UNIVERSITY OF PADUA
UNIVERSITA' DEGLI STUDI DI PADOVA

VerifiedMovies: il cinema in piena sicurezza con l'uso della blockchain

Dipartimento di Matematica "Tullio Levi Civita"

Corso di Laurea in Informatica

Esame di Laurea - 21 Luglio 2023

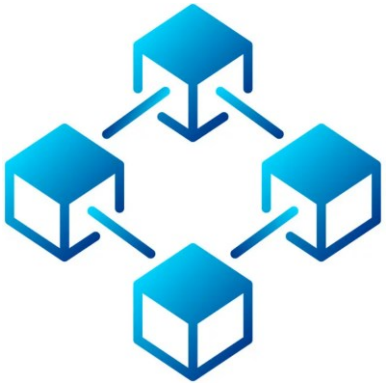
Laureando: Gabriel Rovesti - Matricola n. 2009088

Relatrice: Prof.ssa Ombretta Gaggi

L’azienda

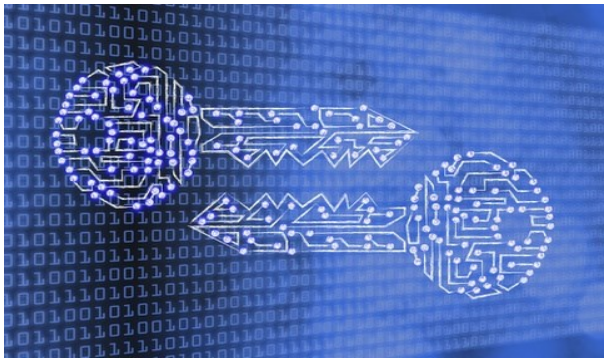
- Software house italiana nata a Napoli nel 2002
- Servizi di consulenza specialistica in ambito web, mobile, sicurezza e networking

L’idea del progetto: Blockchain



- Struttura dati basata su un consenso distribuito tra i partecipanti secondo protocolli definiti a priori
- Dati salvati come hash in blocchi a catena e firmati digitalmente
- Immutabilità dei dati e tracciabilità completa senza intermediari
- Informazioni salvate in modo trasparente e decentralizzato

Obiettivi per il progetto



- Applicazione della tecnologia blockchain ad un caso d'uso reale
- Studio di standard di identità digitale connessi e loro applicazione all'interno di una maschera web
- Creazione di un sistema di riconoscimento basato su metodi sicuri, attento alla privacy e senza divulgazione di informazioni personali

Requisiti del progetto

- Realizzazione di un sito di un cinema applicando questo sistema per film soggetti a limite d'età
- Verifica dell'identità utente con un meccanismo basato su **Self Sovereign Identity** e **Zero Knowledge Proof**
- Utilizzo dell'ambiente blockchain *Ethereum*
- Creazione di un *Proof of Concept* basato sulle librerie **web3.js** oppure **ethers.js**

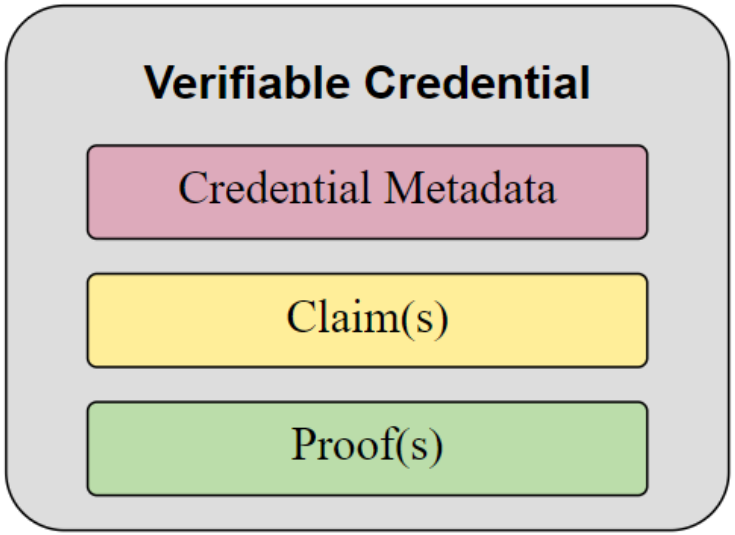
Decentralized Identifiers (DID)

- Identificatori alfanumerici permanenti come degli URL, associati ad un'entità verificabile (*risolvibili*), gestiti dall'utente (*controller*) e senza controllo centrale

- Ad essi è associato un documento che descrive il soggetto associato e i metodi di autenticazione sicuri (*DID* Method), chiamato *DID Document*

- Permettono un accesso sicuro senza dipendere da enti di terze parti, crittografati con la propria chiave privata e la chiave pubblica di un'entità fidata

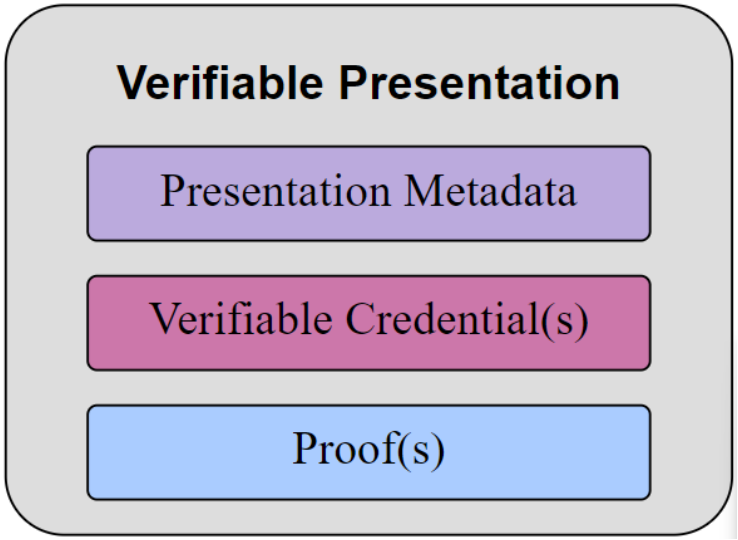
Verifiable Credentials (VC)



- Credenziali rilasciate da un'entità fidata firmate con la sua chiave pubblica, la chiave privata dell'utente e contenente il **Decentralized Identifier** come prova certa di identità

- Create in formato JSON, contengono un'entità che afferma con certezza il rilascio *(claim),* gli attributi base dell'utente che le presenta (*metadata*) e la prova crittografica in formato hash di autenticità (*proof)*

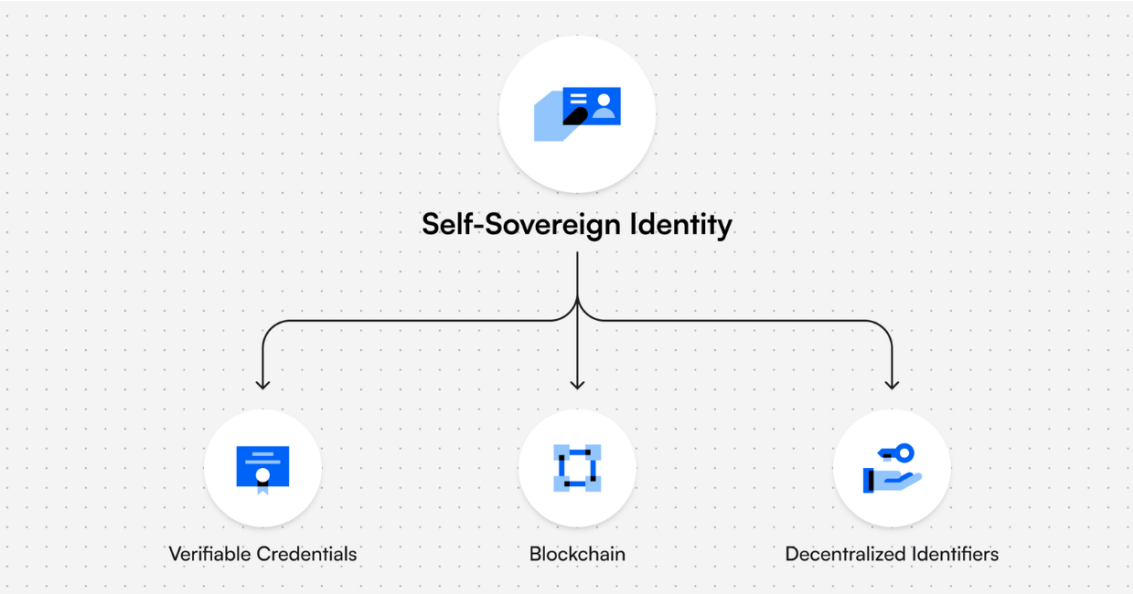
Verifiable Presentations (VP)



- Dati composti da una o più **Verifiable Credentials (VC)** che presentano un insieme di dati codificati con una prova crittografica di non manomissione

- Consentono di esprimere i dati degli utenti in modo tale da permetterne una verifica certa attraverso delle prove comuni di autenticazione (*proofs*)

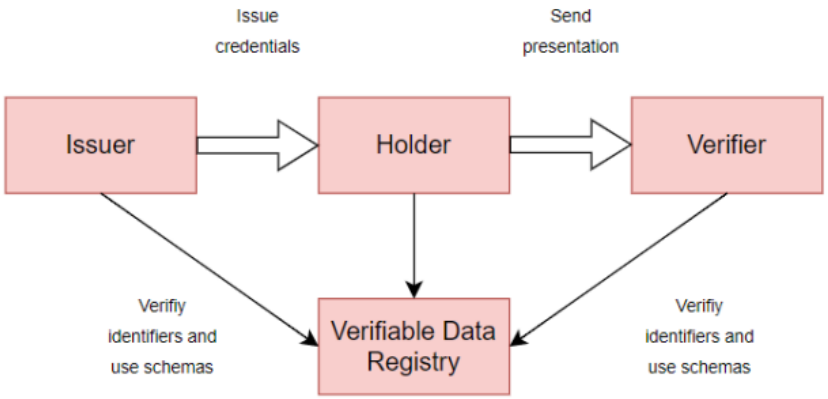
Self Sovereign Identity (SSI)



- Modello che dà il controllo all'utente dei propri dati personali, associando un'identità specifica, portabile tra più sistemi e minimizzando i dati scambiati

- Identificazione univoca tramite un **Decentralized Identifier** firmato con chiave private dell'utente e chiave pubblica di un'entità fidata in blockchain

Catena di fiducia



- La credenziale dell'utente viene rilasciata da un'entità fidata definita **issuer**
- Esiste una «catena di fiducia» formata da una serie di *issuer* fidati partendo da un'unica firma di un'entità padre, definita **certification authority**
- L'utente presenta la credenziale nel proprio *wallet* e li presenta come **holder**
- Il sito controlla la validità dei dati presentati assumendo il ruolo di **verifier,** leggendo i dati dalla blockchain (*verifiable data registry*).

Zero Knowledge Proof (ZKP)

- Metodo crittografico in cui un'entità può dimostrare a un'altra entità di conoscere un determinato valore senza rivelare il valore effettivo

- Occorre dimostrare l'appartenenza ad uno *schema* comune (la catena di fiducia), dimostrando che la credenziale è stata firmata da entità fidate e provando la correttezza di tutti i dati presenti

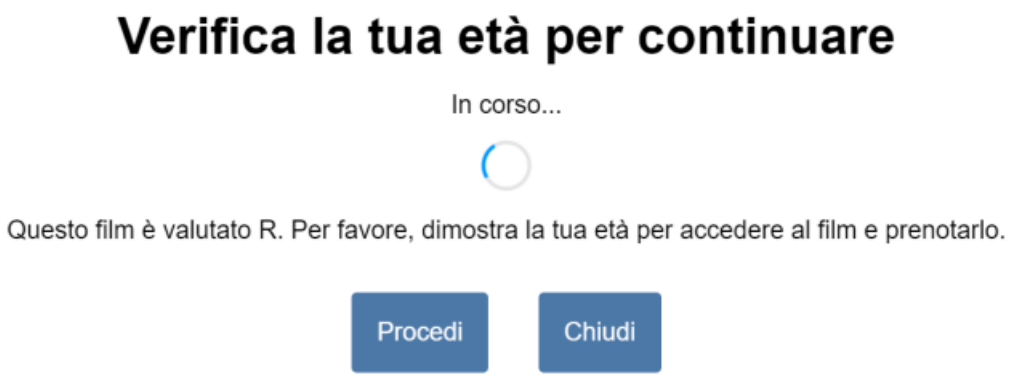
Le caratteristiche del progetto

- Registrazione e login basate su un meccanismo *challenge-response* per associare all'utente un **Decentralized Identifier** firmato con la propria chiave privata

- Implementazione della catena e di **Self Sovereign Identity** usando lo *smart contract* dello stagista e laureando magistrale presso Ca' Foscari Alessio De Biasi

- Meccanismo di verifica dell'età dell'utente in base ai limiti d'età del singolo film basato sulla presentazione di credenziali con **Zero Knowledge Proof**

Verifica dell'età



1. Creazione di una **Verifiable Credential** con i dati dell'utente e il **Decentralized Identifier** usato in fase di autenticazione

2. Creazione di una **Verifiable Presentation** usando come prova di correttezza della credenziale presente lo schema *CLSignature2019,* utile per **Zero Knowledge Proof**

3. Risoluzione delle firme digitali presenti e verifica della catena di fiducia usando **Self Sovereign Identity**

Tecnologie del progetto

Front-end

Back-end e smart contract

Conclusioni e resoconto

Obiettivi raggiunti:

- Soddisfazione totale degli obiettivi obbligatori e desiderabili
- Creazione di un *Proof of Concept* in grado di realizzare correttamente **Zero Knowledge Proof** e **Self Sovereign Identity**

Riflessioni e retrospettiva:

- Importante esperienza in ambito in gran parte sconosciuto
- Realizzazione di un progetto che utilizza tecnologie non del tutto standardizzate, con molti sviluppi futuri e importante oggetto di ricerca
- Autonomia nella realizzazione del progetto e maturazione professionale