Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland

Mirko Zichichi [1,2], Chantal Bomprezzi [2], Giovanni Sorrentino [2] and Monica Palmirani [2]

[1] *Ontology Engineering Group, Universidad Politécnica de Madrid, Campus de Montegancedo s/n, Boadilla del Monte (Madrid), 28660, Spain*
[2] *CIRSFID, University of Bologna, Via Galliera 3, 40121 Bologna, Italy*

Abstract

The Metaverse is expected to enter everyday life to provide users with various activities. In this context, digital identity is paramount for creating a trustworthy environment, even considering that a Metaverse avatar's actions can produce legal consequences in the real world. DLT-based Metaverse platforms shall integrate, with other legally recognised instruments of online identification, in such a way that these can guarantee selective disclosure of identity data. This work references current legal and technical instruments of online identification, such as eIDAS and W3C Verifiable Credentials, to provide the implementation of a use case for selective disclosure in a Metaverse. This implementation is based on a series of Ethereum smart contracts that can already directly interact with the Metaverse of interest, i.e., Decentraland. The final result is implementing a scenario where on-chain verification of anonymous credentials based on Zero-Knowledge Proofs enables a Decentraland user to access an age-restricted movie screening in a decentralised cinema without disclosing his or her real identity.

Keywords

Metaverse, DLT, Digital identity, Smart Contracts, Verifiable Credentials.

1. Introduction

Discussions on personal identity involve various fields of knowledge, from biology and psychology to philosophy. Over time, the concept of personal identity has moved out of purely theoretical discussions, becoming increasingly relevant from a legal perspective. Indeed, courts and legal experts began to conceive personal identity as a person's right. For example, in the US legal tradition, the concept of 'false light in the public eye` [1-3] occurs when someone culpably spreads a misrepresentation of another subject in the public eye, attributing to her facts or opinions that are not her own, and thereby causing feelings of humiliation.

In Italy, the expression' personal identity' dates back to the first half of the 20th century. This concept can be found for the first time in the Nuovo Digesto Italiano, which refers to distinguishing one individual from another, to make her identifiable in the eyes of the community and the public administration. It was intended to include connotations, personal features, and the name [4]. The concept of considering personal identity as a person's interest in identifiability was developed in subsequent years [5,6], leading to the full recognition of this right in Italy in 1974 [7]. The jurisprudential debate resulting from this pronouncement led to the Supreme Court's Veronesi Case', where personal identity consists of the right not to misrepresent or distort the social projection of one's personality. Therefore, this definition includes not only the name but also ideas, thoughts, beliefs, and all those elements that characterise the individual and make him or her recognisable before society.

[1]5th Distributed Ledger Technology Workshop, May 25-26, 2023, Bologna, Italy
EMAIL: mirko.zichichi@upm.es (M. Z.); chantal.bomprezzi@unibo.it (C. B.); giovanni.sorrentino5@unibo.it (G. S.); monica.palmirani@unibo.it (M. P.)
ORCID: 0000-0002-4159-4269 (M. Z.); 0000-0002-5919-7982 (C.B.); 0000-0002-8557-8084 (M. P.)

As evident from the above considerations, the concept of personal identity has evolved over time. This process cannot yet be said to have stopped. In particular, the advent of the Internet and the exponential growth of modern society has led to the concept of digital identity, which refers to the representation of people in the digital world. Digital identity acquires even more interest when people interact in the Metaverse in the form of avatars. The "Metaverse" concept was born in 1992, first introduced by Neil Stephenson in his novel Snow Crash. Obviously, the Metaverse as we know it today is very different from the concept devised by Stephenson. Although the notion of the Metaverse, the literal meaning of which is 'beyond universe', does not have a uniform definition, it has been described as an immersive and constant virtual 3D world where people act as avatars to enjoy entertainment, make purchases and carry out transactions or work without leaving their seat. The development of the Metaverse is still in the nascent stages, but it has the potential to play a large part in human existence [9]. At the moment, it is probably more correct to speak about Metaverse in the plural form, as different platforms have been developed with different features, graphics and functionalities but share the same basic concept.

The European Commission has a strategy for extended reality regulation (XR) and market support that is strictly related to the bigTech Platform regulation using the Digital Single Market, in particular the Digital Services Act[2]. In this perspective the European Commission has launched the "Virtual and Augmented Reality Industrial Coalition" in September 2022 and the recent report "Extended reality Opportunities, success stories and challenges (health, education): executive summary"[3] stresses the importance of the digital identity as pillar for the security[4].

Additionally, the same report remarks how the entertainment sector is one of largest industry in the XR (42% in 2022 and 43% in 2030)[5].

The European institutions have also emitted the "European Declaration on Digital Rights and Principles for the Digital Decade"[6] where "People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights.". The digital identity is part of user-centred policy that includes security, trustworthy, fairness in the access of the services offered by the platforms, protecting the fundamental rights of the consumer[7].

As the Metaverse (s) continues to grow, there is a need for a secure and decentralised infrastructure that can support its various applications. This is where Distributed Ledger Technologies (DLTs) come in. By leveraging DLTs, the Metaverse can create a trusted and transparent environment for its users, where they can safely engage in various activities. Decentraland is one such DLT-enabled Metaverse [10]. It is a decentralised virtual world where users can buy, sell, and develop virtual real estate. Decentraland uses the Ethereum blockchain to manage its digital assets and transactions, allowing for a secure and transparent environment for its users. In Decentraland, users can create and experience different content, including games, art galleries, and social experiences. The platform also features a governance system that enables users to participate in decision-making processes and contribute to the development of the Metaverse [10].

The aim of this paper is to bring the concept of personal identity into a new light, delving into the legal concept of digital identity in the European legal framework and advancing possible issues in managing one's digital personality in the Metaverse. The main research question is: Is there any way

---

[2] http://data.europa.eu/eli/reg/2022/2065/oj.

[3] https://op.europa.eu/s/x3FT.

[4] "Identity hacking could occur in immersive environments. XR could allow virtual copies of people to be made that look, act and talk like a real person, even demonstrating aspects of personality (applying behaviour-based machine learning on recordings of the real person) (Slater et al., 2020). This could lead to fake news (portraying people as having carried out actions that they did not do), identity theft (using other people's identities to gain sensitive information about them by communicating with significant others), or moral disengagement (where people may normalise inhuman actions towards others because the interactions happen virtually and are not 'real')."., pag. 58 out 202.

[5] "Analysis of XR revenue by industry shows that media and entertainment, including gaming, is the largest industry, with a 42% share of the expected XR revenue for 2022. This is followed by industrial and manufacturing. Healthcare comes third with 12% (EUR 1.19 billion), while education offers a potential 3% (EUR 250 million) share of the XR market. The distribution of the XR market between industries is expected to remain relatively stable during the period to 2030.", pag. 101 out 202.

[6] European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.

[7] European Declaration on Digital Rights and Principles for the Digital Decade in Chapter III, Freedom of choice "ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined;" and in Chapter II, Solidarity and inclusion "ensuring that people living in the EU are offered the possibility to use an accessible, voluntary, secure and trusted digital identity that gives access to a broad range of online services;".

to protect the right not to misrepresent or distort the social projection of one's personality in the Metaverse?

The hypothesis, in this case, is that there are already (i) legislative support compatible with a vision of decentralised digital identity in the European legal framework (i.e., the proposed amendment of eIDAS) and (ii) reference frameworks and standards compatible with some implementations of the Metaverse.

The contributions of this paper are therefore twofold, in that, firstly, the need for a personal identity as a person's interest in identifiability in the Metaverse is framed, and, secondly, an implementation of a smart contract-based system in Ethereum for anonymous identity verification in the Decentraland Metaverse is presented. The second contribution is based on a use case involving the fruition of age-restricted audiovisual content in the Metaverse.

The remainder of this paper is organised as follows. Section 2 provides the legal and technical background of online identity. Section 3 discusses a critical analysis of digital identity in the Metaverse, and Section 4 provides a use case related to that. Section 5 describes implementing a smart contract-based system for or disclosing anonymous credentials in the Metaverse. Finally, Section 6 discusses the results and the final conclusions.

2. Legal and technical instruments of online identification

There are different legal instruments of online identification, even though with different levels of trust and legal effects. In the following, some of them will be presented and finally the technical instruments used in this work will be introduced.

2.1. Online identification in Italy, the EU and cross-border

In the European Union, Regulation n. 910/2014 on electronic identification and trust services for electronic transactions (better known as e-IDAS Regulation) was born to build trust in the online environment by providing a common legal basis for secure electronic interactions [11]. Art. 3(1)(1) of the e-IDAS Regulation defines ‘electronic identification’ as ‘the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person’, while Art. 3(1)(2) states that ‘electronic identification means’ is ‘a material and/or immaterial unit containing person identification data and which is used for authentication for an online service’. The same Regulation also contains an obligation of mutual recognition of national electronic identification means among the Member States. The principle of mutual recognition establishes that every Member State can adopt its electronic identification means that must be recognised by the others (upon the respect of some preconditions laid down in Art. 6 of the Regulation). According to recital 9, mutual recognition is aimed to ‘facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities’, taking into account that ‘in most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States’. In Italy, for example, electronic identification means are the Sistema Pubblico per la gestione dell’Identità Digitale di cittadini e imprese (SPID) and the Carta d’Identità Elettronica (CIE) [12]. Electronic identification means can ensure low, substantial or high assurance levels according to technical specifications (Art. 8 of the Regulation).

Another instrument of identification is the electronic signature. According to Article 3(1)(10) of the e-IDAS Regulation ‘electronic signature’ means ‘data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign’. The Regulation recognises three different kinds of electronic signature: the simple (Art. 3(1)(10)), the advanced (Art. 3(1)(11)), and the qualified (Art. 3(1)(12)). Only the latter is considered equivalent to a handwritten signature because of its higher level of reliability and trust (Art. 25(2)). In all other cases, the suitability of the document to satisfy the requirement of the written form can be freely assessed in court, having regard to its security, integrity, and immutability.

Electronic signatures concern natural persons. For legal persons, the e-IDAS Regulation disciplines electronic seals, which are ‘data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity’ (art. 3(1)(25)).

As for electronic signatures, there are three kinds of electronic seals: the simple (art. 3(1)(25)), the advanced (art. 3(1)(26)), and the qualified (art. 3(1)(27)). Qualified seals shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked (Art. 35(2)).

At last, for the sake of completeness, it should be mentioned the work of the UNCITRAL Working Group IV on Electronic Commerce, which on 7 July 2022 provided a set of model legislative provisions that legally enable the use of identity management services for online identification of physical and legal persons, thus facilitating the cross-border recognition of the use of identity management [13]. The UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT) is the first global legislative text on digital identity that sets a uniform legislative standard for promoting trust in digital trade worldwide. Indeed, considering that the Internet is a virtual space and that there are no physical borders, having international rules for the mutual recognition of national electronic identification means could stimulate people to carry out their transactions electronically.

2.2. eIDAS 2.0 and Self Sovereign Identity

On 3 June 2021, the European Commission published the Proposal for a Regulation amending Regulation eIDAS. The Proposal aims to overcome the limitations of the Regulation and accelerate the spread of electronic identity solutions across the EU. The final objective is the setting of a European Digital Identity framework. The Proposal adds the European Digital Identity Wallet to the list of electronic identification means (Art. 3(2)), with a high assurance level (Art. 6a(4)(c)). It allows the user to store and retrieve identity data, including person identification data, electronic attestations of attributes linked to their identity, to provide them to relying parties on request and to use them for authentication (online and, where appropriate, offline); it also enables to sign by means of qualified electronic signatures and seal by means of qualified electronic seals (Art. 3(42)). The peculiar characteristic of this wallet is selective disclosure, which empowers the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only information that is required (recital 29). Therefore, the wallet implements the so-called Self-Sovereign Identity (SSI) because it can store identity data that can be selectively disclosed [14].

Another novelty of the Proposal is the definition of ‘electronic ledger’, a sequence of electronic data records, which ensures their integrity and the accuracy of their chronological ordering. Like electronic signatures, also electronic ledgers can be ‘qualified’ if they meet the requirements laid down in Art. 45i: a) they have to be created by one or more qualified trust service provider; b) they establish the origin of data records in the ledger; c) they ensure the unique sequential chronological ordering of data records in the ledger; d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity along time. Compliance with the above requirements shall be presumed where an electronic ledger meets the specifications and standards established by the EU Commission. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and their integrity (Art. 45h(2)). From these articles, it is evident that the Proposal intends to discipline DLTs.

From the combination of identity wallet and qualified electronic ledgers derives the qualified identity management system based on DLT, which may represent a secure and trustworthy way to share identity data while preserving the privacy of the individuals. The scenario which is described below is based on a system that has been designed to be eIDAS-compliant when its modifications enter into force.

2.3. W3C Decentralized Identifier and Verifiable Credentials

As seen in the previous section, the EU Commission's proposal introduces modifications to the eIDAS to manage a qualified identity management system based on DLT by setting new rules on digital identity wallets and electronic ledgers. In this work, we take as reference the specification of the European Digital Identity Wallet Architecture and Reference Framework [15], with a particular focus on its use of Decentralized Identifiers (DIDs) and Verifiable Credentials (VC) Data Model. These two World Wide Web (W3C) standards, i.e., the DID and VC, are currently the most used implementation of SSI [14]. W3C DID and VC is a set of standards and technologies that enable the

secure exchange of verifiable information between individuals, organisations, and systems. It provides a way for users to store and share information about themselves in a secure, decentralised manner. The DID is a type of identifier entirely under the control of the identity subject, independent from any centralised registry, identity provider, or certificate authority. It relates an entity to means for trustable interactions with that entity, i.e., VCs. A VC is a tamper-evident credential with authorship that can be cryptographically verified. Generally speaking, we have different roles and entities:

- A VC Issuer is an entity's role in asserting claims about one or more subjects, i.e., by issuing VCs. The issued credentials are composed of: (i) a set of (related) statements/claims; (ii) metadata, e.g., date of issuing; (iii) an issuer's digital signature, by which third parties can prove its provenance and integrity. The issuer can also revoke and (un)suspend VC already issued.
- A VC Holder stores VCs securely under its own control through a wallet. This Holder component stores self-signed credentials, or VCs, obtained from third-party issuers. It also stores private keys that can be used to sign or seal data. The holder handles credentials requests that it receives from a verifier, looking for the requested data in the wallet. If the wallet does not store the requested data, the holder may negotiate a transaction with an issuer to obtain the needed VCs.
- A Verifier requests and verifies VCs. The verifier requests the data by creating a request that asks for specific VCs, and then it verifies the VCs received as a response, i.e., checking the signature and other proofs of the veracity of both the construction as well as its contents.
- The Verifiable data registry mediates the creation and validation of identifiers (DIDs), keys, and other relevant data required for issuing, exchanging, and revoking VCs. Examples of verifiable data registries include DLTs.

3. Digital identity in the Metaverse

Within the Metaverse, users act through avatars, virtual alter egos that represent an extension of someone's physicality [16]. The avatar is the mediator that allows the flesh-and-blood individual to move in the digital world in which she is projected. From this point of view, avatars can be considered a new way to express personal identity. Indeed, in the Metaverse, everyone can freely represent himself or herself, even with different physical characteristics. This could be an opportunity.

Think, for instance, of a subject suffering from a disability, which might be able to show herself without that disability being visible or influential at all. Think again of a user who can change his or her sexual characteristics. Avatars allow users to separate themselves from who they are, which would not be possible in the offline world [17]. In Raph Koster's Declaration of The Rights of Avatars, which is modelled on the Bill of Rights, it is declared that 'avatars are the manifestation of actual people in an online medium, and..., their utterances, actions, thoughts, and emotions should be considered to be as valid as the utterances, actions, thoughts, and emotions of people in any other forum, venue, location, or space' [18].

On the other hand, knowing the real identity of subjects in the Metaverse can be necessary when the law requires identification. For example, there could be the need to prosecute people for legal infringements and attribute liability, to establish the jurisdiction or the applicable law in case of controversies, or the legal capacity to conclude valid contracts (i.e., being older than 18 years).

Sometimes the law itself provides identification procedures, such as the Know Your Customer (KYC) rules established by banks or anti-money laundering regulations. (Know your customer (KYC) refers to an analysis activity that financial institutions, companies or other regulated entities are required to perform in order to verify the profile of their customers and ensure that doing business with them does not present a risk profile. KYC and anti-money laundering are closely linked: the primary objective is to verify the user's identity, with the dual purpose of protecting the user and the banking institution from attempted corruption, online fraud and money laundering practices) , which enabled the connection of unknown people from all over the world. The 1993 cartoon of the New Yorker showing a dog sitting behind a computer screen with the famous sentence 'On the Internet nobody knows you are a dog' [19] is very representative of the anonymity which characterises distant electronic communications. For this reason, legislators have developed several methods of online identification when knowing someone's identity becomes relevant in front of the law.

In the Metaverse, the need to guarantee that everyone can freely represent themselves as an expression of her right to personal identity, and the opposite need to verify the belonging of specific attributes of the individual in the offline world for legal reasons, may overlap. Thus, programmers and lawyers should cooperate to find proper solutions, which may protect the privacy of people on the one hand and guarantee online identification on the other. The present work addresses this topic by investigating the process of controlled access to a virtual cinema in Decentraland for an age-restricted movie. The aim of this use case is to show a practical example on how users in the Metaverse can preserve their online identity, i.e., their avatar, while granting the validity of their offline credentials. Thus, users should have the possibility to be represented by their avatar as a set of characteristics that are not related to their offline identity, while being able to (anonymously) demonstrate one trait of their offline identity, i.e., being at least 18 years old.

4. Use case: entering a cinema in the Metaverse

This section focuses on a possible use case for the Decentraland platform to access restricted content. In particular, it foresees an application that lets a Decentraland user purchase a 'decentralised cinema ticket' for an age-restricted movie. This use case is derived from a recent example of the creation of a movie theatre on top of Decentraland by an existing Indian content creator, aggregator and distributor [20]. In our scenario, the Decentraland users must verify their age using W3C Verifiable Credentials to purchase the ticket. The following scenario is constituted by a user, a VC Issuer service, a series of smart contracts deployed on a blockchain, and the decentralised cinema. Within this context, the primary electronic transaction is the provision of an audiovisual content display service by a 'Decentralised' Cinema. In particular, the screening of a movie in Decentraland. A series of prohibitions, obligations, or permissions can constrain media content's traditional distribution and reproduction.

4.1. W3C Verifiable Credential issuing

The ticket purchase process starts with users creating a W3C VC for their age. This credential is a digital representation of the proof of the user's age. The user can then use such a credential to prove an inequation without revealing the actual age value, e.g., age is greater or equal to 18.

Using W3C VCs, the decentralised cinema provides a secure and decentralised way for users to verify their claims and access content. This helps ensure that only users with the appropriate characteristics can access the content and experiences offered in Decentraland. Another example could be the country of residence for targeted content. Additionally, using VCs also provides a more efficient and user-friendly way for users to verify their credentials compared to traditional methods such as submitting a government-issued ID or passport.

Creating a W3C VC that proves a user's age involves several steps:

- **Obtain a trusted source of information**
  Before creating a W3C VC, the user must obtain a trusted source of information about the credential that needs to be verified, i.e., the age. It can be a government-issued ID such as a passport, driver's licence, or a certificate from a trusted third-party organisation.
- **Create a digital representation of the information**
  Once the user has obtained a trusted source of information, the next step is to create a digital representation of that information. This can be done by the user or directly by the VC Issuer by creating a data structure in a standard format, such as JSON-LD, that contains the relevant information.
- **Sign the digital representation**
  After validation of the trusted source of information, the VC Issuer then signs the digital representation of the information using a digital signature. This signature proves that the created information is untampered. The signature also guarantees that the information is authentic and trustworthy.
- **Store the digital representation**
  Finally, the user stores the signed digital representation of the information on her wallet, i.e., the VC Holder component.

- **Use the digital representation as a VC**
  The user can now use the digital representation of the information as a W3C VC. When users want to prove their age, they can present the VC to a relying party (e.g., decentralised cinema service) who can verify the information's authenticity and validity by checking the signature and source of the information.

4.2. On-chain Verifiable Credential verification

When purchasing a ticket for an age-restricted movie in Decentraland, users can use the VC not to disclose their actual age. A set of smart contracts for the provision of the audiovisual content access service is issued by the decentralised cinema in Decentraland.

In particular, one smart contract is dedicated to checking the user's age before allowing the purchase of a ticket. When the user requests to purchase the ticket, the smart contract verifies the user's age by checking the W3C VC that the user has created. If the user is of the appropriate age, the smart contract will allow the user to purchase the ticket. If the user is not of the appropriate age, the smart contract will deny the purchase request, and the user will not be able to watch the movie.

Verifying a W3C VC in a smart contract requires several steps:

1. **Receive the VC**
   The first step is to receive the W3C VC from the user. This can be done by allowing the user to pass the VC to the smart contract as an input parameter.
2. **Verify the signature**
   Once the VC is received, the smart contract must verify the digital signature attached to the credential. This is done to ensure that the information contained in the credential was created by a VC Issuer and has not been tampered with.
3. **Check the issuer**
   The smart contract must also check the issuer of the VC. The smart contract can use a Credential Registry smart contract to verify the signature and check if it matches a registered VC Issuer’s public key.
4. **Validate the information**
   The smart contract must then validate the information contained in the VC. In the scenario, the smart contract would be checking the inequation age proof greater or equal to 18 to ensure that the user is of the appropriate age to watch the movie.
5. **Allow or deny access**
   Once the signature, issuer, and information have been verified, the smart contract can decide whether to allow or deny access. If the verification is successful, the smart contract mints to the user a new Non-Fungible Token (NFT) that represents the ticket.

5. Implementation of a smart contract-based system for the disclosure of anonymous credentials in the Metaverse

The implementation of the use case is based on the Decentraland platform, thus using the Ethereum blockchain. The system has been implemented to run on a local instance for tests execution, however it is feasible to deploy it into the public Ethereum network and possibly plug it in to the Decentraland platform (the local execution was needed to avoid the unfeasible testing in the Ethereum public network in terms of transaction fees).

Given the definition of qualified electronic ledger of the eIDAS amendment, it can be argued that, even if the Ethereum public blockchain does not fall into the qualified criteria, other similar instances (i.e., using the Ethereum Virtual Machine), such as the qualified electronic ledger provided by the European Blockchain Services Infrastructure (EBSI) [21], can be bridged to the Decentraland platform smart contracts [22].

The system is composed of 4 components: (i) the Decentraland platform, that is composed of an off-chain part providing a user interface to the users, and an on-chain part executing the smart contract logic to enable digital asset transactions; (ii) the decentralised cinema is also composed of two parts, i.e., the off-chain module provides a way to let user access audiovisual content and the on-chain smart contracts that enable authorisation (e.g., tickets) and assets; (iii) a Credential Registry to list authorised VC Issuers; (iv) the VC Issuer component for issuing new credentials.

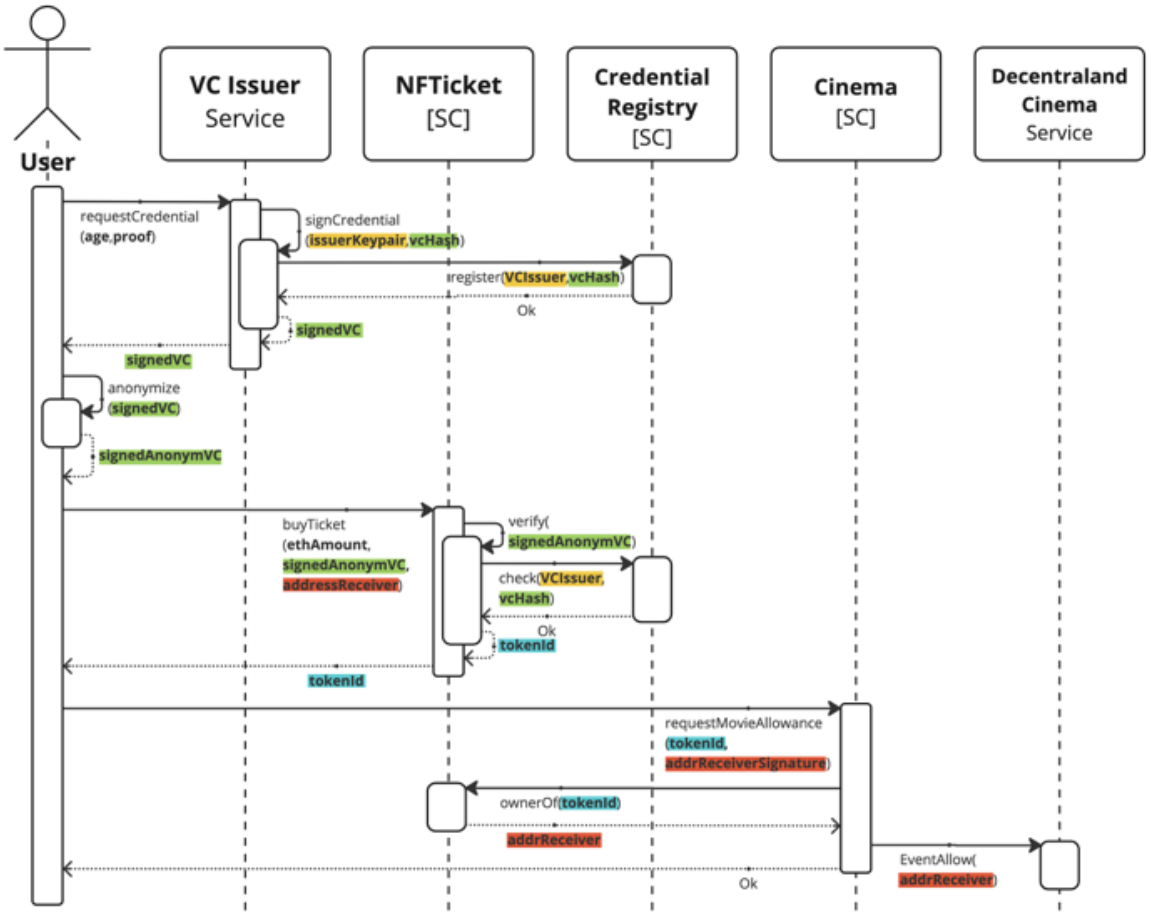

Figure 1 UML Sequence diagram for the purchase of a NFTicket operation

The following sections focus only on describing the implementation of the on-chain decentralised cinema smart contracts, even though it is argued that building/integrating the other components could be feasible.

5.1. Decentralised Cinema Smart Contract

This section describes the implementation of a smart contract for authorising users to access a content. We call such a smart contract 'NFTicket' as the final result of its correct execution is an NFT minted to the user that is authorised to 'access to the cinema'.

- **Verification of anonymous credentials based on Zero-Knowledge Proofs**
  Different Solidity Smart Contract implementations already provide the use of verifiable credentials on-chain [23,24]. We refer to the work presented in [24] to implement the on-chain verification of credentials based on Zero-Knowledge Proofs (ZKP). Authors in that work use Hyperledger Indy's anonymous credentials proofs that builds on (equality and) inequality predicate proofs. ZKPs in anonymous credentials are referred to as Signature Proofs of Knowledge as they enable a credential holder to prove possession of a CL-signature over certain attribute values [25]. The CL signature scheme provides the issuing of a signature on a committed attribute value without revealing to the signer no information about the signed value. This schema also provides the proving knowledge of a signature on a committed value. Moreover, an inequality predicate consists of the credential holder to prove that a specified inequality is satisfied without revealing the actual value of the attribute. This is done by constructing a ZKP that proves that the inequality predicate (i.e., age >= 18 in our scenario) is satisfied.

- **ERC-721**
  The entry-point of the NFTicket mint is the execution of the anonymous credentials verification with an inequality predicate sub-proof. This execution is built on top of an ERC-721 [26] token that implements an interface to being registered in proxy registries. This implementation can be feasibly used in the Decentraland platform to represent assets. Here, a Cinema smart contract enables each address requesting access to a movie that is also the owner of the dedicated NFTicket by issuing an Ethereum event. This event is listened to by the off-chain cinema module that provides the access to the audiovisual content. In particular, we make reference to the soulbound token extension of the ERC-721 [27]. After its issuance, a soulbound token can't be transferred, but can be burned based on a predetermined immutable burn authorization (i.e., only the Decentraland Cinema can burn it).

5.2. Scenario Procedure

The procedures behind the scenario which has been described above can be described as follows (see Figure 1):

1. The user adopts a trusted source of information about their age, such as a certificate from a trusted third-party organisation, to provide a proof of their age and then to invoke requestCredential() from the VC Issuer service.
2. The VC Issuer creates a digital representation of the information, using a standard format such as JSON-LD, and releases the signed VC signed obtained through its keypair.
3. The VC Issuer registers the VC through a Credential Registry contract that acts as a single source of validation with respect to all the possible issuers.
4. The user prepares the anonymous VC proofs.
5. The user issues the proof on-chain by invoking the buyTicket() method from the NFTicket smart contract. He also passes an amount of ether to pay for the ticket and the address to which the NFT will be minted.
6. The smart contract verifies the signature, issuer (by looking into the Credential Registry smart contract), and hash of the info contained in the credential.
7. If the signature, issuer, and information are valid, the smart contract mints a new NFTicket to the address passed as input. If not, the smart contract denies the purchase request.
8. The user can now invoke the Cinema smart contract's requestMovieAllowance() method by passing the id of the newly minted NFTicket and signs the transaction using the address to which the NFT was minted to.
9. The Cinema smart contract checks if the NFT id is owned by that address and then emits an Event that is listened to by the Cinema's off-chain module.
10. The user can now access the decentralised cinema in Decentraland.

5.3. Smart Contract Classes

Smart contracts discussed in the above section can be described as classes as shown in Figure 2. The implementation can be found as open source in GitHub [28].

- **ClaimsVerifier and CredentialRegistryClaims**: Verifier's method verifyCredential() checks if the VC passed as input has been registered in the CredentialRegistry and that the VC signature corresponds to the declared issuer. The VC is an instance of the Verifiable Credential class, where the data attribute corresponds to the hash of the credential parameters, e.g., the age in the cinema scenario.
- **Verify**: Method verify() checks the actual anonymized contents of the VC, i.e., the ZKP that proves that the inequality predicate age >= 18 is true.
- **NFTicket**: The NFTicket smart contract is the main contract. It enables the purchase of a ticket after two validation phases are enacted. The mintTo() method firstly invokes the ClaimsVerifier's method verifyCredential(), then it invokes the Verify's method verify(). If both return true, the mintTo() method mints a token to the address requesting the service, as in a normal ERC721 minting operation.

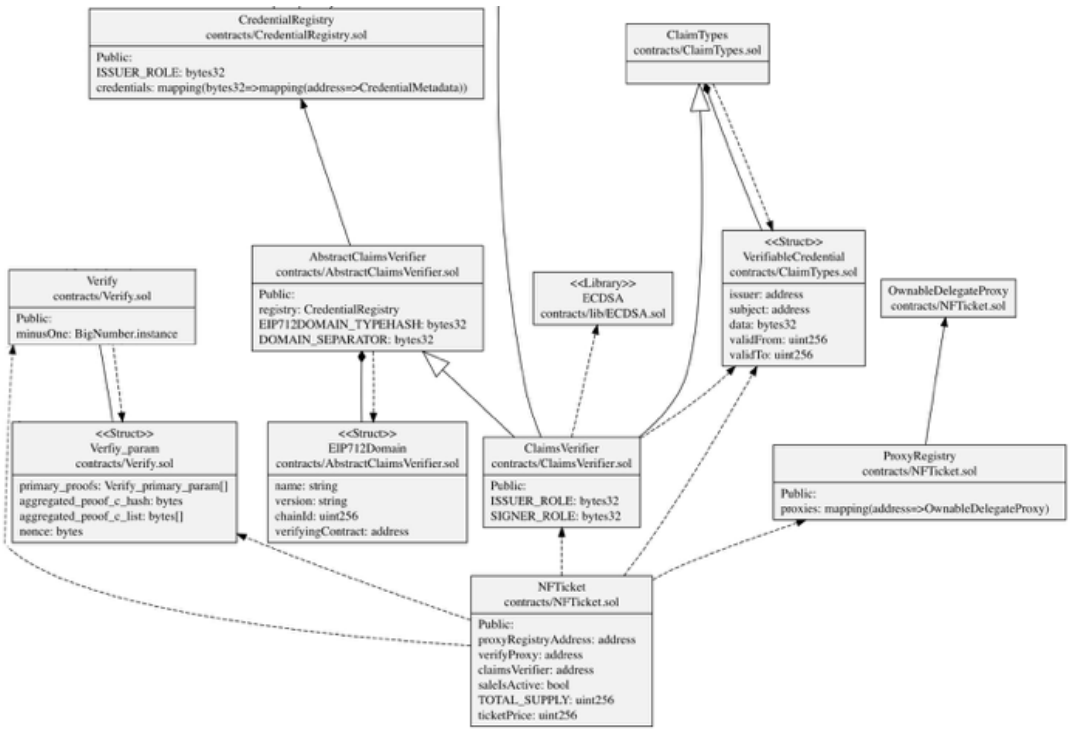

Figure 2 UML Class diagram showing the main smart contracts and their relations

One note must be made regarding this implementation, as the experimental results show that the gas used to execute the mintTo() method is relatively high, i.e., ~84000000 gas units. This is due to the execution of Verify's method verify() that requires a high computational load to verify the ZKP. As anticipated by the authors of this library [24], this gas cost is relatively high for day to day operations, however some optimization can be still implemented. For the sake of this paper, this aspect is left as future work.

6. Discussion and conclusions

The Metaverse is attracting the attention of the market. Initially developed for video games, it is expected to enter everyday life to conduct a wide variety of activities. Even though the latter is carried out in a virtual dimension, they can produce legal consequences in the real world. This concept appears more evident if the Metaverse is considered more like a medium than a place. From this perspective, it is easier to understand that the Metaverse must align with the analogic world.

Having considered this, the matter of digital identity is paramount for creating a trustworthy environment in the Metaverse. As seen under Section 2.2., electronic ledgers (i.e. blockchain technology) only guarantee data integrity and accuracy of their chronological ordering; they do not ensure the identifiability of blockchain users. Thus, blockchain-based Metaverse platforms must integrate with other legally recognised instruments of online identification, which has been described under Section 2.1. Among those methods, it is observed that the European Digital Identity Wallet is the most suitable because it guarantees selective disclosure of identity data.

Indeed, from a legal point of view, the privacy of individuals who do not want to share more data than necessary under the law should be preserved. In particular, the Metaverse is regarded as a further sphere of social relations. Despite the traditional way of interacting online, people appear in their entirety. They can recreate a sort of parallel life in a parallel society, where they should have the right to build their own personality and social representation in the public eye.

In Section 4, we have shown the use case of an avatar entering a cinema in the Metaverse where the real-world age is needed to watch a movie. The disclosure of a user's credentials takes place thanks to the use of Verifiable Credentials. The use case highlights the possibility of verifying real-life credentials thanks to such a tool. Indeed, even if the user maintains the right to be represented and possibly identified by his or her avatar in the Metaverse, whenever a real-life characteristic is

required, the selective disclosure of Verifiable Credentials can intervene. In the presented use case, being over 18 years old is required for access to audiovisual content.

Implementing such a scenario means exploiting the smart contracts that can directly interact with the Metaverse of interest, i.e., the Ethereum smart contracts and Decentraland. The simple act of buying a cinema ticket in Decentraland can be implemented the same as the purchase of an NFT, i.e., an NFT ticket. The act of being age verified by the ticket seller can be implemented as an on-chain verification of anonymous credentials based on Zero-Knowledge Proofs. The combination of the two can possibly enable any avatar in Decentraland to access an age-restricted movie screening in a decentralised cinema without disclosing the user's real identity.

The new technical challenges that we had to address in the implementation of the use case concerned data protection. We argue that it is not trivial to integrate Zero-Knowledge Proofs for the protection of one's identity in the Metaverse, as the current state of the art still does not provide efficient implementations in a decentralised system. In fact, our implementation performances show this limit, but still pave the way for future works in which different combinations of technologies and/or optimisation can be tested. Moreover, integrating bridges for the interoperability of different DLTs and Metaverses will be investigated.

7. References

[1] W. L. P. Prosser, "Privacy", California Law Review, vol. 48, p. 383, 1960.

[2] D. L. Zimmerman, "False light invasion of privacy: The light that failed", In New York University Law Review, vol. 64, p. 364, 1989.

[3] R. Epstein, "Cases and materials on torts", Gaithersburg - New York, vol. 7, p. 1214, 2000.

[4] G. Falco, "Identità personale", Nuovo Digesto Italiano, vol. 6, p. 649, 1938.

[5] F. Degni, Le persone fisiche e i diritti della personalità. Torino: Utet, 1939.

[6] G. Pino, Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale. Bologna: Il Mulino, 2003.

[7] Pretura, 6 mag. 1974, GI, 2, p. 514. (Rome, Italy).

[8] Veronesi, Cassazione civile, 22 giu. 1985, 3769, 2211 (Italy).

[9] C. Hackl. "The Metaverse is coming and it's a very big deal". Forbes, 2020. Online: https://www.forbes.com/sites/cathyhackl/2020/07/05/the-metaverse-is-coming--its-a-very-big-deal/

[10] B. Guidi, and A. Michienzi. "Social games and Blockchain: exploring the Metaverse of Decentraland." 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW). IEEE, 2022.

[11] A. Zaccaria, M. Schmidt Kessel, R. Schulze, A. M. Gambino. "EU eIDAS Regulation – Article-by-Article Commentary." Beck Hart Nomos, 2020.

[12] F. Delfini, G. Finocchiaro. "Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014." Giappichelli, 2017.

[13] United Nations Commission On International Trade Law. "Model Law on the Use and Cross border Recognition of Identity Management and Trust Services." United Nations, 2022. Online: https://uncitral.un.org/en/mlit

[14] A. Preukschat, and R. Drummond. "Self-sovereign identity". Manning Publications, 2021.

[15] European Commission. "The European Digital Identity Wallet Architecture and Reference Framework." European Commission, 2023. Online: https://github.com/eu-digital-identity-wallet/architecture-and-reference-framework

[16] Technopedia "Avatar." Technopedia, 2018. Online: https://www.techopedia.com/definition/4624/avatar

[17] M. A. Franks, "Unwilling avatars: Idealism and discrimination in cyberspace", Columbia Journal of Gender and Law, vol. 20, n. 2, p. 224, 2011.

[18] R. Koster, "Declaring the rights of players", 27 ago. 2000. Online: http://www.raphkoster.com/gaming/playerrights.shtm

[19] New Yorker, 5 July 1993, 61.

[20] The Economic Times. “Now Shemaroo offers movie theatre on metaverse.” The Economic Times, 2022. Online: https://economictimes.indiatimes.com/tech/technology/now-shemaroo-offers-movie-theatre-on-metaverse/articleshow/94538342.cms
[21] European Blockchain Services Infrastructure. “EBSI documentation.” 2022. Online: https://api-pilot.ebsi.eu/docs/apis/ledger/latest#/
[22] Robinson, P., Ramesh, R., & Johnson, S. (2022). Atomic crosschain transactions for ethereum private sidechains. Blockchain: Research and Applications, 3(1), 100030.
[23] S. Ceron, and A.L. Batista. “Verifiable Claims Contracts.” GitHub, 2023. Online: https://github.com/lacchain/vc-contracts
[24] Muth, R., Galal, T., Heiss, J., & Tschorsch, F. (2022). Towards smart contract-based verification of anonymous credentials. Cryptology ePrint Archive.
[25] Camenisch, J., & Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3 (pp. 268-289). Springer Berlin Heidelberg.
[26] Casale-Brunet, S., Ribeca, P., Doyle, P., & Mattavelli, M. (2021, December). Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem. In 2021 IEEE International Conference on Blockchain (Blockchain) (pp. 188-195). IEEE.
[27] Cai, B. “ERC-5484: Consensual Soulbound Tokens.” Ethereum Improvement Proposals, 2022. Online: https://eips.ethereum.org/EIPS/eip-5484#soulbound-token-sbts-as-an-extension-to-eip-721
[28] Zichichi, M. “NFTicket.” GitHub, 2023. Online: https://github.com/miker83z/nfticket