on characteristics of the underlying information problem, including how information and responsibilities are distributed, whether participating actors accept a common intermediary, which information must remain confidential, and how verification and control should be allocated. Comparative studies should therefore examine decentralized, centralized,

and hybrid arrangements under comparable organizational and technical conditions. Such research could investigate when the benefits of distributed verification, reduced reconciliation, organizational autonomy, or more balanced control outweigh the additional complexity associated with governance, integration, cryptographic mechanisms, and ecosystem coordination. Full-scale implementations and longitudinal case studies would be particularly valuable for evaluating whether the artifacts and design principles developed in the RPs produce sustained effects once embedded in established processes and heterogeneous system landscapes. Relevant outcomes include process performance, implementation and operating costs, interoperability, resilience, information quality, governance conflicts, and unintended organizational consequences.

Such comparative work should also test the contingency logic of governance intervention developed in Section 6.2. The dissertation distinguishes pre-decision verification, ex-ante technical constraint, and ex-post monitoring and adjudication as different mechanisms through which IS-enabled verification can address information problems. Future studies should investigate more systematically which characteristics determine whether a particular mechanism is effective. Controlled experiments and field studies could, for example, examine whether verifiable evidence provided before a consequential decision improves decision quality or reduces deceptive signaling, and under which conditions actors actually incorporate such evidence into their decisions. In settings involving formalizable rights and transactions, research could evaluate when smart-contract-based constraints meaningfully reduce monitoring requirements or opportunistic behavior and when they merely relocate problems to data inputs, rule definition, or system governance. Conversely, contexts characterized by ambiguity, discretion, or incomplete information could help identify the limits of technical formalization and the conditions under which tamper-evident evidence primarily strengthens ex-post institutional oversight. Methodological pluralism combining qualitative inquiry with quantitative studies, experiments, surveys, and longitudinal designs would therefore be valuable for testing and refining the mechanisms synthesized across the six RPs (Hesse-Biber & Johnson, 2015; Kaplan & Maxwell, 2005).

A longitudinal perspective is needed to explain how decentralized information-sharing arrangements become governed, institutionalized, and effectively used over time. The dissertation conceptualizes decentralization as a redistribution rather than an elimination of authority. As decentralized IS move from bounded pilots toward larger

ecosystems, questions concerning participation, representation issuance, access rights, protocol modification, liability, exception handling, and dispute resolution become increasingly consequential. Longitudinal research could examine how such governance arrangements emerge and evolve, whether initially distributed control becomes concentrated as ecosystems mature, and how actors with different resources and bargaining power influence technical and institutional rules (Ellinger et al., 2024). Particular attention should be paid to the role of intermediaries. Infrastructure operators, wallet providers, accreditation bodies, trust registries, technology vendors, and other coordinating actors can reduce complexity and enable participation, yet they can simultaneously introduce new dependencies. Future research should therefore distinguish between intermediaries that provide legitimate coordination functions and arrangements that recreate the concentration of information or governance authority that decentralized infrastructures were intended to mitigate.

Beyond formal governance, longitudinal research should examine how representation-based interactions become embedded in sustained use. RP 6 identifies conditions that users associate with the acceptance of SSI applications, but these findings concern prospective perceptions and intention to use rather than sustained interaction in mature ecosystems. Future studies should examine how perceived usefulness, ease of use, trust, confidentiality perceptions, institutional operation, user support, and the availability of relevant use cases influence actual behavior over time. At the organizational level, complementary research should investigate how readiness, digital capabilities, incentives, process compatibility, ecosystem participation, and power asymmetries affect whether technically viable verification mechanisms become institutionalized in everyday work. This would extend the representation-level perspective from the question of whether a digital representation is technically and institutionally verifiable toward the broader question of whether organizations and individuals consistently rely on it when making consequential decisions. In doing so, future research could more precisely distinguish technical validity, institutional legitimacy, individual acceptance, and organizational routinization as complementary conditions of effective interorganizational verification.

Continued technological evolution calls for further refinement of the alignment between decentralized infrastructures, digital representations, and confidentiality-preserving verification mechanisms. Advances in Layer 2 architectures, ZKPs, multiparty

computation, decentralized identity, and related privacy-enhancing technologies increasingly enable the separation of sensitive information processing from the evidence required for shared verification (Babel & Sedlmeir, 2023; Ben Sasson et al., 2014; Principato et al., 2023). Future research should therefore examine how responsibilities for data storage, process execution, validation, rule definition, and governance should be distributed across organizational systems and decentralized components. Consistent with the findings of this dissertation, the objective should not be to decentralize every system function. Instead, research should establish which functions benefit from decentralized verification, which information should remain under organizational control, and where centralized or institutionally assigned responsibilities remain necessary. Such work could further clarify how confidentiality, scalability, security, interoperability, and distributed control can be reconciled without simply relocating trust to less visible infrastructure operators.

The representation level offers a corresponding research agenda. This dissertation distinguishes VCs for attestable claims from tokens for rights or entitlements whose uniqueness and lifecycle state must remain consistent. Subsequent research could develop a broader problem-oriented typology of digital representations based on the verification properties required in a particular interaction. Relevant dimensions may include provenance, integrity, uniqueness, transferability, revocability, delegation, temporal validity, and redemption. Research should also investigate how representations can be combined when complex interorganizational processes require several of these properties simultaneously. Importantly, such frameworks should extend beyond cryptographic correctness. A representation may be technically valid while remaining semantically ambiguous, being issued by an actor without appropriate authority, or lacking recognition within the relevant organizational or legal environment. Further research should therefore investigate the interaction between cryptographic validity, semantic interoperability, and institutional legitimacy, thereby refining the distinction between evidence that can technically be verified and information that can legitimately support organizational decisions.

This research direction becomes particularly important as generative and agentic artificial intelligence (AI) systems increasingly create, interpret, exchange, and act upon information across organizational boundaries (Allmendinger et al., 2026; Holldack et al., 2026). Autonomous or semi-autonomous agents may access organizational

resources, initiate transactions, negotiate with other agents, or delegate tasks within multi-agent structures. Such interactions extend the dissertation's underlying verification problem to actors whose actions may be initiated without direct human involvement. Future research should therefore examine how an agent's identity, organizational affiliation, capabilities, and delegated authority can be represented and verified across organizational boundaries. VCs, cryptographic proofs, and tamper-evident records may support authentication, document delegation chains, or establish the provenance of actions and outputs. Privacy-preserving mechanisms may additionally allow agents to demonstrate that authorization or compliance conditions are fulfilled without exposing the confidential information underlying their actions. At the same time, verifiable provenance must not be confused with substantive correctness. Establishing that an authorized agent produced a particular output does not demonstrate that its reasoning is accurate, its decision is appropriate, or its action is legally permissible. Research at the intersection of decentralized IS and AI should therefore distinguish verification of agent identity and authority, verification of output origin and integrity, and evaluation of the substantive quality and legitimacy of autonomous decisions.

Overall, the next phase of this research trajectory should examine decentralized IS as evolving socio-technical governance arrangements rather than isolated technological artifacts. Future research should address not only whether information that is distributed across organizational boundaries can be made verifiable while preserving confidentiality, but also when distributing verification and control creates durable value. How should infrastructures and representations be aligned as technologies and actor constellations evolve? How can technically verifiable information remain institutionally legitimate and be effectively used? Addressing these questions can advance a more complete understanding of how decentralized information systems support verifiable and confidentiality-preserving interorganizational information sharing.

Introduction References

- Abdelkafi, N., Raasch, C., Roth, A., & Srinivasan, R. (2019). Multi-sided platforms. *Electronic Markets*, 29(4), 553–559. <https://doi.org/10.1007/s12525-019-00385-4>
- Agdas, D., & Ellis, R. D. (2010). The potential of XML technology as an answer to the data interchange problems of the construction industry. *Construction Management and Economics*, 28(7), 737–746. <https://doi.org/10.1080/01446191003767503>
- Ainsworth, R. T., & Todorov, G. (2018). *Fiji – Mandatory Digital Invoices Real-Time VAT Compliance*. <https://ssrn.com/abstract=3580525>
- Akerlof, G. A. (1978). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. In *Uncertainty in Economics* (pp. 235–251). Elsevier. <https://doi.org/10.1016/B978-0-12-214850-7.50022-X>
- Allingham, M. G., & Sandmo, A. (1972). Income tax evasion: a theoretical analysis. *Journal of Public Economics*, 1(3-4), 323–338. [https://doi.org/10.1016/0047-2727\(72\)90010-2](https://doi.org/10.1016/0047-2727(72)90010-2)
- Allmendinger, S., Bonenberger, L., Endres, K., Fetzer, D., Gimpel, H., & Kühl, N. (2026). Multi-agent AI. *Electronic Markets*, 36(1). <https://doi.org/10.1007/s12525-025-00862-z>
- Alm, J., Bahl, R., & Murray, M. N. (1990). Tax Structure and Tax Compliance. *The Review of Economics and Statistics*, 72(4), 603. <https://doi.org/10.2307/2109600>
- Alt, R. (2020). Electronic Markets on business model development. *Electronic Markets*, 30.0(3). <https://doi.org/10.1007/s12525-020-00438-z>
- Anumba, C., & Ruikar, K. (2002). Electronic commerce in construction—trends and prospects. *Automation in Construction*, 11(3), 265–275. [https://doi.org/10.1016/S0926-5805\(01\)00087-5](https://doi.org/10.1016/S0926-5805(01)00087-5)
- Aruoba, S. B. (2021). Institutions, tax evasion, and optimal policy. *Journal of Monetary Economics*, 118, 212–229. <https://doi.org/10.1016/j.jmoneco.2020.10.003>
- Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. *Computers & Industrial Engineering*, 135, 582–592. <https://doi.org/10.1016/j.cie.2019.06.042>

- Babel, M., Ehaus, M., Heeß, P., Körner, M.-F., Schick, L., & Strüker, J. (2025). Introducing the Trust Diamond for Energy Flexibility Provision: On the Tension of Data Verifiability and Privacy. *Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS)*. <https://eref.uni-bayreuth.de/id/eprint/91591>
- Babel, M., & Sedlmeir, J. (2023). *Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs*. <https://doi.org/10.48550/arXiv.2301.00823>
- Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets*, 35(1). <https://doi.org/10.1007/s12525-025-00772-0>
- Babich, V., & Hilary, G. (2020). OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology. *Manufacturing & Service Operations Management*, 22(2), 223–240. <https://doi.org/10.1287/msom.2018.0752>
- Bajpai, A., & Misra, S. C. (2024). Evaluation of success factors to implement digitalization in the construction industry. *Construction Innovation*, 24(4), 865–891. <https://doi.org/10.1108/CI-02-2022-0042>
- Bazart, C., & Pickhardt, M. (2011). Fighting Income Tax Evasion with Positive Rewards. *Public Finance Review*, 39(1), 124–149. <https://doi.org/10.1177/1091142110381639>
- Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business & Information Systems Engineering*, 59(6), 381–384. <https://doi.org/10.1007/s12599-017-0505-1>
- Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19(10). <https://aisel.aisnet.org/jais/vol19/iss10/1>
- Beer, R., Ahn, H.-S., & Leider, S. (2018). Can Trustworthiness in a Supply Chain Be Signaled? *Management Science*, 64(9), 3974–3994. <https://doi.org/10.1287/mnsc.2017.2817>

- Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *IEEE Symposium on Security and Privacy*, 459–474.
<https://doi.org/10.1109/SP.2014.36>
- Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems*, 8(4), 211–218.
- Benbasat, I., Gefen, D., & Pavlou, P. A. (2010). Introduction to the Special Issue on Novel Perspectives on Trust in Information Systems. *MIS Quarterly*, 34(2), 367.
<https://doi.org/10.2307/20721432>
- Bencic, F. M., Skocir, P., & Zarko, I. P. (2019). DL-Tags: DLT and Smart Tags for Decentralized, Privacy-Preserving, and Verifiable Supply Chain Management. *IEEE Access*, 7, 46198–46209. <https://doi.org/10.1109/ACCESS.2019.2909170>
- Bengtsson, M., & Kock, S. (2000). "Coopetition" in Business Networks—to Cooperate and Compete Simultaneously. *Industrial Marketing Management*, 29(5), 411–426. [https://doi.org/10.1016/S0019-8501\(99\)00067-X](https://doi.org/10.1016/S0019-8501(99)00067-X)
- Bergh, D. D., Ketchen, D. J., Orlandi, I., Heugens, P. P. M. A. R., & Boyd, B. K. (2019). Information Asymmetry in Management Research: Past Accomplishments and Future Opportunities. *Journal of Management*, 45(1), 122–158.
<https://doi.org/10.1177/0149206318798026>
- Blumer, H. (1954). What is Wrong with Social Theory? *American Sociological Review*, 19(1), 3. <https://doi.org/10.2307/2088165>
- Bossler, L. F., Buchwald, A., & Spohrer, K. (2024). And No One Gets the Short End of the Stick: A Blockchain-Based Approach to Solving the Two-Sided Opportunism Problem in Interorganizational Information Sharing. *Information Systems Research*, Article isre.2022.0065. Advance online publication.
<https://doi.org/10.1287/isre.2022.0065>
- Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio- Technical Perspective. *MIS Quarterly*, 1(3), 17–32. <https://doi.org/10.2307/248710>
- Bowen, G. A. (2006). Grounded Theory and Sensitizing Concepts. *International Journal of Qualitative Methods*, 5(3), 12–23.
<https://doi.org/10.1177/160940690600500304>

- Buettner, T., Holzmann, C., Kreidl, F., & Scholz, H. (2020). Withholding-tax non-compliance: The case of cum-ex stock-market transactions. *International Tax and Public Finance*, 27(6), 1425–1452. <https://doi.org/10.1007/s10797-020-09602-9>
- Buterin, V. (2014). *Ethereum: A Next Generation Smart Contract & Decentralized Application Platform*. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
- Butijn, B.-J., Tamburri, D. A., & van Heuvel, W.-J. den (2021). Blockchains. *ACM Computing Surveys*, 53(3), 1–37. <https://doi.org/10.1145/3369052>
- Cabinakova, J., Ostern, N., & Krönung, J. (2019). Understanding Preprototype User Acceptance of Centralised and Decentralised Identity Management Systems. In *27th European Conference on Information Systems*. https://aisel.aisnet.org/ecis2019_rp/170
- 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)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICTMOD49425.2020.9380598>
- Carvalho, A., & Karimi, M. (2021). Aligning the interests of newsvendors and forecasters through blockchain-based smart contracts and proper scoring rules. *Decision Support Systems*, 151, 113626. <https://doi.org/10.1016/j.dss.2021.113626>
- Catalini, C., & Gans, J. (2016). *Some Simple Economics of the Blockchain*. <https://doi.org/10.3386/w22952>
- Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, 37(1), 39–67. <https://doi.org/10.1177/0149206310388419>
- Connelly, B. L., Certo, S. T., Reutzel, C. R., DesJardine, M. R., & Zhou, Y. S. (2025). Signaling Theory: State of the Theory and Its Future. *Journal of Management*, 51(1), 24–61. <https://doi.org/10.1177/01492063241268459>
- Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*, 29(2), 381–400. <https://doi.org/10.1287/isre.2018.0794>

- Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, 13(1), 3–21.
<https://doi.org/10.1007/BF00988593>
- Corbin, J. M., & Strauss, A. L. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4. ed.). SAGE.
- Crocker, K. J., & Slemrod, J. (2005). Corporate tax evasion with agency costs. *Journal of Public Economics*, 89(9-10), 1593–1610. <https://doi.org/10.1016/j.jpubeco.2004.08.003>
- Davis, F. D. (1985). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results* [Doctoral dissertation, Sloan School of Management, M.I.T.]. BibTeX.
- Demirkesen, S., & Tezel, A. (2021). Investigating major challenges for industry 4.0 adoption among construction companies. *Engineering, Construction and Architectural Management*. Advance online publication.
<https://doi.org/10.1108/ECAM-12-2020-1059>
- Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis Der Wirtschaftsinformatik*, 58(2), 247–270. <https://doi.org/10.1365/s40702-021-00711-5>
- Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review*, 14(1), 57–74.
<https://doi.org/10.5465/amr.1989.4279003>
- Ellinger, E. W., Gregory, R. W., Mini, T., Widjaja, T., & Henfridsson, O. (2024). Skin in the Game: The Transformational Potential of Decentralized Autonomous Organizations. *MIS Quarterly*, 48(1), 245–272. <https://misq.umn.edu/skin-the-the-game-the-transformational-potential-of-decentralized-autonomous-organizations.html>
- Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1), 107–115. <https://doi.org/10.1111/j.1365-2648.2007.04569.x>

- EY. (2021). *What happens when government, industry and investors seek common digital ground? Withholding tax distributed ledger report*.
<https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/services/tax/documents/ey-withholding-tax-distributed-ledger-report.pdfwithholding-tax-distributed-ledger-report.pdf>
- Faccia, A., & Mosteanu, N. R. (2019). Tax Evasion, Information Systems and Blockchain. *Journal of Information Systems & Operations Management*, 65–74.
https://pure.coventry.ac.uk/ws/portalfiles/portal/30808601/JISOM_SU19_A07.pdf
- Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. *The Journal of Law & Economics*, 26(2), 301–325. <http://www.jstor.org/stable/725104>
- Felden, F., Zelt, T., Bauer, P., Siegert, S., Einaste, T., Müller, M., Lume, H., & Hoffmann, T. (2020). *Zehn Jahre elektronischer Personalausweis; Wie Deutschland ein erfolgreiches eID-Ökosystem aufbauen kann*. <https://web-assets.bcg.com/43/c6/6101a4034a958228b6cce70229e8/bcg-zehn-jahre-elektronischer-personalausweis.pdf>
- Fernandez, A.-S., & Chiambaretto, P. (2016). Managing tensions related to information in coopetition. *Industrial Marketing Management*, 53, 66–76.
<https://doi.org/10.1016/j.indmarman.2015.11.010>
- Fisher, G., Mayer, K., & Morris, S. (2021). From the Editors—Phenomenon-Based Theorizing. *Academy of Management Review*, 46(4), 631–639.
<https://doi.org/10.5465/amr.2021.0320>
- Flick, U., Kardorff, E. von, & Steinke, I. (2010). *A companion to qualitative research*. SAGE.
- Franke, T., Attig, C., & Wessel, D. (2019). A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction*, 35(6), 456–467. <https://doi.org/10.1080/10447318.2018.1456150>
- Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, 16(1), 15–31.
<https://doi.org/10.1177/1094428112452151>
- Gleiss, A., Degen, K., & Pousttchi, K. (2023). Identifying the patterns: Towards a systematic approach to digital platform regulation. *Journal of Information Technology*, 38(2), 180–201. <https://doi.org/10.1177/02683962221146803>

- Gnyawali, D. R., & Park, B.-J. R. (2011). Co-opetition between giants: Collaboration with competitors for technological innovation. *Research Policy*.
- Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1), 186–208.
<https://doi.org/10.1137/0218012>
- Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, 37(2), 337–355.
<https://doi.org/10.25300/MISQ/2013/37.2.01>
- Gregor, S., Kruse, L., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, 21, 1622–1652. <https://doi.org/10.17705/1jais.00649>
- Gregory, R. W., & Henfridsson, O. (2021). Bridging Art and Science: Phenomenon-Driven Theorizing. *Journal of the Association for Information Systems*, 22(6), 1509–1523. <https://doi.org/10.17705/1jais.00703>
- Große, N., Möller, F., Schoormann, T., & Henke, M. (2024). Designing trust-enabling blockchain systems for the inter-organizational exchange of capacity. *Decision Support Systems*, 179, 114182. <https://doi.org/10.1016/j.dss.2024.114182>
- Guggenberger, T., Schweizer, A., & Urbach, N. (2020). Improving Interorganizational Information Sharing for Vendor Managed Inventory: Toward a Decentralized Information Hub Using Blockchain Technology. *IEEE Transactions on Engineering Management*, 67(4), 1074–1085.
<https://doi.org/10.1109/TEM.2020.2978628>
- Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depth investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering*, 173, 108716. <https://doi.org/10.1016/j.cie.2022.108716>
- Gulati, R., Wohlgezogen, F., & Zhelyazkov, P. (2012). The Two Facets of Collaboration: Cooperation and Coordination in Strategic Alliances. *Academy of Management Annals*, 6(1), 531–583. <https://doi.org/10.5465/19416520.2012.691646>
- Gurbaxani, V., & Whang, S. (1991). The impact of information systems on organizations and markets. *Communications of the ACM*, 34(1), 59–73.
<https://doi.org/10.1145/99977.99990>

- Hanneke, B., Hinz, O., Pfeiffer, J., & Wil van der Aalst (2024). The Internet of Value: Unleashing the Blockchain's Potential with Tokenization. *Business & Information Systems Engineering*, 66(4), 411–419.
<https://aisel.aisnet.org/bise/vol66/iss4/1>
- Hassan, A., Makhdoom, I., Iqbal, W., Ahmad, A., & Raza, A. (2023). From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *Journal of Network and Computer Applications*, 217, 103672.
<https://doi.org/10.1016/j.jnca.2023.103672>
- Hesse-Biber, S. N., & Johnson, R. B. (2015). *The Oxford handbook of multimethod and mixed methods research inquiry*. Oxford library of psychology. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199933624.001.0001>
- Hevner, March, Park, & Ram (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75. <https://doi.org/10.2307/25148625>
- Hevner, A. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1017&context=sjis>
- Hoess, A., Lautenschlager, J., Sedlmeir, J., Fridgen, G., Schlatt, V., & Urbach, N. (2025). Toward Seamless Mobility-as-a-Service. *Business & Information Systems Engineering*, 67(2), 149–170. <https://doi.org/10.1007/s12599-024-00856-9>
- Hoffmann, W., Lavie, D., Reuer, J. J., & Shipilov, A. (2018). The interplay of competition and cooperation. *Strategic Management Journal*, 39(12), 3033–3052.
<https://doi.org/10.1002/smj.2965>
- Holldack, F., Banh, L., & Strobel, G. (2026). Agentic information systems. *Electronic Markets*, 36(1). <https://doi.org/10.1007/s12525-025-00861-0>
- Hyvärinen, H., Risius, M., & Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. *Business & Information Systems Engineering*, 59(6), 441–456. <https://doi.org/10.1007/s12599-017-0502-4>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)

- Jussen, I., Möller, F., Schweihoff, J., Gieß, A., Giussani, G., & Otto, B. (2024). Issues in inter-organizational data sharing: Findings from practice and research challenges. *Data & Knowledge Engineering*, 150, 102280.
<https://doi.org/10.1016/j.datak.2024.102280>
- Kaplan, B., & Maxwell, J. A. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. In *Evaluating the Organizational Impact of Healthcare Information Systems* (pp. 30–55). Springer, New York, NY.
https://doi.org/10.1007/o-387-30329-4_2
- Keen, M., & Slemrod, J. (2017). Optimal tax administration. *Journal of Public Economics*, 152, 133–142. <https://doi.org/10.1016/j.jpubeco.2017.04.006>
- Kim, M., & Kim, Y.-W. (2024). Applications of blockchain for construction project procurement. *Automation in Construction*, 165, 105550.
- Krogh, G. von, Rossi-Lamastra, C., & Haeffliger, S. (2012). Phenomenon-based Research in Management and Organisation Science: When is it Rigorous and Does it Matter? *Long Range Planning*, 45(4), 277–298.
<https://doi.org/10.1016/j.lrp.2012.05.001>
- Kruchten, P. B. (1995). The 4+1 View Model of architecture. *IEEE Software*, 12(6), 42–50. <https://doi.org/10.1109/52.469759>
- Lacity, M., & van Hoek, R. (2021). *What We've Learned So Far About Blockchain for Business: The biggest challenge to companies creating blockchain apps isn't the technology — it's successfully collaborating with ecosystem partners*. MIT Sloan Management Review. <https://sloanreview.mit.edu/article/what-weve-learned-so-far-about-blockchain-for-business/?og=Home+Tiled>
- Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, 102, 288–307.
<https://doi.org/10.1016/j.autcon.2019.02.005>
- Loertscher, S., & Marx, L. M. (2020). Digital monopolies: Privacy protection or price regulation? *International Journal of Industrial Organization*, 71, 102623.
<https://doi.org/10.1016/j.ijindorg.2020.102623>
- Mahoney, P. G. (1995). Mandatory Disclosure as a Solution to Agency Problems. *The University of Chicago Law Review*, 62(3), 1047.
<https://doi.org/10.2307/1600055>

- Mayring, P. (2014). *Qualitative content analysis: Theoretical foundation, basic procedures and software solution*. <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173>
- McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, 2(2), 1–25. <https://doi.org/10.1145/1985347.1985353>
- Mishra, R. A., Kalla, A., an Braeken, & Liyanage, M. (2021). Privacy Protected Blockchain Based Architecture and Implementation for Sharing of Students' Credentials. *Information Processing & Management*, 58(3), 102512. <https://doi.org/10.1016/j.ipm.2021.102512>
- Mishunin, D. (2024, January 8). Why Blockchain Falls Short In Supply Chain Management: Here's Why. *Forbes*. <https://www.forbes.com/councils/forbestech-council/2024/01/08/why-blockchain-falls-short-in-supply-chain-management-heres-why/>
- Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J. C., Gelhaar, J., Guggenberger, T., & Otto, B. (2024). Industrial data ecosystems and data spaces. *Electronic Markets*, 34(1). <https://doi.org/10.1007/s12525-024-00724-0>
- Möller, F., Legner, C., Strobel, G., Schoormann, T., Cappiello, C., Loscio, B., & Otto, B. (2025). Data ecosystems in IS research: The road so far, where we are now, and the road ahead. *Electronic Markets*, 35(1). <https://doi.org/10.1007/s12525-025-00860-1>
- Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80–86. <https://doi.org/10.1016/j.cosrev.2018.10.002>
- Nakamoto, S. (2008). *Bitcoin: A Peer-toPeer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>
- Nalebuff, B. J., & Brandenburger, A. M. (1997). Co-opetition: Competitive and cooperative business strategies for the digital economy. *Strategy & Leadership*, 25(6), 28–33. <https://doi.org/10.1108/eb054655>
- Nodehi, T., Zutshi, A., Grilo, A., & Rizvanovic, B. (2022). EBDF: The enterprise blockchain design framework and its application to an e-Procurement ecosystem. *Computers & Industrial Engineering*, 171, 108360.

- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183–187.
<https://doi.org/10.1007/s12599-017-0467-3>
- Pavlou, Liang, & Xue (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, 31(1), 105. <https://doi.org/10.2307/25148783>
- Pedersen, A., Risius, M., & Beck, R. (2019). A Ten-Step Decision Path to Determine When to Use Blockchain Technologies. *MISQE (MIS Quarterly Executive)*, 99–115. <https://doi.org/10.17705/2msqe.00010>
- Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–77.
<https://doi.org/10.2753/MIS0742-1222240302>
- Pickhardt, M., & Prinz, A. (2014). Behavioral dynamics of tax evasion – A survey. *Journal of Economic Psychology*, 40, 1–19.
<https://doi.org/10.1016/j.joep.2013.08.006>
- Prebanić, K. R., & Vukomanović, M. (2021). Realizing the Need for Digital Transformation of Stakeholder Management: A Systematic Review in the Construction Industry. *Sustainability*, 13(22), 12690. <https://doi.org/10.3390/su132212690>
- Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity Decentralized digital identity and verifiable credentials* (11th ed.). Manning Publications.
- Principato, M., Babel, M., Guggenberger, T., Kropp, J., & Mertel, S. (2023). Towards Solving the Blockchain Trilemma: An Exploration of Zero-Knowledge Proofs. *ICIS 2023 Proceedings*. <https://aisel.aisnet.org/icis2023/blockchain/blockchain/5>
- Rederer, T., Eickmeyer, R., Bieber, N., Knierim, M., Schnepf, S., Pagel, D., & Störk, S. (2021). *Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche*. PWC. <https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.pdf>
- Reinganum, J. F., & Wilde, L. L. (1985). Income tax compliance in a principal-agent framework. *Journal of Public Economics*, 26(1), 1–18.
[https://doi.org/10.1016/0047-2727\(85\)90035-0](https://doi.org/10.1016/0047-2727(85)90035-0)

- Richter, D., & Anke, J. (2026). Self-sovereign identity: A conceptual framework and research agenda. *Electronic Markets*, 36(1). <https://doi.org/10.1007/s12525-025-00867-8>
- Rieger, A., Roth, T., Sedlmeir, J., Weigl, L., & Fridgen, G. (2022). Not yet another digital identity. *Nature Human Behaviour*, 6(1), 3. <https://doi.org/10.1038/s41562-021-01243-0>
- Riley, J. G. (2001). Silver Signals: Twenty-Five Years of Screening and Signaling. *Journal of Economic Literature*, 39(2), 432–478. <https://doi.org/10.1257/jel.39.2.432>
- Ross, S. A. (1973). The economic theory of agency: The principal's problem. *The American Economic Review*(Vol. 63, No. 2), 134–139. https://www.jstor.org/stable/1817064?casa_token=p5esh65xarkaaaaa:spnk-wyr9ppbgh-xklhukbgkykvqpkdxvblbs5gr4hiqe4qdpzuspetybo4rrvhx6l5g8zavu-zrfxnwi675snideldd3sqciaaa7f-jrz3oeremncbpb
- Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). "Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda". *Journal of the Association for Information Systems*, 1388–1403. <https://doi.org/10.17705/1jais.00571>
- Saldaña, J. (2013). *The coding manual for qualitative researchers* (2. ed.). SAGE Publ.
- Samuelson, O., & Björk, B.-C. (2014). A longitudinal study of the adoption of IT technology in the Swedish building sector. *Automation in Construction*, 37, 182–190. <https://doi.org/10.1016/j.autcon.2013.10.006>
- Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. *ECIS 2022 Research Papers*. https://aisel.aisnet.org/ecis2022_rp/46
- Schellinger, B., Völter, F., Urbach, N., & Sedlmeir, J. (2022). *Yes, I Do: Marrying Blockchain Applications with GDPR*. <https://scholarspace.manoa.hawaii.edu/items/3d1ceb5b-6d4f-4839-8768-74e10cbdf742>
- Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information & Management*, 103553. <https://doi.org/10.1016/j.im.2021.103553>

- Schubert, B. (2021, October 21). CumEx Files 2.0: How did we calculate €150 billion in tax loss? *Correctiv.Org*. <https://correctiv.org/en/latest-stories/cumex-files-en/2021/10/21/cumex-files-2-0-how-did-we-calculate-e150-billion-in-tax-loss/?lang=en>
- Schweihoff, J., Lipovetskaja, A., Jussen-Lengersdorf, I., & Möller, F. (2024). Stuck in the middle with you: Conceptualizing data intermediaries and data intermediation services. *Electronic Markets*, 34(1). <https://doi.org/10.1007/s12525-024-00729-9>
- Schwiderowski, J., Pedersen, A., & Beck, R. (2024). Crypto Tokens and Token Systems. *Information Systems Frontiers*, 26(1), 319–332. <https://doi.org/10.1007/s10796-023-10382-w>
- Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*. Advance online publication. <https://doi.org/10.1007/s12525-022-00536-0>
- Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63(5), 603–613. <https://doi.org/10.1007/s12599-021-00722-y>
- Sonnenberg, C., & vom Brocke, J. (2012). Evaluation Patterns for Design Science Research Artefacts. In M. Helfert & B. Donnellan (Eds.), *Communications in Computer and Information Science. Practical Aspects of Design Science* (Vol. 286, pp. 71–83). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-33681-2_7
- Spence, M. (1973). Job Market Signaling. *The Quarterly Journal of Economics*, 87(3), 355. <https://doi.org/10.2307/1882010>
- Spengel, C. (2021a). Estimation of Fraudulent Tax Reclaims Caused by Cum/Ex - ADR Transactions. https://www.bwl.uni-mannheim.de/media/Lehrstuehle/bwl/Spengel/Dokumente/Medien/Steuerschaden_Cum-Ex-ADR_Okt2021.pdf
- Spengel, C. (2021b). Estimation of the Tax Revenue Loss Caused by Cum/Cum Transactions. https://www.bwl.uni-mannheim.de/media/Lehrstuehle/bwl/Spengel/Dokumente/Medien/Steuerschaden_Cum-Cum_update.pdf
- Steigenberger, N. (2024). Deceptive signalling: Causes, consequences and remedies. *International Journal of Management Reviews*, 27(2), 283–305. <https://doi.org/10.1111/ijmr.12392>

- Sternberg, H. S., Hofmann, E., & Roeck, D. (2021). The Struggle is Real: Insights from a Supply Chain Blockchain Case. *Journal of Business Logistics*, 42(1), 71–87. <https://doi.org/10.1111/jbl.12240>
- Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary —Digital Infrastructures: The Missing IS Research Agenda. *Information Systems Research*, 21(4), 748–759. <https://doi.org/10.1287/isre.1100.0318>
- Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. *Supply Chain Management: An International Journal*, 23(6), 545–559. <https://doi.org/10.1108/SCM-01-2018-0029>
- Tuunanen, T., Winter, R., & vom Brocke, J. (2024). Dealing with Complexity in Design Science Research: A Methodology Using Design Echelons. *MIS Quarterly*, 48(2), 427–458. <https://doi.org/10.25300/MISQ/2023/16700>
- Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), 77–89. <https://doi.org/10.1057/ejis.2014.36>
- Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46(2), 186–204. <https://doi.org/10.1287/mnsc.46.2.186.11926>
- Vogelsang, K., Steinhueser, M., & Hoppe, U. (2013). A Qualitative Approach to Examine Technology Acceptance. In *ICIS 2013 Proceedings*.
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*. https://misq.umn.edu/misq/article-pdf/26/2/xiii/4948/ob_guested.pdf
- Wiehager, S. (2021). Datenqualität und Datenmanagement in der Bauwirtschaft. In C. Hofstadler & C. Motzko (Eds.), *Agile Digitalisierung im Baubetrieb* (pp. 79–106). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34107-7_3
- Wu, P. F. (2012). A Mixed Methods Approach to Technology Acceptance Research. *Journal of the Association for Information Systems*, 12(4), 299–322.
- Wüst, K., & Gervais, A. (2018). Do you Need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45–54). IEEE. <https://doi.org/10.1109/CVCBT.2018.00011>

-
- Yang, J., Lee, D., Baek, C., Park, C., & Lan, B. Q. (2022). Leveraging Blockchain for Scaffolding Work Management in Construction. *IEEE Access*, 10, 39220–39238. <https://doi.org/10.1109/ACCESS.2022.3165614>
- Yent, K. (2020). *Applying Blockchain Technology to Cross-Border Tax Reporting*. <https://doi.org/10.2139/ssrn.3910741>

Appendices

Appendix A: Declarations of Co-Authorship and the Individual Contributions

RP 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management

This RP was co-authored by Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, and Nils Urbach. The co-authors contributed as follows:

Jonathan Lautenschlager (lead author): Jonathan Lautenschlager initiated and conceptualized the research project. He conducted literature work, developed artifacts, constructs, models, and methodologies, and carried out the evaluation through interviews. He also contributed significantly to the paper's textual elaboration and actively participated in the revision process during peer review. Thus, Jonathan's co-authorship is reflected as lead author across all phases of the research project.

Jan Stramm (co-author): Jan Stramm contributed to the research project through literature review, artifact, construct, model, and methodology development, and textual elaboration. He contributed in a supporting co-author role.

Tobias Guggenberger (co-author): Tobias Guggenberger supervised the research project and provided scientific mentorship. He contributed to the development of artifacts, constructs, models, and methodologies and offered feedback and support during manuscript preparation. He contributed in a supporting co-author role.

Nils Urbach (co-author): Nils Urbach supervised the research project and provided scientific mentorship. He contributed to the development of artifacts and methodologies and offered feedback and support during manuscript preparation. He contributed in a supporting co-author role.

RP 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry

This RP was co-authored by Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, André Schweizer, and Artur Rösch. Their contributions are summarized as follows:

Jonathan Lautenschlager (co-author): Jonathan Lautenschlager initiated and co-conceptualized the research project. He contributed to the literature review, the development of design objectives, artifacts, and methodology, and conducted expert interviews. He also participated in manuscript writing and revision during peer review.

Jan Stramm (co-author): Jan Stramm co-developed the research project and contributed to the literature review, development of design objectives, artifact, constructs, and methodology. He also participated in interpreting findings, manuscript writing, and revision.

Tobias Guggenberger (co-author): Tobias Guggenberger co-developed and supervised the project, providing scientific guidance. He contributed to the theoretical and methodological framing, development of design objectives and artifact, interpretation of findings, and manuscript revision.

Andre Schweizer (co-author): Andre Schweizer co-developed the project and contributed practical and technical expertise. He was involved in specifying requirements, developing and evaluating the IT artifact, interpreting findings, and supporting manuscript revision.

Artur Roesch (co-author): Artur Roesch initiated and co-developed the project, contributing to the practical conceptualization of the research problem and the design, development, and testing of the IT artifact. He also participated in expert interviews and the interpretation of results.

RP 3: Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy

This RP was co-authored by Valeriya Arnold, Tobias Guggenberger, Jan Stramm, and Nils Urbach. Their contributions are summarized as follows:

Valeriya Arnold (co-author): Valeriya Arnold initiated and co-developed the research project. She contributed to the literature review, the paper's theoretical foundations, the derivation of the problem statement and design objectives, and the design, development, and testing of the IT artifact. She also participated in conducting and analyzing the expert interviews, evaluating the artifact, developing the theoretical contributions, and writing and revising the manuscript.

Tobias Guggenberger (co-author): Tobias Guggenberger co-developed the research project and contributed to its theoretical and methodological framing. He participated in research discussions, co-shaped the paper's content and structure, and contributed to developing the design objectives, IT artifact, and resulting design principles. He also engaged in interpreting the findings, formulating the theoretical contributions, and revising the manuscript.

Jan Stramm (co-author): Jan Stramm co-developed the research project and contributed to the literature review, derivation of the problem statement and design objectives, and design and evaluation of the IT artifact. He participated in research discussions, co-shaped the paper's content and structure, and contributed to analyzing the expert interviews and developing the resulting design principles. He also engaged in formulating the theoretical contributions and writing and revising the manuscript.

Nils Urbach (co-author): Nils Urbach supervised and co-developed the research project and provided scientific guidance. He contributed to the theoretical and methodological framing of the study, participated in research discussions, and supported the development of the design objectives and theoretical contributions. He also provided feedback on the paper's content and structure and contributed to manuscript writing and revision.

RP 4: From Documents to Verifiable Credentials: How Digital Signal-Carriers Reconfigure Decision-Making in Buyer–Supplier Relationship Formation

This RP was co-authored by Jan Stramm, Tobias Guggenberger, Jonathan Lautenschlager, and Nils Urbach. The co-authors contributed as follows:

Jan Stramm (lead author): Jan Stramm initiated and conceptualized the research project. He developed the paper's theoretical foundations and qualitative research design, conducted and analyzed the expert interviews, and integrated complementary observational and archival data. He also led the development of the digital signal-carrier construct, the dual-layer explanatory mechanism, and the paper's theoretical contributions. Furthermore, he engaged in most of the manuscript writing and participated actively in the revision process. Thus, Jan's co-authorship is reflected as lead author across all phases of the research project.

Tobias Guggenberger (co-author): Tobias Guggenberger co-developed the research project and contributed to its theoretical and methodological framing. He participated in regular research discussions, supported the interpretation of the empirical findings, and contributed to developing the digital signal-carrier construct and the resulting theoretical contributions. He also provided feedback on the paper's content and structure and participated in manuscript writing and revision. He contributed in a supporting co-author role.

Jonathan Lautenschlager (co-author): Jonathan Lautenschlager co-developed the research project and contributed to the paper's theoretical foundations, content, and structure. He participated in regular research discussions, supported the interpretation and refinement of the findings, and contributed to developing the paper's theoretical contributions. He also engaged in manuscript writing and revision, particularly regarding the theoretical framing and presentation of the study's contributions. He contributed in a supporting co-author role.

Nils Urbach (co-author): Nils Urbach supervised the research project and provided scientific mentorship. He participated in research discussions, contributed to the theoretical positioning of the study, and provided feedback on the paper's content and structure. He also supported the formulation of the theoretical contributions and engaged in manuscript revision. He contributed in a supporting co-author role.

RP 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control

This RP was co-authored by Vincent Schaaf, Jan Stramm, Tobias Guggenberger, Marc-Fabian Körner, and Nils Urbach. Their contributions are summarized as follows:

Vincent Schaaf (co-author): Vincent Schaaf initiated and co-developed the research project. He contributed to the theoretical foundations, problem analysis, and methodological approach. He also participated in deriving the meta-requirements and design objectives, developing and refining the artifact, conducting and analyzing the six interdisciplinary consortium working sessions, and formulating the resulting design principles. Furthermore, he contributed to manuscript writing and revision.

Jan Stramm (co-author): Jan Stramm co-developed the research project and contributed to the theoretical framing and methodological design. He participated in deriving the meta-requirements and design objectives, refining the blockchain-based artifact, and analyzing the working sessions and interviews. He led the analytical feasibility assessment, development of the design principles and theoretical contributions, and writing and revising the manuscript.

Tobias Guggenberger (co-author): Tobias Guggenberger initiated and co-developed the research project and contributed to its theoretical framing. He participated in research discussions and supported the derivation of the meta-requirements, artifact, and design principles. He also contributed to interpreting the feasibility assessment results, developing the theoretical contributions, and revising the manuscript.

Marc-Fabian Körner (co-author): Marc-Fabian Körner co-developed the research project. He participated in developing the paper's theoretical foundations, analyzing the practical problem, and deriving the meta-requirements and design objectives. He also supported the design and evaluation of the artifact, the interpretation of the findings, and the textual elaboration and revision of the manuscript.

Nils Urbach (co-author): Nils Urbach supervised and co-developed the research project and provided scientific guidance. He contributed to the theoretical framing, participated in research discussions, and supported the development design principles, and theoretical contributions. He also provided feedback on the paper's content and structure and contributed to manuscript writing and revision.

RP 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications

This RP was co-authored by Tobias Guggenberger, Lena Neubauer, Jan Stramm, Fabiane Völter, and Till Zwede. The authors contributed as follows:

Tobias Guggenberger (co-author): Tobias Guggenberger initiated and co-developed the research project. He participated in regular research discussions and contributed to the paper's theoretical framing, research design, content, and structure. In particular, he supported the integration of technology acceptance research with the SSI context and contributed to the interpretation and conceptualization of the identified acceptance factors. He also contributed to the textual elaboration and revision of the manuscript.

Lena Neubauer (co-author): Lena Neubauer initiated and co-developed the research project. She contributed to the development of the research question, the TAM2-informed qualitative research design, and the interview approach based on the SSI demonstrator. She participated in the collection and analysis of the empirical data and contributed to the deductive and inductive development of the acceptance categories, the resulting model, and the corresponding hypotheses. She further engaged in the textual elaboration of the introduction, theoretical background, methodology, results, discussion, and conclusion.

Jan Stramm (co-author): Jan Stramm participated in regular research discussions and contributed to connecting the technological foundations of SSI and VCs with the paper's acceptance-oriented research perspective. He supported the development of the research design, the interpretation of the empirical findings, and the formulation of the extended acceptance model and its implications. He also contributed to the textual elaboration and revision of the manuscript.

Fabiane Völter (co-author): Fabiane Völter co-developed the research project. She participated in regular research discussions and contributed to the paper's theoretical foundations, analysis, and conceptual development. In particular, she supported the interpretation of the identified acceptance factors and the derivation of the relationships and hypotheses. She also contributed to the textual elaboration and revision of the manuscript.

Till Zwede (co-author): Till Zwede participated in regular research discussions and contributed to the development of the paper's theoretical foundations, methodological approach, content, and structure. He supported the qualitative analysis and interpretation of the interview material, as well as the development of the acceptance categories, the model, and the corresponding hypotheses. He also contributed to the textual elaboration and revision of the manuscript.

Appendix B: Other Publications by the Author

Authors	Title	Publication outlet and year
Vincent Gramlich, Marc Principato, Benjamin Schellinger, Johannes Sedlmeir, Jan Stramm , Julia Amend, Till Zwede, Prof. Dr. Jens Strüker, and Prof. Dr. Nils Urbach	Decentralized Finance (DeFi) Foundations, Applications, Potentials, and Challenges	Fraunhofer FIT Whitepaper (2022)
Timo Grüneke, Tobias Guggenberger, Jakob Nusser, Anna Maria Oberländer, Jan Stramm , Alexander Varrentrapp	Unlocking AI-based Knowledge Management Potential for SMEs: Exploring Semantic Search Adoption	Published: 19th International Conference on Wirtschaftsinformatik at Würzburg University (2024) (VHB-JQ4: B)
Jan Stramm , Jonathan Lautenschlager, Lars Keppler	Blockchain Technology	Book chapter in: Decentralized Technologies – Financial Sector in Change (2024)
Timo Grüneke, Tobias Guggenberger, Kristina Hall, Tiana Langer, Simon Meierhöfer, Anna Maria Oberländer, Maximilian Röglinger, Jan Stramm , Nils Urbach, Jana Wozar	Einsatz- und Akzeptanzanalyse von KI-basierten Wissenszugängen in KMU am Beispiel einer semantischen Suche	Universität Bayreuth Whitepaper (2025)
Carolin Jung, Jonathan Lautenschlager, Jan Stramm , Tobias Guggenberger, Nils Urbach	Ein Monetarisierungskonzept für digitale Identitäten: Strategien und Ansätze für einen nachhaltigen volkswirtschaftlichen Nutzen	Fraunhofer FIT Whitepaper (2025)
Martina Block, Coco Marie Görlich, Jonathan Lautenschlager, Valentin Mayer, Jan Stramm , Nils Urbach, Janine Wendt, Domenik Wendt	AI literacy requirements according to Art. 4 AI Act Legal analysis and practical measures	HessianAI Whitepaper (2025)
Timo Grüneke, Jan Stramm , Tobias Guggenberger, Anna Maria Oberländer	Asking the Machine: A Literature Review and Research Agenda on Semantic Search	Revised and Resubmitted IEEE Access (2026) (VHB-JQ4: B)

Table 3: Overview of other publications by the author

Research Paper 1: Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management

Authors

Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, Nils Urbach

Publication Status

This Research Paper is published as: Lautenschlager, Jonathan; Stramm, Jan; Guggenberger, Tobias; and Urbach, Nils, "Striking a Balance: Designing a Blockchain-Based Solution to Navigate Coopetition Dynamics in Supply Chain Management" (2025). *Electronic Markets*, 35, 70. <https://doi.org/10.1007/s12525-025-00809-4>

Extended Abstract

Digital supply chains increasingly depend on interorganizational information sharing to coordinate processes, automate transactions, and improve traceability. At the same time, participating organizations often remain competitors and therefore seek to protect commercially sensitive information. This simultaneous cooperation and competition, referred to as coopetition, creates a central design tension for interorganizational information systems. Blockchain technology can support shared and tamper-evident process infrastructures without a single intermediary, but its transparency may conflict with confidentiality requirements in competitive business networks. Against this background, the study investigates: *How to design a blockchain-based information system to facilitate coopetition in supply networks by fostering cooperative interactions while ensuring data confidentiality?*

The study follows a design science research approach and uses digital delivery-invoice processing in the construction industry as its unit of analysis. Construction supply chains comprise fragmented and frequently changing networks of organizations that must cooperate on individual projects while maintaining competitive autonomy. A systematic literature review results in 23 academic publications, which are analyzed through open, axial, and selective coding. Coopetition theory provides the theoretical lens for interpreting the cooperation–competition tension. Based on the resulting

requirements, a conceptual blockchain architecture and prototype are developed and represented through a 4+1 architectural view model. The artifact is subsequently evaluated through nine qualitative ex-post interviews with experts in distributed technologies and the construction industry.

The study derives eight design objectives for blockchain-based information systems in coopetitive supply networks: data protection, accountability, decentralization, performance, interoperability, traceability, transparency, and automation. These objectives demonstrate that decentralized supply-chain infrastructures should not maximize transparency indiscriminately but enable shared process execution and verification while differentiating information access according to organizational roles and confidentiality requirements. The resulting architecture uses Hyperledger Fabric and combines identity management, endorsement policies, channels, and private data collections. These mechanisms establish a shared and traceable process state while restricting sensitive business information to authorized participants. Applied to digital delivery-invoice processing, the artifact illustrates how common validation and automation can be combined with differentiated information access. Reflection on the artifact and its evaluation yields three implementation guidelines. First, decentralized solutions should be adopted when the benefits of network effects in a coopetitive market outweigh their additional implementation complexity. Second, private data collections and channels should protect interorganizational information from unauthorized access. Third, these mechanisms should be complemented by additional privacy-preserving technologies where stronger confidentiality is required.

The study contributes prescriptive design knowledge by integrating coopetition theory with blockchain-based system design. It shows that confidentiality should not be treated as an external restriction on an otherwise transparent blockchain architecture but as a fundamental design requirement shaping the allocation of validation, visibility, and control. The proposed design knowledge is bounded by the construction industry context and expert-based evaluation. Further research should examine its transferability to other industries, implementation at scale, long-term governance, and trade-offs introduced by stronger privacy-preserving mechanisms.

Keywords: Coopetition, Blockchain Technology, Data Transparency, Delivery Invoices, Construction Industry, Supply Chain Automation

Research Paper 2: Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry

Authors

Jonathan Lautenschlager, Jan Stramm, Tobias Guggenberger, André Schweizer, and Artur Rösch

Publication Status

This Research Paper is published as: Lautenschlager, Jonathan; Stramm, Jan; Guggenberger, Tobias; Rösch, Artur; and Schweizer, André, "Overcoming the Data Transparency Trade-Off: Designing a Blockchain-Based Delivery Invoice System for the Construction Industry" (2023). *Wirtschaftsinformatik 2023 Proceedings*. 78. <https://aisel.aisnet.org/wi2023/78>

Extended Abstract

Construction supply chains involve numerous organizations that must exchange information to coordinate deliveries, payments, and related planning activities. Delivery invoices are particularly relevant because they are still frequently handled through paper-based or fragmented digital solutions, resulting in manual processing, media discontinuities, and limited automation. Existing digital solutions can improve this process but often depend on centralized providers and have not achieved broad adoption. Blockchain technology offers an alternative shared infrastructure with enhanced traceability and automation. At the same time, its transparency creates a conflict in cooperative supply chains because firms need to exchange information while protecting sensitive business data from competitors. The study therefore asks: *How can blockchain technology help to digitize the process of handling delivery invoices in the construction industry supply chain while addressing the challenges associated with the coopetition trade-off?*

The study follows a design science research approach to design, develop, and evaluate a decentralized delivery-invoice system. Embedded in a consortium project involving construction-industry and technology partners, the research incorporates practical requirements throughout prototype development. Literature analysis and project workshops inform three overarching design objectives. Secure data exchange requires

confidentiality, integrity, availability, and authenticity. Collaboration concerns integrating heterogeneous supply-chain participants and their systems into a common infrastructure for joint process execution. Competition captures the need to prevent commercially sensitive information from becoming accessible to unauthorized actors. The prototype is evaluated through nine ex-post interviews with experts from construction and decentralized technologies. The architecture consists of frontend, backend, and blockchain layers and uses Hyperledger Fabric as its permissioned blockchain infrastructure. An identity provider establishes organizational roles and access rights, while channels, endorsement policies, and private data collections restrict confidential information. The prototype supports key activities of digital delivery-invoice processing, including creation, transfer, acceptance or rejection, commenting, and status tracking. It thereby establishes a consistent and traceable process state across organizations without making every transaction detail visible to the entire network.

The evaluation yields three design principles. First, organizations should assess whether the network effects and coordination benefits of a decentralized infrastructure justify its additional complexity and operating costs compared with simpler alternatives. Second, private channels and private data collections should restrict sensitive interorganizational information to authorized participants. Third, these mechanisms should be supplemented with additional privacy-preserving technologies where stronger protection is required.

The study contributes process-specific design knowledge for decentralized interorganizational information systems. It demonstrates that blockchain-enabled transparency and automation do not require unrestricted information disclosure. Instead, the data-transparency trade-off can be addressed by differentiating information access while maintaining a shared and verifiable process infrastructure. The findings provide guidance for assessing blockchain-based delivery-invoice solutions and configuring confidentiality mechanisms. The study is limited by its construction-industry focus and the competition-related data-transparency challenge. Scalability, long-term governance, and performance in large-scale operational deployments require further investigation.

Keywords: Blockchain Technology, Data Transparency, Delivery Invoices, Construction Industry, Supply Chain Management

Research Paper 3: Designing a Blockchain-Based Information System for Pro- curement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy

Authors

Valeriya Arnold, Tobias Guggenberger, Jan Stramm, Nils Urbach

Publication Status

This Research Paper is published as: Arnold, Valeriya; Guggenberger, Tobias; Stramm, Jan; and Urbach, Nils, "Designing a Blockchain-Based Information System for Procurement Processes—Balancing Decentralization, Scalability, and Security while Maintaining Privacy" (2026). Information Systems, 140, 102723. <https://doi.org/10.1016/j.is.2026.102723>

Extended Abstract

Procurement processes require continuous information exchange across organizational boundaries but often remain fragmented across heterogeneous information systems, resulting in media discontinuities, manual reconciliation, limited transparency, and trust deficits. Blockchain technology offers a shared, tamper-evident infrastructure but introduces architectural trade-offs. The traditional blockchain trilemma captures tensions between decentralization, scalability, and security; in procurement, privacy constitutes an additional requirement because transaction data such as prices and contractual terms are commercially sensitive. Existing applications often address privacy and scalability through permissioned architectures, thereby reintroducing centralized control and limiting open verifiability. The study therefore asks: *How to design a blockchain-based information system for procurement processes that balances decentralization, scalability, and security while maintaining privacy?*

Following a design science research approach, the study develops and evaluates a blockchain-based procurement information system. A structured literature review establishes the problem statement and initial design objectives, which are refined through expert feedback. The resulting five objectives address integration with interoperable blockchain infrastructure, reliable payment and settlement, decentralized trust and dispute resolution, scalability, and privacy while preserving auditability.

Guided by these objectives, a prototype is developed iteratively and evaluated through technical verification, quantitative assessment, formative feedback, and 16 semi-structured expert interviews.

The architecture addresses the extended blockchain trilemma by allocating requirements to complementary infrastructural layers. A public permissionless Layer 1 serves as the trust anchor, providing consensus, security, tamper resistance, and public verifiability. A privacy-preserving Layer 2 enables scalable and confidential procurement transactions. Zero-knowledge proofs allow relevant computations and state transitions to be verified without disclosing commercially sensitive information, while decentralized inter-layer communication reduces the risk of introducing new centralized control points. The artifact thus demonstrates how responsibilities can be distributed across layers to balance decentralization, scalability, security, and privacy.

The evaluation supports the technical feasibility of this layered approach while identifying boundary conditions concerning Layer 2 maturity, efficient and resilient cryptographic mechanisms, and centralized control structures. Reflection on the build–evaluate cycles yields two design principles. First, blockchain-based information systems should combine a public blockchain as trust anchor with a scaling layer and decentralized inter-layer communication to balance decentralization, scalability, and security. Second, privacy should be preserved through efficient and resilient cryptographic mechanisms while minimizing additional control points.

The study contributes prescriptive design knowledge by extending the blockchain trilemma to incorporate privacy and showing how the resulting tensions can be addressed through architectural allocation. Confidentiality and scalability do not necessarily require abandoning public permissionless infrastructures; open verifiability and decentralized trust can be combined with private execution when requirements are assigned to appropriate layers. The findings remain bounded by the prototype setting and technological maturity of the evaluated architecture. Further research should assess larger operational workloads, evolving Layer 2 technologies, and long-term organizational and governance conditions.

Keywords: Blockchain, Procurement, Blockchain Trilemma, Privacy, Design Science Research, Zero Knowledge Proofs

Research Paper 4: From Documents to Verifiable Credentials: How Digital Signal- Carriers Reconfigure Decision-Making in Buyer–Supplier Re- lationship Formation

Authors

Jan Stramm, Tobias Guggenberger, Jonathan Lautenschlager, Nils Urbach

Publication Status

At the time of submitting this thesis, the corresponding essay is in an advanced status within a peer review process for potential publication in an academic journal.

Extended Abstract

Buyers frequently face information asymmetries when selecting suppliers because characteristics such as capabilities, compliance, or operational quality cannot be directly observed before contracting. Signaling theory explains how suppliers can reduce this uncertainty through costly signals that differentiate high-quality from low-quality actors. In digitally mediated environments, however, such signals are increasingly transmitted through documents, platforms, and other artifacts whose integrity cannot be assumed. Certificates or audit reports can be copied or manipulated while retaining the appearance of legitimate evidence. Existing signaling theory has primarily examined signal properties and content while largely treating the transmission medium as neutral. The study therefore asks: *How can verifiable credentials function as digital signal-carriers during pre-contractual decision-making in buyer–supplier relationship formation?*

The study adopts a phenomenon-based theorizing approach to examine how verifiable credentials (VCs) reshape supplier signaling. The empirical analysis draws on 17 semi-structured expert interviews, complemented by observational and archival material from self-sovereign identity initiatives and implementation contexts. Signaling theory serves as a sensitizing lens while iterative analysis develops concepts and mechanisms from the empirical material.

The findings conceptualize the digital signal-carrier as an analytical construct distinct from both signal content and issuer reputation. The resulting process model comprises three interrelated dimensions: verifiable signal-carrier infrastructure, digital signal

credibilization, and digital signal-informed selection. Together, these explain how VCs preserve the provenance, integrity, and validity of supplier-related claims and integrate verification into decision-making.

Credible digital signaling depends on a dual-layer mechanism. The first layer, technical signal-carrier verification, establishes whether a credential is authentic, unaltered, current, and issued by the claimed source, allowing invalid credentials to be identified before they influence supplier selection. The second layer, signal-information evaluation, determines whether the technically valid credential provides meaningful evidence for the focal decision by considering issuer credibility, the relevance of the attested attribute, and its implications for supplier quality. Cryptographic validity alone is therefore insufficient; credible signaling requires both verifiable transmission and meaningful institutional interpretation.

These mechanisms also alter the temporal structure of signaling. In conventional document-based processes, deceptive signals may only be exposed after contracting through audits, disputes, or operational failures. VC-based verification enables invalid signals to be excluded during pre-selection, shifting part of the control mechanism from ex-post detection toward pre-selection disqualification and reducing the potential payoff from deception.

The study extends signaling theory by showing that observability in digital environments depends on the integrity of the signal-carrier and that credible signaling requires both technical verification and signal-information evaluation. For practice, VCs can transform supplier evidence from static documents into independently and potentially machine-verifiable representations, supporting systematic supplier screening while reducing repeated manual verification. The findings are bounded by the qualitative, predominantly European, and early-stage empirical context. Future research should test the identified mechanisms across industries and institutional settings and investigate their effectiveness, governance, adoption, and longer-term signaling dynamics.

Keywords: verifiable credentials, adverse selection, digital signaling, organizational identities, self-sovereign identities, buyer-supplier relationship formation

Research Paper 5: Tokens against Tax Fraud: Designing a Blockchain-Based Information System for Duplicate Withholding-Tax Refund Control

Authors

Vincent Schaaf, Jan Stramm, Tobias Guggenberger, Marc-Fabian Körner, Nils Urbach

Publication Status

At the time of submitting this thesis, the corresponding essay is in an advanced status within a peer review process for potential publication in an academic journal.

Extended Abstract

Dividend-stripping arrangements such as the German Cum-Ex scheme exposed an information-systems problem in which fragmented tax-remittance, securities-settlement, custody, certification, and refund processes enabled multiple claims against a single withholding-tax payment. More generally, the case illustrates the difficulty of maintaining a consistent entitlement state across regulated organizations. Drawing on principal–agent theory, the study conceptualizes the tax authority as principal and taxpayers and financial intermediaries as agents whose actions and information cannot be fully observed without costly monitoring. It therefore asks: *How can a blockchain-based information system be designed to control duplicate withholding-tax refund claims in a federated tax-administration setting?*

The study follows a design science research approach. Literature and documentary analysis and six interdisciplinary consortium working sessions inform the problem understanding, requirements, and conceptual artifact. The design is subsequently assessed through ten semi-structured expert interviews and an analytical evaluation of modeled transaction workloads and selected recurring technical costs. The study translates the principal–agent problem into two meta-requirements and six design objectives. Effectiveness of control requires preventing duplicate exercise and preserving verifiability of the entitlement lifecycle. Proportionality of control requires limiting the agency costs of stronger control through privacy-preserving verification, interoperability, scalability and availability, and proportionate implementation and operating costs.

The design therefore seeks effective control without maximizing transparency or monitoring.

The conceptual artifact combines a private permissioned consortium blockchain with governed entitlement states, smart-contract-based constraints, and zero-knowledge proofs. A tax entitlement is represented as an event-specific digital state anchored to a withholding-tax payment recognized by the tax authority. The authority defines a maximum entitlement value, while regulated custodians create beneficiary-specific commitments within this authorization. Legally recognized reassignment replaces rather than duplicates the preceding state, while redemption consumes the current entitlement. Zero-knowledge proofs enable relevant properties of authorization, creation, reassignment, and redemption to be verified while concealing unnecessary information. The digital representation itself neither establishes legal entitlement nor guarantees the correctness of authoritative off-chain information.

The evaluation supports the conceptual plausibility of the entitlement-control logic and indicates that modeled transaction workloads are technically manageable under the stated assumptions. Selected recurring blockchain- and proof-related costs are unlikely to constitute the principal implementation barrier. However, the evaluation does not establish realized fraud prevention, reductions in agency costs, production reliability, or total cost-effectiveness. Legal recognition, governance, infrastructure integration, operational resilience, and authoritative off-chain inputs remain decisive boundary conditions.

Reflection on the artifact yields three design principles: formalizable opportunistic actions should be constrained *ex ante* through objectively specifiable rules; governed entitlements should be anchored to authoritative originating events while preserving a unique and conserved state across authorized transitions; and only decision-relevant properties should be verifiable while unnecessary underlying information remains concealed. The study thereby contributes reusable design knowledge for regulated interorganizational settings and shows how information systems can shift selected controls from retrospective monitoring toward *ex-ante* restriction without requiring unrestricted transparency.

Keywords: Blockchain; Design science research; Principal-agent theory; Taxation; Tokenization; Zero-knowledge proofs

Research Paper 6: Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications

Authors

Tobias Guggenberger, Lena Neubauer, Jan Stramm, Fabiane Völter, Till Zwede

Publication Status

This Research Paper is published as: Guggenberger, Tobias; Neubauer, Lena; Stramm, Jan; Völter, Fabiane; and Zwede, Till, "Accept Me as I Am or See Me Go: A Qualitative Analysis of User Acceptance of Self-Sovereign Identity Applications" (2023). Proceedings of the Hawaii International Conference on System Sciences (HICSS). <https://doi.org/10.24251/HICSS.2023.793>

Extended Abstract

Self-sovereign identity (SSI) aims to give users greater control over their digital identities by allowing them to manage and selectively disclose verifiable credentials without centralized identity providers. Although SSI promises increased privacy, portability, and user control, its benefits depend on broad adoption and network effects. Previous digital identity initiatives show that technical functionality alone does not ensure acceptance, particularly when systems are difficult to understand or use. Existing technology acceptance models provide an important foundation but may not capture SSI-specific characteristics. The study therefore asks: *Which attributes, features, and characteristics of Self-Sovereign Identity Systems influence the acceptance of the Identity System?*

The study follows an exploratory qualitative approach informed by the Technology Acceptance Model 2 (TAM2). Participants interact with a demonstrator in which an income-tax certificate is stored as a verifiable credential in a user wallet and selectively presented to a financial institution during a loan application. Thirteen semi-structured interviews with potential SSI users are conducted following this interaction. The material is analyzed through qualitative content analysis combining deductive TAM2 categories with inductive category development to capture additional acceptance factors. The analysis identifies 14 categories influencing SSI acceptance, five originating from

TAM2 and nine emerging inductively. They are organized into three groups: framework conditions, software characteristics, and user characteristics. At the center of the resulting model are perceived usefulness, perceived ease of use, and trust, which are proposed to directly influence intention to use. Perceived usefulness concerns the recognized benefits of SSI, while perceived ease of use reflects the effort required to learn and operate the system. Trust relates to both the technology and the organizations providing and operating it.

Several further factors influence these central constructs. Privacy, output quality, regulation and operation, and comprehensibility contribute to trust. Comprehensibility is particularly important because users must understand both SSI's benefits and the process steps involved in credential-based interactions; it is proposed to strengthen perceived usefulness, perceived ease of use, and trust. The number of available use cases increases perceived usefulness and experience, while positive user experience strengthens perceived ease of use. Technical affinity and prior experience moderate responses to educational measures, support, and system interaction.

The study contributes to technology acceptance research by showing that TAM2 cannot be transferred unchanged to SSI. Established variables including image, subjective norm, job relevance, and voluntariness are not identified as relevant, while nine additional categories emerge. The model therefore extends acceptance research with factors particularly relevant to decentralized identity systems, especially trust, privacy, and comprehensibility. For practice, SSI providers should communicate clear benefits, create understandable interactions, support users with different levels of technical experience, and establish trustworthy organizational and regulatory conditions. The study is limited by its small, relatively homogeneous sample and reliance on a single demonstrator and use case. Future research should quantitatively test the proposed relationships across different user groups, use cases, and levels of data sensitivity.

Keywords: Digital identities, adoption, TAM2, theory building