6-17-2021

Self-Sovereign Identity Ecosystems: Benefits and Challenges

Gabriella Laatikainen
University of Jyväskylä, gabriella.g.laatikainen@jyu.fi

Taija Kolehmainen
University of Jyväskylä

Pekka Abrahamsson
University of Jyväskylä

SELF-SOVEREIGN IDENTITY ECOSYSTEMS: BENEFITS AND CHALLENGES

Research paper

Gabriella Laatikainen, Faculty of Information Technology, University of Jyväskylä, Finland, gabriella.laatikainen@jyu.fi

Taija Kolehmainen, Faculty of Information Technology, University of Jyväskylä, Finland, taija.s.kolehmainen@jyu.fi

Pekka Abrahamsson, Faculty of Information Technology, University of Jyväskylä, Finland, pekka.abrahamsson@jyu.fi

Abstract

Verifiable credentials, coupled with decentralized ledger technologies, have been potential providers of trustworthy digital identity for individuals, organizations, and other entities, and thus, potential enablers of trustful digital interactions. The rapid development of this technology—called self-sovereign identity (SSI)—and the ecosystems built around it have been fostered even more by the societal needs stemming from the current pandemic crisis, when governments, non-profit organizations, businesses, and individuals are working together on different aspects of SSI to enable mainstream adoption. In this study, we build on rich qualitative data gathered from SSI experts and practitioners to give a fresh overview of the perceived benefits and challenges of SSI. The paper advances research on the domain of SSI adoption and provides valuable insights into the feasibility of SSI for practitioners both in the private and public sectors.

Keywords: self-sovereign identity, decentralized identity, SSI benefits, SSI adoption.

1 Introduction

In the current global situation – burdened by, e.g., a vast number of people living without a formalized form of identification, the refugee crisis in Europe, and the corona crises -, providing private and secure digital identity for individuals, organizations, and other entities (e.g. IoT devices), is crucial. The emerging self-sovereign identity (SSI) technology holds the promise to offer a new digital identity infrastructure for the post-industrial age. Around the world, several governments are developing digital identity ecosystems that facilitate trustworthy digital transactions (e.g. the ESSIF initiative of the European Union[1]; ESSIF, 2020, Biometricupdate, 2020) and there are several SSI solutions under evaluation for different use cases, such as healthcare (Lumedic Connect; Lumedic, 2021) and travel passport (IATA, 2021). Furthermore, there are SSI systems in production, such as (1) the Kiva digital identity protocol providing digital and financial inclusion for citizens of Sierra Leone (Kiva, 2020; Wang and De Filippi, 2020), (2) the Building Blocks of World Food Programme, a biometric identity solution, providing better delivery of food assistance and other services for people in need, for example, in Jordan and Bangladesh

[1] Other countries include Canada, New Zealand, Australia, Saudi Arabia, Philippines, Pakistan, Kurdistan, Kyrgyzstan, Bermuda, India and The Bahamas.

(WFP Building Blocks, 2020; Wang and De Filippi, 2020) and (3) the Verifiable Organizations Network in Canada providing a secure and trustful way of data storage and data exchange for governments and organizations (VON, 2020).

The concept of SSI relies on distributed ledger technologies (a broader class of "blockchain-inspired" technology; Zachariadis et al., 2019) and verifiable credentials (i.e., a tamper-evident credential that has authorship and can be cryptographically verified; W3C, 2020) and provides the users with digital identity in a decentralized manner without trusted third parties (Naik and Jenkins, 2020). As a distinction to decentralized identity systems, the SSI paradigm has additional requirements that ensure the users' sovereignty of their identity and the storage-control of the associated confidential data linked to their identity (Naik and Jenkins, 2020). Self-sovereign identities should be secure (i.e., the identity information must be kept secure), controllable (i.e., the user must be in control of who can view and access their data), and portable (i.e., the user must be able to use their identity data wherever they want, and the data should not be tied to a single provider) (Allen, 2016; WebOfTrust, 2017; Tobin and Reed, 2017). It should be noted that the assumption that an SSI solution fulfills all requirements is not fully plausible (Wang and De Filippi, 2020).

Besides its capability of reforming the authentication and authorization, the SSI technology may also enable developing and transforming organizational processes in many industries by providing trustful digital identity to other entities, such as organizations and things (Lemineux, 2017). For example, SSI solutions are able to solve issues related to the privacy and identification of patient data in digital healthcare systems, they might verify the steps in a supply chain, and they might establish trustful communication and transfer of value with customers, partners and regulators in business ecosystems (Zwitter et al., 2020). SSI systems can also enable the creation of new business models, such as stablecoins (i.e., value-stable cryptocurrencies) or identity insurance schemes (Wang and De Filippi, 2020).

SSI is an emerging technology and thus, our current understanding of the phenomenon is rather limited. There are a few studies investigating the technology aspects of SSI (e.g. Dunphy & Petitcolas, 2018; Mühle et al. 2018; Naik & Jenkins, 2020), trust requirements (e.g. Grüner et al. 2020), user requirements (e.g. Ostern and Cabinakova, 2019), and philosophical and legal perspectives of identity (Zwitter et al. 2020). In their study, Wang and De Filippi (2020) describe two real-world cases of SSI adoption focusing on implementation details (2020); however, the literature lacks empirical studies providing a deeper understanding on SSI adoption and especially, providing insights on the behavioural foundations of the managers who make the adoption decisions.

Adopting different technologies is a major management decision made by individuals rather than organizations (Benlian & Hess, 2011). We draw on the theory of reasoned action (Ajzen & Fishbein, 1980) and suggest that the managers' intention to adopt SSI depends on their attitude toward adopting the technology, which is influenced by their salient behavioural beliefs in this regard. Decision makers evaluate future outcome scenarios by balancing the benefits and the challenges associated with SSI adoption and this process can be understood and framed as reasoned action. Thus, in order to deepen our understanding on SSI adoption, we focus on identifying the key benefits and challenges of the technology, as they are perceived by experts working toward SSI adoption. We base our results on rich qualitative data gathered in a field study carried out in close collaboration with (1) a partner company aiming to build SSI infrastructure in Finland, as well as (2) several domain experts who are contributing members in a standard-setting organization working on global SSI standards (i.e., the TrustOverIP Foundation; TrustOverIP, 2020).

In this study, we build on Moore's (1996) definition of innovation ecosystems and define SSI ecosystems as innovation ecosystems describing the collaborative effort of a diverse set of actors toward innovation. In these ecosystems, the key actors are the infrastructure providers delivering a technology and governance dual framework, as well as various partner companies and end customers that provide complementary products and services as well as demands and capabilities. Based on the literature and our investigation, we argue that SSI solutions consist of the components (1) technology solution, (2) governance framework, and (3) business models, and they reside in (4) an environment governed by laws, regulation, and social norms. Using this definition, we describe the perceived benefits and challenges

related to these components. Our findings contribute to the research on SSI adoption and provide valuable insights on the feasibility of SSI for practitioners both in the private and public sectors.

In the next section, we give an overview of recent work. In Section 3, we describe the methodology while in Section 4, we the findings of the study are presented. In the final section, we discuss the findings and limitations of the research.

2 Recent work

2.1 Self-Sovereign Identity Ecosystems

Identity and identification have been investigated from different viewpoints and theories, such as the concept of identity in organizations and online communities, identification infrastructures, and technological, societal, and policy decisions (Whitley et al., 2014). SSI, however, is an emerging concept that can be viewed as (1) an identity management system, (2) a human-centric data management paradigm, or (3) an identity protocol. First, in contrast to the central identity management system, SSI is a decentralized identity management system: it enables individuals, organizations and other entities to manage their identity and associated confidential data by storing them on their own devices locally, or remotely on a distributed network, and by giving access selectively to authorized third parties, without the need to refer to any trusted intermediary to provide or validate these claims (Mühle et al., 2018). Second, SSI can be considered as a human-centric data management paradigm where the users own and control their identity and the personal data linked with their identity (Naik and Jenkins, 2020). Third, SSI can be viewed as an identity protocol, a commodity providing secure, private and trustworthy data storage and communication (Zwitter et al., 2020).

The concepts of SSI and decentralized identity are typically used as synonyms, and there is no consensus in the literature and among experts on the definition of SSI. However, there is a general understanding that SSI "is intended to preserve the right for the selective disclosure of different aspects of one's identity and the various components thereof, in different domains and contextual settings" (Wang and De Filippi, 2020, p. 9). SSI solutions are recommended to incorporate 12 principles that can be used to assess their self-sovereigneity: representation, interoperability, decentralization, control and agency, participation, equity and inclusion, usability, assessibility and consistency, portability, security, verifiability and authenticity, privacy and minimal disclosure, and transparency (Sovrin 2021). While the technology enables fulfilling all these requirements, the actual implementation depends on the governance framework of the solution. It can be noted that the assumption that an SSI solution fulfills all requirements is not fully plausible (Wang and De Filippi, 2020).

Currently, several open-source communities, standard-setting organizations and non-profit organizations[2] aim to define, standardize and provide tools for the SSI architectures and the digital interactions that these enable. There exist some laws and regulations related to digital identification, data exchange, and protection (e.g., eIDAS, GDPR, Data Governance Act, Pan-Canadian Trust Framework); however, there is still legal and regulatory uncertainty in the global SSI market. While there is currently no global standard for SSI implementations, the most prevalent components of SSI technology are proposed by the World Wide Web Consortium[3] (W3C, 2020) and the Decentralized Identity Foundation[4] (DIF,

[2] These include, for example, the World Wide Web Consortium, Decentralized Identity Foundation, TrustOverIP Foundation, MyData, Sovrin, Hyperledger, Open Identity Exchange, CULedger, Internet Engineering Task Force (IETF), OASIS, OpenID, FIDO Alliance, Alastria, uPort, Civic, Alastria, SelfKey and Global ID.

[3] The World Wide Web Consortium (W3C) is supported by major internet and technology companies, universities and governments, such as Amazon, Apple, Boeing, Cisco, Microsoft, Google, Facebook, Alibaba, Tencent, and Baidu.

[4] The DIF is supported by most of major blockchain identity and data companies, such as Hyperledger, Accenture, Mastercard, RSA, Microsoft, IBM, Sovrin, Civic, uPort, and BigChainDB.

2020). The concept of SSI ecosystem has been promoted by a standard-setting organization, the TrustOverIP Foundation[5] (TrustOverIP, 2020). While other decentralized identity communities concentrate on some aspects of SSI solutions (e.g., technological) or some of the industries (e.g., healthcare), the TrustOverIP Foundation focuses on global, "internet-scale" (i.e., pan-industry and cross-country) SSI solutions and the ecosystems built around the technology.

The main components of decentralized identity systems are the decentralized identities (DIDs; DID, 2020) and a secure, private, and encryption-based communication protocol called DIDComm (DIDComm, 2020). DIDs are URL-based identifiers that ensure the portability of the credentials without the need to reissue them (DID, 2020). DIDs are typically used together with verifiable credentials and verifiable claims that enable making any number of attestations about a DID subject that grant access to rights and privileges to trusted authorities (Dunphy and Petitcolas, 2018). The DIDComm specifies the communication between DIDs such as issuing credentials, connecting and maintaining relationships, and providing proof. It is designed to be private, secure, interoperable, transport-agnostic, and extensible (DIDComm, 2020; Windley, 2020). Several companies contributed to implementations of DIDComm by providing libraries, applications and agents in different languages, such as Phyton and .NET (DIDComm, 2020).

SSI solutions are typically developed and managed by a collaborative effort among several actors that form an ecosystem (Wang and De Filippi, 2020). In SSI ecosystems, there are three key roles that together form "the digital trust triangle" presented in Figure 1: issuers, holders, and verifiers (TrustOverIP, 2020; Davie et al., 2019). *Issuers* are the source of credentials; they determine the credentials to be issued and the meaning of these credentials, and the validation method of the information assigned to the credential. *Holders* can be individuals, organizations, or other entities. They request credentials from issuers, and they hold and present them when requested by verifiers and approved by the holder. *Verifiers* request the credentials they need, and then follow their own rules to verify the authenticity and validity of these credentials. The interaction of these roles are managed by a *governance authority* that may represent any set of issuers organized in different forms (for example, consortia, cooperative, government). Governance authorities are responsible of publishing a governance framework that consists of rules for managing the ecosystem: the business, legal, and technical policies for issuing, holding, and verifying the credentials. For example, in a payment card ecosystem (e.g., Mastercard), the governance authority is Mastercard, the holders are the individuals or businesses applying for Mastercard, the issuers are the banks and credit unions, and the verifiers are merchants enrolled in the Mastercard ecosystem that accept payment cards. (TrustOverIP, 2020)

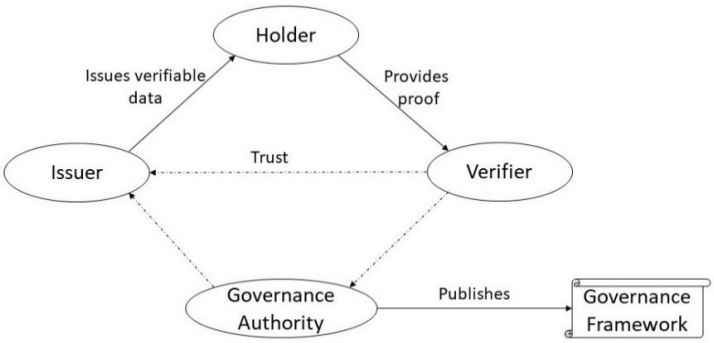

Figure 1. The digital trust triangle (TrustOverIP, 2020).

[5] The TrustOverIP Foundation was founded in May 2020. It aims to combine the open standards, architectures, and protocols developed in other standard setting organizations and technical development partners. Currently, it has more than 150 members, with steering members such as IBM, British Columbia, Accenture, Evernym, Finicity, CULedger, LG CNS IdRamp and Futurewei.

In SSI ecosystems, the trust among actors is established through peer-to-peer interactions assured by (1) the technology that provides secure and immutable data storage and data exchange, and by (2) the governance frameworks consisting of technical, business, and legal rules and policies (Davie et al., 2019; TrustOverIP, 2020). Thus, SSI solutions refer not only to a technological solution, but also require a governance framework, and these two building blocks are interrelated (Zwitter et al., 2020).

2.2 Adoption of Self-Sovereign Identity

Being an emerging technology, the majority of SSI solutions are in pre-adoption phase when the perceptions of decision makers are crucial. The theory of reasoned action (Ajzen & Fishbein, 1980) provides a base to understand the complex cognitive processes that influence individuals' adoption behavior. The decision making process performed by managers can be viewed as cognitive evaluation of different alternatives and the following outcomes. Managers evaluate the advantages and disadvantages of the technology to determine the benefits and the challenges related to its adoption and this process can be conceptualized as reasoned action. Thus, in order to understand the phenomenon, we overview recent work on the benefits and challenges related to SSI and blockchain/DLT adoption.

Current literature describes SSI as a technology that facilitates innovations, cost savings, and increases in job performance (Zwitter et al., 2020). SSI might provide an opportunity to hinder the oligopoly structure of today's Internet where digital identities and personal data are primarily managed by the "Tech Giants" (Apple, Microsoft, Google, Amazon, Facebook; Der et al., 2017). The key challenges in SSI adoption are technical challenges (Wang et al., 2019), the tension between the allocation of citizenship and “innate” individual rights (Gstrein and Kochenov, 2020), the challenge of providing a backup mechanism for lost, stolen, or broken digital identity (Wang & De Filippi, 2020; Zwitter et al. 2019), security and privacy challenges (Wang & De Filippi, 2020), and the challenge of embedding classical privacy and data protection safeguards into technology (Zwitter et al. 2019).

One of the central technology behind SSI is blockchain/DLT. A recent literature review by Upadhyay (2020) groups blockchain opportunities in different categories, such as (1) business practice and excellence (e.g., development of new business models, achieve new revenue streams, lower transaction risks, business process automation), (2) legal benefits (e.g., establishing trust and transparency, building a semantic legal layer), (3) sectoral-specific benefits (e.g., benefits related to finance, government, healthcare), and (4) others (e.g., data provenance, scalability, standards and benchmarking). It has to be noted, that in all these categories, the opportunities of an “effective identity and authentication management system,” “trust and transparency,” and “reliability and trustworthiness” are well emphasized. Furthermore, the growing body of literature on the challenges related to blockchain/DLT adoption can be grouped into several key themes: (1) lack of clarity (e.g., insufficient knowledge, unclear running costs), (2) security and privacy issues (e.g., loss of keys, cyber-attack), (3) lack of standards and interoperability issues, (4) legal barriers (e.g., accountability, SLA, complex semantic legal layer), (5) high costs, (6) complexity of technology, and (7) governance issues (Wang et al., 2019; Upadhyay 2020; Prewett et al., 2020; Chang et al., 2020; Clohessy & Acton, 2019; Schuetz and Venkatesh, 2020; Queiroz et al., 2020; Queiroz and Wamba, 2018).

In summary, while recent work on SSI and blockchain/DLT adoption offers insights into the phenomenon, the literature lacks studies focusing explicitly on SSI adoption and the practitioners’ behavioral perceptions of its benefits and challenges. Moreover, studies suggest that SSI cannot be studied only from the technological viewpoint but investigating its adoption requires a holistic approach. Thus, in this study, we chose to investigate the phenomenon from an ecosystem perspective, focusing on technological, governance, business, and legal and regulatory aspects.

3 Research method

SSI is an emerging technology and thus, changes in the SSI market happen rapidly. To bridge the gap between practitioners and researchers, we chose an exploratory qualitative approach that enables encompassing empirically rich and detailed data related to an emerging complex phenomenon based on

human actions (Edmondson and McManus, 2007; Myers, 2009). We collected the data by conducting field research. Field research involves gathering data using a variety of methods, such as direct observation, interaction with community members, collective discussions, participation in the life of the community, and analyses of data produced within the community. (Myers, 2009)

The study was carried out between April 2020 and February 2021. In this study, we collaborated closely with an IT service provider company in the form of a research project. This company has been developing an SSI infrastructure together with other private organizations and public institutions. As a part of this work, we joined a standard setting organization, the TrustOverIP Foundation (for a short description, please refer to Section 2, footnote 5; TrustOverIP, 2020) as contributing members. During this time, we have established connections with several key domain experts and observed SSI ecosystems in a real context. In our research, we focused on investigating the main characteristics of these ecosystems, the perceived drivers of different actors, and the challenges of orchestrating SSI ecosystems and adopting SSI.

3.1 Data collection

We collected data for this research from several sources. First, we actively collaborated with our partner company in the form of project meetings, informal discussions and emails related to their SSI ecosystem. Second, one of the authors actively participated in TrustOverIP meetings, email conversations, and informal discussions to create a survey for TrustOverIP members that aims to (1) understand the current state-of-practice of SSI adoption, benefits, and barriers, and (2) identify members with common interest and foster active collaboration. In this task, 17 members were asked to provide input and validate the survey questions. We exchanged several emails and organized four meetings to refine the questions. The survey is in the exploratory data collection phase, and the results are not included in this study; however, we used the gathered insights in this work. Third, to advance our understanding of the phenomenon, we participated in webinars and university lectures given by experts. Fourth, we actively followed news, social media postings, and the conversations of the TrustOverIP and MyData communities via Slack. We collected insights from the websites of several companies, non-profit organizations, and standard-setting organizations that are relevant in this domain. The most important events are listed in Table 1; however, the authors have had earlier experience with other blockchain-related research and empirical work that are not included as a form of data collection for this study.

Events	Duration
Project meetings with our collaborative partner and research group meetings	35 meetings with an average of 60 minutes
Active participation in TrustOverIP meetings	5 meetings of cca. 60 minutes
Active participation on webinars (TrustOverIP Launch Event, 2020; Evernym, 2020)	2 webinars sum. cca. 160 minutes
University lectures and webinars by key domain experts (not live) (e.g., Reed, 2020; Nasr, 2020; Jordan, 2018; Tobin, 2019)	4 lectures sum. cca. 280 minutes
Summary	47 hours 20 minutes

Table 1. List of events.

We systematically gathered our observations for further analysis in the form of field notes. First, we listed our observations in the format of date, source, person, and observation/key insight. Second, we took screen captures of some parts of the presentations. Third, we recorded some relevant parts of the meetings. Fourth, we extracted relevant data from Slack chat records, the chat history of the webinars, presentation slides, lectures and websites.

The active collaboration with SSI experts in several forms, as well as following the news, webinars and discussions of the SSI community actively, helped us considerably to understand the phenomenon. How-

ever, in order to get further insights, as an additional data source, we carried out seven in-depth interviews with domain experts. These interviews followed an open-ended interview structure (Darke et al., 1998), and their length varied between 36–68 minutes. These were two group interviews and five individual interviews. All interviews were recorded and transcribed. Table 2 provides an overview of the informants.

Interviewee	Organization/Institution Type	Position at the Organization/ Institution	Other affiliations	Number of interviews
Interviewee 1	IT Service Provider, Organization A	Senior Blockchain Consultant	MyData[6] member	two group interviews
Interviewee 2	IT Service Provider, Organization A	Head of Innovation Center	MyData member	two group interviews and one individual interview
Interviewee 3	Public Digital Trust Service Provider (government), Institution B	Executive Director	Executive Director of the TrustOverIP Foundation	one group interview
Interviewee 4	Provider of Platform for Verifiable Credentials, Organization C	Chief Trust Officer	TrustOverIP Steering Committee Member, W3C DID Co-editor, Sovrin[7] Co-Chair, OpenID Foundation[8] Founding Board member, Identity Commons[9] Steward	one group interview
Interviewee 5	Innovative Consultant Services Provider, Organization D	Founder and CEO	TrustOverIP member	two individual interviews
Interviewee 6	Innovative Consultant Services Provider, Organization E	Consultant and Advisory	TrustOverIP member, DIF contributor, Identity Defined Security Alliance[10] Member, Sovrin Board Member	one individual interview
Interviewee 7	-	-	TrustOverIP member, Sovrin member	one individual interview

Table 2. List of informants.

As observed in Table 2, our interviewees were active contributing members in one or more standard-setting organizations or other non-profit communities in the digital identity domain. Furthermore, they have had work experience in this area for several years in distinct roles. Two of the interviewees were founders of the TrustOverIP Foundation. The diversity of the background of our interviewees made it possible to gather insights from different viewpoints. The interview questions were personalized around the viewpoints and key themes listed in Table 3.

[6] https://mydata.org/

[7] https://sovrin.org/

[8] https://openid.net/

[9] https://www.idcommons.org/

[10] https://www.idsalliance.org/

Viewpoint	Key themes
Open-source communities and standard setting organizations	– SSI ecosystems in general (e.g., definition, key terms) – The roadmap toward mass adoption – Challenges in the journey toward mass adoption – Reasons for founding the TrustOverIP Foundation
Organizational perspective	– The perceived risks and benefits of SSI ecosystems – The key barriers to orchestrating SSI ecosystems and adopting SSI – How customers and other partner companies perceive the value of SSI ecosystems – Organizational factors impacting the attitude towards' SSI ecosystems
Individual perspective	– Personal incentives to work in SSI domain and contribute – Personal objectives

Table 3. Themes for the interviews.

As part of preparation for the data analysis, we combined the data from different sources (field notes, interview transcriptions, etc.). We extracted the relevant information collected in picture and video formats into concise text. As a result, we had cca. 80 pages of relevant data.

3.2 Data analysis

The aim of this study was to identify experts' behavioral patterns from qualitative data consisting of field notes and the transcription of the interviews. Thus, we analyzed the data systematically in an iterative manner using open coding, axial coding, and theoretical coding. In the *open coding* phase, we summarized different parts of the text using succinct codes by applying the constant comparative method (Locke, 2002; Myers, 2009). We concentrated on identifying the aspects that appeared to have significant relevance to the phenomenon. In this phase, the coding was concrete, detailed and, in most cases, followed the wording of the original text (Gioia et al., 2013; Strauss and Corbin, 1994). This phase resulted in several codes, such as "trust in government", "feasibility", "interoperability", "lack of data policies", and "digital inclusion".

In the *axial coding* phase, we focused on finding regularities, patterns, explanations, and causalities between the codes. Based on our observations, we assigned the codes into broader categories using tables that represented different aspects of the phenomenon, such as "Organizational and institutional benefits", "Challenges related to governance of collaborative ecosystems" and "Challenges related to business models".

In the *theoretical coding* phase, we draw on the theory of reasoned action in order to formulate a model that provides researchers and practitioners with a holistic view of the human behavioral patterns and perceptions of the experts towards SSI. Thus, in this phase, we assigned the categories into the following broader categories: (1) Feasibility, (2) Benefits and (2) Challenges.

Finally, we carried out discussions related to this model and its items both in our research group and with experts from our collaborative firm. In all phases of data analysis and validating discussions, we renamed, merged, relocated and deleted the codes several times to eliminate the repetitions and illogicalities. In the end, all authors and the experts of our collaborative firm agreed on the proposed model.

4 Feasibility of adopting SSI and orchestrating SSI ecosystems

Like other technologies, SSI does not provide a solution for every problem in every context. The decision on possible adoption is very complex and depends on several factors. First, our interviewees agreed that the feasibility of SSI depends, among others, on the purpose of the usage:

"Everybody has digital ID, it's just whether it's verifiable or not. Whether you absolutely need to have verifiable, I think in the medical situations that would be essential of course. I wouldn't want someone working on me who I couldn't verify is actually a doctor."

Second, the value of SSI depends largely on the characteristics of the industry (e.g., the level of automatization, data sensitivity) and the legacy systems and processes that need to be changed. As one of our interviewees described:

"When we talk about our customers, and the kinds of problems that we solve with […] SSI is relevant […] for example in certain instances where the customers are end consumers. Like, for example, in banking or in public sector services. If you think about social insurance institution for example where a lot of their processes still rely on paper and paper documents, unstructured data […] and there's a lot of fraud involved. Or insurance companies […] or healthcare welfare. We believe that these sort of solutions will have a huge impact."

One of our interviewees summarized that SSI is a technology that should be used in all cases when there is data exchange outside of organization borders:

"If there is data which is purely internal to certain organization, and there is no need to share that data with anyone else, or there is no need to get information from anyone else, then obviously there's no use case. You shouldn't use SSI for that. Or SSI is not a tool to share information within an organization, but if ever there's a need to interact with the outside, then you would need these sort of solutions I'd say. And also, maybe another one is that let's say that we are dealing with the sensor data and there might be huge amount of data streaming data. Then obviously you use SSI for that. You might use SSI in relation to it to provide context and access to people to that streaming data, but the actual streaming data shouldn't flow through the type of systems that we are developing here."

All the data sources agreed that SSI requires fundamental changes in existing systems and processes, and thus, adopting the technology is not always feasible:

"There are use cases where SSI does not fit. […] some of those federal customers who […] need to make huge changes in the specific ecosystem, […] and their, systems are so desperate that in order to move or change their ecosystem it definitely has to happen a complete technology shift."

In summary, based on our investigation, the feasibility of adopting SSI depends on whether the perceived benefits outweigh the perceived sacrifices required from different actors in the ecosystem. We provide a deeper overview of these in the next subsections.

4.1 Benefits of SSI ecosystems

Our data sources argue that SSI provides a fundamental change in the digital world by facilitating trustful, private, and secure digital interactions, and this implies numerous benefits for society. They describe SSI as a technology that enables the user to control his own data and, therefore, to have the power to disrupt industries and business models. Experts argue that SSI promises equity, liberty, and digital inclusion when these ecosystems are adopted for different use cases, such as digital voting, digital education, or providing identity for third-world citizens or migrants who lack formal identification documents.

The interviewees believe that organizations should prioritize digital trust by adopting SSI to remain competitive in the market. They argued that SSI has not only operative but also strategic value: SSI facilitates customer retention, new opportunities to develop innovations, the possibility to increase financial performance, cost saving, new revenue streams, new business models, and resource efficiency.

Working in this domain typically results in finding strategic alliances, new ways of value creation, and joint actions. Our informants are actively collaborating in several open-source communities, non-profit organizations, and SDOs that play an important role in forming strategic alliances. These communities offer a possibility to learn, get to know new people, but also a possibility to validate a certain SSI solution and achieve interoperability in an uncertain regulatory environment and immature technology. Co-learning and the importance of building long-term relationships were mentioned by the interviewees as typical relational value that SSI ecosystems offer to them. In Table 4, the key benefits of SSI ecosystems are summarized in two categories: benefits for society and benefits for organizations and institutions.

Category	Key benefits
Benefits for society	– Trustful, private and secure digital interactions – Global and interoperable identity – Digital transformation – Data owners' possibility to control their data – Equity – Digital and financial inclusion – Simplified processes and better user experience
Benefits for organizations and institutions	– More private and secure products and services – Development of innovations (e.g., new services, intellectual properties, business models) – Increased financial performance (i.e., cost savings and increased revenues) – Simplified, secure, and private processes – Competitive advantage – Development of strategic alliances and long-term relationships – Better resource efficiency – Opportunity to learn and innovate – Improved brand and reputation – Increased customer' retention, satisfaction, and customers' trust – Regulatory compliance – Rapid and more efficient implementation of business processes – Reduced risks (e.g., money laundering, cyber attacks)

Table 4. Benefits of SSI.

4.2 Challenges in adopting SSI and orchestrating SSI ecosystems

Many of our interviewees saw SSI as an Internet protocol, a commodity, like SMTP or TCP/IP. Therefore, transforming existing processes to be run on SSI infrastructure requires fundamental changes and high upfront investments. Even though SSI has proven benefits, these benefits come only after a long period, while business decisions are made from a short-term perspective. One of the interviewees explained that SSI adoption is risky and requires high investment:

"What we have understood during the years is that blockchain is not inherently a disruptive technology. It's more, it's a foundational technology. Or a solution area which basically means that we need to rethink from the bottom-up, how to approach things. And this is usually a challenge for companies because many of the solutions that we are working on already have some level of established way of doing them. So, we need to always justify, what are the big benefits of rethinking this and restructuring the way that it's currently done. Even though, if we see and everybody sees that in the long term there are even […] tenfold benefits, it still is a huge business risk, to start a transformation from the current, possibly centralized way of doing things into a more decentralized approach. So, it's really always a matter of risk in this business. […] any kind of blockchain or distributed network we see is a high risk, high gain type of thing."

SSI ecosystems typically require collaboration among different actors: profit and non-profit organizations, private and public institutions, providers, and customers. Different actors perceive the value of SSI in different ways. Thus, one of the key challenges is to provide proper incentives and justify the value of inducing collaboration and active engagement. As one of our interviewees explained:

"Everyone needs to agree on joint… let's say, vision. And each one needs to, have their own, sort of business justification to start developing these industry platforms. So that's, that's the main challenge. How to agree on things and development roadmap and governance model in general. But first and foremost, the business value of these industry platforms. That is typically the biggest challenge.…"

Developing a suitable business model and acquiring funding in collaborative ecosystems of public and private organizations is perceived as a key challenge. Some interviewees explained that the incentives

to change strong registry-based legacy systems should come from the market to convince public authorities. Business models should be developed from an ecosystem point of view, as they should provide value for each actor.

One of the key challenges comes from the technological immaturity and lack of interoperability between different technological components and SSI solutions across different countries and industries. There is a high need for standards and legal and regulatory frameworks to reduce risks related to SSI adoption. This is explained by one of our interviewees who founded the TrustOverIP Foundation, a standard setting organization for SSI ecosystems:

"If you think about this a little bit, in the end, why did we do TrustOverIP? Well, it's because we wanna reduce uncertainty. People need to make decisions and… they need a framework in order to guide their decision-making. Because total uncertainty means non-adoption or, inability to interoperate, from a business, from a personal perspective… how do we reduce uncertainty and take away the right, kinds of things, the decisions that don't need to be made again and again and again, so that they can just focus on the specific things that are for their particular activity…. we need to facilitate a common decision-making model so that we know how to, then, identify the pieces of our business or our government, the things that allow us to have trusted interaction."

One of the adoption barriers is information asymmetry and a lack of knowledge and understanding of SSI. SSI concerns many actors with a diversity of interpretations and mental models. Therefore, building a common understanding is challenging. First, non-supportive organizational culture and the lack of commitment of top management were recurring topics among our data sources. When orchestrating SSI ecosystems as a provider, our interviewee mentioned that he does not talk about this initiative to the upper management because of the iterative and risky nature of the task. Another interviewee talked about this problem from the customer organizations' point of view as follows:

"If they include the decentralized solutions in the organization […] they have to get approvals from their executive leadership […] to get their security budgets […] there is a lack of knowledge […] and lack of support from their executive leadership."

Second, SSI requires understanding both technology and governance. One of our interviewees explained the intertwining of technology and governance as follows:

"We organized one training session where… the person who was organizing said that 'okay there are people who are only interested about the technology and then we have people who are interested about the governance'. I told him that's okay. It's like the people who hear about either of these things is like it's like watching dancing without music. That's gonna be funny and you're not gonna understand how the whole thing works if you don't see the dance and hear the music at the same time."

Third, the role of government and the citizens' attitude toward their government has been having an impact on SSI ecosystems. In one of our meetings with practitioners, one expert mentioned that employees of one of the governments found the idea of a digital identity terrifying as it gives back control over the data to the citizen:

"The identity piece—a real, genuine danger to our collective, national, and physical security. The more we want to go away from connecting with a government, the more it opens the door to cybercriminals who are organized at the state level in most cases. It's terrifying now—think about it in the context of a smart city, grid, health system under pressure with a pandemic. Definitely, the relationship with a state ID needs to be balanced out, core concepts like trust need to be much better understood."

Finally, people with different cultural backgrounds perceive SSIs in different ways. Especially in developing countries, citizens do not have smartphones to store their private keys securely:

"For us in the west, a wallet makes perfect sense. If you grow up in an African village or in Polynesia, your wealth and status might be in jewelry, shells or cows. Wallets make no sense."

As a summary, in Table 5, the key challenges are summarized related to different aspects of the ecosystems: governance, technology, business, legal and regulatory environment, and societal and organizational culture.

Category	Key challenges
Governance of collaborative ecosystems	Challenges in developing governance rules and policies Lack of formal leading roles of the ecosystem Contradicting incentives and objectives of the actors Challenges in attaining collaborative actors, customers, public authorities (value justification)
Technology	Immaturity of technology Complexity Scalability Challenges in user interface/usability
Business aspects	Challenges in business model development Need for fundamental changes in existing processes/systems High investment costs Lack of resources (money, skills, tools, etc.) Need for users' training
Uncertain legal and regulatory environment	Lack of standardization Legal and regulatory uncertainty Interoperability with current/ legacy systems Horizontal interoperability of different SSI solutions Vertical interoperability of different components of SSI solutions
Societal and organizational culture	Information asymmetry Diversity of interpretations and mental models Lack of knowledge and understanding Non-supportive organizational culture

Table 5. Challenges in adopting SSI and orchestrating SSI ecosystems.

5 Conclusions

In this paper, we draw on theory of reasoned action (Ajzen & Fishbein, 1980) in order to shed light on the human behavioral pattern in the decision-making strategy on SSI adoption. The results suggest that the feasibility of SSI largely depend on the decision makers' beliefs and attitude toward the advantages and required sacrifices needed for SSI adoption. Practitioners consider all available information and weigh their alternatives and the implications of their choices. SSI is a feasible choice especially for use cases when there is a high demand for keeping the data trustworthy, secure, and private because it has the potential to revolutionize data exchange. Consequently, adopting the technology is highly rewarding for industries that require management of sensitive or confidential data, process automatization, or structured data. On the other hand, SSI requires building an infrastructure, high investment costs, and fundamental changes in existing systems and processes. Thus, in certain contexts, the perceived sacrifices outweigh the potential benefits, and in these cases, adopting SSI is not perceived as a feasible choice.

Domain experts perceive that adopting SSI has the potential to provide several benefits for society and individuals. SSI enables embedding trust, privacy, and security into digital interactions, simplified processes, and better user experience. It also provides means to achieve equity, digital transformation, and digital and financial inclusion. From organizations' and institutions' points of view, SSI might facilitate the development of innovations, increase the privacy and security of digital services, and improve organizations' financial performance. Among the strategic benefits, SSI enables competitive advantage in the market, the formation of new strategic alliances, improved brand and reputation, and increased customer retention and satisfaction. On top of SSI infrastructure, business processes can be implemented rapidly and more efficiently, and fraud and money laundry risks are reduced.

Experts experience several challenges related to orchestrating SSI ecosystems and adopting the technology. First, there are barriers related to attaining collaborative partners and customers, providing incentives, and developing the governance rules and policies without having an actor empowered with authority. Second, the immaturity and complexity of technology, missing key components, scalability issues, and challenges in developing suitable user interfaces are also identified. Third, the need for developing an "ecosystem business model" is perceived as a key barrier, as without monetary incentives, the actors' commitment is rather low for active participation. High investment costs, need for fundamental changes in existing processes, and lack of resources lower the adoption intention as well. Fourth, SSI relies on a legal and regulatory uncertain environment characterized by a lack of standards and interoperability issues. Fifth, there is a lack of knowledge and understanding of SSI among different actors. The information asymmetry and diversity of mental models create challenges, for example, between top management and employees, people with different cultural backgrounds, profit and non-profit organizations and public institutions, and individuals with technical and business backgrounds and objectives.

This study aims to take the first step to investigate the behavioral foundations of the decision makers in the adoption decision by identifying experts' perceptions of the benefits and challenges of SSI. We found that the theory of reasoned action provides a suitable base to understand the attitude and beliefs of different actors and to identify the key factors that play an important role in adoption decisions. Further studies are needed to investigate the relative importance of these factors. As a next step, we plan to deepen our understanding of the phenomenon in future work by integrating insights from additional theoretical framework(s) (for example, Theory of Planned Behavior, Ajzen, 1991; Technology-Organization-Environment, Tornatzky, 1990; Diffusion of Innovation, Rogers & Rogers, 2003; Unified Theory of Acceptance and Use of Technology, Bagozzi 2007;Technology Acceptance Model, Davis 1989).

The study has several limitations. First, the data sources are experts and practitioners who are familiar with SSI; thus, the viewpoints of possible end users of SSI are not considered in this article. Second, due to the qualitative research approach, the findings of this study cannot be fully generalized. Finally, the topic is rather new and developing quickly, and this might affect the validity of the results. To mitigate the possibility of this bias, we integrated the experts' insights with the newest work from both scientific and grey literature.

Acknowledgment. This research has been conducted in the Security And Software Engineering Research Center (S^2 ERC, 2020-21) in the COOL-Appia and StrokeData projects funded by Business Finland. We are grateful for all experts who contributed to this research by sharing their insights.

References

Allen, C. (2016). The Path to Self-Sovereign Identity, URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 21 February 2021).

Ajzen, I. & Fishbein, M. (1980). Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs, NJ, Prentice-Hall Inc.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-221.

Bagozzi, R. P., (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift, Journal of the Association for Information Systems (8)4, 244–254.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232–246. https://doi.org/10.1016/j.dss.2011.07.007

Biometricupdate, 2020. Government investments in digital identity and biometrics programs progress around the world, URL: https://www.biometricupdate.com/202009/government-investments-in-digital-identity-and-biometrics-programs-progress-around-the-world (visited on 21 February 2021).

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change, 158, 120166. https://doi.org/10.1016/j.techfore.2020.120166

Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. Industrial Management and Data Systems, 119(7), 1457–1491. https://doi.org/10.1108/IMDS-08-2018-0365

Creswell, J.W., W. E. Hanson, V. L. C. Plano and A. Morales (2007). Qualitative research designs: Selection and implementation. The Counseling Psychologist. 35(2), 236–264.

Darke, P., G. Shanks and M. Broadbent (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. Information Systems Journal. 8(4), 273–289.

Davie, M., D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell and D. Reed (2019). The Trust over IP Stack. IEEE Communications Standards Magazine. 3(4), 46–51. https://doi.org/10.1109/MCOMSTD.001.1900029

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Quarterly (13)3, 319–342.

Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity $-$ opportunities and challenges for the digital revolution. arXiv preprint arXiv:1712.01767.

DID, 2020. Decentralized Identifiers (DIDs) v1.0, URL: https://www.w3.org/TR/did-core (visited on 21 February 2021).

DIDComm, 2020. Aries RFC 0005: DID Communication, URL: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0005-didcomm/README.md (visited on 21 February 2021).

DIF, 2020. Decentralized Identity Foundation, URL: https://identity.foundation/ (visited on 21 February 2021).

Dunphy, P. and Petitcolas, F.A., 2018. A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), pp.20-29.

Edmondson, A.C. and McManus, S.E., 2007. Methodological fit in management field research. Academy of management review, 32(4), pp.1246-1264.

ESSIF, 2020. Working for development, integration and adoption of Self-Sovereign Identities (SSI) technologies, URL: https://essif-lab.eu/ (visited on 21 February 2021).

Evernym (2020). The Future of Digital Wallets. URL: https://vimeo.com/473440729?width=640&height=480 (visited on 21 February 2020).

Gioia, D.A., Corley, K.G. and Hamilton, A.L., 2013. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational Research Methods, 16(1), pp.15-31.

Grüner, A., A. Mühle, T. Gayvoronskaya and C. Meinel (2019). A comparative analysis of trust requirements in decentralized identity management. In: International Conference on Advanced Information Networking and Applications. 200–213. Springer, Cham.

Gstrein, O. J. and D. Kochenov (2020). Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World? Frontiers in Blockchain 3(10). doi: 10.3389/fbloc.2020.00010

Jordan, J. (2018). Digital Trust: How the Orgbook Enables the Digital Economy. URL: https://bcvon.s3.amazonaws.com/2018-06-VON-Webinar-for-Sovrin-Indy-Community.mp4 (visited 15 November)

IATA, 2021. IATA Travel Pass Initiative, URL: https://www.iata.org/en/programs/passenger/travelpass/ (visited on 21 February 2021).

Kiva, 2020. Kiva Protocol, URL:https://www.kiva.org/protocol (visited on 21 February 2021).

Lemieux, V.L., 2017, May. In blockchain we trust? Blockchain technology for identity management and privacy protection. In Conference for E-Democracy and Open Government (p. 57).

Locke, K., 2002. The grounded theory approach to qualitative research. In F. Drasgow & N. Schmitt (Eds.), The Jossey-Bass Business & Management Series. Measuring and analyzing behavior in organizations: Advances in measurement and data analysis, pp. 17–43.

Lumedic, 2021. Lumedic Connect, URL: https://www.lumedic.io/ (visited on 21 February 2021).

Mühle, A., Grüner, A., Gayvoronskaya, T. and Meinel, C., 2018. A survey on essential components of a self-sovereign identity. Computer Science Review, 30, pp.80-86.

Myers, M. D. (2009). Qualitative Research. Business & Management Sage Publications. London, UK.

MyData, 2020. MyData, URL: https://mydata.org/ (visited on 21 February 2021).

Naik, N. and Jenkins, P., 2020, April. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. In 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 90-95). IEEE.

Nasr, J. (2020). Blockchain as the Practical Layer of Application Trust: Myth or Reality?! URL: https://www.youtube.com/watch?v=iDQRMGoTKN8&feature=youtu.be (visited on 21 February 2021).

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate Accounting & Finance, 31(2), 21–28. https://doi.org/10.1002/jcaf.22415

Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46, 70–82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

Queiroz, M. M., Fosso Wamba, S., De Bourmont, M., & Telles, R. (2020). Blockchain adoption in operations and supply chain management: Empirical evidence from an emerging economy. International Journal of Production Research. https://doi.org/10.1080/00207543.2020.1803511

Reed, D. 2020. Who Will Own The Wallet of the Future?, URL: https://www.youtube.com/watch?v=bwsHW_QOM7k&list=PLXW4bzMu4rtEkubOi7467e2LqDKz_5sLx&index=5&t=7s (visited on 21 February 2021).

Rogers, E.M., Rogers, E., 2003. Diffusion of Innovations, fifth ed. Free Press.

Schuetz, S., & Venkatesh, V. (2020). Blockchain, adoption, and financial inclusion in India: Research opportunities. International Journal of Information Management, 52, 101936. https://doi.org/10.1016/j.ijinfomgt.2019.04.009

Sovrin, 2021, Principles of SSI, URL: https://sovrin.org/principles-of-ssi/ (visited on 21 February 2021).

Strauss, A. L. and J. M. Corbin (1994). Grounded Theory Methodology. Handbook of Qualitative Research. 17(1), 273–285.

Tobin, A. (2019). What is Self-Sovereign Identity? URL: https://vimeo.com/351733971?width=640&height=480 (visited on 21 February 2021).

Tobin A. and D. Reed (2017). The Inevitable Rise of Self-Sovereign Identity. URL: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (visited on 21 February 2021).

Tornatzky, L.G., Fleischer, M., Chakrabarti, A.K., 1990. The Processes of Technological Innovation. Issues in Organizationand Management Series. Lexington Books.

TrustOverIP, 2020. TrustOverIP Foundation, URL: https://trustoverip.org/ (visited on 21 February 2021).

TrustOverIP Launch Event (2020). https://zoom.us/rec/play/HwyCYE9koKazZGA1w4mPvsFeL3oxDNmDJbZXeMIImOGgOOzZbgL-Hxi-COg-VyFetdemg7-Q8-I3CFZ6.6_SQ8c6IPj9SBfKH?continueMode=true&_x_zm_rtaid=uaourSXaSYmNJhU-JtId2Uw.1605439802450.43a8507de064c2dee4d6e94d0a401ef3&_x_zm_rhtaid=531(visited on 21 February 2021).

Ostern, N. and J. Cabinakova (2019). Pre-prototype testing: empirical insights on the expected usefulness of decentralized identity management systems. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, 54, 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

VON, 2020. Verifiable Organizations Network, URL: https://vonx.io/ (visited on 21 February 2021).

Zachariadis, M., G. Hileman and S.V. Scott (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization. 29(2), 105–117

W3C, 2020. Verifiable Credentials Data Model 1.0. URL: https://www.w3.org/TR/vc-data-model/ (visited on 21 February 2021).

Wang, F. and De Filippi, P., 2020. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. Frontiers in Blockchain, 2, p.28.

Wang, Y., Singgih, M., Wang, J., & Rit, M. (2019). Making sense of blockchain technology: How will it transform supply chains? International Journal of Production Economics, 211, 221–236. https://doi.org/10.1016/j.ijpe.2019.02.002

Web Of Trust (2017). The Path to Self-Sovereign Identity. URL: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-Sovereign-Identity.md (visited on 21 February 2021).

Whitley, E.A., U. Gal and A. Kjaergaard (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. European Journal of Information Systems. 23(1), 17-35. doi: 10.1057/ejis.2013.34

Windley, P. (2020). DIDComm and the Self-Sovereign Internet. URL: https://www.windley.com/archives/2020/11/didcomm_and_the_self-sovereign_internet.shtml (visited on 21 February 2021).

WFP Building Blocks, 2020, Building Blocks. https://innovation.wfp.org/project/building-blocks (visited on 21 February 2021).

Zwitter, A., O. J. Gstrein and E. Yap. (2020). Digital identity and the blockchain: Universal identity management and the concept of the 'self-sovereign' individual. Frontiers in Blockchain, 3(26). doi: 10.3389/fbloc.2020.00026