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

Romain Laborde, Afonso Ferreira, Cristian Lepore, Abdelmalek Benzekri, Mohamed Ali Kandi, Michelle Sibilla

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

Romain Laborde[1]✉, Afonso Ferreira[2]✉, Cristian Lepore[1], Mohamed-Ali Kandi[1], Michelle Sibilla[1], Abdelmalek Benzekri[1]
Institut de Recherche en Informatique de Toulouse
[1]*Université Paul Sabatier Toulouse III*
[2]*CNRS*
Toulouse, France
{firstname.lastname@irit.fr}

***Abstract*—This paper explores the interplay between public policy in areas related to digital privacy and security and the development of new metaverse technologies that need to be compliant-by-design. Such interdependency is illustrated here through the proposal of a solution to implement seamless cross-metaverses avatar interoperability that preserves data privacy and portability. The new proposed scheme is based on the Self-Sovereign Identity concept and architectures, along with off-line governance agreements, in order to ensure that avatars can travel between metaverses while keeping whatever attributes they possess and that are compatible in the crossed metaverses. Many new and exciting avenues for technological research arise from such an interdisciplinary perspective.**

***Index Terms*—metaverse, security, privacy, data-protection, digital policy, governance, EU legislation, self-sovereign identity**

I. Introduction

Metaverse research witnessed a first wave of "hype" between the years 2000 and 2006, with many results and visibility. Currently, in 2023, it is going through a second wave of interest, now brought about by commercial players that started to market their metaverses and events held inside them, but also by a widely publicised metaverse-related public announcement by one of the Western Big-Techs in late 2021.

As a consequence, many people outside the metaverse community think that the metaverse is a product, or a brand of some social network company, and not a name given to a set of Web platform technologies that intend to implement digital worlds. Nevertheless, the concept of virtual worlds dates back at least to the 19th Century [1], while the very term *metaverse* was coined to describe a futuristic concept in a science fiction book in 1992 [2].

In practice today, metaverses refer to a new type of Web platform, supported through a comprehensive set of technologies, some of which already consolidated and others in evolution, which will allow users greater interactivity and socialisation in immersive 3D digital environments, represented by a universe of new digital worlds, mirrored or not in the physical world. Examples of such commercial endeavours include Second Life, Decentraland, Somnium Space, The Sandbox, Roblox, Horizon Worlds, Avakin Life, Mesh, and others.

On the other hand, nowadays, software and other digital infrastructures can no longer be developed in isolation, as in the past, and must closely follow policy and regulation trends. In this respect, we note that the emergence of such powerful technologies is already catching the attention of regulators, in particular in the European Union (EU) [3]. And, just like with its General Data Protection Regulation (GDPR) [4], data privacy and portability will rank high in the EU policy making with respect to metaverses.

But, in clear contrast with such policy intentions, the sample metaverses mentioned above operate as entities that are fully silo-ed from each other ,where there is a lack of interoperability, as avatars are confined to a single metaverse and its worlds, not being allowed to move from one metaverse to another platform, without logging in again from the physical world.

In this paper, we explore first steps in the direction of implementing metaverse data privacy and portability, through a new solution to implement seamless cross-metaverses avatar interoperability. Based on offline agreements, we propose to use the Self-Sovereign Identity (SSI) concept and fully distributed architectures in order to ensure that avatars can travel between metaverses while keeping whatever attributes

that are compatible in the crossed metaverses.

This paper is organised as follows. The next section frames the metaverse concepts used in our work. Then, we explore some interesting aspects related to digital governance, taken from the EU perspective, that will likely regulate the metaverse space within this decade. In sequence we recall the main technical features of the Self-Sovereign Identity solution promoted by the W3C and introduce our proposed Self-Sovereign Identity architecture for seamless cross-metaverses travelling by avatars. We close the paper with some concluding remarks and avenues for further research.

II. The nexus of policy, governance, and technology

The metaverses considered in this paper encompass their full vision as digital worlds that are massive (can host an unlimited number, or at least a very high number of concurrent users), immersive (offer three-dimensional and embodied experiences), persistent (never stop or reset, as perceived by users), open (anyone with good Internet connectivity and enough computing power can have access) and economically developed (have extensive trade in goods and services within them) [5].

The governance **inside** such metaverses will be different from that of the interface between the digital world of a metaverse and our physical world, which is becoming already heavily regulated, at least in the EU, where the rule-of-law is dominant and its institutions are mostly fit for purpose. However, in this new technological frontier that are metaverses, it is not clear what will be regulated, who will establish and enforce rules, or how this will be done.

Indeed, as commerce will be ubiquitous inside metaverses, regulations about products, transactions, property rights, and other businesses will be necessary for markets to thrive. Then, all kinds of conflicting situations will have to be resolved by some form of authorities, police, and courts. As well, there must be rules of trade, taxation, income, etc.

An analysis of the evolution of metaverse support technologies and especially when thinking about Web platforms with great interactivity and greater social reach, brings many questions and concerns, especially regarding cybersecurity, privacy, and protection of (personal) data, regulations, and various aspects of the governance of such digital worlds [6].

III. From EU policy to software design requirements

The very technological offer of interactivity and immersion of next-generation metaverses will heavily depend on wearable devices monitoring both biometric (e.g., gait, facial expressions, temperature) and neurometric (e.g., fear, satisfaction, attention) data, which will imply continuous and full surveillance of users. In Western societies, where privacy and protection of personal data are fundamental rights, commercial and public interests will have a very difficult relationship concerning this topic.

Therefore, the emergence of metaverses raises a wide range of concerns regarding their compatibility with the law. It will be thus necessary to go beyond the well-known concepts of security-by-design and privacy-by-design towards an encompassing *Compliance-by-Design* paradigm, if at all possible.

Accordingly, the impact of public policies on the metaverses market will be felt in a wide range of technical fields, such as interoperability, digital identity, privacy, and data portability. It should for instance be possible for avatars who are experiencing a digital world on a particular metaverse platform of a company, to be able to move, without impediments and in a transparent way, into another metaverse platform, from another company, without the need to identify themselves again in the physical world.

And this leads us to the technological focus of this work, namely the implementation of a digital identity architecture in metaverses that integrate data protection and portability by design.

IV. Self-Sovereign Identity

Identity in a wide sense encompasses every attribute of an entity, i.e., any characteristic or property of the entity that can be used to describe its state, appearance, or other aspects [7]. The Self-Sovereign Identity (SSI) concept aims to give people control of their identity information in the digital realm. Allen [8] defined the principles of self-sovereign identity as: access, existence, protection, consent, minimalization, control, persistence, portability, interoperability, and transparency. Self-sovereign identity illustrates a new decentralized identity model where users are at the center and control the sharing of their identity. Different implementation strategies have been experimented in the last recent years [9], [10]. Currently, the W3C verifiable credentials standards is considered as the reference for exchanging proofs of identity [11]. This architecture encompasses the following entities: the issuer, the subject / holder, and the verifier.

An *issuer* asserts a claim and releases verifiable credentials (VC) about *subjects* for *holders*. A *subject* is a human being, an animal, or something for which claims are issued. In many cases, the subject and the holder are the same person. However, they can be different, like when a parent may hold credentials about his/her child, the owner of an object about it, etc. Once a credential is received, for instance an ID

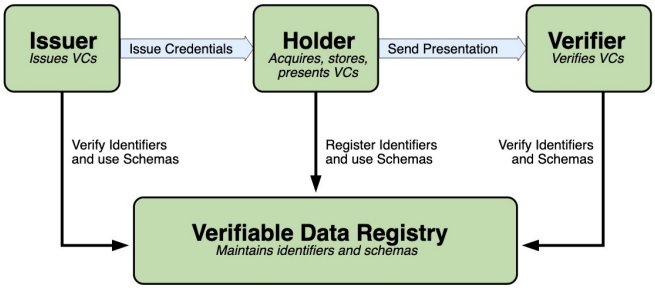

Fig. 1. The W3C Verifiable Credentials architecture [11]

card, a payslip, or an insurance policy, the holder can store it in a *digital wallet*. To assert a composition of attributes of a subject to a *verifier*, the holder can compose a *verifiable presentation* by combining those different VCs required by the verifier. The *verifiable data registry* mediates the creation and verification of identifiers, keys, and other relevant data, like VC schemes and revocation registries.

The W3C also proposes a complementary standard called the Decentralized identifiers (DID) [12]. This new type of identifier is controlled and created by individuals and lasts for as long as their controller wishes to use it in a decentralized registry. A DID is simply a URI which resolves to a DID document that contains the key material and other metadata to reference services relevant to interactions with the DID subject. A DID is composed of three parts separated by ":" such as *did:scheme:identifier*. The *scheme* refers to the technology-specific verifiable data registry used for recording DID documents, which can be any form of trusted data storage (e.g., distributed ledgers, decentralized file systems, databases of any kind, or peer-to-peer networks etc). The scheme specifies the operations by which DIDs and DID documents are created, resolved, updated, and deactivated. The *identifier* is a unique value within the scope of the scheme. A DID is governed by its DID controller which has the capability to manage the life cycle of the associated DID document. The controller of the DID can be the subject of the DID or another entity.

V. Cross-metaverses avatar interoperability

Avatars can be created via a dedicated avatar editor that may be provided by a metaverse or an independent service. In our perspective, once created, one avatar is dependent on its physical person owner, implying that it does not evolve autonomously and only is present in a metaverse at a given time if its owner has been granted access to that metaverse.

An avatar is unique and therefore cannot "exist" in different metaverses at the same time (Property of

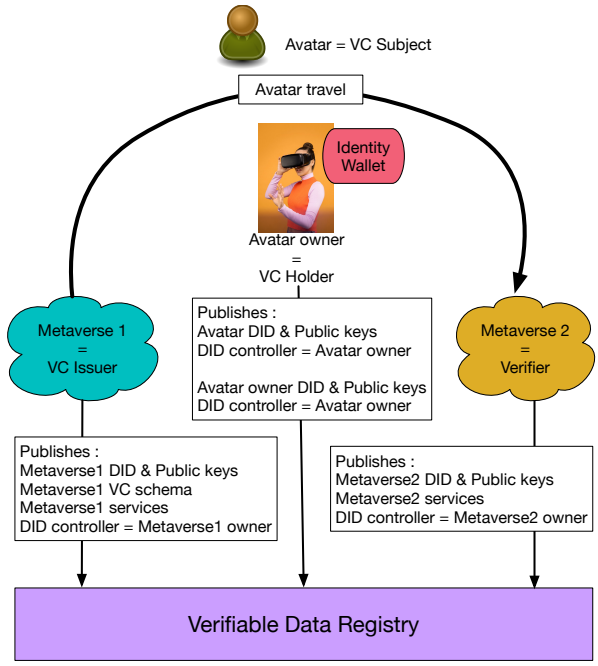

Fig. 2. The cross-metaverses avatar interoperability architecture

cross-metaverse avatars' uniqueness). Once an avatar leaves a metaverse to enter into a new one, it should be deactivated from the metaverse of origin before being able to interact in the destination metaverse.

Furthermore, in an ideal implementation of metaverses, an avatar would evolve during its life time. It may gain experience and/or new features in the metaverse it is visiting. While this evolution should be reported in the next metaverse where the avatar will travel, at the same time a feature may be omitted by the destination metaverse when it is in contradiction with the metaverse rules.

We propose to apply the principles of SSI to create a sort of passport system so that avatars may travel across metaverses that accept such a proof of identity. The general idea consists in exchanging avatar data in the form of verifiable credentials, like in passports. When an avatar travels from Metaverse1 to Metaverse2, the owner will request Metaverse1 to issue a verifiable credential for its avatar and send it to Metaverse2 which plays the role of VC verifier. This allows avatar owners to keep control of their avatars and provide a proof of the avatars' characteristics and features to destination metaverses, signed by the source metaverse. To do so, we assume that there exists a minimum trust relationship between metaverses, which must be formalised by a dedicated governance organisation: i) a metaverse does not lie to another metaverse about the presence of an avatar, and ii) all signatories agree to use verifiable credentials. A standard VC schema for a

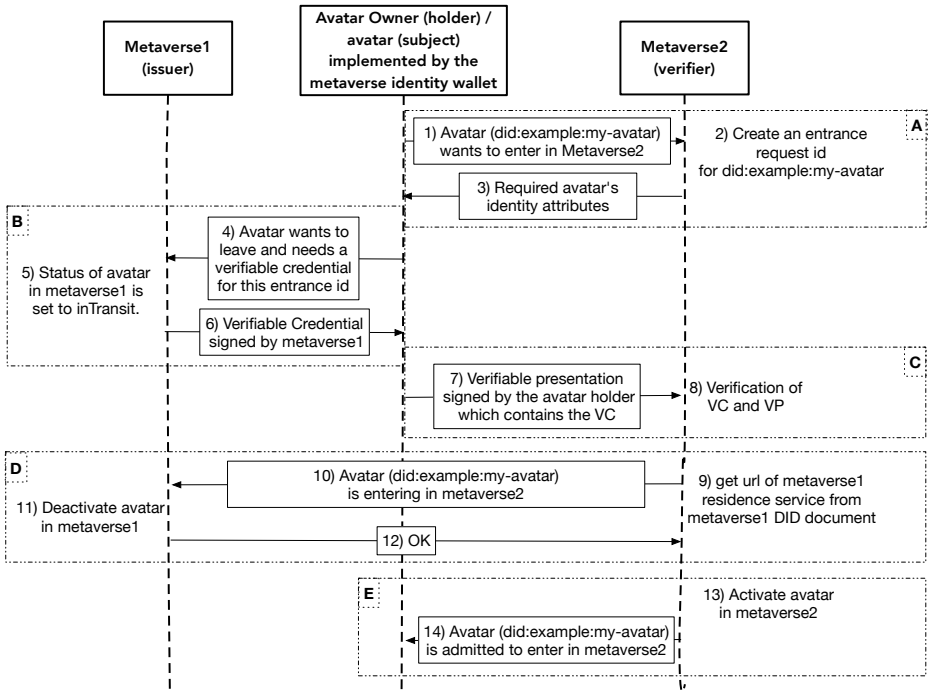

Fig. 3. Our XMAT Protocol

minimum set of globally recognised avatars' attributes would improve interoperability but is not mandatory. The whole architecture is described in Fig. 2.

Our proposed system assumes that each metaverse has a DID and publishes the DID document in a verifiable data registry. The DID document should contain its public keys, the verifiable credential scheme it can issue, and also the URLs of the required services (the metaverse entrance request service, the metaverse entrance application submission service, the metaverse departure request service and the residence service used between metaverses to coordinate the management of avatars' places-of-stay uniqueness). To protect the privacy of the avatar and thus of its owner, the residence service can only be called by trusted metaverses.

For their part, users (called avatar owners) have a metaverse identity wallet system in their device. Any avatar owner has also a DID and publishes the DID document with its public keys in the verifiable data registry[1]. An avatar owner may have several DIDs for privacy reasons. When an owner creates an avatar, a new DID is created for the new avatar. An owner may have multiple avatars. The keys of the avatar are managed by the owner in the metaverse identity wallet. Therefore, the owner is the controller of the avatar's DID document. One of the advantages of this proposed solution appears in the case where the owner wants to transfer or sell its avatar to another user: (s)he only needs to change the controller in the avatar's DID document to validate the transaction.

Once these requirements are met, cross-metaverses travel can be implemented by our XMAT (Cross-Metaverses Avatar Travel) protocol. Fig. 3 depicts the different messages in a generic and natural language. The following explanations will provide inputs for implementing it as a REST API. The XMAT protocol expects the communication channel to be secure (e.g. HTTPS) and consists in the five following phases:

Phase A - Entrance request. When an avatar wants to travel from Metaverse1 to Metaverse2, it needs to start by calling the Metaverse2 *entrance request service*. The URL of this service shall be available in the Metaverse2 DID document. The avatar provides its DID and Metaverse2 returns to the avatar a unique entrance request identifier and list of identity attributes required by Metaverse2.

Phase B - Verifiable credential request. After having received the entrance request application, the avatar calls the Metaverse1 *departure request service* to obtain the VC of the attributes required by Metaverse2. This request shall be signed by the avatar's private key and the associated public key shall be available in the avatar's DID document. The VC request only includes the entrance request identifier and the list of required avatar identity

[1]The management of the keys and the authentication of the person on the device is out of the scope of this paper, but password-less solutions such as [13] can be employed.

attributes. It should not contain the destination metaverse DID to prohibit a metaverse to control where an avatar can travel. To maintain the properties of avatars' uniqueness and consistency, the status of the avatar is changed to inTransit in Metaverse1 once the request is received. Indeed, values of identity attributes included in the VC shall not change until the travel of the avatar is either finalized or refused by Metaverse2. For security reasons, the VC also contains the entrance Request Identifier (entranceRequestId) and an expiration date to avoid malicious users to reuse the VC and an avatar to be in status inTransit forever.

Phase C - Verifiable presentation submission. After receiving the VC from the metaverse, the owner encapsulates it into a verifiable presentation (VP), signs the VP and sends it to Metaverse2. This can be done by calling a specific service provided by Metaverse2, whose URL is specified in the DID document of Metaverse2. The VP is a proof that the avatar owner wants its avatar to travel to that specific metaverse. Thus, it shall include the entranceRequestId and the destination of the travel. The destination metaverse can then verify the VC and the VP (validity period, signatures, attributes values, etc).

Phase D - Current avatar residence modification. If the VC and the VP are correct, i.e. are complying with the destination regulations, Metaverse2 indicates the new residence of the avatar to the metaverse of origin. This can be implemented by calling a residence service listed in the Metaverse1 DID document. This message shall include the VC and VP to prove the acceptance of the avatar owner. Then Metaverse1 can deactivate the avatar so that it doesn't exist anymore in Metaverse1.

Phase E - Notification of the decision. The last phase consists in creating or activating the avatar and notifying the decision to the avatar owner.

Our proposed XMAT protocol allows avatars to travel across metaverses while preserving their fundamental rights as well as of their owners. The protocol respects the sovereignty of the avatar owner and of destination metaverses, that keep control of places where the avatar can travel, while the metaverse of origin has no authority on it. Privacy of the avatar owner is also preserved because DID can be used as a pseudonym and the owner can have multiple DIDs. Finally, the avatar's privacy is controlled by its owner, who can monitor any data related to the avatar to be shared with a destination metaverse, since (s)he generates the verifiable presentation. Noticeably, this protocol requires previous off-line agreements about policies to govern the relationships between metaverse platforms.

VI. Conclusion

In this paper we explored impacts that public policy and legislation may have on questions of metaverse security and privacy. Our XMAT solution, based on the SSI architecture, is fully decentralised and respects data privacy and portability.

Plethora of open questions remain, when we confront current digital policies and the technological requirements of such ambitious systems as metaverses, including implementation tests of our proposed protocol. Research will be required about adapted technical regulations to guide hardware manufacturers and software developers with respect to compliance with the law, including data governance and operational governance rules. We note that technological and systems research in this area are intrinsically transdisciplinary and cross-dependent with research in policy and governance.

Acknowledgments

This work was partially supported by the European research projects H2020 CyberSec4Europe (GA 830929) and LeADS (GA 956562), Horizon Europe DUCA (GA 101086308), and CNRS EU-CHECK.

References

[1] T. Boellstorff, "The metaverse isn't here yet, but it already has a long history," The Conversation, Tech. Rep.

[2] N. Stephenson, Snow Crash. United States of America: Bantam Books, 1992.

[3] E. Commission, "People, technologies & infrastructure – europe's plan to thrive in the metaverse," https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5525.

[4] ——, "General data protection regulation," https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[5] S. Gilbert, "The political economy of the metaverse," Briefings de l'IFRI, IFRI, Tech. Rep.

[6] J. Smart, N. Cascio, and J. Paffendorf, "Metaverse roadmap – pathways to the 3d web: A cross - industry public foresight project," https://metaverseroadmap.org/MetaverseRoadmapOverview.pdf.

[7] I. 24760, "ISO/IEC 24760-1:2011 - Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts," ISO/IEC, Tech. Rep., 2011.

[8] "The Path to Self-Sovereign Identity," http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[9] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and fido," IEEE Communications Standards Magazine, vol. 3, no. 4, pp. 14–20, 2019.

[10] A. Preukschat and D. Reed, Self-sovereign identity. Manning Publications, 2021.

[11] W3C, "Verifiable Credentials Data Model v1.1," https://www.w3.org/TR/vc-data-model/.

[12] ——, "Decentralized Identifiers (DIDs) v1.0," https://www.w3.org/TR/did-core/.

[13] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "A user-centric identity management framework based on the w3c verifiable credentials and the fido universal authentication framework," in 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2020, pp. 1–8.