Enterprise Business Models Leveraging Self-Sovereign Identity: Towards a User-Empowering Me2X Economy

Tobias Kölbel
Karlsruhe Institute of Technology
Bosch Corporate Research
tobias.koelbel@kit.edu

Mahia-Cara Härdtner
ETH Zurich
mahia.haerdtner@haerdtner.de

Christof Weinhardt
Karlsruhe Institute of Technology
weinhardt@kit.edu

Abstract

The Self-Sovereign Identity (SSI) paradigm aims to transition online identity silos exhibiting privacy issues to user-controlled sharing mechanisms. While various governments back and promote its development, business models often play a subordinate role in these efforts. Building on academic literature and practical projects, our study addresses this and contributes a taxonomy of business enabled by SSI with 12 dimensions, 9 sub-dimensions, and 51 characteristics.

Keywords: Self-Sovereign Identity, Blockchain, Business Model, Privacy, Taxonomy

1. Introduction

Digital identity (ID) is something we rarely think about in our day-to-day lives, but it affects humans and businesses alike. Every time users open an online account, make a purchase, interact with social media, or browse the web, they leave a data trail. Single Sign-On (SSO) services operated by private companies such as Apple, Amazon, and Google collect, analyze, and store this data, creating digital footprints that they feed into profiles to sell data-driven business models (BMs) like targeted advertising (Human & Cech, 2021; Richter & Anke, 2021). Interactions in regulated contexts (e.g., finance) further require user verification through effortful know-your-customer (KYC) processes (Schlatt et al., 2021). Overall, technological progress is outpacing security (Boysen, 2021), with our web having no built-in ID protocol (Richter & Anke, 2021). Users are dependent on ID providers acting as pivotal ecosystem entities (Toth & Anderson-Priddy, 2019). They operate isolated data silos and integrate trust and reputation mechanisms that are beyond the users' control, entailing inherent security, economic, and ethical risks (Sartor et al., 2022; Sedlmeir et al., 2021).

Recently, the increased prevalence of data breaches, cybersecurity incidents, and detriments of data silos have fueled a public discourse and a strong push for user-empowering data control, autonomy, and sovereignty (European Commission, 2021; Human et al., 2020; Sedlmeir et al., 2021). Particularly in the European Union (EU), this altruistic shift manifests in regulatory initiatives such as the Data Governance Act (DGA), which could pave the way for a user-centric identity management (IDM) (European Commission, 2022) that embraces the social notion of sustainability (Alt, 2020). The DGA argues that users should have self-determined and trusted digital interactions while maintaining privacy. Instead of ID brokers managing data indirectly on a user's behalf, they store their IDs in digital wallets (European Commission, 2021). An emerging technology that overlaps the intensions of this new data strategy has been labeled as *Self-Sovereign Identity* (SSI). It describes a trusted network approach for authentic, verifiable, and seamless identification (Tobin & Reed, 2017). Users receive a master copy of their data, issued once by accredited entities, authenticated with digital signatures, and cryptographically secured using distributed structures like blockchain. With SSI, users can independently and selectively share their ID credentials and prove the trustworthiness of their information (Allen, 2016). Once issued and accredited, SSI credentials are interoperable and portable (Richter & Anke, 2021; Sedlmeir et al., 2021), enabling cross-service KYC and a user-empowering Me2X economy, what we define as an SSI-driven movement from a B2C world where intermediary third parties provide IDs to a user-centric world where users can bring their IDs to any service.

URI: https://hdl.handle.net/10125/103121
978-0-9981331-6-4

National governments like Germany ('Secure ID program') and Canada ('VON'), EU initiatives ('ESSIF'), the World Economic Forum ('KTDI'), firms (e.g., Microsoft), and research institutions (MIT's 'DCC') actively explore the IDM based on the SSI paradigm. Academic publications on SSI to date focus primarily on technical design (Mühle et al., 2018), user experiences in wallet software (Sartor et al., 2022), SSI use cases (Bartolomeu et al., 2019; Schlatt et al., 2021), and SSI network design (Kölbel et al., 2022; Kubach & Sellung, 2021). Some authors further emphasize an intertwined SSI perspective of technical and business aspects (Kölbel et al., 2022; Laatikainen et al., 2021). While technical maturity, design, and user acceptance are prerequisites for the adoption of Me2X IDM, scholars argue that studying BMs in SSI is essential for economic success and requires a distinct analysis (Kölbel et al., 2022). However, to the best of our knowledge, there is no empirically-based research on how SSI can serve as the basis for BMs in IDM. To avoid this pitfall, our work focuses on the following research question: *What BM characteristics distinguish enterprises leveraging SSI ecosystems?*

To contribute a tangible analysis relevant to academic and practitioner communities, we develop a taxonomy of business enabled by SSI (acronym: BESSI) following Nickerson et al. (2013). Here, we consider BMs that rely on SSI ecosystems as an integral part of their offering. Our analysis is guided by Al-Debei and Avison's (2010) BM dimensions and incorporates data from literature and real-world projects. For practitioners, we identify BMs in SSI to reduce complexity and assist in selecting and developing viable BESSI. From a theoretical perspective, we develop a tool for researchers to model and systematically compare enterprise BMs leveraging SSI ecosystems to achieve comparable results and scientific rigor.

The article proceeds as follows. Section 2 presents SSI fundamentals, and Section 3 explains our research design. Section 4 discusses results and presents the BESSI taxonomy. Section 5 highlights contributions, states limitations, and suggests further research avenues.

2. SSI Fundamentals

The SSI paradigm places users at the center of ID ecosystems (Richter & Anke, 2021), enables direct control over pertaining data, and ensures that users must explicitly consent to the sharing, use, and processing of their data (Toth & Anderson-Priddy, 2019). It aims to create a trusted data economy that allows users to verify, control, and trust the people they interact with, both in physical and digital realms (Kronfellner et al., 2021).

From an ecosystem perspective, SSI revolves around three specific actors: the issuer, the holder, and the verifier, who communicate peer-to-peer (P2P) with each other (Kubach & Sellung, 2021; Richter & Anke, 2021). Together, these three actors form the so-called *trust triangle* (Davie et al., 2019), which facilitates data collection, resolution, updating, and revocation without the need for centralized ID intermediaries (Mühle et al., 2018). An **issuer** is an entity capable of issuing trusted data as verifiable credentials (VCs). VCs refer to a tamper-proof data file that contains a set of statements ('claims') about a holder that can be cryptographically verified. Several types of VCs offer advantages such as privacy protection (e.g., selective disclosure). Issuers can come in many shapes and sizes (e.g., governments, financial service providers). They verify and attest to a fact or attribute about another entity. The degree of reliance on this attestation is at the discretion of the verifier. A **holder** can be a person, organization, or object with a set of attributes attested by an issuer. The holder may hold these attributes in the form of VCs and manage them through software clients ('wallets'). Upon request, holders can bundle VCs into a verifiable presentation to self-prove attributes to third parties. A **verifier** is an entity that can check the authenticity and validity of a VC against a presented verifiable presentation. It can verify that the data presented was issued by the correct, legitimate issuer and that the VC has not been tampered with or revoked. As such, the trust triangle allows the verifier to trust the data it receives directly from a holder without the need for direct interaction

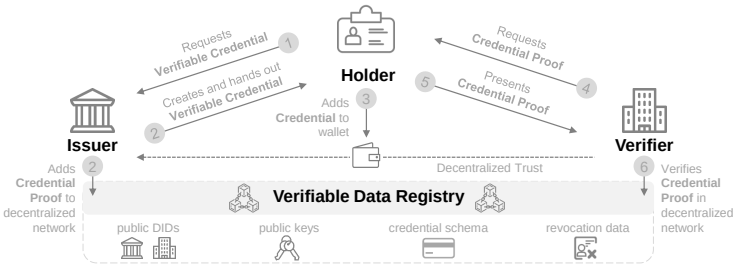

Figure 1. SSI Trust Triangle (Davie et al., 2019; Kölbel et al., 2022)

or relationship with the issuer (Davie et al., 2019; Kölbel et al., 2022). This decentralized trust, which extends beyond the validity of VCs, is enabled by cryptographic signatures and decentralized identifiers (DIDs) that are anchored in **immutable data registries** (Tobin & Reed, 2017). The World Wide Web (W3C) Consortium, seeking to standardize the technological basis of SSI amid other open source communities and non-profit organizations (e.g., TrustOverIP and Decentralized Identity Foundation), describe DIDs as "a globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network" (Reed et al., 2019).

3. Methodological Approach

To develop the BESSI taxonomy of enterprise BMs leveraging SSI ecosystems, we adopted Nickerson et al.'s (2013) methodology. We argue that this approach is particularly suitable as it applies across disciplines and combines practical relevance with scientific rigor. Moreover, it assists researchers and practitioners in understanding a complex domain by providing a well-documented and systematic process for defining dimensions and characteristics (Nickerson et al., 2013). Our taxonomy development process consists of an iterative approach with seven steps (see Figure 2). First, we defined meta-characteristics that reflect the purpose of our taxonomy and serve as guidance throughout the process (Step 1). We then defined ending conditions that determine when the iterative development process is complete (Step 2). In total, Nickerson et al. (2013) propose eight objective and five subjective ending conditions, which we borrowed for our research design. Subsequently, we started the iterative process of taxonomy development, choosing between inductive and deductive reasoning (Steps 3-6). While the conceptual-empirical approach is guided by empirical evidence, the empirical-conceptual approach focuses on extracting dimensions and characteristics from the scientific knowledge base (Nickerson et al., 2013). Our research process considers both options with a conceptual-empirical literature review and the analysis of real-world SSI projects as part of the empirical-conceptual approach. We iterated the process until the ending conditions were met (Step 7) and evaluated our results with three individual raters classifying five evaluation cases. We ensured that most of the required information was available on the companies' websites in selecting the cases. To compare the rater results and measure the level of agreement, we used Fleiss kappa (Fleiss, 1971). The analysis yielded a value of 63% that corresponds to a "substantial agreement" (Landis & Koch, 1977) and thus indicates that our taxonomy is suitable for a consistent classification and concise description of BESSI.

Meta-characteristic. As a first step, we define the Unified BM framework by Al-Debei and Avison (2010) as meta-characteristics that reflect the purpose of our taxonomy and serve as guidance throughout the process. Accordingly, each of our taxonomy dimensions must relate to one of their **Value[4]BM dimensions**, namely value proposition, architecture, network, and finance (further described in Section 4). We argue that this guidance is particularly appropriate for our endeavor as it first explicitly addresses digital BMs and, second, covers the multidimensionality of BMs.

Conceptional-to-empirical. The starting point of our taxonomy development process forms a **structured literature review (SLR)**. With this procedure, we build a knowledge base on BMs in SSI, incorporate state-of-the-art research and strive to increase scientific rigor. The SLR follows the methodological suggestions of Webster and Watson (2002) and builds on querying a wide range of interdisciplinary databases[1] concerning several topic-related key terminologies[2]. To ensure that only high-quality and topic-relevant literature is considered, we applied the following criteria: First, we concentrate on peer-reviewed publications available in English and published between 2016 and 2022. Second, we review literature that concentrates on SSIs and explicitly or implicitly addresses BMs. This comprises

[1] ACM, AISeL, EBSCOHost, Emerald Insight, IEEEXplore, ProQuest, ScienceDirect, Taylor & Francis, Web of Science

[2] (Self-Sovereign Identit* OR Self Sovereign Identit* OR SSI)

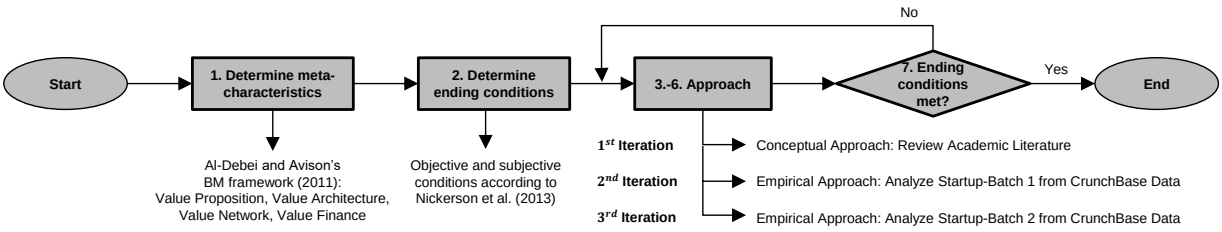

Figure 2. Applied Methodology following Nickerson et al. (2013)

papers relating to specific BMs in SSI as well as ecosystem initiatives and projects that consider SSI an integral part of their business activity. Consequently, we excluded studies that focus on SSI fundamentals and technological aspects, especially blockchain-related specifications such as asymmetric encryption (Fan et al., 2020; Rana et al., 2019). The search returned a total of 295 hits. Screening all papers' titles and abstracts resulted in 56 articles that met our inclusion criteria, including 12 removed duplicates. By analyzing the main texts, 35 additional publications were excluded from the analysis corpus. An iterative backward and forward search with the remaining nine publications yielded five additional relevant articles. In sum, we identified a total of 14 articles that provide the basis for our initial taxonomy.

Empirical-to-conceptional. Given the novelty of SSI and the moderate number of scientific publications related to BMs, our second and third iteration phase incorporates projects that engage in SSI ecosystems. With this empirical data, we aim to address the topic's recency and improve the practical relevance of our taxonomy. The dataset for the **project analysis** relies on the *CrunchBase* new venture database and our SLR. We first considered all CrunchBase-listed projects for the keyword "self-sovereign identity" and identified 32 ventures. To ensure that our sample includes only relevant projects, we applied the following selection criteria. First, projects are relevant if they have already been mentioned in our SLR (e.g., Evernym, uPort/now Serto and Veramo, Trinsic, Spherity, Esatus, Kiva). Furthermore, to consider potentially successful projects, we only selected those firms that had already received funding. Projects that were not active anymore (Learning Machine Technologies, Space Elephant) or did not have an English homepage were excluded. In addition, we only considered projects that introduce SSI as an integral part of their BM, thereby excluding five enterprises (Synacts, Yat Labs, Coinplug, Ohanae, life.io). Finally, we excluded projects that did not provide sufficient information on the aforementioned criteria (Konsent, Cultu.re, Avila Security, Spidchain, Object Tech, Mooti). After considering all factors, the final set of analyzed enterprises covered 18 cases (see Table 1). For the taxonomy development, we considered the first nine projects in iteration two, and analyzed the remaining nine projects in iteration three.

Table 1. Analyzed Projects

Iter.	*ID*	*Name*	*Website*
2	P1	Passbase	passbase.com
2	P2	Evernym	evernym.com
2	P3	Cheqd	cheqd.io
2	P4	Tykn	tykn.tech
2	P5	Liquid Avatar	liquidavatarech.com
2	P6	Finema	finema.com
2	P7	iGrant	igrant.io
2	P8	Vereign	vereign.com
2	P9	Trinsic	trinsic.id
3	P10	Blockpass	blockpass.org
3	P11	Metadium	metadium.com
3	P12	uPort	uport.me
3	P13	EarthID	myearth.id
3	P14	CoR	corinc.io
3	P15	Equideum	equideum.health
3	P16	Esatus	esatus.com
3	P17	Spherity	spherity.com
3	P18	Kiva	kivaprotocol.com

4. Taxonomy of Businesses enabled by Self-Sovereign Identity (BESSI)

This section presents our BESSI taxonomy. Figure 3 illustrates 12 dimensions and nine sub-dimensions, while two to six characteristics further describe each (sub) dimension. The right column of Figure 3 indicates whether an element is exclusive (E) or non-exclusive (N). Exclusive elements imply that a BM can solely be described by one characteristic per dimension. Conversely, non-exclusive elements suggest that one or more attributes characterize a BM. In addition, the superscripted numbers in Figure 3 indicate the iteration in which a dimension or characteristic was added. We present the taxonomy elements in detail below and structure our findings along the Value^{4}BM dimensions of Al-Debei and Avison (2010). We choose this framework because its multidimensionality appears appropriate and sufficiently comprehensive to capture all aspects of BESSI while avoiding conceptual ambiguity (Kölbel et al., 2022).

4.1. Value Proposition

The first perspective addresses mechanisms of BESSI to satisfy diverse customer needs. It comprises three dimensions, namely *stakeholder value*, *target audience*, and *customer relationship*.

Stakeholder value deals with the benefit of a specific business idea (product or service) that BESSI implies. It is a non-exclusive dimension since an enterprise can provide more than one value for its customers and leveraging SSI may have multiple benefits for enterprises. The first of six characteristics introduces *operational convenience*, which involves augmenting traditional BMs with SSI attributes. Examples include ID verification and

exchange (Bernabe et al., 2019; Kubach & Sellung, 2021), digitization of physical ID documents and access management through wallet solutions (Shuaib et al., 2021; Stockburger et al., 2021, P6, P16), portability of digital IDs across multiple services (Richter & Anke, 2021), and the elimination of passwords through biometric SSI authentication solutions (Wang & De Filippi, 2020, P4), thereby reducing administrative burden and improving customer experience. In addition, *interoperability* addresses the ability of a BESSI to communicate and exchange information with other SSI networks. Besides adhering to technical standards and communication protocols such as DIDcomm, BESSI offerings also differentiate based on the verifiable data registry used. For example, Cheqd (P3) supports multiple networks with a Cosmos-based system that promotes communication between blockchains, while other projects rely on single-network solutions with limited interoperability (e.g., P4, P6, P14). More characteristics include *efficiency gains* through SSI-based automation of processes (Ertemel, 2018; Gebresilassie et al., 2020; Naik & Jenkins, 2020, P1, P9, P10, P12) and *cost reductions* through simplification of costly and cumbersome compliance regulations (Schlatt et al., 2021, P3, P11), which are particularly important when the cost and speed of verifying information is an essential business activity. While cost-saving measures and improved customer experience are potentially the quickest wins for businesses leveraging SSI ecosystems, SSI further unlocks *revenue extensions*, empowering companies to generate new BMs and seamlessly engage (new) customers faster with customer-direct data (P2). Examples include cross-service KYC and due diligence processes (Schlatt et al., 2021, P10, P17, P18), platforms for self-determined data exchange and monetization (e.g., for health data; (Stockburger et al., 2021; Thomason, 2021), SSI-based IDs and avatars in the metaverse (e.g., P5, P10), and all-in-one SSI enterprise suites (e.g., P12, P16). In addition, SSI also enables credentialing-as-a-service offerings and role-based, privacy-preserving access to lifecycle credentials of objects and machines along value chains of complex B2B supply chain structures (e.g., P17). Empowering the characteristic of *digital trust*, which describes user self-determination and secure data exchange through cryptographically secured SSI ecosystems, BESSI allows users to exchange data quickly, efficiently, and respectfully. In this context, real-world projects (e.g., P2, P4, P11) indicate that SSI also minimizes risk and complicates ID theft by keeping individual data in the hands of users and allowing companies to securely and independently validate their customers via the verifiable data registry. For example, Evernym's value proposition that their products are carefully designed to protect privacy (P2) is exemplified by cryptography and zero-knowledge proofs for data minimization. Similarly, Finema aims to reduce fraud-related costs by offering an automated, document-centric ID verification service that checks any document using artificial intelligence and computer vision (P6).

	Dimension		Characteristic						E/N*
Value Proposition	Stakeholder Value[1]		Operational Convenience[1]	Interoperability[2]	Efficiency[1]	Cost Reduction[1]	Revenue Extension[1]	Digital Trust[1]	N
	Target Audience[1]	Customer Group[1]	Natural Person[1]		Legal Person[1]		Non-Profit Entity[1]		N
		Segment[2]	Business-to-Business (B2B)[2]		Business-to-Consumer (B2C)[2]		Business-to-Government (B2G)[3]		N
		Market Specialization[2]	Global Audience[2]		Geographically Limited[2]		Industry-specific[3]		E
	Customer Relationship[2]		Customizability[2]			Customer Support[2]			N
Value Architecture	Verifiable Data Registry[1]		Blockchain-enabled[1]			Other Network[2]			E
	Data Storage[2]		On-Device-Storage[2]			Cloud-Storage[2]			N
	Compliance	Regulatory[1]	Know-your-Customer (KYC)[1]	Anti-Money-Laundering (AML)[2]		EU General Data Protection Regulation (GDPR)[1]	Other[2]		N
		Technological[1]	W3C-Standards[1]			Other[2]			N
	Customer Channel[2]	Wallet Provisioning[2]	Own Wallet[2]		Third Party Software[2]		Technology Provision Only[2]		E
		Interface[2]	Web-based Solution[2]			Mobile App[2]			N
Value Network	Ecosystem Role[2]		Software-as-a-Service (SaaS)[2]		ID-as-a-Service (IDaaS)[2]		Technical Enabling[2]		N
	Key Partner[1]	Enabling Partner[1]	Technical Infrastructure Provider[1]		Standard-Setting Community[1]		Trust Provider[1]		N
		Industry Partner[2]	Technology Provider[2]	Developer Community[2]		Auxiliary Service Provider[2]		Stand Alone[2]	N
Value Finance	Customer Charge[2]		Cost-per-Transaction[2]		Subscription Fee[2]		Not Specified[2]		N
	Payment Integration[2]		Fiat-Currency[2]		Token-System[2]		Not Integrated[2]		N
	Cost Structure[2]		BESSI Development Costs[2]		External Registry User Costs[2]		Own Registry Provisioning Costs[2]		N

*E = Exclusive dimension (one characteristic observable); N = Non-exclusive dimension (more than one characteristic observable)
Dimensions and characteristics were added in the following iteration: [1] first, [2] second, or [3] third iteration

Figure 3. Taxonomy of business enabled by Self-Sovereign Identity (BESSI)

The second dimension of **target audience** involves three characteristics. The first is the *customer group* addressed by a BESSI. Following research on the stakeholder landscape in SSI ecosystems (Kubach & Sellung, 2021; Laatikainen et al., 2021), we distinguish between natural persons, legal entities, and non-profit entities. The second characteristic of *customer segment* differentiates business-to-business (B2B), business-to-consumer (B2C), and business-to-government (B2G). BESSI can also address multiple audiences (Me2X). For example, an offering may include a B2C wallet app (e.g., P9, P16) or SSI-secured email signatures (e.g., P8). Other options comprise software development kits (SDKs) sold as white-label products that can be customized and rebranded for B2B (e.g., P1, P6, P12, P14) or standards-based authentication platforms to connect government ID systems with financial services and payment infrastructures (e.g., P18). The *market specialization* additionally describes whether a BESSI is available to a global audience and thus does not target a focus market (e.g., P2, P3, P14) or whether availability is geographically limited to a specific country (e.g., P13) or region (e.g., P6) (e.g., to comply with specific legislation), or is industry-specific (e.g., P1, P13, P15).

Next, **customer relationship** classifies the connection between a BESSI and its customers. We distinguish two characteristics: First, *customizability* characterizes a customer's involvement and the flexibility of a BESSI. Here, our project analysis identifies the provisioning of different service packages that vary in functionality and price (e.g., P1, P8, P16). Second, *customer support* specifies the support mechanisms and responsiveness of employees working for a BESSI regarding assistance. Here, the level of support can vary. For example, Passbase (P1) offers its customers 24-hour assistance via email, chat, or phone at no additional cost, while Evernym (P2) conditions this service on the package size purchased by customers.

4.2. Value Architecture

The second perspective describes the architecture and structural design of BMs, including the technological and organizational infrastructure that facilitate BESSI to create and deliver value. It comprises four dimensions, namely *verifiable data registry*, *data storage*, *customer channel*, and *compliance*.

Verifiable data registry describes the technical infrastructure a BESSI relies on to establish trust. Our taxonomy distinguishes between *blockchain-based* (e.g., P2-13) and *other networks* (e.g., P1, P16). In the first case, we identify different blockchain types, differing between public chains (e.g., P2-4, P10-13) and consortium chains (e.g., P5, P6, P9). In terms of blockchain networks, we observe the utilization of Ethereum (Stockburger, P10, P12, P15), Hyperledger (Shashank, P2, P4, P8, P9), and other networks (e.g., P3, P7, P11). We further acknowledge different consensus mechanisms. These include, for example, proof-of-work (e.g., P10), proof-of-stake (e.g., P3, P6), proof-of-authority (e.g., P11), proof-of-elapsed-time (e.g., P8), and self-created mechanisms (e.g., P2, P14).

The **data storage** dimension specifies a BESSIs data retention. We distinguish *on-device-storage*, where users self-host and locally store their data (e.g., P2, P11, P14), and *cloud-storage* (e.g., P1, P7, P12), where users store data in a self-hosted cloud or the environment of a contracted service provider. A combination of both storage types is also feasible (e.g. P4).

With the **compliance** dimension, we further indicate whether a BESSI complies with regulatory and/or technical standards. *Regulatory standards* involve, for example, KYC and Anti-Money Laundering (AML) legislation in regulated industries (e.g., financial sector). It also extends to compliance with the EU's General Data Protection Regulation (GDPR), a data protection law endorsed by the EU Commission that governs the third-party processing of personal data and addresses the so-called 'CIA triad' (confidentiality, integrity, and availability) of data protection (Almeida et al., 2022). In this regard, researchers indicate that GDPR compliance could be operationalized by SSI (Davie et al., 2019; Kronfellner et al., 2021). Weigl et al. (2022) note that user-centric data management and privacy-enhancing characteristics of SSI systems (e.g., selective disclosure) support privacy compliance. In addition, our taxonomies *technical standards* dimension indexes whether a BESSI follows W3C-defined standards for DIDs and VCs, which Richter and Anke (2021) describe as the "most notable" initiatives in terms of the technical standardization and interoperability of SSI. Beyond, the 'other' category includes any other standards adopted by a BESSI (e.g., Aries Interoperability Standard; P2).

The **customer channel** describes how a BESSI connects with its target audience. *Wallet provisioning* distinguishes businesses that offer their wallet software (e.g., P2, P13, P16), offerings reliant on access to third-party software (e.g., P7, P11), and technology provisioning only (e.g., P3). Concerning BESSI *interfaces*, we differentiate web-based solutions (e.g., P4, P9, P13) and mobile apps (e.g., P4, P9, P13). In this context, Evernym (P2) offers a mobile SDK to embed the company's proprietary wallet functionality into apps of B2B customers. In addition, customers can build a customized, new app according to their needs and

requirements. Cheqd, on the other hand, works with a technology partner that offers an interchain wallet that can be used for both web and mobile applications (P3).

4.3. Value Network

The third perspective refers to inter-organizational actors that form SSI ecosystems and describes how they collaboratively create value. We distinguish two dimensions, namely *ecosystem role* and *key partner*.

Ecosystem role describes the type and vertically integrated value proposition by a BESSI. *Software-as-a-Service (SaaS)* vendors provide B2B software that other ecosystem participants use for their SSI offerings. These include, for example, function-specific (e.g., P3) or all-in-one SSI suites (e.g., P16). *ID-as-a-Service (IDaaS)* offerings, on the other hand, have a direct customer interface and aim to enable users to interact in SSI ecosystems. They offer an array of applications that can range from issuing DIDs (e.g., P2, P9) and verifying VCs (e.g., P1, P6, P12) to providing a metaverse where users can leverage their SSI-enabled ID (P5). In addition, *technical enabling partner* provide services such as application programming interfaces (APIs) that allow, for example, to transfer verifiable data between ID wallets (e.g., P9). This category also includes SDKs that enable the plug-and-play integration of VCs into mobile applications (e.g., P2, P12, P17). In this context, we see a variety of programming languages being offered. For example, Passbase (P1) provides solutions in JavaScript, Python, Java, and Ruby, while Evernym (P2) focuses on Java, Node.Js, Python, and .NET.

The **key partner** dimension characterizes complementary actors involved in a BESSI provision. In general, this refers to the issuer, holder, and verifier of the SSI trust triangle (see Section 2), which Davie et al. (2019) consider universal stakeholder roles in SSI ecosystems. Schlatt et al. (2021) further describe these actors in the context of KYC processes as a service-providing bank (i.e., verifier) that validates a service-seeking customer's (i.e., holder's) claim issued by a trusted third party (i.e., issuer). Beyond, our taxonomy considers more fine-grained partner relationships. By *enabling partner*, we first mean infrastructure providers that support various technical aspects (e.g., node services, consensus mechanisms) and act as active stakeholders of SSI ecosystems (Kubach & Sellung, 2021, P10). Second, we consider standard-setting communities (e.g., TrustOverIP Foundation, Decentralized Identity Foundation) that support and evolve SSI's technological foundations and establish standards that active stakeholders build upon (Kubach & Sellung, 2021). In addition, we consider trust providers such as government institutions and non-profit organizations to be BESSI partners, acting, for example, as trusted third parties and issuers of VCs (Laatikainen et al., 2021, P1). Similarly, we categorize companies that are directly or indirectly involved in the creation of a BESSI as *industry partners*. Here we distinguish between technology providers and developer communities involved in developing a service, auxiliary service providers (e.g., consulting firms), and the stand-alone provision of a BESSI. In this context, Evernym (P2), for example, considers consulting firms, insurance companies, telecommunication technology companies, and service-related development service providers as their BESSI partners.

4.4. Value Finance

The fourth dimension represents monetization strategies and costs associated with a BESSI. We distinguish three dimensions, namely *customer charge*, *payment integration*, and *cost structure*.

Customer charge indicates how a consumer pays for a BESSI (Kuperberg, 2020). First, we distinguish *cost-per-transaction* models, where, for example, consumers pay a fee for each issue, verification, and storage operation (e.g., P3, P9, P11). Second, BESSI projects adopt *subscription* models where consumers pay a monthly or annual fee (e.g., P16). Furthermore, we identify combinations within BMs where, for example, using a wallet app is free. At the same time, services (e.g., document authentication, APIs, SDKs) cost a monthly subscription fee, and auxiliary services (e.g., AML and KYC compliance verification) get charged on a per-transaction basis (e.g., P1, P5).

The **payment integration** dimension further describes whether payment transactions are offered as part of a BESSI. Here, we distinguish between *fiat-currency* integrations (e.g., P2, P4), *token systems* (e.g., P3), and a *not-integrated* option where a BM does not provide monetary transactions (e.g., P5, P7).

Lastly, the **cost structure** dimension describes expenses related to a BESSI. First, we distinguish *BESSI development costs* incurred for the implementation of a BM (e.g., personnel costs). Second, *external registry user costs* indicate whether a BESSI provider relies on third-party cooperation and has no direct impact on, for example, transaction costs when using a blockchain network as a verifiable data registry (e.g., P2, P6, P7). In contrast, the characteristic *own registry provisioning costs* allows to include expenses if a provider, for example, operates its own network whose governance and financial design are subject to its influence (e.g., P3).

5. Discussion and Conclusion

The SSI paradigm is a rapidly evolving topic (Sedlmeir et al., 2021). It embodies a user-centric sharing mechanism to present trusted and verified data (Boysen, 2021), that offers humans, businesses, and smart devices a convenient and privacy-oriented alternative to both physical means of identification and centralized ID platforms (Kölbel et al., 2022). Several researchers suggest that SSI, by virtue of its decentralized approach, changes the underlying principles of established services' BMs that rely on collecting, analyzing, and selling user data, traffic, or advertisements (Laatikainen et al., 2021; Sedlmeir et al., 2021). However, while the technical benefits of SSI to end-users are clear, we argue that business benefits remain rather ambiguous. We address this matter by adopting a multilayered research approach that incorporates both academic sources and real-world projects. Our main contribution is the theoretically grounded and empirically validated BESSI taxonomy, which follows the methodological guidelines of Nickerson et al. (2013). Structured along the Value^{4}BM dimensions of Al-Debei and Avison (2010), we present a market overview, analyze and abstract individual BMs, and highlight variations.

Our analysis shows that BESSI address several user groups, ranging from natural and legal persons to non-profit entities, spanning multiple segments (B2B, B2C, B2G). Besides a customizable offering and sophisticated customer support, vendors differ in value propositions. Examples include SSI networks' operational convenience and interoperability, where users profit from improved customer experience and reduced administrative complexity. Furthermore, BESSI promote efficiency gains and cost reductions and transform how customers are treated, enabling businesses to 'level-up' on digital trust while serving users and services (Boysen, 2021). Beyond influencing traditional BMs in IDM, SSI facilitates the exploration of new revenue. This includes platforms for secure exchange and private data sales, along with innovative ideas such as IDs for the metaverse. Although platforms in SSI can't sell any data they want, researchers indicate a potential for fair monetization through SSI-based systems (Stockburger et al., 2021; Thomason, 2021). However, we note a gap between theory and practice, as incentive mechanisms in SSI are being pursued by only one real-world project (P3). Concerning value architectures, we observe a widespread use of blockchain-based verifiable data registries as trust anchors, whereas user data is stored in wallets or cloud services following the SSI principle of control (Allen, 2016). Businesses can develop their own (web or mobile) wallets, rely on open source from third parties, or act as technology providers. BESSI is influenced by growing regulatory efforts like DGA, GDPR, and KYC - especially regarding data collection and usage - and compliance with technical standards. We support Richter and Anke (2021)'s thesis that W3C standards for DIDs and VCs are the "most notable" technical initiatives related to SSI as they are being followed by most of our projects. For value networks, we consider SaaS-focused BESSI for B2B, IDaaS vendors targeting B2C, and offerings limited to technical support. As key partners, we identify enabling partners and industry-specific partners. In value finance, we observe that many BESSI rely on subscription or cost-per-transaction models. We notice an indifferent structure concerning payment integration, as BESSI come with payments in fiat currency and cryptocurrencies or without payment. Finally, as costs to consider, we identify offer-related development costs and costs related to the operation of a BESSI.

Our study contributes to the descriptive knowledge of the SSI phenomenon by exploring the poorly grasped area of BESSI. From a theoretical perspective, we add to the SSI ecosystem literature by providing the BESSI taxonomy that identifies tangible dimensions and characteristics to help understand how SSI affects BMs. It serves as a basis for analyzing, designing, and configuring offerings, as well as analyzing antecedents. We contribute a common understanding of this complex topic and propose a tool for future research. In doing so, we follow the call for an economic perspective on SSI that examines business model aspects besides technological features (Kölbel et al., 2022; Laatikainen et al., 2021; Sedlmeir et al., 2021). Practitioners may use the BESSI taxonomy and related case studies within ideation phases to identify options for BM innovation toward SSI and assess its impact on their current business. As a technology-specific tool, it assists decision-makers in evaluating and implementing business ideas in an enterprise context, such as building their own SSI solution or integrating and extending their current BM with an external SSI solution. We provide executives with an overview of existing BMs that can be used to systematically analyze niches of not yet offered services, identify potential market entry opportunities, and rank relevant startups.

In interpreting our results, we acknowledge **limitations** that inherently constrain our study. First, Nickerson et al. (2013) notes that taxonomies are never perfect nor exhaustive. While we describe the current state, SSI ecosystems are subject to rapid technological evolution, which means that concepts and

BMs constantly evolve. Therefore, our taxonomy is a contemporary snapshot that requires periodic updating. However, we designed our taxonomy to be revisable and extensible so that new perspectives, characteristics, and dimensions can be added (Nickerson et al., 2013). Second, we were unable to evaluate analyzed BESSI concerning firm performance, and third, we cannot ensure that all businesses exploring SSI are part of our sample. We aim to address this issue by relying on projects cited in the literature and incorporating new ventures from the CrunchBase database. However, we note that our sample does not include SSI projects from incumbents (e.g., those funded by the German government's 'Secure Digital ID' program, such as Bosch, Commerzbank, and Deutsche Bahn).

Besides the limitations, which vice versa present **research opportunities**, the business potential of SSI is still in its infancy and will evolve further, thereby indicating avenues for future research. For example, scholars could reexamine the same projects we analyzed later to explore potential transformations in their BMs. Future research could also adopt our taxonomy's dimensions and characteristics as constructs for further empirical studies, qualitative or quantitative. Qualitative interviews with representatives from research and practice, for example, could evaluate our findings to confirm further or iteratively revise them. This review for completeness and applicability would improve the validity of our results. In addition, researchers can build on our taxonomy and explore archetypes that describe recurring patterns in BESSI offerings. These patterns could serve as a starting point to understand superordinate configurations, anticipate comparative trends, and identify key BESSI success factors. We argue that SSI infrastructures require close collaboration between business peers and competitors, exemplifying the coopetition model. Like blockchain solutions, SSI works best in contexts where different entities collaborate in a decentralized and distributed network, thereby turning SSI implementations toward business rather than technology challenges. In this context, we see a need for research on governance and collaboration models that ensure networks are reliable, secure, and provide adequate data protection. As SSI progresses in real-world applications, researchers can also extend our taxonomy toward a maturity model for BESSI. In addition, studying Me2X economies foci and SSI ecosystems from a service-dominant logic perspective or developing an artifact using Design Science Research represent attractive research avenues. Given our observation that in current BESSI, network benefits appear to accrue predominantly to holders and verifiers, we suggest that future research could also analyze whether current SSI systems face bootstrapping and chicken-and-egg problems familiar from research on multi-sided markets that impact the adoption of SSI-based IDM. We argue that SSI ecosystems could benefit from self-reinforcing network effects when a critical mass of actors of the SSI trust triangle are interconnected and propose studies that focus on BESSI revenue streams as a function of their respective values. In this context, we note that current monetization strategies depend primarily on issuers bearing the costs of key operations in SSI ecosystems (e.g., DID document creation, VC signing, verification). However, we argue that they are not the primary beneficiaries of these operations and suggest exploring the extent to which holders and verifiers should bear these costs or whether, for example, governments could subsidize network operations. Here, attention could also be given if fees for each transaction add value or if SSI systems should ideally be able to distinguish SSI operations and charge only for value-adding processes.

References

Al-Debei, M. M., & Avison, D. (2010). Developing a unified framework of the business model concept. *EJIS*, *19*(3), 359–376.

Allen, C. (2016). *The Path to Self-Sovereign Identity*. https : / / www . coindesk . com / path - self - sovereign-identity Accessed: 19.05.2022

Almeida, J., da Cunha, P. R., & Pereira, A. D. (2022). GDPR-Compliant Data Processing: Practical Considerations. *437 LNBIP*, 505–514.

Alt, R. (2020). Electronic Markets on Sustainability. *Electronic Markets*, *30*(4), 667–674.

Bartolomeu, P. C., Vieira, E., Hosseini, S. M., & Ferreira, J. (2019). Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT. *IEEE ETFA*, 1173–1180.

Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*.

Boysen, A. (2021). Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. *Frontiers in Blockchain*, *4*, 11.

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The Trust over IP Stack. *IEEE Communications Standards Magazine*, *3*(4), 46–51.

Ertemel, A. (2018). Implications of Blockchain Technology on Marketing. *JITAL*, *4*(2), 35–44.

European Commission. (2021). *European Digital Identity*. https://ec.europa.eu/info/strategy/

priorities-2019-2024/europe-fit-digital-age/european-digital-identity Access: 08.06.2022

European Commission. (2022). *Data governance act — Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/data-governance-act Accessed: 19.05.2022

Fan, X., Chai, Q., Xu, L., & Guo, D. (2020). DIAM-IoT: A decentralized identity and access management framework for IoT. *BSCI Proceedings*, *6*(20), 186–191.

Fleiss, J. L. (1971). Measuring nominal scale agreement among many raters. *Psychological Bulletin*, *76*(5), 378–382.

Gebresilassie, S. K., Rafferty, J., Morrow, P., Chen, L. L., Abu-Tair, M., & Cui, Z. (2020). Distributed, Secure, Self-Sovereign Identity for IoT Devices. *IEEE WF-IoT Forum*.

Human, S., & Cech, F. (2021). A human-centric perspective on digital consenting: The case of GAFAM. *Smart Innovation, Systems and Technologies*, *189*, 139–159.

Human, S., Gsenger, R., & Neumann, G. (2020). End-user Empowerment: An interdisciplinary perspective. *HICSS Proceedings*.

Kölbel, T., Gawlitza, T., & Weinhardt, C. (2022). Shaping Governance in Self-Sovereign Identity Ecosystems: Towards a Cooperative Business Model. *WI Proceedings*.

Kronfellner, B., Merey, T., Beron, D., & Terbu, O. (2021). Me, myself and (SS)I Why everybody must have a Self-Sovereign Identity in 5 years.

Kubach, M., & Sellung, R. (2021). On the Market for Self-Sovereign Identity: Structure and Stakeholders. *Open Identity Summit*, 143–154.

Kuperberg, M. (2020). Blockchain-Based Identity: A Survey from the Enterprise and Ecosystem Perspective. *IEEE-TEM*, *67*(4), 1008–1027.

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., & Abrahamsson, P. (2021). Towards a trustful digital world: exploring SSI ecosystems. *PACIS Proceedings*.

Landis, J. R., & Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical Data. *Biometrics*, *33*(1), 159.

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of SSI. *Computer Science Review*, *30*, 80–86.

Naik, N., & Jenkins, P. (2020). SSI Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology. *IEEE MobileCloud Proceedings*, 90–95.

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *EJIS*, *22*(3), 336–359.

Rana, R., Zaeem, R. N., & Suzanne Barber, K. (2019). An assessment of blockchain identity solutions: Minimizing risk and liability of authentication. *IEEE WI Proceedings*, 26–33.

Reed, D., Sporny, M., & Allen, C. (2019). Decentralized Identifiers (DIDs) v1.0. *W3C*. https://www.w3.org/TR/did-core/. Accessed: 19.05.2022

Richter, D., & Anke, J. (2021). Exploring Potential Impacts of SSI on Smart Service Systems. *Business Information Systems*, 105–116.

Sartor, S., Sedlmeir, J., Rieger, A., & Roth, T. (2022). Love at First Sight? A User Experience Study of SSI Wallets. *ECIS Proceedings*.

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a Framework for Digital KYC Processes Built on Blockchain-Based SSI. *Information and Management*.

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *BISE*, *63*(5), 603–613.

Shuaib, M., Alam, S., Shabbir Alam, M., & Shahnawaz Nasir, M. (2021). SSI for healthcare using blockchain. *Materials Today*.

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity: The case of SSI in public transportation. *Blockchain: Research Applications*, *2*(2).

Thomason, J. (2021). Big tech, big data and the new world of digital health. *Global Health Journal*, *5*(4), 165–168.

Tobin, A., & Reed, D. (2017). *The Inevitable Rise of Self-Sovereign Identity*. https://sovrin.org/library/ Accessed: 19.05.2022

Toth, K. C., & Anderson-Priddy, A. (2019). Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Security and Privacy*, *17*(3), 17–27.

Wang, F., & De Filippi, P. (2020). SSI in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, 28.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of SSI: An Extended Model of Interpretive Flexibility. *HICSS Proceedings*.