Promises and Problems in the Adoption of Self-Sovereign Identity Management from a Consumer Perspective

Marco Hünseler[1] and Eva Pöll[2(✉)]

[1] Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin, Germany
marco.huenseler@h-brs.de
[2] University of Münster, Münster, Germany
eva.poell@uni-muenster.de

Abstract. Online identification is a common problem but so far resolved unsatisfactorily, as consumers cannot fully control how much data they share and with whom. Self-Sovereign Identity (SSI) technology promises to help by making use of decentralized data repositories as well as advanced cryptographic algorithms and protocols. This paper examines the effects of SSIs on responsible, confident, and vulnerable consumers in order to develop the missing understanding of consumer needs in SSI adoption and define preconditions and necessary considerations for the development of SSI-based platforms and applications.

Keywords: blockchain · self-sovereign identity · SSI · criticism · consumers · triad model · vulnerable consumer · confident consumer · responsible consumer

1 Introduction

Digitalisation found its way into all parts of everyday life [27], from studying and applying to a new job to entertainment and using online platforms to keep in touch with friends. A common entry requirement is to register and authenticate one's identity during which personal information is requested. All means of commonly used digital identification today have in common that consumers cannot fully control how much data they disclose and to whom. A current technology promises a solution: the concept of Self-Sovereign Identity (SSI) aims to give back full control to the consumer, while allowing a broad applicability [2]. But albeit these promises, consumers still barely adopted it [16]. The research done in the section of SSIs so far does not focus on the consumer as a central part, but rather highlights technical aspects [3,16,27]. We find that a consumer-focused perspective is underrepresented in the research of SSI so far. This paper looks into the promises of SSI and how consumers can access them. Precisely, we seek to answer the following questions:

1. Can SSI solve the problem of easy and user-centric identification online?
2. Is this solution available and advantageous for all consumers, or does it differ, depending on the consumer type?

Published by Springer Nature Switzerland AG 2023
F. Bieker et al. (Eds.): Privacy and Identity 2022, IFIP AICT 671, pp. 85–100, 2023.
https://doi.org/10.1007/978-3-031-31971-6_8

To supply an answer we will first set the context, stating the problem of digital identity management systems and pointing out shortcomings in current solutions. Also we present Micklitz's triad model of the responsible, the confident, and the vulnerable consumer, to fathom the characteristics of consumers in the following. Thirdly, the technical basics of SSI are introduced and then the promises it holds are presented. The fourth section moves on to the problems that consumers face. Finally, we sum up our findings, that most consumers can benefit from the use of SSIs, given that a widely-adopted ecosystem of related software, hardware and services exists.

2 How to Manage One's Digital Identity?

Even though the identification and authentication of consumers are fundamental for digital participation, it is still considered as "one of the major present challenges in the World Wide Web" [3]. A digital identity is the partial representation of a real-world entity. Usually the entity is a person, but digital identities can also represent legal persons, i. e. a company or institution, or physical objects [27]. A digital identity holds a number of attributes, i. e. information about the entity that can be used to identify it (e. g. name, date of birth) [17]. Attributes can also be used to claim something about the entity, such as associated bank credentials or which groups it associates with [2].

2.1 The Current State of Digital Identities

One of the most common models for establishing an online identity today is the *isolated model*. In the isolated model, consumers register accounts and identify themselves and share their data separately with each service provider [14]. From a consumer perspective, this model shows some flaws: Every service provider is in full control over the data shared with them and it is complicated to keep an overview over all service providers one has ever shared any information with. The lack of overview makes it difficult to exercise rights related to data privacy such as updating personal data or revoking consent to use it [27]. In order to help with the management burden, consumers often reuse passwords for several accounts [27]. These can subsequently be stolen if any one of the service providers fails employ proper security measures, oftentimes leading to a compromised online identity [17]. Solutions like password managing software need digital literacy, as in being aware of the risk and the knowledge how to mitigate it.

One solution to ease the burden and centralise an identity scattered across several accounts are *Single Sign-On (SSO)* providers. They offer to create a central digital identity on their platform and communicate this identity towards other platforms. Still, the data governance remains with the providers, which have an economic rather than protective interest in the data [12]. Thus the consumer gives up control over their digital identity, granting access and insight, practically transferring the authority to these providers [27]. Furthermore, it

allows the authentication providers to gather even more data (e. g. by tracking user behaviour) [17] which they might use without the consumer's actual consent [12].

Another alternative are state-issued digital identities (*National ID Cards*): These are useful in cases where an unambiguous mapping between a specific natural or legal person and their online identity is needed (e. g. regulated industries such as banking) [24]. In order to provide their citizens with a strong way to prove their identity online multiple states around the world provide their citizens with ID cards that are electronically readable, digitally verifiable [19] and, for example in the European Union (EU), operable across the union [5]. However, the EU Commission finds that adoption of this service remains low and subsequently tries to establish a successor to the current scheme, based on SSI principles [6].

2.2 Consumer Models

At the core of EU regulations is the model of an ideal consumer who is genuinely willing and able to search, understand and use necessary information on a topic sufficiently well [1]. This model is widely criticised to bypass reality, in posing idealistic rather than realistic expectations of competences and capacities on consumers. It also overestimates that relevant information is available and accessible for all consumers [28]. An alternative to this idealistic model is brought forward by Micklitz who proposes a dynamic consumer model, made up of three overlapping consumer types (the *triad model*), consisting of *responsible*, *confident* and *vulnerable consumers* [18]. Each type represents a set of behavioural patterns that characterise strengths and weaknesses and allows an internal differentiation, aiming for tailored support for each type, protecting the weaker, without patronising the stronger consumers [18,28]. The *responsible consumer* is close to the ideal consumer also applied in EU law, but acknowledging that consumers only have limited cognitive capacities. Thus, they are best supported with accessible, thorough, and ideally also processed, additional information. They can and want to take full responsibility in their decision process [1]. The *confident consumer* is de facto the most common role [15]. These consumers aim for fast and easy consumption decisions and therefore rely on the judgement of others. In lifting some responsibility from them, e. g. by offering certified products and services, these consumers are supported in their decision-making. To offer them further information is only partially helpful, as they do not wish to spend much time on getting informed before making a decision [18]. *Vulnerable consumers* are barely capable to fathom the complexity of the respective consumption context and are hardly able to decide intentionally in their best interests. This might be due to cognitive limits (age, disability, ...), or a language barrier. They need profound protection, for example by laws and institutions, regulating markets and business practices [18].

As the triad model is still novel, the boundaries between consumer types remain vague and are in need of further research [1]. To illustrate the differentiation, habits of agreeing to general standard terms and conditions (GTC)

of software products can be used: Responsible consumers are genuinely interested in the topic at hand and will consequentially invest time and effort to gather background information and make a well-informed decision. Thus, they would read the GTC thoroughly and – if they disagree with the terms – try to find a different solution. Confident consumers, however, will agree to the terms, without reading or even skimming through the text. They trust jurisdictional standards to protect their interests. Vulnerable consumers might agree to the GTC, without having the ability to understand what they agreed to and what the terms and conditions imply.

2.3 Introduction to SSI

While established identification systems offer a central place to store data, but without sufficient control over the data for the consumer, Self-Sovereign Identity (SSI) promises to establish consumers as "the rulers of their own identity" [2]. The term SSI surfaced in 2011 [20] and gained momentum with Allen's manifesto on ten fundamental principles for SSI in 2016.

The basic building blocks for SSI systems are Decentralised Identifiers (DIDs), Verifiable Credentials (VCs), and Verifiable Presentations (VPs) [3]. DIDs are an address (similar to an URL) that can be resolved to a DID document which can in turn contain information such as cryptographic keys or information about a subject [26]. Using DIDs, it is possible to issue and receive VCs [25]. VCs consist of information about a particular identity such as the address, or banking information, but can also represent certificates (like university degrees) or state-issued identities [31]. Consumers can use these credentials attached to their identifiers to create *VPs* – a set of consumer-chosen claims originating from the VCs issued to them – in order to prove aspects of their choice regarding their identity to third parties [25]. VCs are used to selectively reveal personal information to a service provider [3], e. g. to register on a streaming platform or to apply for a job. In this process the data remains under control of the consumer, as the data is stored with them. They can use their issued credentials without the permission or any further participation of either the service provider or issuer [12,31].

Additionally to these basic building blocks, more components are necessary to operate a service which can be used by consumers: On the technical side, protocols, algorithms and data formats for exchanging or revoking credentials, network communication, cryptographic key management or the management of credential-related data (such as DIDs, VCs or revocation information) inside a central data registry (e. g. blockchain) are needed. Organizational arrangements concern the operation of the managing organization itself, public relations, the software provided, the central data registry and related policies such as entities allowed to read, write and verify the registry, associated costs, and terms for using the provided services [7].

To guide the ongoing development of SSI Allen proposed ten conceptual principles for identity management systems in his manifesto, demanding transparency, fairness, and protection for consumers [2]: (i) *Existence:* an individual exists beyond their online identity, they cannot solely exist digitally; (ii) *Control:*

the individual has control of the central aspects of their identity and is supported in this by trustworthy and secure algorithms; (iii) *Access:* the individual must have access to all information that is known about them; (iv) *Transparency:* the system and its algorithms must be transparent in how they work and how they are managed; (v) *Persistence:* the individual is able to use their digital identity as long as they choose to; (vi) *Portability:* the online identity should be portable across systems and jurisdictions; (vii) *Interoperability:* the digital identity is interoperable, i. e. individuals can use their identity where they want to (i. e. as widely as possible); (viii) *Consent:* no parts of an individual's identity are used without their consent; (ix) *Minimalization:* an individual should be able to minimise disclosed data, i. e. they only have to share as much personal information as strictly necessary; and (x) *Protection:* the individual's rights and freedom are protected, including cases where the needs of consumers and identity networks may conflict [2].

2.4 Criteria to Evaluate SSI from a Consumer Perspective

To assess which consumer types could benefit from SSIs to which extent, we examine various aspects related to the technology. In this we conceptually combine the consumer model by Micklitz with the insights of current SSI literature. The results are summarised in Table 1. First, we consider if for the ten principles put up by Allen [2] the potentials of SSI can outweigh the risks and difficulties for each consumer type (Sect. 3.1, Sect. 4.1). In the second part (Sect. 3.2, Sect. 4.2), we examine typical aspects related to implementation decisions, such as usability and market factors. The third part presents two illustrative use cases that are commonly referred to as examples where SSI can benefit consumers (Sect. 3.3, Sect. 4.3).

3 Promises: The Concept of Self-Sovereign Identity as a Solution

SSI claims to be the "vision for how we can enhance the ability of digital identity to enable trust while preserving individual privacy" [2]. In the following these promises are analysed and differentiated for the three consumer types. In a second step (Sect. 4) they will be contrasted to the cases in which consumers cannot access the promise.

3.1 Promises in Allen's Manifesto

Existence. Allen highlights in his manifesto the relevance of the individual holding the identity. However, even with multiple overlapping digital identities, the individual exists beyond these descriptions and must be respected as an autonomous entity [2]. An ecosystem that respects the whole existence and sovereignty of a person is advantageous to all consumer types (Table 1: Existence).

Table 1. Potential of correctly implemented SSI properties for consumers, weighted against possible risks

	Vulnerable	Confident	Responsible
Existence	▲	▲	▲
Control	○	▲	▲
Access	▲	▲	▲
Transparency	○	▲	▲
Persistence	↯	○	○
Portability	○	○	○
Interoperability	○	○	○
Consent	↯	○	▲
Minimalization	↯	○	▲
Protection	○	○	▲
Key Management	↯	↯	▲
Trust Management	↯	↯	▲
Wallet/Agent Availability	↯	○	▲
Costs	↯	↯	○
Healthcare	○	○	▲
Professional Certification	○	○	▲

Legend: ▲: high potential to access benefits; ○: benefits are accessible, given certain preconditions, mitigating risks or difficulties; ↯: risks outweigh the benefits or the ability to use this aspect is not given

Control, Consent. Using SSI, consumers can gain exclusive control over their digital identities and exercise sole authority over whom they share related data with. For confident and responsible consumers, this is a significant advantage over established isolated identity systems or SSO providers (Table 1: Control). Setting the consumer at the centre of control over their data also satisfies the need for informational self-determination, which is also proclaimed by the EU[1] and which could be realized by SSI if it is consistently implemented [30]. Consumers also benefit from being able to grant or revoke consent to use their identity at all times. In centralised systems this would only be possible when assuming identity providers are fully trustworthy. In order to give consent, consumers need to understand what exactly they consent to, including what consequences this decision entails. Especially responsible consumers are assumed to be able to give informed consent decisions and thus able to profit from extensive control over their data sharing practices (Table 1: Consent).

Access. The access property promises users to always be able to retrieve all data that is related to their identity while at the same time this data is only accessible for others with their permission [2]. This is an universal advantage for every consumer type in comparison to traditional systems, where identity

[1] The Court of the EU deduces the right to information self-determination from article 8.1 of the Charter of Fundamental Rights of the EU: "Everyone has the right to the protection of personal data concerning him or her" [10].

providers are able to store and share data at their own discretion and possibly without asking for consent of the consumer.

Transparency. The transparency property states that operational matters (i. e. governance, algorithms, software) should be freely accessible and publicly visible by everyone [2]. Responsible consumers are likely to profit the most from this property because they are the most likely to actually check that the system works in their own interest while confident consumers can choose to rely on assessments by institutions they trust or the public hand as with open-source software in general.

Persistence, Portability, Interoperability. Providing a digital identity that is self-managed with the possibility of using it across different user agents and across services (portability), widely accepted (interoperability) and guaranteed to be usable for an extended period of time (persistence) is a promise no other identity system architecture has delivered on to date [2,6]. In principle (given an established infrastructure), all types of consumers could benefit from a central place to manage *all* of their registrations, certificates, permissions and further data about them. It enables them to see with whom they share their data and offers a central place to manage granted permissions. It also offers them a uniform experience, i. e. they only need to learn how to manage their identity using the provided tools once. Especially responsible consumers could freely choose which software they trust and move between alternatives, if they find one that better fits their needs. Consumers could rely on being able to use their established identities how they see fit and even dispose of it, provided they are still able to control it (i. e. hold the relevant cryptographic keys).

Minimalization, Protection. The selective disclosure of a subset of attributes related to the consumer's identities brings high potential to increase privacy, especially for responsible consumers who are expected to understand the implications of sharing their data. Correctly implemented and used, it is a property that could lead to significant reduction of data sharing and thus possibility for misuse, for example by only providing a proof of possession of information, instead of sharing the information itself (through zero-knowledge-proof algorithms) [12] (Table 1: Minimalization). Similarly, the protection requirement, stating that the employed algorithms should be censorship-resistant and decentralized, protects the rights of the individual and can benefit all consumers in upholding their sovereignty and integrity.

3.2 Promises of Related Technology and Concepts

Key and Trust Management. Both key and trust management enable users to take full control over the use of their digital identity and an autonomous assessment of relationships to other people, organizations and things inside the SSI ecosystem. Cryptographic keys are used to prove aspects about the consumer's identity and restrict access to use this identity to the key holders. Using advanced key management techniques [21], consumers can take appropriate measures to counter the risk of losing their keys or make stolen keys unusable.

The measures include distributing parts of the key material to commercial providers, people they trust, or creating analogue backups on paper. However, they must set up these measures preventively, which primarily responsible consumers can be expected to do (Table 1: Key Management).

Additionally, consumers need to know to whom exactly they reveal their data. They consequently need a way to correlate cryptographic keys (of relying parties such as online services) to real-world identities. Centralized solutions solve this by regulating who is able to guarantee a specific identity, which potentially limits the freedom of consumers [16]. Using SSIs however, consumers are able to manage trust relationships by themselves, i. e. they choose which issuers they trust to make claims about themselves and others. This includes checking that corresponding cryptographic key material is legitimately owned by these issuers. Using these techniques, especially responsible consumers could implement a fully sovereign Web-of-Trust that does not rely on institutional credential issuers [4] (Table 1: Trust Management). Furthermore, this could lead to the development of new use cases that are difficult to implement using established technology (e. g. to transitively grant friends' trusted friends access to one's flat).

Wallet and Agent Availability. A diverse ecosystem of wallets and agents, i. e. applications consumers use to participate in the SSI ecosystem, can lead to healthy competition and the availability of functionally rich software that is easy to use and able to help consumers fulfilling their needs. Assuming wide adoption, there is a high probability that a suitable solution for every type of consumer exists. Confident consumers could benefit from software products that align with their interests and support them in making safe decisions (i. e. have sensible defaults that protect them, are easy to use and provide them with support options in case problems arise).

3.3 Promises for the Real World

Healthcare. Today's healthcare systems often rely on different types of proof and certificates consumers need to handle in order to access medical services. For example, they need a proof of insurance in order to be treated and then obtain prescriptions, medical reports or other certificates regarding their health. The methods in use are often not interoperable (e. g. prescriptions in digital form obtained in one EU country can usually not be redeemed in another [9]) and often not internationally accepted (e. g. Switzerland does not accept prescriptions from EU countries at all [9]). SSI offers the potential to provide interoperable solutions that are privacy-friendly and offer consumers control over the processing and sharing of their health-related data [23,33]. All consumer types would generally benefit from such a solution.

Professional Certification. A common use case is the need to present educational credentials to interested parties, for example when applying for a job, changing the school or university. Oftentimes, only specific information like whether a degree was awarded or claims about the distribution of certain grades are required. SSI is able to simplify the proof of having obtained a certain degree

and thus processes needing this information [11,24]. Because credential issuance can be frictionless and offered by various institutions, even online or short term courses could issue them. All consumer types could highly benefit from this possibility to quickly demonstrate all facets of their specific skillset and help them to compete on the job market [11].

4 Problems: Limits of Usability of the Concept of Self-Sovereign Identity

SSI seems to answer the call for user-centric identity management with sparkling promises. However, in light of practice, not all promises can be kept, especially for vulnerable and confident consumers. This section examines where risks occur among the promises made and what additional difficulties SSI brings about.

4.1 Broken Promises in Allen's Manifesto

Persistence, Portability, Interoperability. To be able to use the same digital identity across several platforms is said to be a main reason for the adoption of SSI [22]. So far, this remains a promise. No standard has evolved yet, which would lay the foundation for this [27]. On the contrary, currently there are more than 130 methods to implement DIDs [29]. While projects like Sovrin [24] or European Self-Sovereign Identity Framework (ESSIF) [8] aim to provide a technical and organizational foundation for a widely-used SSI ecosystem, their solutions are not readily usable for consumers, yet. While Sovrin is generally usable, standards, e. g. for advanced key management techniques, that facilitate complex aspects of using SSI are not implemented by now [21]. ESSIF and the related European Identity Wallet [6] are not yet available either. This makes it risky for consumers as well as for the industry to settle on one implementation, as it might not be supported long-term or will not be adopted broadly [27]. But specifically wide adoption, and thus also broad applicability, are among the main factors for consumers to use a technology [16,22]. Thus, the settled implementation that is assumed by Allen [2] and that would benefit all three consumer types, is not yet available. Consumer must invest effort to maintain an overview of all options on the market and understand their advantages and in case switch to a new application. Confident consumers, however, seek quick and easy decisions and would rather stick with a solution they chose once than adopting a new one [15]. The need for a settled ecosystem is even more evident for vulnerable consumers who do not have the capacities to make an informed decision on an implementation in the first place. Therefore, currently the ability to use the same identity across different platforms and in several environments is obstructed, restraining portability and interoperability to be only conditionally advantageous for all consumers (Table 1: Portability, Interoperability). Due to the missing standard and the ongoing development also the promise of persistence is only conditionally applicable for consumers until a standard is settled. For vulnerable consumers persistence might also bear the further risk of credentials persisting

past their intended use. Both, knowing about the criminal use of a credential and the process of revoking it are assumed to be complex [16] and thus above the abilities of vulnerable (and confident) consumers (Table 1: Persistence).

Control, Consent. By definition SSI allows the user to have central control over their identity [2]. However, this might be difficult to utilise for vulnerable consumers, who have a very low digital literacy, obstructing their ability to actually understand and intentionally use SSI applications (Table 1: Control). Technical research highlights the advantage of enhanced privacy and security through SSI (i. e. consent in [2]) as well as minimization of the data that needs to be shared [12]. But despite these findings consumer oriented studies show "that privacy concerns are of little importance" for consumers [22]. They would value convenience higher than privacy [16,30] and experience sharing personal data as "a part of modern life" [22]. This corresponds to the result of Kenning and Wobker stating that confident consumers are the most common type [15], and also corresponds to our understanding that confident consumers aim for convenient rather than more secure solutions. SSI cannot solve the problem that the consumer remains responsible for sharing their data [27]. Especially vulnerable and confident consumers are often not literate or willing enough to consent to what parts of their identity is used and how. These types need to be supported by presenting data sharing requests in a way that nudges consumers to question their action and reflect over whether it is in line with their own interests. Responsible consumers should be trusted to have sufficient digital literacy to manage their data responsibly. Vulnerable consumers, however, are under higher risks in the aspect of consent and need more support: Here it would be advisable to set up certified intermediaries or mechanisms that restrict which data is reasonable to share in the consumer's interest [18,22] (Table 1: Control, Consent). Note that restricting consumers in such a way contradicts control and consent requirements put up by SSI.

Minimalization. The protection of personal data is made even more difficult by the industry's greed for data, which SSI might even aggravate: Although SSI enables the minimization of disclosed private data [2], this does not yet mean that the industry will also submit to this option. Still, they can ask for whatever data they please as a condition of entry – very much like what is common practice now [13]. The interests might rise further as it can be assumed that information extracted from externally verified credentials could be more valuable than, potentially false, data entered directly by consumers. Also aligning to current practice, platforms might continue to ask for additional information as a proof of authorisation (e. g. asking for credit card credentials to prove one's age) [27]. Confident and vulnerable consumers will be open to disclose this data, when they should actually be reluctant to do so. Furthermore, SSI might open new contexts of data collection where current solutions for digital identification are too elaborate, e. g. when entering a building [27]. Once the information is disclosed, it is stored with the service providers and under their control, making it hard for consumers to enforce the rights on their personal data [3]. Thus, consumers carry a high responsibility with regard to their data. While responsible

consumers can be expected to handle the risk, vulnerable and confident consumers are incapable to do so and should be supported by juridical frameworks and employing nudges.

Protection. While responsible consumers can be expected to inform themselves sufficiently to claim their own position in the trade-off between transparency and anonymity as well as choosing applications with secure data storage, vulnerable and confident consumers are missing the literacy or interest to do so. They can only benefit from the property of protection under the condition that standards and regulations in which they trust are in place to protect them.

4.2 Broken Promises of Related Technology and Concepts

Wallet and Agent Availability. SSI demands additional effort to learn to use the new mechanisms that it introduces and that consumers are barely used to, e. g. agents, wallets and cryptographic keys. This poses a hurdle on less literate consumers [16,27]. While it is desirable to have different options for SSI-related software, especially wallets, it also makes it harder to choose a safe solution. To support confident consumers public clues should be offered (e. g. certifications) to protect them from malware or products that do not sufficiently secure the sensible information that is stored with them. Vulnerable consumers should not be left alone with the choice of software and key management, but be supported by intermediaries, software regulations or strong public clues. Still, security risks in using wallets remain for vulnerable as well as confident consumers.

Key Management. Connected to the risks in using wallets are the risks of managing cryptographic keys. The complex mechanisms of cryptography with private and public keys are hard to understand [27], thus it might be hard for confident, but especially for vulnerable consumers to keep the private key secret and yet memorised [3,20]. A lost private key is impossible to restore (very much in contrast to resetting a forgotten password), blocking the consumer permanently from accessing their data. Furthermore, if a private key is disclosed to a criminal, the consumers privacy is diminished and their identity might be stolen. Vulnerable and confident consumers are barely expected to be able to manage their keys on their own without putting their assets at high risk. A mitigation of the additional responsibility is to introduce an intermediary who manages the keys in place of the consumer. This hybrid approach would still enable responsible consumers to manage their keys themselves, while supporting confident and vulnerable consumers at the same time [32].

Trust Management. To be able to share their data responsibly, consumers need to know, whom they disclose information to, i. e. if the entity actually is, who it claims to be and if it is authorised to grant the claimed credentials. Following a self-sovereign approach, consumers should be able to choose who to trust by themselves. However, the problem to transfer trust relationships to the digital world by cryptographic means remains [3]. One mitigation might be the use of a Web-of-Trust (see above), which offers a decentralized approach on trust

that fits well to SSI [4]. Alternatively, classical hierarchical models like a Public Key Infrastructure, involving institutions that are considered trustworthy, can be used to delegate the decisions who to trust. Although these entities might help to anchor trust in a network, they are also valuable targets for attackers. Depending on the implemented process on how consumers decide whom to trust, central trust anchors are prone to be forged [13]. While responsible and confident consumers should be able to identify fake identities when they are supported by public clues (similar to the verified badge on social networks), vulnerable consumer will be at risk to fall for scams with forged identities Table 1: Trust Management.

Costs. The operation of a SSI platform requires financial investments, providing the infrastructure and gaining a profit margin [27]. Thus it is to be expected that consumers have to pay fees at least for certain operations [16,27]. However, because this is a serious hindrance to adoption, costs should be as low as possible [22]. Consumers appear to prefer free solutions over paid options with higher privacy or security [22]. This can be assumed to apply especially to vulnerable and confident consumers. Responsible consumers, however, can be expected to act according to those study participants who value privacy and were willing to pay for more secure systems [22]. Thus, responsible consumers would still prefer a good, free solution, but if that is not available, they would choose to pay a fee.

4.3 Broken Promises in the Real World

The healthcare sector is in high demand of digitalization, which SSI could push forward. As described above, all three consumer types could benefit from an SSI ecosystem in terms of healthcare. In this use case especially the aspects of interoperability and control come into effect, which are both (conditionally) advantageous for all consumer types. Most of all, consumers will be hindered by having to adjust to a new procedure and system. If this learning effort is supported by intermediaries and good software, also confident and vulnerable consumers will be able to benefit (Table 1: Healthcare). The same argument applies in case of professional certification. If the weaker consumer types can be enabled to use the SSI system, they would be able to benefit from it (Table 1: Professional Certification).

4.4 Further Issues

Aside from the promises that cannot be delivered on so far, some aspects of usability are also impeding widespread consumer adoption of SSI. Current solutions of identity management are usually based on registering with username and password, which is quick, well-known to all consumers and thus highly convenient. This convenience is hard to outweigh with the advantages of SSI, especially as it is based on complex mechanisms that are hard to understand [27] and benefits like increased privacy and data security are of little interest to most consumers [22]. The on-boarding is already too complicated for broad

adoption [16]. Particularly if a second device is need for logging in consumers are disturbed in their convenience and thus hesitant to adopt [27]. Also indirect network effects hamper the adoption: as soon as a significant amount of users join a SSI system, others will follow. Vice-versa, consumers will perceive the low adoption as a signal that it is not lucrative to join, yet [16].

Even if a certain SSI system is eventually generally accepted, this might cause further problems: If it is easily possible to ask for verified credentials, it might become normal to prove (verifiably) various qualities that are currently accepted without proof (e. g. language skills or soft skills in a job application). But it seems questionable if every quality can indeed be standardized to be able to prove it. This endeavour, of general standardization of one's identity, seems normatively outdated and also appears to contradict Kenning and Wobker's idea that a digital identity is never able to wholly cover a person's existence.

5 Answer: SSI is a Promising Solution for Most Consumers

In a digitalised world, there is a strong need for reliable digital identities. In reality, however, consumers' digital identities are scattered throughout many different services or are controlled by few commercial providers. SSI claims to be the "vision for how we can enhance the ability of digital identity to enable trust while preserving individual privacy" [2]. We find, however, that in practice, depending on the particular consumer, conceptual risks associated with the concepts of SSI itself remain, in addition to the risks of current implementations. Still, most consumers could benefit from a widely available SSI ecosystem.

Especially responsible consumers benefit from SSIs, because it enables them to both, taking unprecedented control over their digital identity and additional convenience in completing day-to-day tasks. Due to their higher digital literacy and interest to understand the technology, they are able to effectively use SSIs and prevent the entailed risks. As shown in Table 1, this consumer type benefits in most categories and is only hampered by the practical limitations of currently available implementations. Confident consumers, the biggest group, seek for convenience and will choose an easy, accessible solution over a more secure one. Thus, they are less likely to adopt SSI in the first place, but if they do, confident consumers are prone to struggle in the contexts of security and privacy. These struggles are similar to difficulties in current identity management solutions, and could be mitigated by a widely available and trustworthy software and hardware ecosystem that is able to support them with decisions related to consent and technical challenges. Especially when SSI is broadly adopted, they can benefit from an easier control of their digital identity. Vulnerable consumers however can barely benefit from using SSIs because they are likely struggling to use the technology and are incapable to asses and handle the implied risks. Still, with support of a reliable software and hardware ecosystem and further with intermediaries that can protect them in more sensitive aspects, they might become enabled to use SSIs.

We diagnose that currently available solutions fall short of the promises made and cannot provide them to all consumer types. By today, wallet software and agent services are not widely available and barely used. A single SSI ecosystem that is widely in use and that could deliver on the stated requirements has not been established. Even if adoption rises, issues related to providing a safe, yet useful environment to all consumers are hard to solve, especially while maintaining full control and decentralization properties demanded by proponents. However, assuming a widely-used SSI ecosystem emerges (especially enabled by a settled standard for SSI), most of the stated advantages could be realized for most consumers, making SSI a promising solution for managing and conveniently using digital identities online.

Acknowledgements. The BlockTechDiVer project is supported by funds of the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV) based on a decision of the Parliament of the Federal Republic of Germany via the Federal Office for Agriculture and Food (BLE) under the innovation support programme.

References

1. Achilles, N.: Vom Homo Oeconomicus zum Differenzierten Verbraucher: Ana-lyse von Begriff. Entwicklung und neuen Herausforderungen des verbrauchervertragsrechtlichen Leitbildes auf EU-Ebene. Nomos (2020)
2. Allen, C.: The Path to Self-Sovereign Identity (2016). http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
3. Brunner, C., Gallersdörfer, U., Knirsch, F., Engel, D., Matthes, F.: DID and VC: untangling decentralized identifiers and verifiable credentials for the web of trust. In: ICBTA 2020. Association for Computing Machinery (2020). https://doi.org/10.1145/3446983.3446992
4. Caronni, G.: Walking the web of trust. In: IEEE 9th International Workshops on Enabling Technologies (2000). https://doi.org/10.1109/ENABL.2000.883720
5. European Parliament and Council. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014). http://data.europa.eu/eli/reg/2014/910/oj/eng
6. European Parliament and Council. Proposal for a Reglation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
7. Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., Reed, D.: The trust over IP stack. IEEE Commun. Stand. Mag. **3**(4), 46–51 (2019). https://doi.org/10.1109/MCOMSTD.001.1900029
8. European Commission. High-level scope (ESSIF). https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=555222265
9. European Commission. FAQS - presenting a prescription abroad. https://europa.eu/youreurope/citizens/health/prescriptionmedicine-abroad/prescriptions/faq/index_en.htm

10. European Union: Charter of fundamental rights of the European union. Off. J. Eur. Union **C83**, 53 (2010)
11. Grech, A., Sood, I., Ariño, L.: Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. Front. Blockchain **4**, 616779 (2021). https://doi.org/10.3389/fbloc.2021.616779
12. Ishmaev, G.: Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics Inf. Technol. **23**(3), 239–252 (2020). https://doi.org/10.1007/s10676-020-09563-x
13. Ishmaev, G., Stokkink, Q.: Identity management systems: singular identities and multiple moral issues. Front. Blockchain **3**, 15 (2020). https://doi.org/10.3389/fbloc.2020.00015
14. Jøsang, A., Pope, S.: User centric identity management. In: AusCERT Asia Pacific Information Technology Security Conference (2005). https://www.mn.uio.no/ifi/english/people/aca/josang/publications/jp2005-auscert.pdf
15. Kenning, P., Wobker, I.: Ist der, "mündige Verbraucher" eine Fiktion? Zeitschrift für Wirtschafts- und Unternehmensethik **14**(2), 282–300 (2013). https://doi.org/10.5771/1439-880X-2013-2-282
16. Kubach, M., Schunck, C.H., Sellung, R., Roßnagel, H.: Self-sovereign and Decentralized identity as the future of identity management? In: Open Identity Summit 2020. Gesellschaft für Informatik e.V. (2020). https://doi.org/10.18420/ois2020_03
17. Lyons, T., Courcelas, L., Timsit, K.: Blockchain and Digital Identity. White paper, EU Blockchain Observatory and Forum (2019). https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf
18. Micklitz, H.-W.: The future of consumer law - plea for a movable system. Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht **2**(1) (2013)
19. Pöhn, D., Grabatin, M., Hommel, W.: eID and self-sovereign identity usage: an overview. Electronics **10**(22), 2811 (2021). https://doi.org/10.3390/electronics10222811
20. Piekarska, M., Lodder, M., Larson, Z., Young, K.: When GDPR Becomes Real. White paper, Rebooting the Web of Trust (2018). https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/final-documents/gdpr.pdf
21. Reed, D., Law, J., Hardman, D., Lodder, M.: DKMS (Decentralized Key Management System) Design and Architecture v4. https://github.com/hyperledger/aries-rfcs/blob/0323c5ae/concepts/0051-dkms/dkms-v4.md
22. Roßnagel, H., Zibuschka, J., Hinz, O., Muntermann, J.: Users' willingness to pay for web identity management systems. Eur. J. Inf. Syst. **23**(1), 36–50 (2014). https://doi.org/10.1057/ejis.2013.33
23. Shuaib, M., Alam, S., Alam, M.S., Nasir, M.S.: Self-sovereign identity for healthcare using blockchain. In: Materials Today: Proceedings (2021). https://doi.org/10.1016/j.matpr.2021.03.083
24. Foundation, S.: Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. White paper (2018). https://sovrin.org/library/sovrin-protocol-and-token-white-paper/
25. Sporny, M., Longley, D., Chadwick, D.: Verifiable Credentials Data Model v1.1. W3c recommendation, World Wide Web Consortium (W3C) (2022). https://www.w3.org/TR/vc-data-model
26. Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., Allen, C.: Decentralized Identifiers (DIDs) v1.0. W3c recommendation, World Wide Web Consortium (W3C) (2022). https://www.w3.org/TR/did-core

27. Strüker, J., et al.: Self-Sovereign Identity - Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. White paper, Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT (2021). https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf
28. Strünck, C., et al.: Ist der "mündige Verbraucher" ein Mythos? Statement at the BMELV, Scientific Advisory Board on Consumer and Nutrition Policy (2012)
29. Swick, R.: Director's decision on did 1.0 proposed recommendation formal objections. https://www.w3.org/2022/06/DIDRecommendationDecision.html
30. Uhlmann, M., Pittroff, F., Lamla, J.: Vertrauensinfrastrukturen der digitalen Gesellschaft. In Der vertrauende Verbraucher. Zwischen Regulation und Information. Verbraucherzentrale NRW (2020). https://doi.org/10.15501/978-3-86336-922-4_2
31. Urbach, N.: Selbstbestimmte Identitäten zur Stärkung der digitalen Souveränität. (Vortrag 8) (2022). https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-8-urbach-selbstbestimmte-identitaeten-zur-staerkung-der-digitalen-souveranitaet.pdf
32. Wang, F., De Filippi, P.: Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. Front. Blockchain **2** (2020). https://doi.org/10.3389/fbloc.2019.00028
33. Zhang, P., Kuo, T.-T.: The feasibility and significance of employing blockchain-based identity solutions in health care. In: Patnaik, S., Wang, T.-S., Shen, T., Panigrahi, S.K. (eds.) Blockchain Technology and Innovations in Business Processes. SIST, vol. 219, pp. 189–208. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-6470-7_11