Jan 17th, 12:00 AM

Shaping Governance in Self-Sovereign Identity Ecosystems: Towards a Cooperative Business Model

Tobias Kölbel
Karlsruhe Institute of Technology, tobias.koelbel@kit.edu

Tobias Gawlitza
Karlsruhe Institute of Technology, tobias.gawlitza@student.kit.edu

Christof Weinhardt
Karlsruhe Institute of Technology, weinhardt@kit.edu

Shaping Governance in Self-Sovereign Identity Ecosystems: Towards a Cooperative Business Model

Tobias Kölbel[1,2], Tobias Gawlitza[1] and Christof Weinhardt[1]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
{tobias.koelbel, weinhardt}@kit.edu, tobias.gawlitza@student.kit.edu
[2] Robert Bosch GmbH, Corporate Research, Renningen, Germany
tobias.koelbel@de.bosch.com

Abstract. The Internet has created great opportunities for consumers. With the digitalization wave breaking, Single Sign-On services emerged that satisfy the desire for seamless online journeys and provide users with their digital identities. On a global scale, oligopoly structures evolved where "tech giants" primarily manage identities and personal data. Conversely, recent developments stemmed from the desire for data privacy, digital sovereignty, and self-determination, both from the user perspective and legislature. In line with recent discussions, this study focuses on Self-Sovereign Identity, a new paradigm that promises independence from intermediary identity providers. We follow an appeal for further research on business aspects and strategic alliances and adopt an exploratory research approach with semi-structured interviews. We identify cooperatives as suitable to govern Self-Sovereign Identity Ecosystems, shape their business model along Al-Debei and Avison's V[4]Business Model dimensions, and outline paths for future inquiries.

Keywords: Self-Sovereign Identity, Cooperative, Business Model, Governance

1 Introduction

Today, we live in a world where our digital footprint is rapidly growing. Digital services become increasingly available as digitization progresses. Recently, the Corona pandemic accelerated this development and strengthened the desire for seamless online journeys [1]. This trend has spawned interest in and increased the importance of digital identities (IDs), which are used to identify people, organizations and things in the digital world. Organizations like Apple, Amazon, Google, or Facebook quickly recognized the importance of identification on the Internet [2] and created Single Sign-On (SSO) services that allow users to have one ID across systems. Tied to this convenience is a shift from multiple to a few accounts, where users do not need a separate username and password for each website but rely on the ID service provided by SSO operators. As long as they use this service, users can have a trusted ID and build a reputation. Meanwhile, companies with SSO solutions position themselves as de facto ID gatekeepers, as they have their own isolated data storage, as well as trust and reputation systems that are beyond users' control [1]. By analyzing user data, they further obtain valuable information about individual user behavior, interests, purchases, and locations [3]. However, users often do not know how their data is being processed [4]. As a result, they relinquish control over their data and become transparent and traceable across multiple services [3–6].

17th International Conference on Wirtschaftsinformatik
February 2022, Nürnberg, Germany

Consequently, addressing identification in the digital space, what data is collected about users, where that data is stored, and who owns and controls the data is a complex, timely, and important matter [7]. As the desire for data privacy, digital sovereignty, and self-determination has increased in recent years, the independence from intermediary ID providers becomes more and more prominent [1]. An initiative by the European Union, increasing its focus on digital IDs as a strategic asset, also illustrates this development [8]: *"We want rules that puts people at the center. This includes control over our personal data, which we still have far too rarely today. Whenever an app or website asks us to create a new ID or easily log on via a big platform, we have no idea what happens to our data. That is why the Commission will propose a secure European e-identity."*

A new idea for digital IDs that various initiatives devote their attention to [9] is a technical concept called "Self-Sovereign Identity" (SSI). In contrast to centralized ID systems, the SSI paradigm builds on decentralized technologies like Blockchain [10, 11] and allows users to manage their credentials (e.g., a person's age, organizations' master data, or a machine certificate) independently in self-determined contexts [3, 9]. Without user tracking and with a high degree of interoperability [12], SSI-based ecosystems aim to be user-friendly and economically beneficial[1]. Academic publications on SSI to date examine technological aspects [9], different SSI solutions [12], the user's perspective [14], trust requirements [15, 16], legal prospects [10, 17] and the real-world adoption of SSI [18, 19]. Some authors further emphasize considering SSI as an ecosystem in which technology and governance are intertwined [10, 20]. This perspective sparks interest in research that conceptualizes SSI ecosystems as strategic alliances [11, 18].

The "Secure Digital Identities" (SDI) initiative, a project funded by the German government with more than €40 million, pursues this idea as several consortia develop SSI infrastructures for secure exchanges of digital ID attributes [21, 22]. Referring to SSI ecosystem collaboration, Laatikainen et al. (2021) emphasize the need for further research on business aspects that provide fair value to each actor [7]. We follow this appeal by addressing business models (BMs) in strategic alliances governing SSI ecosystems. Studying BM concepts is not a fairly new endeavor. It has garnered attention in several research disciplines (e.g., strategic management, entrepreneurship, and information systems), but - today - it remains largely unexplored in the SSI domain. In light of its increasing importance, this seems all the more surprising. This study presents the results of an inductive, qualitative approach with expert interviews conducted in collaboration with an SDI project and aims to answer the following research question: *"What are BM design considerations in strategic alliances governing SSI ecosystems?*

The remainder of the paper is structured as follows. First, we introduce SSI and BM fundamentals (Section 2) and describe our methodological approach (Section 3). Then, we analyze the qualitative expert interviews and outline BM design considerations along Al-Debei's and Avison's [23] V^4BM dimensions (Section 4). Finally, we discuss our findings and conclude with an appeal for further research on BMs in SSI (Section 5).

[1] The McKinsey Global Institute estimates the economic value of digital ID programs that aim to strengthen civic and social empowerment at 3 to 13 percent of GDP in 2030 [13].

2 Fundamentals

2.1 Self-Sovereign Identity and its Ecosystem

In essence, the novel topic of SSI may be considered from three different angles, as there is no consensus in the current literature [7]. First, SSI is an ID management system that centers on users in digital environments. It enables them to manage their IDs and associated data in a secure manner without the need for a trusted intermediary to provide or validate information [3, 9, 18]. Second, SSI is a human-centric data management paradigm [7], where self-determined users share their data, either stored locally on their devices or managed decentrally on a (Blockchain-based) network [12]. Third, the SSI concept is tied to an ID protocol that, as an infrastructure component, enables private, secure, and trustworthy communication in the digital space [10].

From a technological perspective, SSI's key components and standards are primarily developed by open source communities and non-profit organizations (e.g., TrustOverIP Foundation) as well as standard-setting institutions and regulatory authorities (e.g., eIDAS, GDPR). At the core of SSI are decentralized identifiers (DIDs) and verifiable credentials (VCs) designed by the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation (DIF). In addition, the encryption-based communication protocol DIDcomm enables secure and private communication.

From an ecosystem perspective, SSI thrives on the symbiosis of technological and organizational interrelation of three actors [7, 10]: issuers, holders, and verifiers. Technically, issuers represent the origin of a credential, determine its creation and meaning, and define the means of verifying associated information. Holders may be individuals, organizations, or other entities that hold a credential in their wallets. They request it from issuers and present it to verifiers upon request. Finally, verifiers are ecosystem actors that may require certain parts of a holder's ID. For example, an e-commerce service may request a user's credit card information. Organizationally, the "digital trust triangle" [20, 24] of issuer, holder, and verifier is managed by strategic alliances that can be organized in various shapes (e.g., a consortia). The alliance organizes the ecosystem regarding business, legal, and technical concerns by publishing a governance framework.

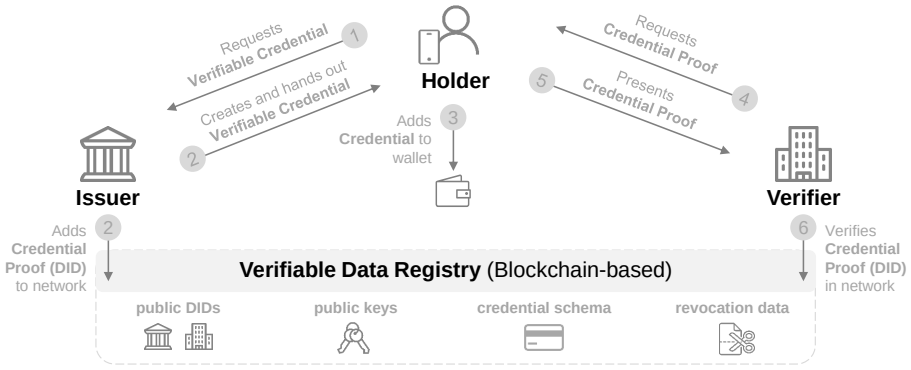

Figure 1. Schematic Representation of the SSI Concept

2.2 Business Models and Representation Techniques

In the late 1990s, the Internet boom triggered research on the construct of BMs. Since then, the research stream gained momentum and is still growing [25]. Despite numerous publications, a clear definition of the term itself is still missing [23, 26]. In general, BMs can be seen as a blueprint or framework that elucidates basic principles of how value is created, delivered, and captured by organizations and their network partners [23, 26–28].

BM representations, as a specific tool to analyze, design, and compare different value-creation and value-capturing approaches, support practitioners in shaping coherent conceptualizations of BMs [29]. Since conceptualization can pursue different goals, various representations exist that differ in their goals and structures [29]. For this research, we build upon the Unified BM Framework proposed by Al-Debei and Avison [23] and apply it as meta-characteristics. Essentially, the framework contains the V^4BM dimensions of "value architecture", "value network", "value finance", and "value proposition".

3 Research Methodology

Our research aims to apply extant knowledge about BM representations to the emerging phenomenon of governance in SSI networks. We follow an exploratory, design-oriented approach to explore this previously uncharted phenomenon inductively with rich contextual insights [30]. Accordingly, we adopt a qualitative empirical research design and conduct semi-structured interviews [31] with experts at the intersection of SSI and BMs.

Following the recommendations of Rubin and Rubin [31], we conducted ten interviews (see Table 1) during the period from May to July 2021. By involving multiple experts with substantial experience in the area of interest, the overarching goal was to collect empirical data from various organizational contexts and explore a broad range of affordances. Consequently, we selected a diverse group of interviewees from a wide range of industries, governmental organizations, and company sizes.

Table 1. List of expert interviews (#1 to #10) with details on interview partners

ID	*Interviewee job position*	*Organizational context*
1	Business Architect Blockchain	IoT Solutions & Services
2	Head of Communication & Deputy Project Manager	Banking Services
3	Project Manager & Cooperative Lead	Banking Services
4	Portfolio Manager Blockchain	Transportation
5	Senior Manager & Project Lead SSI	Connected Industry & Ecosystems
6	Chief Innovation Officer	SSI Solutions & Services
7	Research Associate in SSI	Governmental Institution
8	Senior Information Security Consultant	SSI Solutions & Services
9	Manager Identity & Access Management	Standard-Setting Institution
10	Expert Innovation	Connected Industry & Ecosystems

All interviewees were recruited through the authors' personal network. To avoid an overemphasis of one occupation's expertise and respect the interdisciplinary nature

of our research endeavour, we selected about the same number of interviewees with and without knowledge in BMs. The interview process was conducted virtually and lasted between 32-60 minutes, with an average of 44 minutes. After informed consent, interviews were recorded and transcribed before being returned to respondents for approval to increase the validity of our findings [32]. We conducted the interviews either in German or English to prevent misunderstandings and enhance informative value, depending on the interviewees' native languages. In general, interviews were based on a questionnaire and separated into three parts. The respondents were first asked to describe their experience in the area of interest (e.g., job position and tasks). Then, we asked questions relating SSI value propositions, customer relationships, and network finances. Finally, we moved from key activities and key partners towards questions that address challenges for successfully shaping BMs in SSI ecosystems. Due to the semi-structured nature, we were able to dig deeper when the interviewees mentioned interesting and unexpected insights [30]. In addition, open-ended questions offered the opportunity to describe actual experiences without being limited to a narrow, predefined structure.

As part of a qualitative, cross-sectional analysis [33], we analyzed and coded [34] the interview content using MAXQDA software [35]. In doing so, codes (e.g., "data privacy" and "trafficking user data") were combined into inductive dimensions (e.g., "pains") that relate to deductive categories following V^4BM axioms [23]. This approach allowed us to identify shared perspectives in the experts' perceptions rigorously. We present the results of our analysis below.

4 Qualitative Insights for Business Model Designs

This section presents the results of our qualitative expert interviews (cited with # interview ID), serving as input toward shaping BM designs in strategic alliances governing SSI ecosystems. We introduce why the interviewed experts consider cooperatives the most appropriate legal form to govern the ecosystem and what specific issues they perceive related to BM design (i.e., cross-category remarks). The presentation of findings in subsequent sections follows the V^4BM dimensions We choose this framework because it is parsimonious and includes all BM dimensions mentioned in previous representations [23]. Moreover, its multidimensionality appears appropriate and sufficiently comprehensive to capture all relevant aspects while avoiding conceptual ambiguity. Figure 2 provides a synthesized illustration for the dimensions further described below.

4.1 Cross-Category Remarks

First, experts believe that a **COOPERATIVE LEGAL FORM** is particularly suitable to govern SSI ecosystems through strategic alliances and shape their BM (further referred to as "Cooperative Business Model", CBM). On the one hand, cooperatives would create a legally binding framework, allowing companies to pursue their interests within these boundaries (#9). Nonetheless, a bilateral exchange would promote and strengthen ties between involved actors, resulting in two key benefits: First, it would create a mutually beneficial innovation ecosystem around SSI that could leverage synergies between companies within an industry or even across domains (#3-5). Second, cooperation between

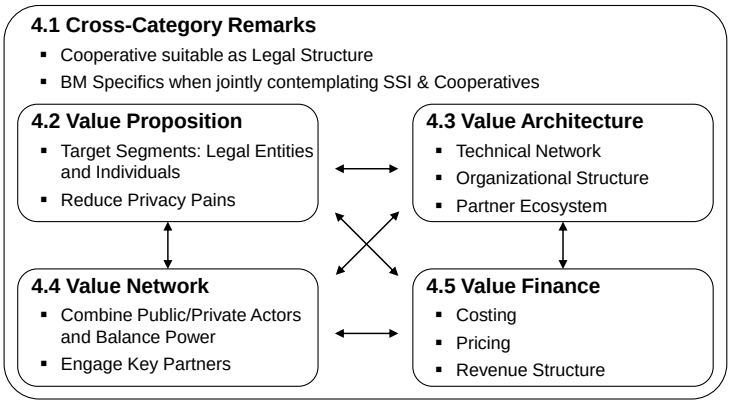

Figure 2. Business Model Design Dimensions

several actors along the entire value chain is essential for decentralized technologies in general to meet both user needs (i.e., seamless online journeys) and the technological requirements of a decentralized network with distributed node operation (#2, #10). On the other hand, the legal form of a cooperative is in line with SSI principles. From a technological point of view, operating nodes in distributed networks would be decentralized; structuring governance as a cooperative would reflect that idea on an organizational level. Some experts also emphasize the de-commercialized nature of cooperatives, which pursue not-for-profit purposes and act on behalf of their users (#1, #5).

Second, experts believe **BM DESIGN SPECIFICS** needs to be respected when jointly contemplating SSI and cooperatives. They argue for the distinction of BMs in SSI ecosystems on two levels: infrastructure and application (#1-2). The infrastructure level deals with the network operation, while the application level refers to actors who use a given SSI network and build their BM on top. As two experts point out, different requirements have to be considered in this context, yet they are closely related (#1, #3). For example, transaction costs set at the infrastructure level influence the feasibility of different services at the user level. Accordingly, experts consider three addressees for BMs: (1) companies that want to build up their own business based on a SSI network, (2) the perspective of individuals who are primarily interested in user-friendly processes and SSO-alike solutions, and (at some point in time) (3) things that need to interact automatically with the system (#5, #7, #10). Related to this is the financing of the network (#3-4, #10). Current models in ID management (i.e., SSO solutions) rely on earning money from user data to provide a service to users for free (#9). However, SSI creates a basic infrastructure where traditional data monetization without user consent should no longer be possible. As a result, the costs incurred for building and operating the ID infrastructure could no longer be cross-financed via data monetization. Accordingly, other forms of financial means have to be identified. This transformation could also impact existing BMs and services offered by companies since data monetization as a traditionally attractive source of revenue would no longer be available. As a result, companies would have to find other solutions to cover their costs for service offerings. Conversely, this could also mean that services that were previously free of charge

would have to be paid for by users. In terms of BMs at the infrastructure level, experts pointed out that cooperatives do not maximize profits but rather have an obligation to the community while primarily aiming to cover their operating costs and make sustainable reinvestments (#2, #6, #8). One author commented that cooperatives do not have a real BM in this context but rather a "sustainability model" (#3). Another issue stemming from the technological design of SSI is that data verifiers receive a significant benefit from the network but cannot be asked to pay for it as the system is designed for privacy. For example, an e-commerce service that wants to verify user data would benefit from an SSI network. However, costs in SSI networks are caused mainly by writing operations (i.e., issuer's expense) and not by presenting (i.e., holder's expense) or verifying (i.e., verifier's expense). Accordingly, adequate solutions have to be developed that reflect both benefits and incentives of each actor (#1, #3, #9-10). Other challenges mentioned in the interviews were the incentivization of cooperative members (CMs) (#1), the coordination of CMs (#3), and the initial agreement on governance rules (#3). One expert also noted that SSI is a greenfield where efforts and benefits are difficult to assess (#8).

4.2 Value Proposition

As part of the value proposition dimension, representing offer and customer segments [23], the interviewed experts believe it is essential to address both issues related to current ID management systems (pains), and the benefits users derive from SSI (gains).

An essential **PAIN**, which also reflects in the public discourse on digital ID [1], is data management by third parties and associated concerns about data privacy and data security. Here, the interviewed experts perceive a particular risk if users do not control their data but rather rely on ID service providers they have to trust. Both the substantial leverage of SSO providers (#2-3, #4-5, #7-9), their ability to block user IDs, which could result in the loss of access to services (#7, #9), and trafficking user data without their consent (#1, #6, #8-10) are perceived to be related aspects. A further issue describes the topological design of traditional ID management systems and a perceived lack of trustworthiness in interactions. On the one hand, central databases would be vulnerable to hacker attacks (#3-5, #7, #9). On the other hand, when a holder presents data to a third party (i.e., a verifying service), they might not be able to verify whether the data truly belongs to the claimant or if it was deceived (#10). Furthermore, it would also be challenging to determine issuer IDs and the validity of the data. On the contrary, users might be confronted with phishing attacks, exposing their data based on false information presented by their counterparts, which they cannot verify unequivocally (#5). Ultimately, another criticized aspect is the lack of interoperability between different SSO providers, which leads to lock-in effects and switching costs (#4).

Identified **GAINS** arising from SSI-based ID networks may be divided into two groups, both considered being target segments of CBMs: legal entities (i.e., companies and institutions) and individuals (i.e., private persons). Experts suggest that LEGAL ENTITIES particularly benefit from process improvements (#1-2, #4, #6). For example, master data and certificates that companies need for interactions along the value chain are (today) usually maintained manually, requiring simultaneous data updates in several databases (push principle). As a result, the effort scales linearly to the product of

customers and suppliers (N*M relationship) or is handled by service providers. As experts see it, this process might be transformed into a pull-based system by using SSI, which would reduce not only costs for redundant data maintenance but also create a single point of truth that would increase data quality (#1-2, #5). At the same time, organizations would retain end-to-end control over their data. For authorities that mainly perform certification activities and frequently have to verify data, digital verifications through VCs would both be a considerable simplification and increase security (#7-9). Furthermore, intermediaries who charge service fees could be prevented, and interoperability between different SSI networks could avoid switching costs by allowing users to own their data and migrate their wallets as desired. Ultimately, improving processes would enhance customer experience and increase security in handling customer data (#9-10).
INDIVIDUALS would significantly benefit from regaining control over their data and having better access to digital services while at the same time avoiding lock-in effects (#3-5). Transparency about who shares what data with whom adds another advantage (#8). SSI further allows for the selective disclosure of information. If, for example, only one attribute (e.g., a person's age) of a credential of several attributes (e.g., an ID card) is requested by a verifier, SSI allows to present only this attribute selectively (#3). Consequently, a service provider only receives data it needs to provide a service. If users do not want traceable profiles, SSI enables them to work with a separate identifier for each service (#9). This could prevent data correlations and brings advantages in terms of privacy and data protection. Furthermore, independence from third parties and flexibility in wallet software choice and data storage are also emphasized positively (#7, #9). In addition, actor authentication in SSI networks (e.g., via VCs) could impede phishing attempts (#3, #5). For example, users who want to register a bank account or initiate a wire transfer should be able to identify their transaction partners (#2-3).

4.3 Value Architecture

The value architecture perspective focuses on a holistic structural design. It encompasses both technological infrastructure and organizational architecture with their respective configurations as well as assets, resources, and core competencies [23]. Experts consider a balanced equilibrium of a technologically trustworthy infrastructure and a transparent model of organizational cooperation to be particularly important in SSI (#1, #5).

The **TECHNICAL NETWORK** forms the first pillar and core of the ecosystem, providing integrity and trust through decentralized technologies that operate on multiple servers (i.e., nodes). In principle, experts propose a hybrid approach where read access to the network's distributed database (i.e., ledger) is unrestricted to facilitate the scaling of applications (#2-3, #10). However, node operation (i.e., stewards), write permissions (i.e., endorsers), and transaction initiations (i.e., transaction author) should be limited to known entities and governed by a cooperative (#3, #5). In addition, to be compliant with regulations on data protection, a suggestion is that the ledger should not hold contextual data (e.g., personal data), but only "reference data" (e.g., via the public key of the issuer of credentials) (#10). However, interoperability between SSI networks and alignment with worldwide standards (i.e., VCs, DIDs, DIDComm) is crucial. Based on these standards, further network and technology development constitutes a cooperative key

activity (#2). Alongside monetary resources, this requires necessary competencies such as human capital (#1, #6, #10). Monitoring technical parameters such as node operation is also considered essential (#4-5). Thus, the cooperative's tasks would include incident management, network maintenance, and bug-fixing to avoid technical malfunctions.

The holistic designs' second pillar consists of the cooperative's **ORGANIZATIONAL STRUCTURE**. Experts anticipate rules and regulations for the interaction between ecosystem CMs - defined in statutes, rules of procedure, and other contracts, that describe the rights and obligations of actors involved - to be crucial for a successful project (#2-3, #7). As long as they sign relevant contracts, it should be possible for any interested legal entity to participate in the network without being CM (#5). These agreements would include stewards, endorsers, and transaction authors. Moreover, structuring the cooperative in several committees and working groups with operational representation by a MANAGEMENT BOARD appears to be a viable strategy (#2-3). Management leads the cooperative's business following committee resolutions and existing contracts (#3). A SUPERVISORY BOARD, elected by CMs (according to the principle of one actor, one vote) and acting as a trustee, appoints and dismiss the management board members. Experts also suggest that the supervisory board should determine preliminary rules of the network at the time of its establishment (#2-3, #5, #10). However, CM should be able to change these rules per prescriptive voting rules (#10). As the third building block, a TECHNICAL STEERING COMMITTEE should deliberate and decide on the network's technical issues and advancements (e.g., development resource allocation) while coordinating with the international developer community (#2-3, #10). The fourth building block might consists of SPECIFIC TOPICS COMMITTEES. These include public relations or legal aspects, IP protection, and compliance with current regulations such as GDPR, eIDAS, and the Money Laundering Act (#2). According to experts, a key competence and potential competitive advantage involve the successful coordination between working groups and committees (#1, #6). Another goal of governance should be to remain efficient in decision-making and maintain trustworthy and non-monopolistic structures as the number of CMs increases. Three experts (#2-3, #5) propose the legal form of the European cooperative (Sociedad Cooperativa Europea, SCE). This would align with European values, be scalable, and allow a high degree of digitization (#2-3).

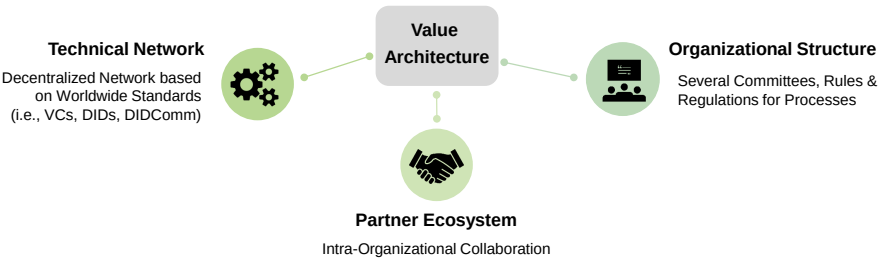

Figure 3. Cooperative Value Architecture Pillars

The third pillar involves building and developing a **PARTNER ECOSYSTEM**. This constitutes the support of cross-company collaboration, for example, by offering use case matching between cooperative partners (#1, #6). Public relations and the availability of

public resources might also be necessary (#3). On the one hand, it would help promote awareness regarding SSI technology and the network and attract new members. On the other hand, transparency might foster trust (#7-8).

4.4 Value Network

The value network construct represents an inter-organizational perspective and describes how transactions are enabled through coordination and collaboration among ecosystem actors [23]. With respect to the CBM, experts distinguish between the organizational structure of network actors and technology-based characteristics that deserve attention.

As for the **ACTORS** of an SSI ecosystem, several interviewees suggest a combination of public and private actors (#2, #4, #7, #10). They argue a balanced mix of CMs would be decisive. This would allow different perspectives and would exploit potential synergies between CMs. Considering a fair value for each CM, a balanced distribution of power is considered vital. Therefore, experts suggest a clear delineation between actor roles and the need to prevent that any actor dominates the ecosystem (#5, #10).

KEY PARTNERS in SSI-based systems would be wallet service providers, as they provide the primary interface between the SSI network and its customers (#6, #8). To avoid lock-in effects, wallets should be network agnostic and allow a certain degree of interoperability (#4, #7). Other partners include standards-setting institutions, as close collaboration is critical to develop solutions that comply with applicable law and enable interoperability among SSI networks (#9-10). If SSI networks handle regulatory use cases such as digital ID cards, governments and public authorities would be another key partner group (#5, #7). Further, the cooperative should foster a dialog with industry associations to ensure that it is informed about specific issues in certain domains (#2-3).

4.5 Value Finance

BMs appear to be strongly related to the economic and financial design of organizations. Therefore, the value finance dimension considers how organizations generate revenue [23]. It includes information on costing, pricing methods, and revenue structure [26], that affect each of the other three dimensions, especially the value proposition [23].

Concerning cooperatives, experts unanimously emphasized that the CBM's primary goal should not be to maximize profits but to cover all expenses of the cooperative. Corresponding **COSTS** would arise through the network's further development. This includes costs for personnel in marketing to increase the network's visibility (#2, #5), the coordination with standard-setting institutions and communities (#2, #9), as well as technical development and maintenance costs for operating the network (#4). In addition, node operation incurs costs (#2-3, #5, #10). According to an expert's estimate, these could amount from €150,000 to €200,000 per year and 25 node operators (#5). Yet, these costs would not have to be borne by the cooperative but by institutions that operate a network node (#3, #5). However, since node operators are essential for network operation, governance has to incentivize them (#1). Several possibilities were discussed during the interviews. One involves a minimum wage for node operation, paid at a fixed rate (#4). Another possibility would be to compensate node operators based on their

actual expenses, distributing the average amount to each operator (#4). Incentivizing nodes indirectly would be another possibility (#3, #10). For example, if node operators would have lower costs for writing operations on the ledger, they could build their own BM that refinances node operations. Non-monetary approaches and intrinsic motivation to operate nodes might also be feasible (#3, #5). One expert refers to this as "skin in the game" (#5), meaning that companies with many use cases based on the ID network would be interested in its stability, and therefore, want to operate their own node.

To **COVER EXPENSES**, experts consider that a CBM can draw on three sources of income. First, membership fees that are collected via annual fees and depend on the size of an organization (#3, #7). While noting that network utilization should, in principle, be open to all, participation in and influence on the network's governance (e.g., in committees) might be conditional on memberships (#2, #5). Second, various security services could provide revenue (#10). For example, a cooperative's certification of trusted wallet software and the issuance of certificates to wallet providers could increase users' trust in a particular service. The third revenue stream might be endorser write permissions, which are required for network transactions. An option for this would be volume packages that allow a certain amount of writes at a fixed price (#3-5). Then, if more writes are needed than a corresponding package contains, companies might automatically switch to a different category (#3). However, this solution entails a problem: mainly issuers perform write operations on the ledger - hence, their costs would be high while having relatively low value (see Section 4.2). For a sustainable CBM, most consulted experts advocate that the cooperative's cost recovery should be based on quantity-based pricing derived from the previous year's costs (#2-5, #7-8). Stewards may receive a fixed amount for operating nodes, factored into the cooperative's costs. The costs incurred could then be divided among endorsers on a source-by-cause basis. Experts suggest not charging for each write operation individually but introducing a consumption index consisting of the write operations of a respective CM divided by the total number of write operations (reference: previous year). To calculate the contribution of each CM, the consumption index could then be multiplied by a cost estimate for the cooperative's following year (#3-4). This process may be governed and monitored by the cooperative's committees and contracts (#3, #5).

5 Discussion and Research Opportunities

In line with recent discussions, this study focuses on SSI ecosystems, as this new paradigm promises independence from intermediary ID providers. Following the appeal for further research on business aspects and collaborative efforts [7], we address BM design considerations in strategic alliances governing SSI ecosystems. To answer our research question, we follow an exploratory and design-oriented approach. Through a qualitative research design featuring semi-structured expert interviews, we derive rich contextual insights that are fruitful for practitioners and researchers.

The presentation of findings follows Al-Debei and Avison's established V^4BM dimensions [23] and provides cross-category remarks. Stakeholders seeking to develop SSI ecosystems can draw on our insights to guide their design. We discuss why cooperatives seem particularly for governance and indicate considerable aspects related to their BM.

Considering both the user perspective of legal entities (i.e., companies, institutions) and individuals (i.e., private persons), our value proposition dimension specifies pains of classic ID management (e.g., SSO systems) and gains arising from SSI-based ID networks. With respect to the value architecture, we identify three crucial pillars that ecosystem orchestrators must consider: Technical network, organizational structure, and partner ecosystem. Experts believe a balanced equilibrium of a technologically trustworthy infrastructure and a transparent organizational cooperation model is essential. Referring to SSI value networks, we propose a combination of public and private actors and identify key partners. The value finance dimension further addresses network costs and suggests possible revenue streams. Experts propose to cover the consortium's costs as primary rationale, as it does not operate for profit but in its users' interest. For essential ecosystem stakeholders, we further outline basic BMs. We highlight that SSI networks' core values are user-centricity and secure data sharing, and CBM design must align with these objectives. Our findings increase transparency in SSI network governance by providing insight into the BM layer and, therefore, set to foster user adoption and trust in SSI ecosystems. Moreover, we enhance the understanding and extend the applicability of the V^4BM Framework [23] to CBMs in an SSI context. We demonstrate that it provides an interdisciplinary framework to strategically structure, analyze, and design novel initiatives. Researchers and practitioners may draw on our findings to communicate BM dimensions and characteristics or add additional elements. This is particularly useful as studies in SSI are a fairly new and rapidly evolving area of research.

Although we took a first step toward shaping governance in SSI ecosystems, there are limitations and numerous areas for future research. We discuss some of these avenues in our work and add three additional directions below. First, our qualitative interviews with experts working in an SDI project may only tell one side of the story. While their assessments are based upon day-to-day experience, all hold strong convictions about SSI's potential. In order to neutrally assess CBM concepts, further research should also embrace the customer perspective. This might entail the understanding and acceptance of SSI systems from a user perspective and other aspects such as SSI's impact on perceived privacy. Evaluating our findings with experts who do not represent an SDI project might also be helpful. Second, SSI is a new paradigm for data management that is dependent on widespread adoption. Our experts point out that SSI could also disrupt existing services offered by CMs (see Section 4.2). Therefore, future research might either (1) investigate the impact of SSI on existing BMs, (2) explore new BM designs based on SSI, or (3) analyze how to leverage SSI and legacy BMs together. Third, our results represent the first draft of a CBM. It can be argued that the concept is still fuzzy and insufficiently defined. We suggest that researchers extend our study to evaluate and, if necessary, revise the findings following an iterative process. For example, surveys with individuals and institutions might provide in-depth insights into anticipated problems and the magnitude of outlined benefits to test hypotheses about value propositions. Further inquiries could also examine the organizational structure and the partner ecosystem of the value architecture in more detail. In addition, studies on optimal value network structures of SSI ecosystems as well as assessments of costs and revenue streams of the value finance dimension might be worthwhile. In general, drawing on the iteration loops' knowledge, we propose to explore CBMs based on prototypes or real-world applications.

References

1. European Commission: Report from the commission to the european parliament and the council on the evaluation of regulation (eu) no 910/2014. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290rid=8 (2021), accessed: 30.08.2021
2. Birch, D.G.: Apple Pay Was Not Disruptive But Apple ID Will Be. https://www.forbes.com/sites/davidbirch/2020/08/29/apple-pay-was-not-disruptive-but-apple-id-will-be/?sh=7b4e67c44d0f (2020), accessed: 30.08.2021
3. Allen, C.: The Path to Self-Sovereign Identity. https://www.coindesk.com/path-self-sovereign-identity (2016), accessed: 30.08.2021
4. Cinnamon, J.: Social injustice in surveillance capitalism. Surveillance and Society 15(5), 609–625 (2017)
5. Zuboff, S.: Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology 30(1), 75–89 (2015)
6. Morley, J., Cowls, J., Taddeo, M., Floridi, L.: Ethical guidelines for COVID-19 tracing apps. Nature 582, 29–31 (2020)
7. Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., Abrahamsson, P.: Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems. In: PACIS 2021 Proceedings (2021)
8. European Commission: European Digital Identity. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity (2021), accessed: 30.08.2021
9. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Computer Science Review 30, 80–86 (2018)
10. Zwitter, A.J., Gstrein, O.J., Yap, E.: Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Frontiers in Blockchain 3, 26 (2020)
11. Zachariadis, M., Hileman, G., Scott, S.V.: Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization 29(2), 105–117 (2019)
12. Naik, N., Jenkins, P.: Self-Sovereign Identity Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology. In: IEEE 2020 Proceedings. pp. 90–95 (2020)
13. White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., Sperling, O.: Digital Identification: A Key to Inclusive Growth. McKinsey Global Institute pp. 1–32 (2019)
14. Ostern, N., Cabinakova, J.: Pre-prototype testing: Empirical insights on the expected usefulness of decentralized identity management systems. In: HICSS 2019 Proceedings. pp. 1834–1843 (2019)
15. Kubach, M., Roßnagel, H.: A lightweight trust management infrastructure for self-sovereign identity. In: Roßnagel, H., Schunck, C.H., Mödersheim, S. (eds.) Open Identity Summit 2021 Proceedings. pp. 155–166 (2021)
16. Grüner, A., Mühle, A., Gayvoronskaya, T., Meinel, C.: A Comparative Analysis of Trust Requirements in Decentralized Identity Management 926, 200–213 (2020)
17. Kondova, G., Erbguth, J.: Self-sovereign identity on public blockchains and the GDPR. In: ACM 2020 Proceedings. pp. 342–345 (2020)
18. Wang, F., De Filippi, P.: Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain 2, 28 (2020)
19. Lockwood, M.: Exploring Value Propositions to Drive Self-Sovereign Identity Adoption. Frontiers in Blockchain 1, 4 (2021)
20. Trust Over IP - Defining a complete architecture for Internet-scale digital trust. https://trustoverip.org/ (2021), accessed: 30.08.2021

21. Bundeskanzleramt: Digitale Identität. https://www.bundesregierung.de/breg-de/suche/whitepaper-oekosystem-digitaler-identitaeten-1881840 (2021), accessed: 20.08.2021
22. Showcase programme “Secure Digital Identities”. https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere _Digitale_Identitaeten/sichere_digitale_ident.html (2021), accessed: 30.08.2021
23. Al-Debei, M.M., Avison, D.: Developing a unified framework of the business model concept. European Journal of Information Systems 19(3), 359–376 (2010)
24. Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., Reed, D.: The Trust over IP Stack. IEEE Communications Standards Magazine 3(4), 46–51 (2019)
25. Zott, C., Amit, R., Massa, L.: The business model: Recent developments and future research. Journal of Management 37(4), 1019–1042 (2011)
26. Osterwalder, A., Pigneur, Y., Tucci, C.L.: Clarifying Business Models: Origins, Present, and Future of the Concept. Communications of the Association for Information Systems 16(1), 1 (2005)
27. Chesbrough, H., Rosenbloom, R.S.: The role of the business model in capturing value from innovation: Evidence from Xerox Corporation's technology spin-off companies. Industrial and Corporate Change 11(3), 529–555 (2002)
28. Osterwalder, A., Clark, T., Pigneur, Y.: Business Model Generation: A handbook for visionaries, game changers and challengers. Wiley (2010)
29. Veit, D., Clemons, E., Benlian, A., Buxmann, P., Hess, T., Kundisch, D., Leimeister, J.M., Loos, P., Spann, M.: Business models: An information systems research agenda. Business and Information Systems Engineering 6(1), 45–53 (2014)
30. Paré, G.: Investigating Information Systems with Positivist Case Research. Communications of the Association for Information Systems 13 (2004)
31. Rubin, H.J., Rubin, I.S.: Qualitative interviewing: the art of hearing data. SAGE (2011)
32. Brink, H.I.: Validity and reliability in qualitative research. Curationis 16(2), 35–38 (1993)
33. Wilde, T., Hess, T.: Forschungsmethoden der Wirtschaftsinformatik Eine empirische Untersuchung. Wirtschaftsinformatik 49(4), 280–287 (2007)
34. Corbin, J., Strauss, A.: Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory. SAGE Publications, Inc. (2008)
35. P. Mayring: Qualitative content analysis: Theoretical foundation, basic procedures and software solution (2014)