Article

JIM
ISSN: 2183-0606
(CC BY 4.0)
Vol. 13, 2 (2025)
p. 52-69
AM: Feb/2025
SM: May/2024

The Self-sovereign Way to the Value-sensitive Metaverse

Federico Pierucci[1]

[1]Sant'Anna School of Advanced Studies, Piazza Martiri della Libertà, 33, 56127 Pisa PI, Italy | *Federico.pierucci@santannapisa.it*

Abstract

The metaverse is poised to significantly transform how humans experience cyberspace, necessitating novel approaches to defining digital identity. Self-Sovereign Identity (SSI) has emerged as a potential solution for designing an identity layer for the metaverse, with proof-of-concept models for decentralized access currently under discussion among scholars and technologists. Adopting a socio-technical perspective, this paper examines the values that should underpin digital identity solutions for the metaverse. The analysis highlights control over identity and interoperability as fundamental components of any viable identity solution in this context. Using Value Sensitive Design as an analytical framework, the paper evaluates two proposals for applying SSI to the metaverse. While these proposals advocate for decentralized identification methods that facilitate cross-platform access, they also encounter challenges related to usability and achieving fully interoperable services across metaverse platforms.

Keywords: metaverse, self-sovereign identity, value-sensitive design, human-centric design, digital identity.

Cite paper as: Pierucci, F., (2025). The Self-sovereign Way to the Value-sensitive Metaverse, *Journal of Innovation Management*, 13(2), 52-69.; DOI: https://doi.org/10.24840/2183-0606_013.002_0003

1 Introduction

The metaverse promises to be a ground-breaking innovation in the everyday use of digital technology. Harnessing the raw power of cloud and edge computing, with the adoption of AI and of 5G/6G technologies, this revolution might redefine the possibilities of human-machine interaction in unprecedented ways. Neal Stephenson's groundbreaking novel *Snow Crash* (1992) introduced the concept of the metaverse as an expansive virtual reality where users engage and interact through digital representations of themselves, known as avatars. With the subsequent proliferation of broadband internet, platforms like *Second Life* gained significant traction in the early 2000s, offering immersive environments that fostered parallel economies and societies (Sonia Huang, 2011). The development of digital identity technologies, platforms and governance structures has been, as natural, strongly influenced by the possibilities that the web offers. Nowadays, with the unprecedented increase in personal data shared through social media (Ghani et al., 2019), Internet of Things (Tsai et al., 2014) and wearable devices (Jung, 2011; Motti & Caine, 2015; Xue, 2019; Niksirat et al., 2024), digital identity providers need to take into account privacy, security, and the protection of personal data as never before.

The amount of sensitive and personal content that is shared everyday calls for a more thoughtful approach to define rules and best practices to guarantee a digital identity, while addressing the risks that the increase in quantity and scope of data poses. Further to this, the migrant crisis in Europe and elsewhere have brought activists, regulators, and policymakers to spur a reflection on how to

guarantee that this need is also respected for vulnerable individuals and communities (Gabrielsen Jumbert et al., 2018; Kaurin, 2019). The technical revolution provided in the metaverse, through the widespread adoption of Extended Reality (XR) technologies, points to the necessity of a critical reflection on how to assure that individual data defining the digital double (Ruckenstein, 2014), – the avatar – is protected by a set of basic rights that define their digital life. As the increase in the data produced verges towards a constant increase in the "Datafication" (Mejias & Couldry, 2019; Southerton, 2020) of everyday life, principles of Responsible Innovation are more than ever needed (Anand & Brass, 2021). Following the European Commission effort to enshrine basic capabilities and rights (European Union, 2022) through the regulation on digital identity (Gregušová et al., 2022), this paper aims to discuss from an ethical and philosophical perspective the challenges of a digital identity model that is suited to the massive use of the metaverse. I will explore how these challenges can be addressed using a self-sovereign model of digital identity.
The aim of this paper is to provide an outline of how a self-sovereign identity model can be used to guarantee a *user-centric* and *human-centric* design of the metaverse through the theory of value-sensitive design.

Without ignoring the challenges of designing both SSI and the metaverse from a technical perspective, this paper will focus on the socio-political background that shows the need to analyze the metaverse from a philosophical and political perspective. This paper will try to go beyond a techno-solutionist approach which has been repeatedly shown to miss the mark in understanding the socio-political and ethical issues of digital identity (Schoemaker et al., 2023; Wang & De Filippi, 2020). This paper will show how digital identity – and its application on the metaverse – can be conceptualized as a set of policies. These policies are in place to define a governance framework to regulate capabilities of digital individuals in their online lives (*Section 2*). I maintain that the added value of implementing a self-sovereign paradigm might be found in the ability of the SSI to guarantee crucial aspects of a fully realized metaverse: *control over identity* and *interoperability*. I will show how these elements define the properties of an SSI based digital identity model. Further to this, these are the requirements for the realization of the metaverse from a user-centric and human-centric perspective (*Section 3)*. Finally, I will show how a self-sovereign identity model can accommodate both the technical and political aspects regarding the implementation of control over identity and interoperability using the framework provided by value sensitive design, in which a technology is designed to be regulated entrenching rights and principles in the code itself. Analyzing two proposals for an SSI-based identity solution for the metaverse through value sensitive design, I will describe how those can be investigated and connected to the benefits and risks that underpin the SSI-based proposals (Section 4).

The content of this paper will thus be speculative, given that it will investigate the interplay between two artifacts (self-sovereign identity and the metaverse) which are still in their infancy, especially when it comes to their adoption in real-world use cases. Its speculative nature is not necessarily a weakness, but it could be seen as a creative investigation into a domain that has not yet been fully explored.

2 An SSI based user-centric and human-centric metaverse

Individuals constantly interact with various online services, platforms, and institutions, each requiring some form of digital identity verification. Traditional centralized identity management systems rely on trusted third parties, such as governments, corporations, or identity providers, to issue, manage, and validate digital identities. However, these systems raise significant privacy and security concerns, as users have limited control over their personal data, which is often stored and

processed by multiple entities without their explicit consent throughout the pipeline. Traditionally, online identity has been managed through centralized or federated protocols (Preukschat & Reed, 2021). In a *centralised model*, the credentials are managed centrally by a service provider that behaves also as an identity provider. The provider issues the credentials to the users (usually username and password), and has its own system of identification, without relying on third parties. The credentials are then locked within the service provider and cannot be used on other services (user can however decide to use the same username and password on other platforms, but this will create another pair of credentials). A *federated model* instead offers an entity that works as an intermediary between various service providers. This entity is the identity provider. The user possesses one identity account, and through the user can access different services and application relying on a single identity provider (as it's the case for Google or Facebook accounts). Self-sovereign identity has emerged as a promising solution to address these challenges. Self-sovereign identity at its core starts with the idea of a secure peer-to-peer network that allows secure communication without relying on a third party (as the centralised and federated models do). In the SSI, users can freely share identity data through a verifiable presentation (a method in which users can prove the ownership of a set of attributes). The credentials disclosed, however, remain always stored locally in users' wallets, similarly to a physical document. The development of this approach was related to the idea that individuals should have access and control over a permanent online identity. Solutions such as OpenID (Recordon & Reed, 2006) and FIDO (Loutfi & Jøsang, 2015) were crafted having this concept in mind. In the self-sovereign identity, the users are the holders of the credentials, which are issued by an identity provider (much like the identity cards or driving licenses are issued). When users wish to access an online service, they use a verifiable presentation to show their credentials to the service provider, which verifies them before granting access. If the service provider verifies the credentials, access is granted (Figure 1).

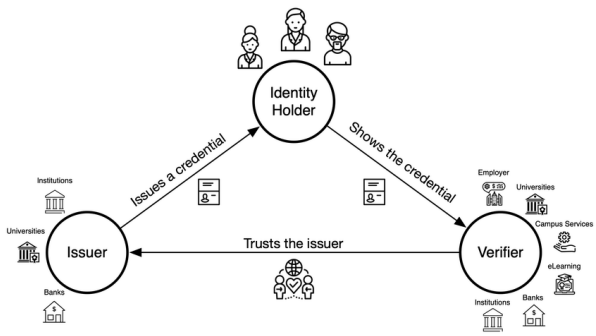

Figure 1. SSI triangle (from Yildiz et al., 2023)

SSI models utilize blockchain technology (or other decentralized ledgers) as a decentralized and tamper-proof data registry, employing cryptographic proofs with decentralized identifiers (Mohanta et al., 2019). This framework facilitates secure and trustless data exchange among various entities, including public administration, vendors, and service providers. SSI is "the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity" (Allen, 2016). Following Allen, SSI can be understood as:

- **A mathematical policy**, where cryptography is used to protect a user's autonomy and control.

- A **legal policy** that defines contractual rules and principles that members of a network agree to follow.
- An **international policy** on how to manage the identity of people who have no way to prove their own without state validation.

According to Loffredo (2016), "Self-Sovereign Identity must emanate directly from an individual human life, and not from within an administrative mechanism created by, for, as abstractions of individual human activities, and must remain amenable in design and intent directly by individual humans with original source authority". The political and ethical consideration behind SSI entails the existence of a fundamental right to identity (Wang & Filippi, 2020; Ishmaev, 2021). This right is embedded in the design principles of SSI, aiming to give an identity to individuals without necessarily passing through the validation of a state authority. The possibility of self-asserting one's identity is dubiously realizable, but at its core the SSI model recognizes a fundamental right for individuals to *control* their digital identity, regardless of the issuer.

I have argued elsewhere that, in the case of SSI, control can be understood as "local ownership of verifiable credentials" (Pierucci and Cesaroni 2023). Although an exploration of the notion of control is beyond the scope of this paper, it is important to have at least an operational definition to work with. The control that an online user can exercise over their identity is not affected only by the design of the identity model itself, but it is also connected to the set of policies that a service provider defines as a rule to provide its services. Control over identity is strictly connected to the data that comes from the use of an online identity itself. Traditional models of digital identity (such as a centralized model) leave room for the identity provider to define the access rules, the storage and the ownership of the data produced within the interaction between the user and the service. The most optimistic claims of SSI technologists are that the very structure of SSI grants the user the ability to extend the control over their identity and over the byproducts (data) of the identity itself when used in a service. In the case of the metaverse, where a centralized or federated model would leave the verifiable credentials (such as the username and password to access one's avatar) in the hands of the service provider, in an SSI model these credentials would be owned by the user (stored locally on a smartphone or on another device). A claim of the SSI model is that, through the localization of verifiable credentials, the user can port their own credentials across multiple platforms without relinquishing their own credentials to the single platform provider. This is achieved through specific design principles within the identity layer that grounds the access to certain services. Cryptographic proofs that keep the transaction on a decentralized ledger (such as a blockchain) manage to guarantee the security of digital interactions. Local ownership of credentials provides a fail-safe mechanism in case of data breaches on the service provider that the identity gives access to. A decentralized public-private key infrastructure for the verification of identity grants the ability to prove the identity of an individual through the exchange of information under ciphering. This avoids the necessity of a trusted third party to verify that the two-way communication occurring between two individuals (or between an individual and a service provider) is secure (Halder et al., 2024).

So far, I have touched upon the question of identity only from the perspective of the user of digital identity and digital services qua human user. The properties of control and cryptography-based trust between two parties can be easily applicable to a human individual or to an artificial individual within a network, such as a device connected to the web in an Internet of Things (IoT) environment (Fedrecheski et al., 2020). In fact, where a verifiable credential is associated with an agent that acts on behalf of an individual in a machine-to-machine or a

machine-to-individual type of interaction, there is no need for the individual identified by the verifiable credential to be a human. SSI (Sovrin Foundation, 2022) is considered to be a perfectly viable solution also when it comes to guaranteeing the security of the transactions between devices in an IoT network. When it comes to the design principles that underpin the creation of a secure and decentralized identity for humans, user-based principles of design should also consider the values that the designer deems essential in crafting an identity layer. Human-centric design is concerned with the best methods and practices to embed user needs, principles and values in the process of creating and developing technologies (Steen, 2011). Through human-centric design, we can consider how the user-centric values relate to human-centric values. As such, we can read as a right-based claim the statement quoted by Loffredo in the previous section, in which every individual's digital identity should stem *de iure* from their existence.

Although it is far from clear that this line of reasoning is correct, meaning that we should consider the possession of a digital identity as a *prima facie* right as we do for legal (physical) identity, at the cornerstone of some of the SSI enthusiasts (such as Loffredo and, to a certain extent, Christopher Allen) there is an implicit theory that considers the right to digital identity controlled by the user as analogous to having an ID card which, although issued by a government, is still under the physical control of the individual. It is however difficult to prove that, once we take for granted that the normative equivalency holds both for physical and for digital identity, the only mode of providing this identity should be through a self-sovereign model. If for instance basic services that are accessible through physical identity (e.g. welfare institutions or banks) can be accessed using a centralized or federated identity model, one could argue that the rights are respected. One could see this argument unfolding in analogy with digital identities that are connected to the physical one at the national level. The SPID model in Italy (Buccafurri et al., 2016), for instance, allows for a federated model in which the Italian Minister of Interior (the identity provider for Italian ID card) grants to different identity providers (such as the Italian Post systems) the ability to give verifiable credentials to Italian citizens that can be used to access online services such as the National Agency for tributes (Agenzia delle Entrate). Without having to adopt any self-sovereign model, this approach is equally capable to grant the citizens access to all the digital services required to live in a state, such as the possibility to interact with the public administration both at national and municipal levels. While it is outside of the scope of the paper to discuss in detail the extent to which the strongest claims of SSI enthusiasts can be realized, it is important to recognize that SSI might be only one of the possible solutions to the issues we are discussing.

In the context of the metaverse, guaranteeing interoperability and control over identity is key, and I argue that a self-sovereign method is the best approach that, by design, might grant this capacity. I will now show how the notion of an interoperable and controllable identity solution on a digital avatar can be framed within the technical specification of the SSI and the metaverse. I will show how these can be connected within a user-centric (Table I) and human-centric (Table II) analytical frame:

Table 1. User-Centric Design

	Metaverse (Avatar)	Self-Sovereign Identity
Control over identity	The ability to port avatar-related data and properties across different platforms within the metaverse.	Information and services tied to one's identity should be readily transferable across platforms.
Interoperability	Avatars can be used as widely as possible across different platforms within the metaverse	The identity layer should enable individuals to use their single online identity to access various services directly, bypassing the need for an intermediary.

Table 2. Human-Centric Design

	Metaverse (Avatar)	Self-Sovereign Identity
Control over identity	The principle of user autonomy is fostered in data management and transfer, ensuring privacy and control in various digital platforms.	Advocates for the individual's right to transfer their identity claims freely and securely across systems.
Interoperability	Integration of the avatar across platforms, guaranteeing immersion.	Ensures that identities are accepted across various systems, respecting control, privacy, and data minimisation.

An important aspect to investigate here is that human-centric and user-centric design meet halfway when it comes to their purpose in a larger frame. Following the seminal work of Lessig (2000) "code is law". This dictum implies that code (software, algorithms, and digital architectures) can serve as instruments for control, much like traditional laws. According to this perspective, private and public actors may embed their values and rules into technological artifacts, effectively shaping and constraining our actions in the digital environment. In fact, a special property of the law of the internet is that the guiding rules and principles can be binding directly to the mode in which the technical architecture of a digital intermediary, platform or digital world is designed (Lessig, 1997).

This grants an important ability when it comes to entrenching certain values, rights, and principles in the regulation of cyberspace. Beyond the ordinary modality of the rule of law, in which national and international (or trans-national, in the European case) courts and judicial bodies, the cyberspace can be first and foremost regulated throughout its *design.* Design choices, however, are not only technical decisions, but are taken against the backdrop of values and principles that underpin the different choices made by stakeholders involved in the design process (Miller & Taddeo, 2017). Far from defining a technical solution, I argue that the political origin of self-sovereign identity is a value-based solution to empower users of digital identity. The interplay between the metaverse and the self-sovereign identity model paves the way toward a *socio-technical* solution to a political problem of having a digital world that is built upon the needs of users qua humans (and vice-versa).

This solution establishes a *functional coupling* between the SSI and the metaverse. For interoperability, where the avatar must remain consistent to guarantee the seamless integration of experience among different platforms, the SSI grants the ability to port data and identity

claim across the metaverse. As such, it fosters a seamless and immersive experience within a unified virtual world. For the control, where the platforms that constitute the building block of the metaverse are interconnected and can be navigated preserving the possibility of interacting with a continuous digital world, the SSI can manage an *identity layer* based on the technical interoperability among the platforms. In this identity layer, the identity claims, properties of the avatar, as well as the digital asset in its possession, are preserved and maintained transferable through the use of the DPKI, a public–private key cryptography in a decentralized public key infrastructure (Papageorgiou et al., 2020). This cryptographic aspect is crucial for introducing the next section, which will explore desirable constraints in cyberspace through the structure of the web itself – its code. Within the following section, I will argue that embedding human factors through an SSI model (within a user-centric approach) can enable a value-based appraisal of a SSI solutions for the metaverse.

3 Embedding Values through code

Value Sensitive Design is a holistic approach that aims to incorporate fundamental human values into the process of developing new technologies (Doorn et al., 2013). It recognizes that the design phase inherently embeds certain values and assumptions, which may not be immediately apparent (Friedman et al., 2002). This approach posits that the design process is not value-neutral, and it seeks to identify and carefully consider the moral, ethical, and societal implications that are intrinsically woven into the creation of new technologies. By employing a multi-level methodology, Value Sensitive Design attempts to scrutinize the design process holistically, capturing the crucial values that shape the development of these technologies and their potential impact on individuals and society. VSD operates throughout a three-tiered approach. *Conceptual investigations* provide an abstract and high-level description of what values come into play in the creation of technology, and what tensions are present when designer, stakeholders and users have different values in mind when it comes to the final product they would like to be realized. *Empirical investigations* refine the conceptual investigation with a more precise analysis of values and core beliefs of each stakeholder, drawing from empirical modes of research such as surveys and focus groups. *Technical investigation* deals with the design itself of the technology, trying to bridge both the conceptual and the empirical phases blending them in an operational framework that helps understand how to embed values within the design of the technology itself (Friedman & Hendry, 2019). Value sensitive design investigates how stakeholders who participate in the creation of a technology negotiate and resolve *value tensions*. Value tensions (Miller et al., 2007) can be described as disagreement on the inclusion and the hierarchy of values that ought to be supported by the design of a technology. Trade-offs are important aspects to have in mind when it comes to technologies. In the case of digital identity, if privacy and security are fostered, this might negatively impact the intuitiveness and usability of an identity solution. Password-based identification mechanisms can be cumbersome if the password reaches a sufficient level of complexity, making it harder to remember. Another instance of this trade-off appears when it comes to biometric identification or two-stage identification with smartphone. In the first case, the user might feel a violation of its privacy by the necessity of using a biometric identifier (such as fingerprint, an iris scan or face recognition algorithms). In the second case, the use of two-factor authentication through smartphones might represent a hindrance for those users who are not comfortable in using smartphones in their daily life, or simply do not possess them. This might represent a barrier when designing an inclusive technology that can be used by a wide population that consists also of the elderly.

To the best of my knowledge, when it comes to digital identity solutions, only (Ishmaev et al., 2023) deals with the ethical aspects of SSI through VSD, describing a use-case of COVID-19 digital passport adopted in the Netherlands. When it comes to the application of the SSI in the metaverse, currently it appears that there is no VSD-grounded analysis. In this section I will then propose a cursory value sensitive design analysis of current proposals for an SSI model for digital identity in the metaverse. My investigation will be oriented to analyze how these proposals fare in integrating the principles of control over identity and interoperability. The investigation will be inevitably conceptual and will deal with trying to understand from a human centric and user centric perspective, trying to frame what benefits and risks each of the two proposed solutions entail.

Self-Sovereign Identity for Trust and Interoperability in the Metaverse (Ghirmai et al., 2023)

The Metaverse's identity management system that is proposed combines the principles of Self-Sovereign Identity with non-fungible tokens (NFTs) and decentralized end-to-end encryption techniques. NFTs temporarily provide each Metaverse user with a unique, unalterable identifier that they cannot transfer to anyone else. Such tokens are digital passports that are recognized and validated by every virtual service requiring authentication. NFTs ensure that a user identification token is secure and untransferable, making it very difficult to counterfeit or transfer between users and practically eliminating the threat of identity theft. For several types of services that necessitate a user's critical identifiers to be under a certain level of trust, other parties, such as a trusted government, may provide attestations. These third parties electronically sign and issue a certificate that signifies a user's definite claims. In their first interaction, users exchange NFTs. This information allows users to recognize and verify each other's avatars in subsequent encounters. For additional security, especially in transactions involving digital assets, mutual contacts trusted by both parties can further attest to the authenticity of the exchanged tokens. To secure communications within the Metaverse, the solution employs a decentralized version of the Signal protocol (Ermoshina & Musiani, 2019). Users self-attest their public keys and use them to establish secure communication channels directly with one another. This method involves performing a triple Diffie-Hellman key exchange (Maurer & Wolf, 2000).

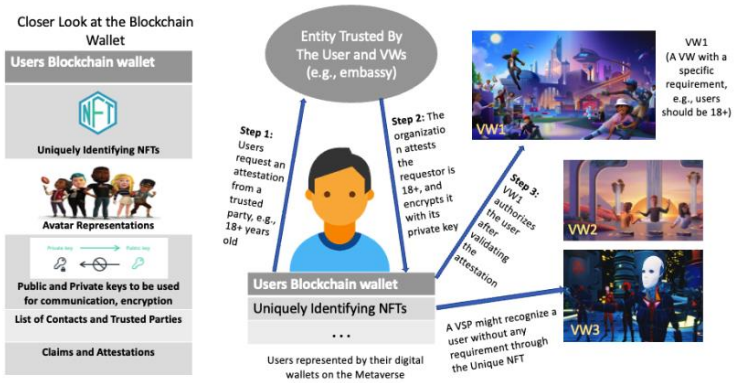

Figure 2. Model for SSI in the metaverse (from Ghirmai et al. 2022)

Table 3. Value Trade-offs for Ghirmai et al. 2022

Values	Benefits	Trade-offs
Control over identity		
Authentication via NFTs	Users maintain *control* over their identity tokens. Decentralized *control* reduces dependency on single points of failure	Users are responsible for safeguarding their NFTs. Loss of NFT can lead to impossibility of access until recovery mechanisms are implemented.
Trusted Attestations	Users have proof of attributes (e.g., age) independently of the issuing organization. Persistent trust even if the attesting organization ceases to exist.	Reliance on third parties for attribute verification. Potential privacy concerns if attestations are not managed securely. Risk of platform provider not accepting the credentials if the attesting organization ceases to exist.
Immersion through Interoperability		
Avatar Recognition	Ensures identity recognition across different virtual environments. Facilitates seamless interactions in the Metaverse.	Initial setup requires sharing and storing NFT data. Interoperability depends on the widespread adoption of the NFT standard.
Decentralized End-to-End Encryption	Enhances security and privacy in communication. No central server dependency, aligning with the goal of decentralized access to the Metaverse.	Complexity in key management for users. Requires robust infrastructure to handle decentralized key exchanges and validations.

The Interplay Between Policy and Technology in Metaverses: Towards Seamless Avatar Interoperability Using Self-Sovereign Identity

(Laborde et al., 2023)

This solution provides a protocol to enable secure transfer of avatar between different metaverses. Users manage their identities and avatars using a local wallet system installed on their devices. Each user is paired with a DID that is created for each new avatar. The owner remains in possession of the avatar's DID document and control the associated keys through their identity wallets. Through changing the name of the controller in the DID document of the avatar, user can transfer or sell avatars, thus enabling a transaction process. A user initiates the connection by calling the entrance request service of a Metaverse whose address is available in the metaverse DID document. The metaverse then returns an identifier with a list of required identity attributes. The avatar requests verifiable credentials from the metaverse from which the user wants it to be ported. If the identity attributes are accepted by the destination metaverse, the process is concluded, deactivating the avatar on the first metaverse.

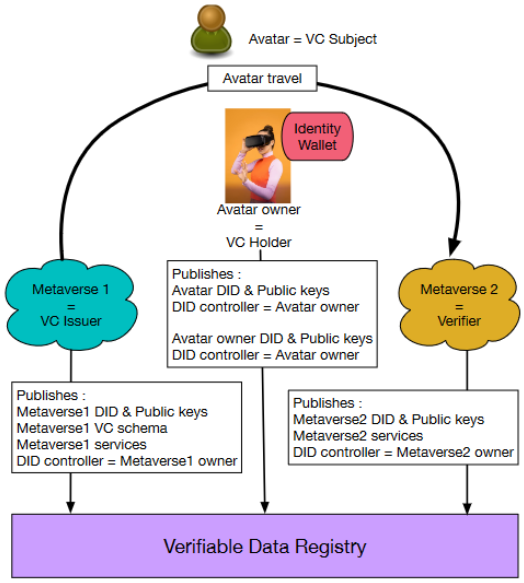

Figure 3. Model for SSI in the metaverse (from Laborde et al. 2023)

Table 4. Value trade-offs for Laborde et al. 2023

Values	Benefits	Trade-offs
Control over identity		
Identity Wallet	Users have full *control* over their DIDs and associated keys. Enhanced *privacy* through DIDs.	Responsibility for securing identity and keys rests with the user. *Usefulness* and ease of use of the solution, as well as its *inclusivity*, are problematic. SSI-based solutions might appear too cumbersome for people who lack technical knowledge and mastery over these technologies. *Usefulness* and ease of use of the solution, as well as its *inclusivity*, are problematic. SSI-based solutions might appear too cumbersome for people who lack technical knowledge and mastery over these technologies. Complexity in managing multiple DIDs and keys.
DID-based avatar management	Users can transfer avatars by simply updating the controller in the DID document. Simplifies the transaction process.	Risk of DID document manipulation if security is compromised. Dependence on the verifiable data registry's availability and integrity.

Values	Benefits	Trade-offs
Immersion through Interoperability		
Interoperable Avatars	Allows avatars to move between different metaverses, enhancing user *experience* and fostering an *immersive* experience. Ensures that avatars maintain their unique identity and attributes during transfers.	Requires consistent handling procedures of avatar data across metaverses.
Cross-Metaverse Protocols	Facilitates transitions and interactions between various virtual worlds. Encourages a more connected and unified metaverse ecosystem.	Dependence on the implementation of cross-metaverse protocols. Risk of interoperability issues if one metaverse does not support the protocol. *Trust* is required among metaverse platform providers.
Standardization	Establishes a common standard for avatar interactions across different metaverses. Ensures uniform processes and expectations for identity verification and avatar management.	Requires all metaverses to adopt and comply with the standardized protocol. Implementation may vary, leading to potential inconsistencies.

Results

The two abovementioned solutions provide visible strengths and weaknesses. While the presence of a decentralized mechanism to identify credentials fosters interoperability and user-centric control, the responsibility of managing these credentials falls completely in the hands of the user. While in fact the solutions grant control over identity and offer privacy-preserving and secure solutions, *security* as a fundamental value might be compromised, especially if proper practices of cyber-hygiene are not put into place. This might prove a heavy burden that users of SSI-based solutions (as based on a public-private key infrastructure) might have to face when adopting similar solutions (Dumitrescu & Pouwelse, 2024). Further to this, establishing recovery mechanisms when designing decentralized approaches to the identity layer in the metaverse is key. Models such as the DPKI require the user to keep the possession of the private key to access their identity wallet. Once the private key is lost or stolen, the user might face hardships in taking control again of their identity wallet. As such, while on the one hand a cryptography-based protocol increases the security of the identity wallet, on the other hand it makes the recovery of lost credentials harder than a centralized model with username and password. Strategies to mitigate this risk might be adopted, but the proposed solutions do not discuss that. Possible solutions might be to bind the access to the identity wallet with some biometric data (such as fingerprints) that might reduce the risk of a malicious actor gaining access to the wallet. Further to this, protocols for credential revocation in case an identity wallet is compromised (or in case of the loss of the phone when the wallet is stored) are necessary (Hardman, 2019). DID and NFT-based credentials, through the underlying trust guaranteed by the blockchain, offer an overarching layer of privacy and security, especially if the communication protocols favor the use of zero-knowledge proofs when disclosing identity credentials (Feige et al., 1988). However, the lack of knowledge over the

mechanisms that underlie these protocols might make users less willing to adopt decentralized solutions, favoring instead more traditional models of accessing online metaverse platforms. Thus, the control over identity-related data that SSI offers must be evaluated against the backdrop of the *perceived usefulness* and *ease of use* (Al-Suqri & Al-Aufi, 2015) of the technology when compared with other more widely adopted models. *Inclusion* might prove itself problematic: as uncommon technological solutions require a certain level of knowledge, people with low familiarity with the blockchain or with decentralized and cryptography-based methods of identification might face significant hardships when adopting those models of digital identity.

When it comes to the interoperability of the avatars that the SSI solution aims to offer, cross-metaverse travel of avatars might leverage the ability of the SSI to provide a single set of credentials which can be reused on each platform. However, the level of interoperability that different platform providers might offer is dependent on design and economic choices of each platform. While a user-centric identity solution that maintains local control of credentials can guarantee interoperability from the side of the identity layer, the same cannot be said for the other side of the service provider. In fact, choices regarding the extent of portability of data and interoperability of services between different platforms are in the hands of the owner of the platform. Hence, interoperability is not solely achievable through a change in the user-side identity wallet but requires both ends to be tuned on this approach. Providers of metaverse platforms might want to limit the amount of interoperability that their platform will offer. The benefits of an interoperable identity layer are thus dependent upon the structure of the service that the layer will grant access to. *Immersion*, a desirable property for the full experience of a virtual world, might be at stake. *Trust* might also represent an issue. While in fact the technical specification of the protocols that we discussed ensure a basic level of cryptographic trust, when it comes to the human trust among the platform providers the challenge goes beyond the reach of technical solutions. The limitations that are put on the interoperability across metaverse might in fact depend not solely on technical aspects but also on socio-technical issues of competitive edge that each provider would, foreseeably, like to keep.

Further to this, interoperability of avatars for cross-metaverse migration is dependent on the adoption of a unique set of technical standards that will make this migration possible. Standards that will probably have a different scope than the W3C standards of the SSI ecosystem, such as those for verifiable presentations and DID documents. As such, SSI-based solutions will necessarily have a limited say on the modality in which those standards will be deployed. While in fact the question of interoperability and control over identity are reflected both in the values within the metaverse and the SSI, their development follows a parallel track that might not cross if not momentarily, reducing the capacity of those who discuss and aid the design of the identity layer to shape the structure of the metaverse for which the identity layer will be grounded.

Thus, while the proposals that have been discussed offer an interesting perspective on how an SSI-based identity model might enshrine values of control over identity and guarantee immersion through interoperability, and on how the effective adoption of said solutions will be tied to the structure that the metaverse will have, I argue that the feasibility of this approach has to be evaluated having more information, as we currently possess limited data on the extent to which these proposals will be achieved.

4 Conclusions

The creation of the metaverse, as the creation of every technological solution, entails inevitable trade-offs. As we saw, crafting an identity management solution that fosters interoperability

and control ensures an autonomous and immersive experience where the user can connect and verify their identity. However, the technical requirements in setting up this solution, as well as the necessity of having a standardized and unified metaverse ecosystem, make the realization of such proposals dependent on the structure that the metaverse will have once fully deployed. As observed in the introduction, predicting what shape a fully realized metaverse will have is a difficult task. The promise of a truly unified metaverse appears difficult to realize. As the metaverse promises an immense possibility of value-creation, it seems more likely that we will see platforms with the necessary capabilities (such as Meta or Apple) create their own separated metaverse. As for the interoperability of the avatars, as well as for the control that the users will be able to exercise over their identity and data, the question will be to what extent the terms of use that will be implemented in the future metaverse will allow the possibility of cross-platform migration of avatars. Possible solutions might be, following the example of the EU Data Act[1], to establish a set of incentives and constraints that grants the user the possibility of porting their own data across various platforms. As the instrument of hard law might impose sanctions on platform providers that do not prevent the lock-in of users on the services provided by their platforms, it is open to debate whether this approach might provide for the best solution. A sanction mechanism might make platform providers less willing to provide their services in the regions in which the rules apply, thus preventing the consumers from the ability to participate in the benefits of an interconnected and augmented virtual experience offered by the metaverse. It is out of the scope of this paper to investigate what possible approaches might best suit the needs of both consumers and service providers in designing the metaverse. Regardless of its future shape, supporters of SSI-based identity solutions might very well claim that a self-sovereign and blockchain-based identity model might yield a more secure and human-centric proposal. Applying this proposal to the metaverse, however, requires careful evaluation of the downsides in terms of usability of the envisioned solutions. Further to this, it calls for a realistic assessment of what (on the side of the identity layer) can be achieved in shaping the structure of the metaverse for which this identity layer will be used. Trade-offs when it comes to perceived usefulness, ease of use, security and inclusion must be addressed.

Starting from the first section, in which we reflected on the importance of fostering a broader discussion on the social and political implications of the metaverse, we discussed the identity layer of the metaverse as a crucial aspect of the realization of user centric and human centric design principles. Furthermore, we briefly highlighted the main structural component of the SSI, considering it as shaped through a set of policies that enable to entrench the principles of control over identity credentials and interoperability. Then, we analyzed the interplay between the SSI model and the metaverse, investigating how interoperability and control over identity is at the cornerstone of each technology. Through Section 5, finally, we discussed two possible identity solutions for the metaverse, probing their benefits and possible shortcomings. Without the claim to have offered a comprehensive discussion of the challenges of the synergies between the SSI and the metaverse, this paper aimed to provide a preliminary assessment (through the application of value sensitive design) of the applications of Self-Sovereign identity to the metaverse. The reckoning that we offered is necessarily preliminary, having focused on two proposals. As the metaverse is still in its infancy, the actual applicability of every SSI based proposal is to be considered inevitably of limited application. However, by an initial clarification of the main concepts and issues that underpin this approach to the design of the identity layer for the metaverse, I hope I have offered a foundation that might spur a reflection and further investigation. Future lines of research might

1. https://digital-strategy.ec.europa.eu/en/policies/data-act, accessed on the 22-05-2024

investigate more in detail proposals that will likely follow those analyzed in this paper. Moreover, a comparative study of SSI-based and other forms of identity management for the metaverse might, in the future, show a more comprehensive picture of the value trade-offs that designing an identity layer for the metaverse entails. As the metaverse will come closer to a full-scale adoption, providing a viable answer to challenges of privacy, security, control over identity, interoperability and immersion will become more pressing. The contribution of interdisciplinary paradigm that joins different forms of expertise and knowledge will be of the utmost importance. The preliminary investigation that I have carried out in this research aims to represent a first step in this direction.

Acknowledgements

The author(s) received no financial support for the research, authorship, and/or publication of this article

5 References

Al-Suqri, M. N., & Al-Aufi, A. S. (A c. Di). (2015). *Information Seeking Behavior and Technology Adoption: Theories and Trends*. IGI Global. https://doi.org/10.4018/978-1-4666-8156-9

Anand, N., & Brass, I. (2021). *Responsible Innovation for Digital Identity Systems*. https://doi.org/10.5281/ZENODO.5175334

Buccafurri, F., Fotia, L., & Lax, G. (2016). Implementing Advanced Electronic Signature by Public Digital Identity System (SPID). In A. Kő & E. Francesconi (A c. Di), *Electronic Government and the Information Systems Perspective* (Vol. 9831, pp. 289–303). Springer International Publishing. https://doi.org/10.1007/978-3-319-44159-7_21

Doorn, N., Schuurbiers, D., Van De Poel, I., & Gorman, M. E. (A c. Di). (2013). *Early engagement and new technologies: Opening up the laboratory* (Vol. 16). Springer Netherlands. https://doi.org/10.1007/978-94-007-7844-3

Dumitrescu, A.-T., & Pouwelse, J. (2024). *Failures of public key infrastructure: 53 year survey* (No. arXiv:2401.05239). arXiv. http://arxiv.org/abs/2401.05239

Ermoshina, K., & Musiani, F. (2019). "Standardising by running code": The Signal protocol and *de facto* standardisation in end-to-end encrypted messaging. *Internet Histories*, *3*(3–4), 343–363. https://doi.org/10.1080/24701475.2019.1654697

European Union. (2022). *European Declaration on Digital Rights and Principles for the Digital Decade*. https://ec.europa.eu/newsroom/dae/redirection/document/94370

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T., & Zuffo, M. K. (2020). Self-Sovereign Identity for IoT environments: A Perspective. *2020 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS49054.2020.9119664

Feige, U., Fiat, A., & Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of Cryptology*, *1*(2), 77–94. https://doi.org/10.1007/BF02351717

Friedman, B., & Hendry, D. (2019). *Value sensitive design: Shaping technology with moral imagination*. The MIT Press.

Friedman, B., Kahn, P., & Borning, A. (2002). Value sensitive design: Theory and methods. *University of Washington technical report*, *2*(8).

Gabrielsen Jumbert, M., Bellanova, R., & Gellert, R. M. (2018). *Smart Phones for Refugees. Tools for Survival, or Surveillance?*

Ghani, N. A., Hamid, S., Targio Hashem, I. A., & Ahmed, E. (2019). Social media big data analytics: A survey. *Computers in Human Behavior*, *101*, 417–428. https://doi.org/10.1016/j.chb.2018.08.039

Ghirmai, S., Mebrahtom, D., Aloqaily, M., Guizani, M., & Debbah, M. (2023). *Self-Sovereign Identity for Trust and Interoperability in the Metaverse* (No. arXiv:2303.00422). arXiv. http://arxiv.org/abs/2303.00422

Gregušová, D., Halásová, Z., & Peráček, T. (2022). eIDAS Regulation and Its Impact on National Legislation: The Case of the Slovak Republic. *Administrative Sciences*, *12*(4), 187. https://doi.org/10.3390/admsci12040187

Halder, R., Das Roy, D., & Shin, D. (2024). A Blockchain-Based Decentralized Public Key Infrastructure Using the Web of Trust. *Journal of Cybersecurity and Privacy*, *4*(2), 196–222. https://doi.org/10.3390/jcp4020010

Hardman, D. (2019). *What if I lose my phone? And how do I mitigate such disasters before they happen? Sovrin Identity For All [Whitepaper]*. https://sovrin.org/wp-content/uploads/2019/03/What-if-someone-steals-my-phone-110319.pdf

Ishmaev, G., Noordhoek, R., Van Steenbergen, M., & Vermaes, N. (2023). Value Sensitive Design for Self-Sovereign Identity Solutions: Conceptual Investigation of uNLock Use Case. *Digital Society*, *2*(2), 24. https://doi.org/10.1007/s44206-023-00046-2

Jung, Y. (2011). Understanding the Role of Sense of Presence and Perceived Autonomy in Users' Continued Use of Social Virtual Worlds. *Journal of Computer-Mediated Communication*, *16*(4), 492–510. https://doi.org/10.1111/j.1083-6101.2011.01540.x

Kaurin, D. (2019). *Data protection and digital agency for refugees*.

Laborde, R., Ferreira, A., Lepore, C., Kandi, M.-A., Sibilla, M., & Benzekri, A. (2023). The Interplay Between Policy and Technology in Metaverses: Towards Seamless Avatar Interoperability Using Self-Sovereign Identity. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 418–422. https://doi.org/10.1109/MetaCom57706.2023.00080

Lessig, L. (1997). Reading The Constitution in Cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.41681

Maurer, U. M., & Wolf, S. (2000). The Diffie–Hellman Protocol. *Designs, Codes and Cryptography*, *19*(2/3), 147–171. https://doi.org/10.1023/A:1008302122286

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1428

Miller, J. K., Friedman, B., & Jancke, G. (2007). Value tensions in design: The value sensitive design, development, and appropriation of a corporation's groupware system. *Proceedings of the 2007 International ACM Conference on Conference on Supporting Group Work - GROUP '07*, 281. https://doi.org/10.1145/1316624.1316668

Miller, K., & Taddeo, M. (A c. Di). (2017). *The ethics of information technologies*. Routledge.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things*, *8*, 100107. https://doi.org/10.1016/j.iot.2019.100107

Motti, V. G., & Caine, K. (2015). Users' Privacy Concerns About Wearables: Impact of Form Factor, Sensors and Type of Data Collected. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (A c. Di), *Financial Cryptography and Data Security* (Vol. 8976, pp. 231–244). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-48051-9_17

Niksirat, K. S., Velykoivanenko, L., Zufferey, N., Cherubini, M., Huguenin, K., & Humbert, M. (2024). Wearable Activity Trackers: A Survey on Utility, Privacy, and Security. *ACM Computing Surveys*, 3645091. https://doi.org/10.1145/3645091

Papageorgiou, A., Mygiakis, A., Loupos, K., & Krousarlis, T. (2020). DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System. *2020 Global Internet of Things Summit (GIoTS)*, 1–5. https://doi.org/10.1109/GIOTS49054.2020.9119673

Pierucci, F., & Cesaroni, V. (2023). Data Subjectivation—Self-sovereign Identity and Digital Self-Determination. *Digital Society*, *2*(2), 21. https://doi.org/10.1007/s44206-023-00048-0

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning.

Ruckenstein, M. (2014). Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles. *Societies*, *4*(1), 68–84. https://doi.org/10.3390/soc4010068

Schoemaker, E., Martin, A., & Weitzberg, K. (2023). Digital Identity and Inclusion: Tracing Technological Transitions. *Georgetown Journal of International Affairs*, *24*(1), 36–45. https://doi.org/10.1353/gia.2023.a897699

Sonia Huang, J. (2011). An Examination of the Business Strategies in the Second Life Virtual Market. *Journal of Media Business Studies*, *8*(2), 1–17. https://doi.org/10.1080/16522354.2011.11073520

Southerton, C. (2020). Datafication. In L. A. Schintler & C. L. McNeely (A c. Di), *Encyclopedia of Big Data* (pp. 1–4). Springer International Publishing. https://doi.org/10.1007/978-3-319-32001-4_332-1

Sovrin Foundation. (2022). *Self-sovereign identity and IoT*. *Sovrin identity for all [Whitepaper]*. https://sovrin.org/wp-content/uploads/SSI-in-IoT-whitepaper_Sovrin-design.pdf

Steen, M. (2011). Tensions in human-centred design. *CoDesign*, *7*(1), 45–60. https://doi.org/10.1080/15710882.2011.563314

Stephenson, N. (1992). *Snow crash*. Bantam Books.

Tsai, C.-W., Lai, C.-F., Chiang, M.-C., & Yang, L. T. (2014). Data Mining for Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 77–97. https://doi.org/10.1109/SURV.2013.103013.00206

Wang, F., & 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*, 28. https://doi.org/10.3389/fbloc.2019.00028

Xue, Y. (2019). A review on intelligent wearables: Uses and risks. *Human Behavior and Emerging Technologies*, *1*(4), 287–294. https://doi.org/10.1002/hbe2.173

Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., & Herbke, P. (2023). Toward Interoperable Self-Sovereign Identities. *IEEE Access*, *11*, 114080–114116. https://doi.org/10.1109/ACCESS.2023.3313723

Biographies

Federico Pierucci. Federico Pierucci is a PhD Candidate in Human Rights, Global Politics, and Sustainability at Sant'Anna School of Advanced Studies, investigating the philosophical foundations of the European digital transition. Previously, he worked as a researcher and project manager for Horizon 2020 and Horizon Europe projects in Rome and Brussels. He studied EU project management through the executive program on Management and Control of EU Funding" at LUISS Business School. He also gained research experience in computational social sciences at ISTC-CNR. He holds a bachelor's degree in philosophy from Sapienza University of Rome and a master's degree in philosophy from Alma Mater Studiorum – University of Bologna.
ORCID: https://orcid.org/0000-0001-9809-3978
CRediT Statement: Conceptualisation, Methodology, Investigation, Writing – Original Draft, Writing – Review and Editing.