SSI meets Metaverse for Industry 4

Umit Cali [1], Md Sadek Ferdous [1], Enis Karaarslan [2], Sri Nikhil Gupta Gourisetti [1], and Michael Mylrea [1]

[1]Affiliation not available
[2]Mugla Sitki Kocman University

October 30, 2023

Abstract

As the global industrial complex gears toward fulfilling the tenets of Industry 4.0 and beyond, technologies such as distributed ledger technologies, digital twins, and artificial intelligence become pivotal enablers. In the last decade, metaverse as a concept and technology found its place among crucial enablers for technology and digital advancement across several engineering domains. Metaverse has the potential to combine the elements from distributed computing platforms, the digital evolution of physical systems, and advanced learning systems to unearth a fully digitized world of comparative properties of the real world. We should ensure the privacy, integrity, and confidentiality of personal data. These requirements will lead to proper identity management in the metaverse. Given the complex nature of the metaverse, traditional centralized systems may not offer a viable identity management solution. Therefore, this study explores a decentralized identity management system called the Self-sovereign Identity (SSI) as a logical alternative to traditional centralized identity management systems. The proposed holistic framework aims to ignite new ideas and discussions related to the combined deployment of DLT, SSI, and metaverse to inspire new implementation areas within the Industry 4.0 environment. The paper also discusses various opportunities, enablers, technical \& privacy aspects, legislation requirements, and other barriers related to SSI implementation.

SSI meets Metaverse for Industry 4.0 and Beyond

1st Umit Cali
Department of Electric Power Engineering
Norwegian University of Science and Technology
Trondheim, Norway
umit.cali@ntnu.no

2nd Md Sadek Ferdous
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sadek.ferdous@bracu.ac.bd

3rd Enis Karaarslan
Department of Computer Engineering
Muğla Sıtkı Koçman University
Muğla, Türkiye
enis.karaarslan@mu.edu.tr

4th Sri Nikhil Gupta Gourisetti
Department of Security Architecture
National Resilience
La Jolla, CA, USA
gigupta@ualr.edu

5th Michael Mylrea
Department of Security Architecture
National Resilience
La Jolla, CA, USA
Michael.mylrea@resilience.com

***Abstract*—As the global industrial complex gears toward fulfilling the tenets of Industry 4.0 and beyond, technologies such as distributed ledger technologies, digital twins, and artificial intelligence become pivotal enablers. In the last decade, metaverse as a concept and technology found its place among crucial enablers for technology and digital advancement across several engineering domains. Metaverse has the potential to combine the elements from distributed computing platforms, the digital evolution of physical systems, and advanced learning systems to unearth a fully digitized world of comparative properties of the real world. We should ensure the privacy, integrity, and confidentiality of personal data. These requirements will lead to proper identity management in the metaverse. Given the complex nature of the metaverse, traditional centralized systems may not offer a viable identity management solution. Therefore, this study explores a decentralized identity management system called the Self-sovereign Identity (SSI) as a logical alternative to traditional centralized identity management systems. The proposed holistic framework aims to ignite new ideas and discussions related to the combined deployment of DLT, SSI, and metaverse to inspire new implementation areas within the Industry 4.0 environment. The paper also discusses various opportunities, enablers, technical & privacy aspects, legislation requirements, and other barriers related to SSI implementation.**

***Index Terms*—metaverse, digital identity, Self-sovereign Identity, SSI, industry 4.0**

I. Introduction

COVID 19 accelerated the rapid adoption of Industry 4.0 technologies and triggered new paradigm shifts. The digitalization technologies such as Artificial Intelligence (AI), Distributed Ledger Technology (DLT), metaverse (MV) and other emerging information communication technologies (ICT) are considered the core of the upcoming full digital economies. The most updated phase of the Industrial Revolution is the Fourth which is aiming to leverage the existing verticals of the industrial verticals by deploying state-of-the-art emerging digital technologies. Industry 4.0 covers a relatively large spectrum of technologies that offer a fruitful landscape for metaverse applications. Such an undiscovered metaverse landscape offers new opportunities and markets that will be providing high-value-added products and services. The digital transformation of critical infrastructures, from transportation to energy, advanced manufacturing to life sciences, is rapidly changing how data are being collected, aggregated, and exchanged. The 5Vs (velocity, volume, variety, veracity, and value) of data [1] are required to manage, secure, and advance digital processes. These also increase human reliance on automation and machines. AI and machine learning (ML) algorithms help translate insight from these prodigious data sets into automated processes that govern robotics [2]. At the nexus of cyber and physical interaction and data exchange, a new environment is born that combines augmented reality (AR) and virtual reality (VR) to create a metaverse. It is expected that such metaverse will increasingly be applied to manage critical industrial control systems (ICS), the Industrial Internet of Things (IIoT), and other critical cyber-physical systems.

These systems are inherently vulnerable to human error and cyber exploitation and would require to ensure the confidentiality, integrity, availability, accountability, non-repudiation, authentication, access control as well as privacy requirements [3]. Identity Management (IdM) would be the foundation to guarantee many of these properties. Unfortunately, the traditional identity management models are mostly centralized in nature and may not offer a viable identity management solution. Therefore, a decentralized identity management system called the Self-sovereign Identity (SSI) is explored in this paper as a logical alternative to traditional centralized identity management systems. Towards this aim, this paper presents a novel SSI-based Identity Management framework which could be integrated within a metaverse. The proposed holistic framework aims to ignite new ideas and discussions related to the combined deployment of DLT, SSI, and metaverse to inspire new implementation areas within the Industry 4.0 environment.

Contributions. The major contributions of this paper are:

- An SSI-based identity management architecture for metaverse.
- A use-case which leverages the framework is illustrated,

detailing how this framework could be utilized to access services from a metaverse.
- Various opportunities, enablers, technical & privacy aspects, legislation requirements, and other barriers related to the SSI implementation in metaverse are discussed.

Structure. We present a brief background on identity management, SSI, metaverse and identity in metaverse in Section II. The proposed architecture is presented in Section III along with an exploration of its use-case, security, technical, privacy and legislative aspects. Section IV discusses other aspects, opportunities and barriers with respect to the proposed architecture. Finally, we conclude in Section V with a hint of future works.

II. Background

A. Identity Management

Identity Management (IdM) is the process to manage on online identities [7]. It consists of different technologies and their associated policies which dictate how identities are represented and identified within an application domain and how such identities can be utilized to access the corresponding online services. The system which is used for identity management is known as an Identity Management System (IMS). There are several identity management models, SILO Model Federated Model is discussed as they are widely used.

SILO is the most dominant IdM model on the Internet. In this model, a user needs to create different online identities for different application domains (websites) [8]. The user needs to generate different identifiers (e.g. username/email address) and credential (e.g. password) pairs for utilizing their identities on different websites. As the user interacts more with different websites, the number of identities starts growing and their management becomes increasingly difficult. The majority of the current online services utilize this model.

In order to reduce the identity plurality issue of the SILO model, the federated model has been introduced [9]. In this model, there is a central Identity Provider (IdP) which is responsible for creating and managing user identities. The Service Providers (SP) rely on the IdP for the authentication and other identity services. This model can also provide a notion of trust between the IdP and SPs as they create this virtual circle of trust, known as the Identity Federation or federated identities. This model is quite popular among the educational and governmental settings.

Even though extensively used, both of these models are provider-centric so all identity data are maintained by the respective providers. The providers have the ultimate control over the identity data, and users do not know how their identity data are being abused [10]. In case the respective ceases to exist, all identity data of the user might be lost. Also, the IdP is a single source of failure in the federated model. If the IdP malfunctions for some reason (e.g. DoS, technical problems) the SPs which rely on the IdP cannot function properly.

B. Self-sovereign Identity

A new model of identity called Self-sovereign Identity (SSI) has been introduced to address the issues in the existing IdM models. The core motivation of SSI is to offer more controls to the user in managing their identity data [11]. A user can generate as many identities as required and share with others. These identities are fully controlled by the user and devoid of any control from the provider.

SSI components are shown in Figure 1. SSI extensively uses the concept of Decentralized Identifiers (DIDs) and Verifiable Credentials (VC). A DID is a string generated by the user and is linked with the public key of the user. SP uniquely identifies a user by a DID. A VC is a cryptographically-signed claim (a statement consisting of attribute names and their values) about a user. The issuer is responsible to issue a VC to the user after cryptographically signing it with their private key. The user then stores the VC in a mobile wallet. That is why a user is also known as the Holder in the SSI terminology (Figure 1). The user accesses a service provided by an SP by submitting the VC to the SP. The SP verifies the VC, thus acting as a verifier. A DID Document (DID Doc) is used to share the DID. It is a JSON object containing the DID, its linked cryptographic public keys, and other metadata. The DID docs are stored in a verifiable data registry. This registry can also be a blockchain for immutability and decentralization. SSI steps are as follows:

- **Establishing a connection:** Any two entities (e.g. issuer & holder and holder & verifier) within SSI establish a connection.
- **Issuing and exchanging a VC:** The issuer issues a VC to the holder, upon receiving the which is transmitted using the previously established connection. The holder stores the VC in their wallet.
- **Providing a presentation:** The user issuer prepares a presentation (a collection of different VCs) upon receiving a presentation request from a verifier. It transfers it to the verifier using the previously established connection. Then verifies each VC and acts accordingly.

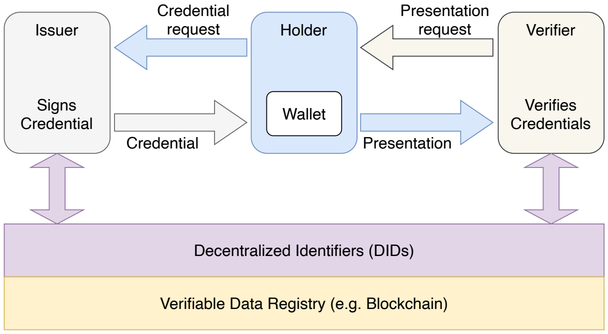

Fig. 1: SSI Components

C. Metaverse

Metaverse is an umbrella term for the future Internet. It will consist of virtual worlds that are called verses. There are virtual worlds in computer games, but the specific characteristics of the metaverse make the difference. These characteristics are being syncronized, secured, wide range attendance, full working economy, persistent, interoperable and decentralized. For the best user experience, all the user operations should be synchronized and alive. The systems should be secured against cyber attacks. The systems should ensure the privacy of the user. Also, the metaverse should serve interesting experiences to attract a wide range of attendance. There is a need for the sustainability of the metaverse. This can be accomplished with the token economy [5]. Interoperability is possible when digital assets are stored and used in other verses. Decentralization will be needed to ensure these characteristics.

An ideal metaverse architecture would be influenced by many subjects of research such as fundamental sciences, social sciences, humanity and engineering sciences. Those research fields will play a crucial role in architecting the metaverse. Some of such merges are given in [21]. Once designed, metaverse spans a long list of use-cases of which many could be synonymous with physical world activities. The metaverse use cases could range from entertainment and gaming to industry advancement, manufacturing optimization through industry 4.0, energy-efficient architecture studies, etc. For most use cases; humans or digital representations are the ultimate beneficiaries of the metaverse and the advancements that come with it. Therefore, real-world physical security, cybersecurity, and resiliency requirements apply to the metaverse at the same levels if not more. Furthermore, technology derivatives from distributed ledger technologies (DLT), Digital twin, and machine learning are crucial foundational elements. Architects are already working towards proposing various architectural frameworks that can be used as the basis of the metaverse design.

The metaverse value-chain proposed by Jon Radoff [4] highlights a seven-layer reference model according to the functionality. The stack depicts a top-to-down approach (or bottom-up depending on the analysis approach) where human experience through applications stays at the very top. Others are discovery, creator economy, spatial computing, decentralization, human interface, and infrastructure. Elements such as privacy, security, and the confidentiality of the data become critical. The SSI approach proposed in this paper can add such identity-related security aspects to the metaverse value chain stack without compromising any of the integral elements of the stack.

The framework presented in [22] heavily approaches from a metaverse functionality perspective with emphasis on interoperability. One of the persistent challenges with distributed ledgers (DLT) is interoperability. The discussion of this challenge in the metaverse raises several philosophical questions as follows[23]:

1) Should each (meta)verse continue to exist as a digital country of nature with digital borders?
2) Who will serve the interoperability features? Prime owners (technology architects) of the metaverses or independent impartial entities?
3) How would the end-users traverse the (identity) digital artifacts between (meta)verses?
4) Would the technology eventually evolve into a single metaverse that holds various digital containers with their features and use cases for the end-users?
5) How would decentralized ownership evolve in a metaverse?

The metaverse standards forum has recently started evaluating some metaverse-related digital artifacts and API standards [Ref]. The proposed SSI approach should be adaptive to support current and future interoperability goals.

A metaverse use-case framework discussed in [24] shows a simplified relationship view which connects the physical and digital worlds. According to the authors, digital twin and blockchain technologies will play a significant role in the metaverse ecosystem. There is a need for cybersecurity aspects such as identity management, and privacy, among other security requirements.

Existing efforts regarding a holistic metaverse framework and architecture that spans the various research fields are either non-existent or currently a work-in-progress effort. Nevertheless, there is a strong need for a framework to enable the design and development of metaverse-based high-value use-cases across sectors.

D. Identity in Metaverse

Avatars, the visual images of our digital selves, will represent our digital identity in the metaverse. Avatars will be connected with the users' characteristics and owned assets. These will also be linked with the digital memory and experiences of the user [13]. Identity will be a crucial component for any metaverse [12]. VR authentication methods [14] will be used to enter the metaverse. These will play a central role to ensure the security and privacy of every single user within the metaverse. Using IMS with the existing IdM models will cause the metaverse to suffer from the same issues discussed in the paper. We argue that a decentralized identity system, e.g. SSI, would be better suited for any metaverse application. In the following, we present our vision of how SSI could be utilized within a Metaverse.

III. Proposed Approach

In this section, first we present a generic architecture of SSI for the metaverse that aims to be used for various Industry 4.0 use cases. We illustrate how such an architecture can be utilized to access services within a metaverse. We then discuss different aspects such as opportunities and barriers to introducing such a system, and its technical aspects. Finally, we discuss different privacy and legislative aspects.

A. Generic Architecture

The envisioned SSI-based architecture for SSI is presented in Figure in 2. As per the architecture, there is no entity (e.g. IdP) that issues identities to the users. Each user provides and controls their own identity by using their wallet to generate an identity for a particular (meta)verse (also known as Virtual

World or VW in short). In Figure 2, such virtual worlds are represented as VW1, VW2, and VW3.

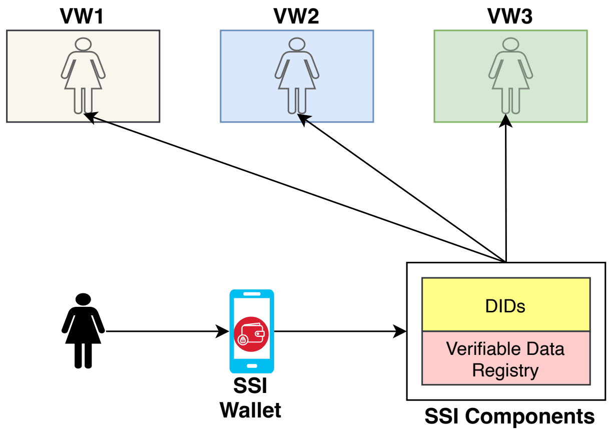

Fig. 2: A generic SSI Architecture for Metaverse

B. Use-case

This section elaborates on how the SSI architecture could be utilized to access services from a virtual world. The steps of the use-case are presented in Figure 3 and given with associated step numbers as follows:

1) The VW1 needs to be equipped with an SSI agent to facilitate SSI functionalities. The SSI agent generates a connection invitation which is then displayed as a QR code on the VW1 page.
2) The user uses her mobile wallet to scan the QR code and initiate the connect establishes process between the user and the VW1.
3) DIDs of each entity are exchanged and the corresponding DID Docs are resolved from the blockchain and finally validated. At this point, the connection is established between the user and VW1.
4) The user prepares a VP (Virtual Presentation) consisting of one VC or several VCs to access the service by VW1. This VP is then released to the VW1 using the previously established connection
5) The VW1 retrieves each VC from the VP and verifies them.
6) The VW1 generates and shares a new VC (denoted with VC') that is then stored in the wallet of the user.
7) The user generates an avatar for her.
8) the user shares VC' to access services using the previously created avatar and a VR device

C. Security & Technical Aspects

The proposed SSI-based IMS offers a new way of managing users. The VW1 does not need to carry the burden of managing a huge amount of identity data. Instead, the users can manage and control their identities all by themselves in a decentralized fashion. As users are identified with the corresponding DIDs that are created from the respective public keys associated with a blockchain, such DIDs are mostly anonymous by default. However, the user can prefer to reveal their real identity. The integration of such mechanisms enables the user to control what information they want to share with whom [13]. Also, the metadata and different relevant information associated with each DID are stored in the blockchain, ensuring the immutability and availability of this information.

There are multiple available solutions to adopt such a system. For example, the Hyperledger Aries [16] provides a framework for deploying SSI solutions. Aries utilizes Hyperledger Indy [17] as the underlying blockchain platform for the SSI and has several different SDKs such as Aries Cloud Agent Python [18] and an SSI wallet called Aries Mobile Agent React Native [19]. It provides a full set of toolkits that can be used to integrate SSI solutions within any system such as the metaverse.

D. Privacy and legislative Aspects

One of the strong motivations for SSI is privacy from the user's point of view. The user has full control over its identity data which reduces the possibility of being abused without the user's knowledge. In addition, the users can protect the privacy of their data by utilizing zero-knowledge proof [15] protocols along with the VCs. This is advantageous for service providers as well as they do not need to curate such sensitive data at their end by following strict legal regulations such as General Data Protection Regulation (GDPR). The right to be forgotten can be served with ease.

Beside privacy aspects data sharing and portability are among the other topics that shall be regulated by legislative authorities. Since industry 4.0 accommodates various industrial segments such as energy, heath, real-estate, education and defense, it is essential to adjust the existing commercial law framework for the upcoming digital economies. More precisely, current antitrust, merger regulation and contractual law related legislative law codex shall be updated by considering the potential boundaries of emergency technologies like metaverse, DLT and AI.

SSI-based IMS also offers additional benefits. It provides a complete passwordless authentication process, thus, reducing the burden of password management. SSI creates a full P2P communication between a user and a virtual world which could be easily broken when any entity wishes to sever its ties. Also, an SSI channel provides an encrypted channel to communicate with each other to ensure the security of transferred data between the entities.

IV. Discussions and Outlook

Traditional Identity Systems have gone through several evolutionary rounds and this resulted in several identity management systems [20]. The organizations had to adopt different types of IMSs in different stages and eventually increased operational costs. We argue that adopting a decentralized SSI-based IMS would be much more convenient for the decentralized metaverse systems because of the advantages it brings. In this paper, we have presented an example of our vision of how SSI could be integrated within a metaverse. The success of this unique combination would mostly depend

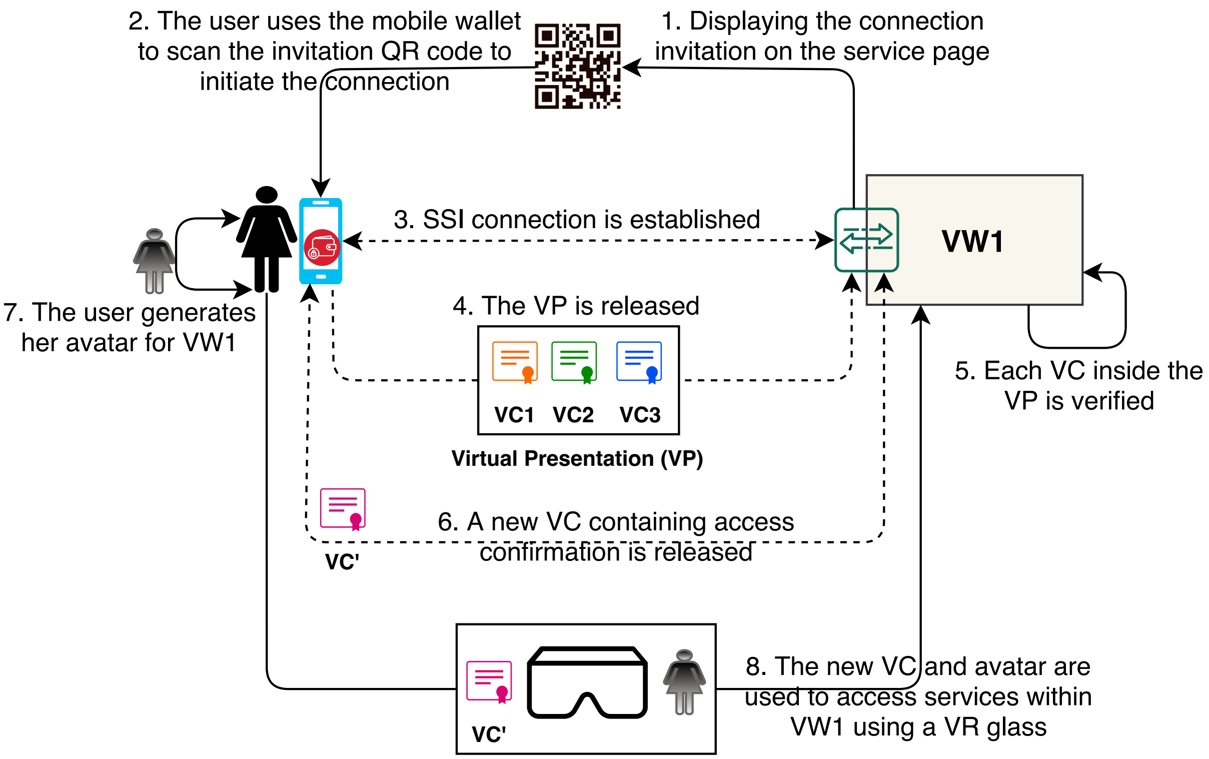
2. The user uses the mobile wallet to scan the invitation QR code to initiate the connection
1. Displaying the connection invitation on the service page
3. SSI connection is established
VW1
7. The user generates her avatar for VW1
4. The VP is released
VC1
VC2
VC3
Virtual Presentation (VP)
5. Each VC inside the VP is verified
VC'
6. A new VC containing access confirmation is released
VC'
8. The new VC and avatar are used to access services within VW1 using a VR glass

Fig. 3: Potential use-case for a generic Industry 4.0 implementations

on how well this approach is adopted by the metaverse. We hope that our paper will motivate the metaverse industry to embark on the vision presented here.

Future research should explore opportunities and gaps in securing the metaverse from multiple dimensions. This should include but not be limited to cognitive behavioral dimensions, such as human-machine teams' challenges with autonomy. What does trust mean when AI algorithms in a metaverse are sentient? Trust concerns the assumption that a person or technology will help achieve specific goals in a situation characterized by uncertainty and vulnerability [25]. How will humans respond to an AI-driven metaverse that is a distributed autonomous organization? What trust anchors would be required for a critical infrastructure DAO? [3] The algorithms that govern the data and systems in a metaverse will increasingly be underpinned by AI/ML algorithms. These algorithms in turn will increasingly control and optimize the metaverse which is complex adaptive systems (CAS) or "systems in which a perfect understanding of the individual parts does not automatically convey a perfect understanding of the whole system's behavior" [26] [27]. For this reason, any future security, functionality, and interoperability framework for a metaverse must include a holistic – people, process, and a technology approach.

Two integral components of any future metaverse will be confidentiality or the ability to preserve sensitive data as well as the integrity of data and processes through the lifecycle. The will introduce some compelling use cases for privacy-preserving technology as well as blockchain and DLT to track and trace data exchanges and processes throughout their lifecycle while preserving privacy. Combining these advances with the metaverse identity framework established in this chapter could help move the ecosystem towards resilience and interoperability to realize the full potential of these uses cases. This would improve the scalability of metaverse for a privacy-preserving form of federated learning that leverages the use of AI and ML-based algorithms (combined with cryptography such as homomorphic encryption, trusted execution environment (TEE) to securely generate actionable insights from complex data sets and mathematical models. While application of these solutions is being applied to this research underway, critical questions remained unanswered: 1) How do we quantify trust or zero trust in a metaverse? 2) How do quantify zero-trust and apply it to a metaverse framework to advance interoperability, functionality, and adaptability [2]?

Answering these questions in a timely way is part of harnessing advances in the metaverse so that the form of the metaverse complements the function, the ideal metaverse architecture would be influenced by a holistic – people, process, technology approach. However, the technologies which will enable the metaverse are not mature yet. First and foremost; the communication infrastructure can not handle the amount of traffic generated on time. The graphics processing (GPU) power is not advanced, and the communication infrastructure is not enough for a realistic view. Also, the human interfaces are not comfortable to use yet. There are more deficiencies to name, but the technological advances in the field are promising. Decentralized systems are evolving and can be used to provide confidence in the system and the persistence of digital assets. Token economy can be used for the creator economy that will ensure the sustainability of the system. Information can be tokenized and smart contracts can be used for information sharing in a trusted way.

V. Conclusion

It is conspicuous that COVID19 triggered massive and fundamental changes and transitions in our society. Undoubtedly, important Industry 4.0 verticals such as energy, health, supply chain, transportation, and defense are the most critical ones that are impacted by the digital transition. DLT, AI, IoT, and metaverse can be considered the mainstream technology trends that shape Industry 4.0 and beyond. This article presented a holistic framework that brings the most recent digital technologies, especially DLT and metaverse, together to be used for various Industry 4.0 use cases. Metaverse will be designed to bring various virtual realms (verses) to form an interconnected ecosystem. Users of these systems represent their digital selves with digital identities. These identities play a central role to ensure the cybersecurity and privacy of every single user within the metaverse.

We aim to ignite new ideas and discussions related to the joint deployment of DLT, SSI, and metaverse to inspire new application areas within the Industry 4.0 landscape. This study proposed a decentralized SSI-based IMS for decentralized virtual worlds that will form the metaverse in near future. The advantages such as privacy, integrity and availability are explained. This work also emphasized the legal and legislative aspects of the proposed approach.

There is a need for more sophisticated and diversified frameworks and architectures. Technical, social, physiological, legislative, and financial barriers and enablers of the extended domain shall be investigated in a broader and interdisciplinary manner. Future works will include developing and deploying the presented envisioned architecture to test its applicability for real-world applications.

References

[1] A. Jain, ”The 5 V’s of big data-Watson Health Perspectives”, 2022 [Online].

[2] M. Mylrea, ”Building a Trustworthy Digital Twin: A Brave New World of Human Machine Teams & Autonomous Biological Internet of Things (BIoT)”, Book Chapter. Elsevier Books. Pending publication September, 2022.

[3] M. Mylrea, ”Manufacturing in the Metaverse”, Conference Abstract. The Association for the Advancement of Artificial Intelligence. March, 2021.

[4] B. Ryskeldiev, Y. Ochiai, M. Cohen, J. Herder, ”Distributed metaverse: creating decentralized blockchain-based model for peer-to-peer sharing of virtual spaces for mixed reality applications”. In Proceedings of the 9th Augmented Human International Conference, 2018 Feb 6,pp. 1-3.

[5] S. Voshmgir, Token Economy: How the Web3 reinvents the Internet (Vol. 2). Token Kitchen, 2020.

[6] J. Radoff, ”The Metaverse Value-Chain”, 2022 [Online]. Available: https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7

[7] M. Ferdous, G. Norman,A. Jøsang, R. Poet & Others, ”Mathematical modelling of trust issues in federated identity management”, *IFIP International Conference On Trust Management*, 2015, pp. 13-29.

[8] A. Jøsang & S. Pope, ”User centric identity management,” AusCERT Asia Pacific information technology security conference. Vol. 22. 2005.

[9] D. Chadwick, ”Federated identity management,” *Foundations Of Security Analysis And Design V*. pp. 96-120, 2009.

[10] M. Ferdous & R. Poet, ”Portable Personal Identity Provider in Mobile Phones,” *12th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-13)*. pp. 736-745, 2013.

[11] M. Ferdous., F. Chowdhury, & M. Alassafi, ”In Search of Self-Sovereign Identity Leveraging Blockchain Technology,” *IEEE Access*. **7** pp. 103059-103079, 2019.

[12] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. Luan & X. Shen, ”A survey on metaverse: Fundamentals, security, and privacy,” *ArXiv Preprint ArXiv:2203.02662*, 2022.

[13] S. Altundas and E. Karaarslan, ”Cross-platform & personalized Avatars in the Metaverse: Ready Player Me”, Digital Twin Driven Intelligent Systems and Emerging Metaverse, Springer Nature, in press.

[14] P. Kürtünlüoğlu, B. Akdik, E. Karaarslan ”Security of Virtual Reality Authentication Methods in Metaverse: An Overview”, *ArXiv Preprint ArXiv:2209.06447*, 2022.

[15] O. Goldreich and Y. Oren, “Definitions and properties of zero-knowledge proof systems,” Journal of Cryptology, 1994, 7.1: 1-32.

[16] “Hyperledger Aries”. . Accessed: 2022-09-10. [Online]. Available: https://www.hyperledger.org/use/hyperledger-aries

[17] “Hyperledger Indy”. Accessed: 2022-09-10. [Online]. Available: https://www.hyperledger.org/use/hyperledger-indy

[18] “Hyperledger Aries Cloud Agent - Python”. Accessed: 2022-09-10. [Online]. Available: https://github.com/hyperledger/aries-cloudagent-python

[19] “Aries Mobile Agent React Native”. Accessed: 2022-09-10. [Online]. Available: https://github.com/hyperledger/aries-mobile-agent-react-native

[20] M. Ferdous & R. Poet, ”A comparative analysis of Identity Management Systems,” *High Performance Computing And Simulation (HPCS), 2012 International Conference On*. pp. 454-461, 2012.

[21] A. N. D. R. E. A. Moneta, ”Architecture, heritage and metaverse: New approaches and methods for the digital built environment,” Traditional Dwellings and Settlements Review, 32(2), 2020.

[22] ”The Metaverse: Framework, Building Blocks and Market Map”, 2022 [Online]. Available: https://levelup.gitconnected.com/the-metaverse-framework-building-blocks-and-market-map-3bb2ccf0241c

[23] ”Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability”, 2022 [Online]. Available: https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/

[24] N. A. Dahan, M. Al-Razgan, A. Al-Laith, M. A. Alsoufi, M. S. Al-Asaly & T. Alfakih, ”Metaverse Framework: A Case Study on E-Learning Environment (ELEM)”. Electronics, 11(10), 1616, 2020.

[25] J.D. Lee and K.A. See, “Trust in Automation: Designing for Appropriate Reliance,” Human Factors, 46(1), 2004, 50-80.

[26] A. K. Raz, J. Llinas, R. Mittu & W. Lawless, ”Engineering for emergence in information fusion systems: A review of some challenges”, Fusion 2019, Ottawa, Canada — July 2–5, 2019.

[27] W. F. Lawless, R. Mittu, D. A. Sofge, T. M. Shortell & T. A. McDermott (Eds.). ”Systems Engineering and Artificial Intelligence”. Springer, 2021.