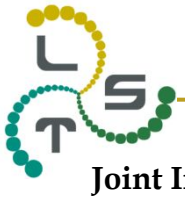
Law, Science and Technology
MSCA ITN EJD n. 814177

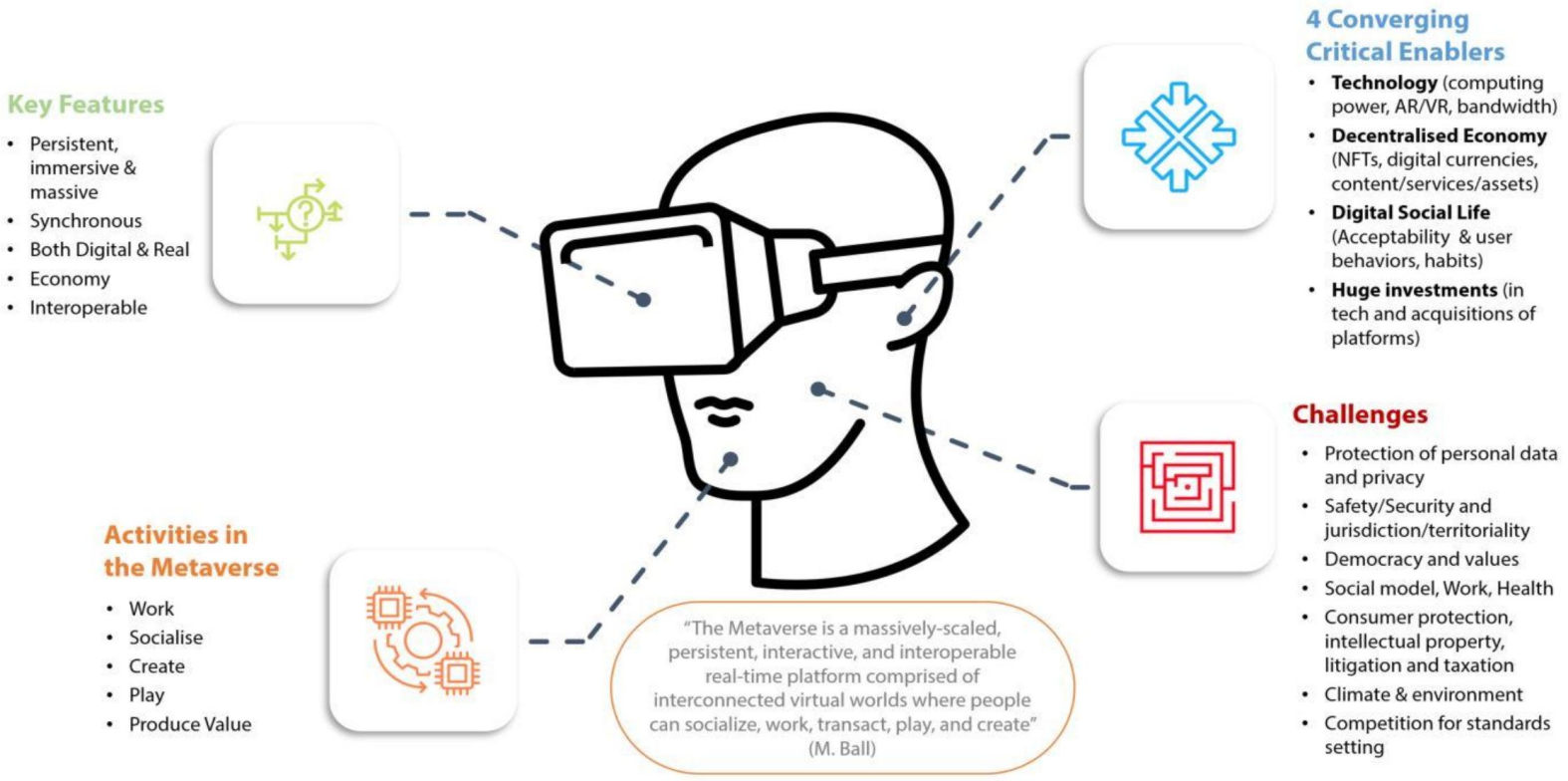
Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland

Mirko Zichichi[1,2,3], *Chantal Bomprezzi*[2], ***Giovanni Sorrentino***[2] *and Monica Palmirani*[2]

1 Ontology Engineering Group, Universidad Politécnica de Madrid
2 CIRSFID, University of Bologna
3 IOTA Foundation



What is "Metaverse(s)"?

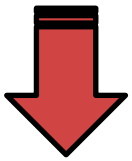


Source: ART

A new perspective of personal identity

«*If the metaverse lets you be whoever you want,*
will you be you?»
Steven Zeitchik, The Washington Post

Potentially, the Metaverse allows us to be who we want, through our avatar



A possibility, but also a problem!

A cinema in the Metaverse

The goal of the paper

To find a balance between:

1) Real user identification
2) disclosure of only strictly necessary data *(age < or > of 18 years)*

Balancing privacy and freedom using blockchain

Online identification

- **e-IDAS** (electronic Identification Authentication and Signature)

Aims at providing a basic legislation at the EU level for trust services and electronic identification of member states.

Defines the «electronic Identification» (Art. 3)

EXAMPLES OF IDENTIFICATION INSTRUMENTS:

- SPID
- CIE
- Electronic signature (for natural person)
- Electronic seals (for legal person)

- **UNCITRAL**

eIDAS 2.0 and Self Sovereign Identity

Final objective of eIDAS 2.0: setting of a European Digital Identity framework

HOW?

1) **European Digital Identity Wallet**
   - Selective Disclosure of data
   - Self Sovereign identity (SSI)

2) **Electronic ledger** (DLT Technology)

= Qualified identity management system based on DLT - A secure and trustworthy way to share identity data while preserving the privacy of the individuals.

Object of the paper: to design a system to verify the identity in the Metaverse compliant with eIDAS 2.0

W3C Decentralized Identifier (DID) and Verifiable Credentials (VC)

- European Digital Identity Wallet Architecture and Reference Framework

- **DID** -> identifier entirely under the control of the identity subject, independent from any centralised registry, identity provider, or certificate authority.
- **VC** -> tamper-evident credential with authorship that can be cryptographically verified.

- Roles and entities:
  - *VC Issuer* -> entity's role in asserting claims about one or more subjects;
  - *VC Holder* -> stores VCs securely under its own control through a wallet;
  - *Verifier* -> requests and verifies VCs.
  - *Verifiable data registry* -> mediates the creation and validation of identifiers (DIDs), keys, and other relevant data required for the exchange -> DLTs.

Use case: entering a cinema in the Metaverse

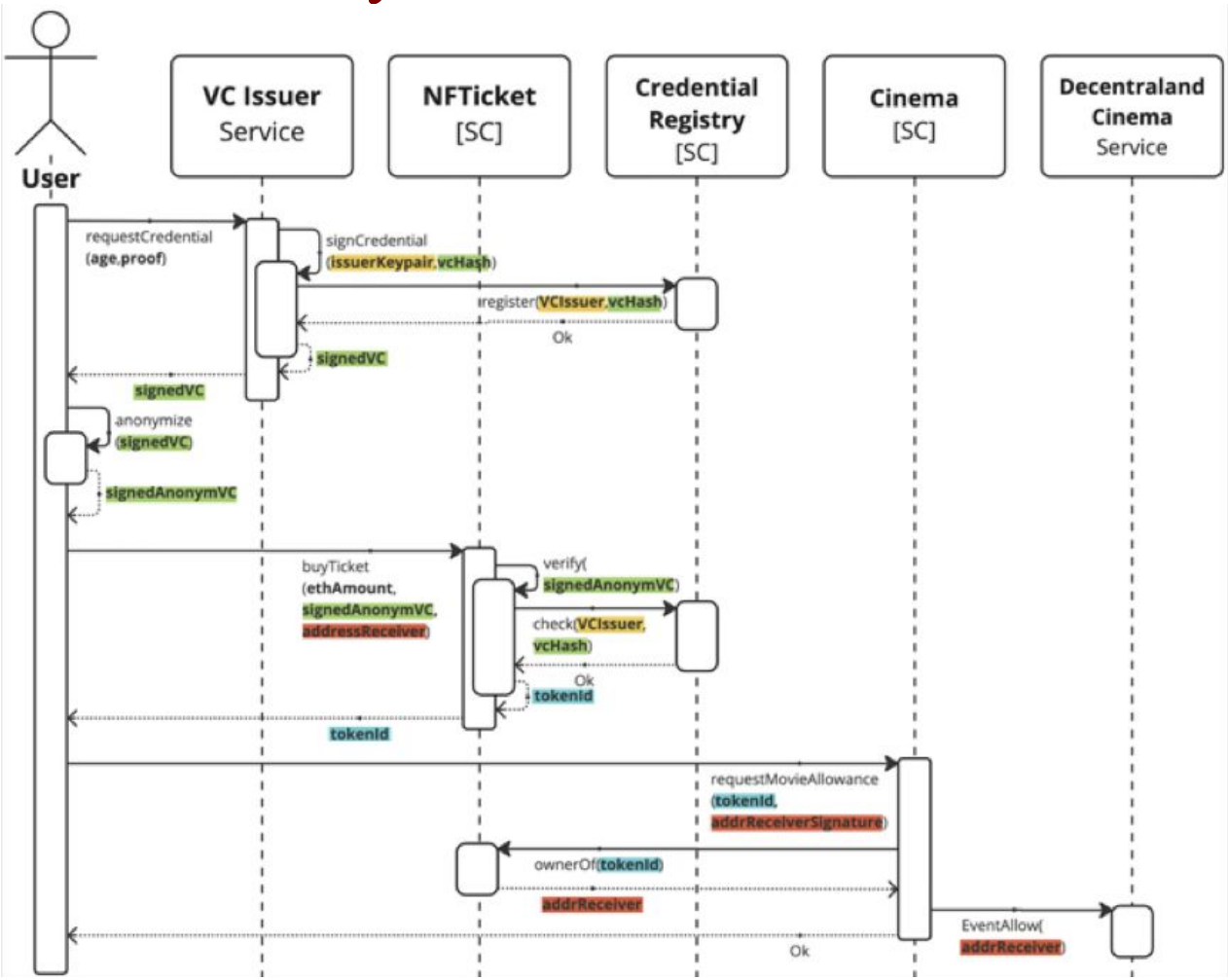
https://kotaku.com/watching-inception-in-fortnite-is-weird-but-doesnt-mak-1844175790

Use case: entering a cinema in the Metaverse

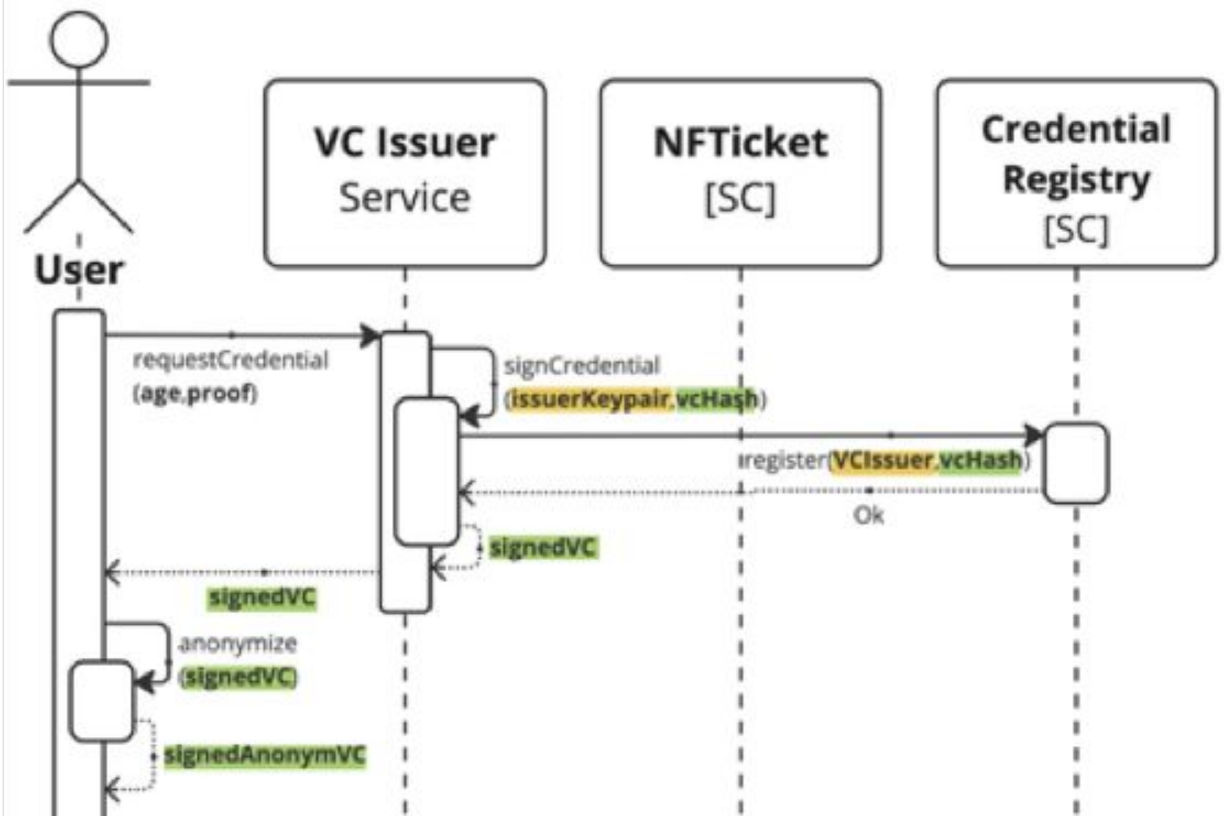
- **W3C Verifiable Credential issuing**
  - Obtain a trusted source of information -> VC Issuer
  - Create a digital representation of the information -> VC in JSON-LD
  - Sign and Store the digital representation -> Wallet
  - Use the digital representation as a VC

- **On-chain Verifiable Credential verification (smart contract)**
  - Receive the VC
  - Verify the issuer signature
  - Check the issuer -> DID - Credential Registry smart contract
  - Validate the information -> e.g. subject >= 18
  - Allow or deny access -> issue a NFT ticket

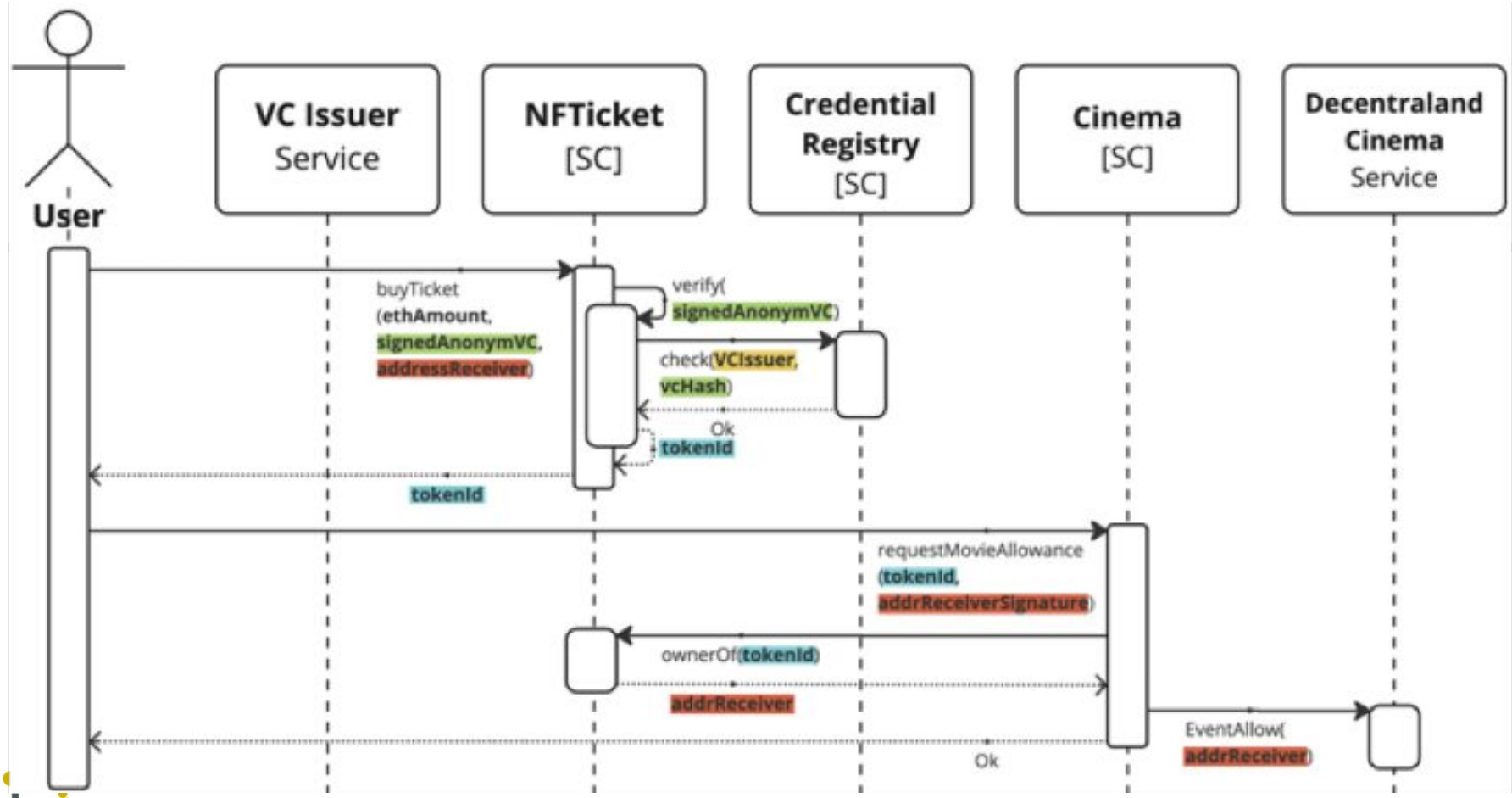
Implementation of a smart contract-based system for the disclosure of anonymous credentials in the Metaverse



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



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



Decentralised Cinema Smart Contract

- **Verification of anonymous credentials based on Zero-Knowledge Proofs**
  - Different Solidity Smart Contract implementations already provide the use of verifiable credentials on-chain.
  - ***anonymous credentials*** Signature Proofs of Knowledge enabling a credential holder prove possession of a CL-signature over certain attribute value .
  - CL signature scheme provides the proving knowledge of a signature on a committed value.
  - an inequality predicate consists of the credential holder to prove that a specified inequality is satisfied without revealing the actual value of the attribute (i.e., age >= 18 in our scenario).

- **ERC-721**
  - NFTicket is minted after the execution of the anonymous credentials verification with an inequality predicate sub-proof.
  - this implementation can be feasibly used in the Decentraland platform to represent assets.
  - We make reference to the soulbound token extension of the ERC-721.

Results Discussion

- User maintains right to be identified by their avatar in the Metaverse
  -> whenever a real-life characteristic is required, the selective disclosure of anonymous Verifiable Credentials can be used.

- 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 experimental results show that the gas used to execute the *mintTo()* method is relatively high, i.e., ~84000000 gas units

Conclusions

- The matter of digital identity is paramount for creating a trustworthy environment in the Metaverse.
- Electronic ledgers (i.e. DLT) 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 be integrate with other legally recognised instruments of online identification
- The European Digital Identity Wallet might be the most suitable
- The use case of an avatar entering a cinema in the Metaverse shows how 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.