PROOF OF CONCEPT: SELF-SOVEREIGN IDENTITY IN METAVERSE

Raluca-Veronica BRĂCĂCESCU[1*]

The Self-Sovereign Identity (SSI) model is the most modern approach to digital identity management. The metaverse is one of the future technologies, providing users with virtual experiences from gaming to social, business, and education. Like any other platforms, metaverses must manage user identities, but in a secure, transparent, privacy-preserving, and decentralized way. This paper aims to analyze if Self-Sovereign Identity can be integrated inside metaverse and be used there, bringing its intrinsic advantages. System architecture and technical implementation are documented in detail as proof of concept demonstrating the feasibility of SSI in the metaverse.

Keywords: , metaverse, decentralization, blockchain

1. Introduction

David Birch, in his book "Identity is the New Money", has mentioned, since 2014, modern services have required a new infrastructure for managing digital identities. Existing centralized identity models are no longer viable in the new era of the Internet, as a result, users should regain control over their digital identities [1].

The metaverse is one of the most popular topics now, attracting both enthusiasm and skepticism. According to [2], the metaverse is more likely to be embraced in countries such as China, India, Mexico and Peru, while countries such as Canada, the UK, and Japan have more concerns about it. China is making significant investments in metaverse development. Shanghai has announced plans to establish 30 metaverse attractions by the end of 2025, as part of a broader smart tourism initiative [2]. These actions reflect a growing recognition of the metaverse's transformative potential.

Mordor Intelligence, as cited in [3], estimates that the metaverse market size will reach USD 165.57 billion in 2025 and grow at a CAGR of 41.83%, rising to USD 950.23 billion by 2030.

The metaverse is one of the technologies of the future, so managing digital identities securely and efficiently is critical. It must also align with the Web3 key principles and the most modern ideas of decentralization, blockchain and minimal

[1] PhD Student, NUST POLITEHNICA Bucharest, Romania, corresponding author, e-mail: raluca.bracacescu@stud.acs.upb.ro

data disclosure of users. In this context, Self-Sovereign Identity (SSI) emerges as a suitable model, offering users full control over their digital identities without relying on centralized intermediaries.

This paper presents the intersection of SSI and the metaverse. A proof-of-concept project architecture and implementation is proposed for the idea of SSI based authentication/access into metaverse's scenes. Decentraland is the metaverse platform choice and Veramo Framework for SSI. Verifiable credentials are integrated and used alongside decentralized identifiers to verify users' identity and attributes. To the best of our knowledge, this study provides the first concrete documented implementation of SSI verifiable credentials in Decentraland.

2. Related Works

Self-Sovereign Identity (SSI) is a modern digital identity management model where user control and decentralization are the focus. In traditional centralized or federated systems, third-party identity providers are totally in charge of digital identities. Instead, SSI enables users to handle their identification, authentication, and authorization processes. This model allows users to generate and manage their own digital identifiers and associate personal information. By leveraging cryptographic techniques and blockchain technology, SSI offers enhanced security and privacy protection.

Decentralized Identifiers (DIDs) are unique, cryptographically verifiable identifiers, defined by the W3C standard, and fundamental concept of SSI [4].

Verifiable Credentials (VCs) are digitally signed credentials that allow secure and privacy-preserving exchange of claims, personal information, about a subject (name, age, qualifications, address). The credential is cryptographically signed by the issuer using their private key. Verifiers can then validate the authenticity and integrity of the credential using the issuer's public key [4].

The term "Metaverse" was used for the first time in the science fiction novel Snow Crash written by Neal Stephenson and published in 1992. The book shows a dystopian future dominated by corporate states and hyper-capitalism, in which the metaverse represents an escape from the downgrade and inequity of society. Metaverse is described as a virtual reality in which users interact through avatars [5,6].

Metaverse is a virtual world where users can play and create games, socialize, explore, participate in different events or make business transactions. The concept integrates for the users all the possible online experiences in one platform.

Metaverse has some main characteristics that were classified in four categories [7]: time-space permeability (persistence, consistency and stability, scalability, multidimensionality), real-virtual mirroring (perfect integration, multisensory experience, virtual object interaction, personalized experience, real

time interaction, special mapping and simulation, virtual representation), technology converge (cross-platform compatibility, user content generation, identity and rules, large scale access, real-time communication and collaboration, decentralization, interoperability and standardization) and human-computer linkage (multi-modal interface, minimal cognitive load, gesture recognition, understanding and anticipating human behavior, intuitive navigation, connectivity and accessibility).

The metaverse is still considered to be in its conceptual and evolutionary stages, but there are several key technologies that are shaping it: communications networks (6G) [8], extended reality (XR), edge computing, digital twins, blockchain, and machine learning [9].

There are already many Metaverse platforms widely used today. These platforms are either centralized or decentralized, and are more focused on gaming or social experiences, business transactions.

Decentraland [10], built on Ethereum blockchain, is one of the main decentralized metaverse projects, offering a virtual environment governed by its users through a Decentralized Autonomous Organization (DAO) [11]. Decentraland functions using two tokens LAND and MANA. LAND is an NFT (Non-fungible token) for properties and MANA is platform's cryptocurrency [12].

The Sandbox [13] operates on the Ethereum blockchain and has three main components: LAND, SAND, and user-generated content. Sandbox gives creators the ability to monetize their contributions and participate in the governance through DAO, like Decentraland.

Roblox [14] is a very popular virtual platform that allows users to create, explore, and share 3D experiences and games. Launched in 2006 by Roblox Corporation, Roblox has now millions of daily active users.

Fortnite [15], developed by Epic Games and released in 2017, is a multiplayer online Battle Royale game that has evolved into a virtual platform, a space for social interaction, virtual events, and experiences.

Horizon Worlds [16] is the virtual reality (VR) platform developed by Meta. It operates on a centralized governance model, Meta has full control over platform rules, content moderation, and user data management. This approach has drawn criticism regarding data privacy and the security of personal information.

Mesh for Microsoft Teams [17] is a business-focused metaverse solution introduced by Microsoft. Designed to enhance hybrid work models, Mesh for Teams integrates with the Microsoft ecosystem, providing a new way to connect across physical and digital spaces.

Table 1

Classification of Metaverse Platforms and their purposes

Metaverse Platform	Management type	Blockchain -based	Governance Model	Purpose	Platform Access

Decentraland	Decentralized	Yes	DAO	Digital commerce/ Social	Web/Desktop
The Sandbox	Decentralized	Yes	DAO	Gaming/ Commerce	Web/Desktop
Roblox	Centralized	No	Corporate	Gaming/ Creation	Desktop/Mobile
Fortnite	Centralized	No	Corporate	Entertainment	Cross-Platform
Horizon Worlds	Centralized	No	Corporate	Social/VR	VR-only
Mesh	Centralized	No	Corporate	Professional/ Corporation	Cross-Platform

3. Proposed solution for Self-Sovereign Identity in the Metaverse

Self-Sovereign Identity (SSI) can contribute to the development of a decentralized and interoperable metaverse. Currently, most metaverse platforms, whether centralized (such as Horizon Worlds or Roblox) or blockchain-based (Decentraland, The Sandbox), use digital identity management models which limit user portability and autonomy [18]. Authentication is achieved through Metamask [19] (Decentraland, Sandbox, Voxels) or via email and user account on the platform (Roblox, Fortnite, Horizon Worlds).

SSI allows users to create and manage their digital identities through verifiable credentials (VC) and decentralized identifiers (DID). In metaverses, SSI provides interoperability and security by removing the reliance on centralized authentication. A user can use the same digital identity to access different virtual worlds without having to create multiple accounts, avoiding the risks of identity theft or excessive data exposure [20]. SSI enhances digital economy by facilitating secure and verifiable transactions between users, creators, and entities [21].

The system proposed in this paper aims to serve as proof-of-concept for using Self-Sovereign Identity (SSI) with Verifiable Credentials in the metaverse. To achieve this, a set of essential SSI-related functionalities has been incorporated into the developed system.

In Fig. 1, the use case diagram includes two actors: the user (owner of the digital identity and verifiable credentials) and issuer (the entity issuing the verifiable credentials). The most important functionality is the validation of the credential presented in the metaverse. However, this requires several prior steps, such as creating a Decentralized Identifier (DID) for both the user and the credential issuer, and issuing the credential, which must be signed with the issuer's private key.

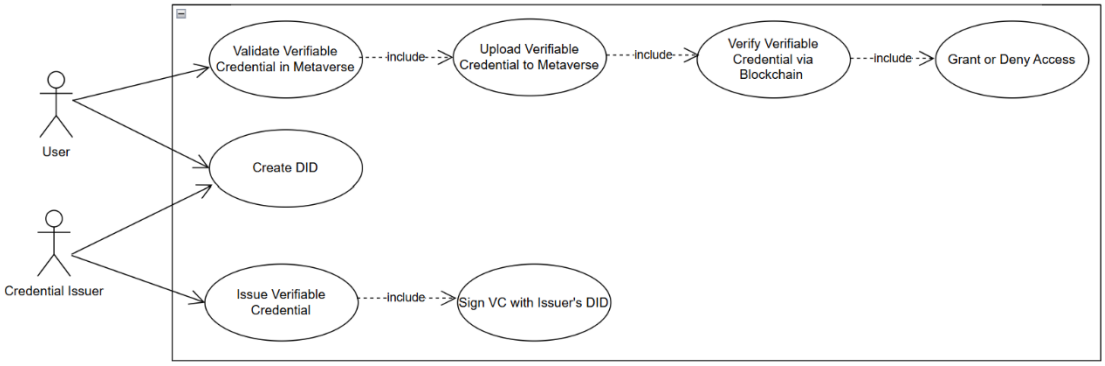

Fig. 1. User-case diagram of the proposed system

To validate a verifiable credential in the metaverse, the credential is first uploaded within a virtual scene by its owner. It will be verified using SSI cryptographic mechanisms via the blockchain. Its digital signature is checked using the issuer's DID. A call to the blockchain is made using the issuer's DID which returns the corresponding DID Document containing the issuer's public key. This key is then used to verify the credential's signature and determine whether it is valid or not. Based on the result, the user is either granted access to another scene or denied access.

These represent the core functionalities of the system. It can be extended in future work to include additional features, which may be explored in subsequent publications.

4. Architecture and implementation details

The objective of this paper is to present a proof-of-concept system architecture and implementation for SSI-based authentication and access control within metaverse environments. Users can validate their identities and attributes using verifiable credentials, disclosing only minimal personal information, and thereby gaining access to specific events, scenes, or transactions in the metaverse.

As already mentioned, there are two types of Metaverses, decentralized metaverses and centralized metaverses. Self-Sovereign Identity can be integrated only into decentralized Metaverses to be still able to follow its main principles of digital identity - decentralization, selective disclosure, user control over personal data and interoperability. Therefore, among the existing Metaverses platforms, Decentraland was chosen for the proof-of-concept implementation due to its blockchain-based infrastructure, decentralized governance through a Decentralized Autonomous Organization and its status as one of the most popular open metaverses to date. In the official form of Decentraland Metaverse, user authentication is done

using cryptocurrency wallets (MetaMask). This study proposes use of Verifiable Credentials, with the help of Veramo Framework in Decentraland scene.

Fig.2. illustrates the system architecture. The first layer consists of the Decentraland metaverse, where the user (the owner of a verifiable credential) interacts with a scene and uploads their credential. To verify the credential, Decentraland initiates a request to the Veramo Agent and its plugins, components of the Veramo Framework, that handle SSI related operations such as credential verification and DID resolution.

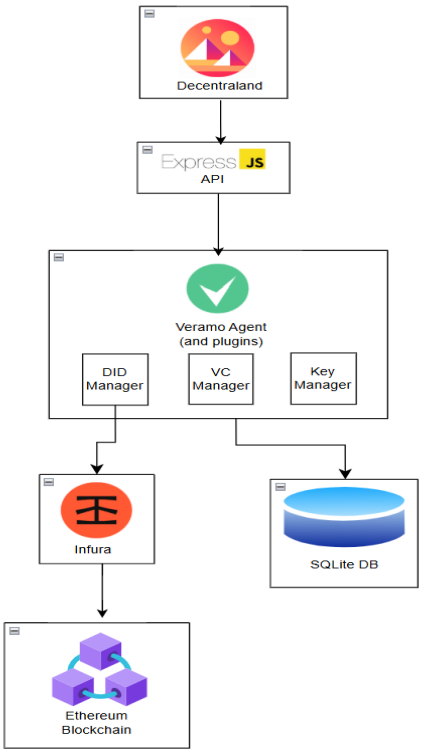

Fig.2. Architecture of the proposed system

This request is intermediate by an API layer implemented with Express.js, which serves as in-between the Decentraland frontend and the Veramo Agent running on the backend.

The next layer involves the blockchain, accessed via a gateway Infura, which allows for DID document retrieval and creation of the DIDs. Additionally, a local database (SQLite) is used to cache some requests and to store essential information keys, identifiers, and credentials required for the Veramo Agent to function properly.

Fig.3. further explains the proposed solution in detail by illustrating the main flow for verifying a verifiable credential (VC) presented by the user.

The credential is uploaded by the user within the Decentraland scene. The content of the VC is then forwarded to the Veramo Agent's VC Manager plugin via the Express.js API. The system must now validate its digital signature. This is done by extracting the issuer's DID, which is embedded within the credential itself.

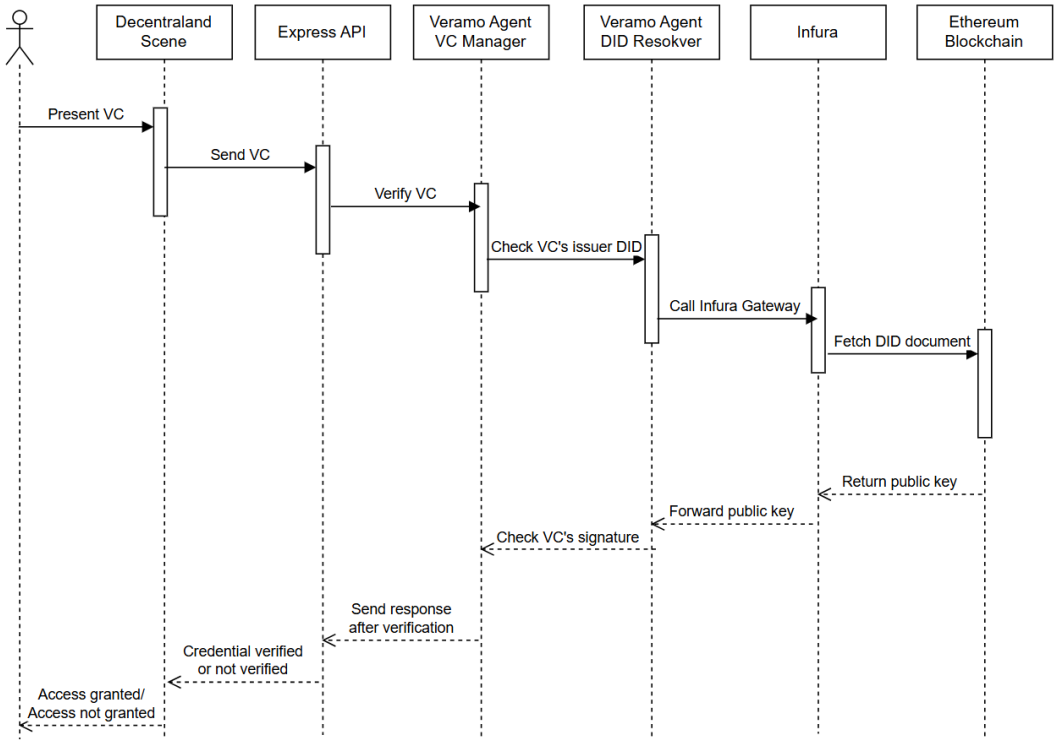

Fig.3. Flow Diagram of the proposed system

The DID Resolver plugin of the Veramo Agent uses the issuer's DID to retrieve the corresponding DID Document. This is accomplished by querying the Ethereum blockchain via the Infura Gateway. The retrieved DID Document contains the public key of the issuer.

The public key is then passed back to the VC Manager, which uses it to verify the signature on the credential. Once the verification is complete, the result is returned through the Express.js API to the Decentraland scene. Based on the outcome (valid or invalid), the access to a scene will be or will not be granted to the user.

Decentraland comes with a complete SDK for developing, making it easy to add new features. Several tools were needed to technically support the developement: Decentraland SDK, Veramo Framework and specific TypeScript

packages. Decentraland SDK is the official software development kit provided by Decentraland for the creation of custom scenes in the metaverse. It is TypeScript/JavaScript based; the code is written in .ts files. 3D scenes, games and experiences can be added using Decentraland SDK.

Veramo Framework [22] was used for managing the generation and verification of verifiable credentials. Veramo also allows development in TypeScript/JavaScript, which ensures compatibility with Decentraland SDK and runs in a local environment. It uses also a local sqlite database to manage the DIDs and VCs and Infura as blockchain infrastructure provider. Also, Sepolia test network was set up as Ethereum test network. All the logic is running on a local server made available with express and cors packages for TypeScript.

Tabel 2

Components and technologies

Component	Technology/Tool	Role
SSI Framework	Veramo	VC and DID management and operations
Blockchain	Ethereum	Resolves VC and DID and DID creation
Metaverse	Decentraland SDK	Main interface and 3D environment for user interaction
Code development	TypeScript/JavaScript	Used to develop both the metaverse scene and backend logic
Blockchain Gateway	Infura	Provides API access to the Ethereum blockchain
API	Express JS	Facilitates communication between Decentraland and Veramo Agent
Persistence	SQLite DB	Local storage for DID keys, metadata, and agent configuration

For further improvements, Metamask wallet can be used to store the verifiable credentials. MetaMask Snaps, an innovative extension of the MetaMask wallet, allows users to add additional functionality. These are individual applications, called Snaps, that can be installed directly into MetaMask to extend the wallet's capabilities. One such snap has already been initiated for managing SSIs in MetaMask, namely Mask [23].

5. Results and discussions

The system implementation was tested with various verifiable credentials containing different claims and issuers. In all cases where the credential's signature

was valid and the issuer's DID could be successfully resolved on-chain, access was granted in the Decentraland scene. Conversely, in cases where the credential was invalid, access was denied. This behavior confirms the correctness and robustness of the full verification flow, from credential upload to access decision. The implemented solution follows key SSI principles, such as user control, selective disclosure, and decentralization. Users remain in full control of their credentials, and only the minimum required information is disclosed during the verification process. This ensures privacy and security in line with the foundational goals of the SSI model.

The metaverse is still a relatively new topic within the scientific community, but there is already interest in it and in the challenges related to digital identities. In the article [24], a review of the application of digital identity in metaverse is presented. The authors conclude that, for the metaverse, secure and trusted digital identity technology must be decentralized. The digital identity management system must reestablish the user's sovereignty over their data and protect their privacy.

Studies [25] and [26] introduce frameworks for Metaverse Identity. Article [25] focuses more on defining the core principles and critical challenges of digital identity in the metaverse. Mentions interoperability, legal aspects, privacy and management, deepfake and synthetic identities, identity fragmentation and psychological well-being as challenges, but at the same time it presents methods for addressing these potential issues.

Article [26] introduces MetaSSI, a framework focused on personal data protection, security and privacy in metaverse environments. The authors propose a technical solution that includes an SSI-based authentication algorithm and a complete credential management flow for access granting to a service in the metaverse based on verifiable credentials. The system relies on Hyperledger Aries for SSI operations and tested in simulated 3D environments built with Unity or Unreal Engine, rather than in a public metaverse platform.

Furthermore, study [27] comes with an SSI solution for the metaverse that integrates (NFT with Non-Fungible Tokens) and encryption algorithms. This work focuses on trust and interoperability in the metaverse, remaining mostly theoretical, with emphasis on architecture and no technical details on the possible implementation.

Article [28] is thematically the closest to our work. It presents a use case for access to a virtual cinema in Decentraland controlled using verifiable credentials to validate user age, with NFT-based ticket issuance. While the authors present UML sequence diagram and smart contracts class diagram, they do not detail the implementation of SSI components such as credential verification, DID resolution, or integration with SSI frameworks.

Tabel 3

Comparative Summary of Related Work

Feature/Study	MetaSSI	SSI for Trust and Interoperability	Cinema Access in Decentraland	This paper
Metaverse platform used	Unity / Unreal	Not Specified	Decentraland	Decentraland
SSI framework	Hyperledger Aries	Not Specified	Not Specified	Veramo
On-chain DID resolution	No	No	No	Yes (Infura + Ethereum)
VC-based access control	Simulated	Conceptual	Yes	Yes
Implementation status	Conceptual	Conceptual	Real implementation (ZKP + NFT)	Functional prototype (VC)

This comparison shows that all three referenced works contribute to the theoretical development of SSI in the metaverse topic. However, only the present study proposes a system with a functional implementation on a real metaverse platform, Decentraland. By using the Veramo framework, the system follows the SSI principles and provides verifiable credential-based access control for the users. It validates credentials in real-time and offers a foundation for future identity-based access control applications in metaverses. Although the current implementation focuses on a specific access scenario, the system design is flexible and can be extended to other use cases such as transactions, avatar identity verification. Users maintain full control over the disclosed data reinforcing privacy, confidentiality and security.

6. Conclusions

Integrating SSI into Decentraland Metaverse comes with benefits for users:
• Decentralized Authentication: Users could log in using decentralized identifiers (DIDs) and verifiable credentials (VCs).
• Proof of ownership and reputation: Users could prove the authenticity of their digital assets and interaction history without disclosing personal data.
• Interoperability: Verifiable digital identity could be used on other metaverse platforms.
• Privacy protection: Self-Sovereign Identity (SSI) allows users to reveal only the necessary information; no extra private data will be shared.

Another contribution is the interaction between blockchain-based digital identity and virtual worlds; a connection has been created between the avatar in Decentraland and a verifiable identity in the real world with VCs. Also, it has been demonstrated that restricted access can be implemented in Decentraland based on a

verified VC. This means it can be created exclusive areas in the Metaverse (for example virtual classroom only for students), age restrictions (for example access only for people over 18 in virtual casinos), voting in the Decentralized Autonomous Organization (DAO) (for example only users with a certain verifiable credential can vote). It represents the first step towards a standardized decentralized identity for Metaverse.

The main objective stated at the beginning, demonstrating how Self-Sovereign Identity can be applied in virtual worlds, has been successfully achieved. A functional architecture and the implementation of a working prototype in Decentraland was documented in detail throughout this paper. The system was validated with the successful verification of the credential inside the Decentraland scene. These results confirm the feasibility of SSI based access control in metaverse environments. By adopting SSI, metaverses would increase trust and security in the virtual economy, enabling new business models and digital interactions.

R E F E R E N C E S

[1] *D. Birch*, Identity is the new money, 2014.
[2] DB report. Available at: https://www.db.com/what-next/digital-disruption/Metaverse/virtual-reality-virtuelle-Realitaet/index?language_id=1.
[3] Mordor Intelligence Report. Available at: https://www.mordorintelligence.com/industry-reports/metaverse-market.
[4] *A. Preukschat, D. Reed,* Self-Sovereign Identity: decentralized digital identity and verifiable credentials*,* Manning Publications Co., 2021.
[5] *N. Stephenson*, Snow crash, Bantam Books, 1992.
[6] *M. Böckle, F. Booler-Stewart, K. Woolsey*, How to Design for the Metaverse: A Strategic Design Perspective, IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), pp. 99-103, 2023, DOI:10.1109/MetaCom57706.2023.00029.
[7] *I. Marinescu, Ion, D. Iordache*, Explorarea tehnologiilor relevante pentru simularea interacțiunii utilizatorului în spațiile virtuale Metavers, (Exploring the relevant technologies to simulate the user's interaction in virtual Metaverse spaces - in Romanian), RRIA, Vol. **33**, pp. 129-142, 2023, DOI:10.33436/v33i3y202310.
[8] *F. Tang, X. Chen, M. Zhao, and N. Kato*, The roadmap of communication and networking in 6g for the metaverse, IEEE Wireless Communications, 2022
[9] *R. Cheng, N. Wu, S. Chen and B. Han*, Will Metaverse Be NextG Internet? Vision, Hype, and Reality, IEEE Network, Vol. **36**, no. 5, pp. 197-204, 2022, DOI: 10.1109/MNET.117.2200055.
[10] Decentraland. Available at: https://decentraland.org/
[11] *S. Hassan, P. De Filippi*, Decentralized autonomous organization, Internet Policy Review, Vol. **10**, no. 2, pp. 1-10, 2021.
[12] *K. Wolfenstein*, Metaverse platforms in comparison: A comprehensive analysis – From Roblox to Horizon: Where is it worth getting started?, Xpert.Digital, 2025. Available at:https://xpert.digital/en/comparison-of-the-metaverse-platforms/
[13] Sandbox. Available at: https://www.sandbox.game/en/
[14] Roblox. Available at: https://www.roblox.com/
[15] Fortnite. Available at: https://www.fortnite.com/

[16] Horizon. Available at: https://horizon.meta.com/
[17] Mesh. Available at: https://learn-microsoft-com.translate.goog/en-us/mesh/overview?_x_tr_sl=en&_x_tr_tl=ro&_x_tr_hl=ro&_x_tr_pto=sc
[18] *A. Ghosh, Lavanya, V. Hassija, V. Chamola, A. El Saddik*, A Survey on Decentralized Metaverse Using Blockchain and Web 3.0 Technologies, Applications, and More, IEEE Access, Vol. **12**, pp. 146915-146948, 2024, DOI: 10.1109/ACCESS.2024.3469193
[19] Metamask. Available at: https://metamask.io/
[20] *R. Laborde, A. Ferreira, C. Lepore, M. -A. Kandi, M. Sibilla, A. Benzekri*, 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), pp. 418-422, 2023, DOI: 10.1109/MetaCom57706.2023.00080.
[21] *D. Mebrahtom, S. Hadish, A. Sbhatu, M. Aloqaily, M. Guizani,* Trust But Verify - Blockchain-Empowered Decentralized Authentication Schema on the Metaverse: A Self-Sovereign Identity Approach, 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), pp. 1-8, 2023, DOI: 10.1109/iMETA59369.2023.10294349.
[22] Veramo. Available at: https://veramo.io/
[23] Masca. Available at: https://masca.io/
[24] *S. Wang, W. Wang,* A review of the application of digital identity in the Metaverse. Security and Safety, 2023, DOI:10.1051/sands/2023009.
[25] *L. Yang, P. Hui, Y. Xu,* Framing metaverse identity: A multidimensional framework for governing digital selves. Telecommunications Policy, Vol. **49**, 2025, DOI: 10.1016/j.telpol.2025.102906.
[26] *F. Fiaz, S. Sajjad, Z. Iqbal, M. Yousaf, Z. Muhammad*, MetaSSI: A Framework for Personal Data Protection, Enhanced Cybersecurity and Privacy in Metaverse Virtual Reality Platforms, 2024, DOI:10.3390/fi16050176
[27] *S. Ghirmai, D. Mebrahtom, M. Aloqaily, M. Guizani, M. Debbah*, Self-Sovereign Identity for Trust and Interoperability in the Metaverse, 2023, DOI:10.48550/arXiv.2303.00422.
[28] *M. Zichichi, C. Bomprezzi, G. Sorrentino, M. Palmirani,* Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland, 2023.