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

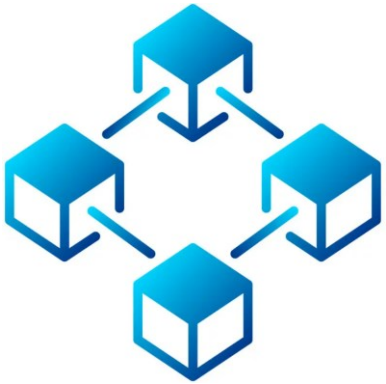
Laureando: Gabriel Rovesti - Matricola n. 2009088

Relatrice: Prof.ssa Ombretta Gaggi

L’azienda

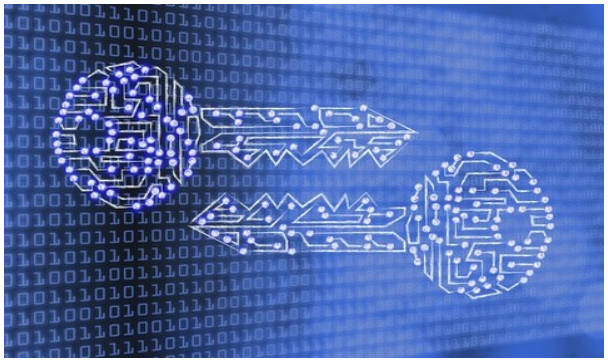
- Software house italiana nata a Napoli nel 2002
- 6 sedi presenti nel territorio
- Servizi di consulenza specialistica in ambito web, mobile, sicurezza e networking

L’idea del progetto: Blockchain



- Struttura dati basata su un consenso distribuito tra i partecipanti
- 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



- Uso delle tecnologie blockchain in un caso d'uso reale
- Studio di standard di identità digitale e valutazione delle loro potenziali applicazioni all'interno di una maschera web
- Creazione di un sistema di riconoscimento basato su metodi sicuri, che garantisce la privacy senza divulgazione di informazioni personali

Requisiti del progetto

- Realizzazione di un sito di un cinema con film soggetti a limite d'età

- Verifica dell'identità e prenotazione di un film con un meccanismo basato sullo studio di **Self Sovereign Identity** e **Zero Knowledge Proof**

- Creazione di un meccanismo di riconoscimento senza divulgazione di dati personali basato su blockchain *Ethereum* e sugli standard di identità digitale connessi

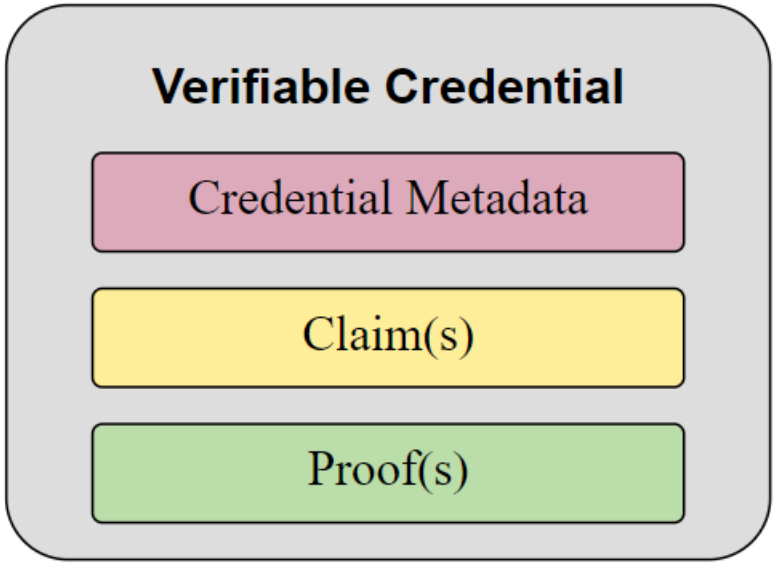
Decentralized Identifiers (DID)

- Identificatori univoci composti da una stringa alfanumerica a associati ad un'entità verificabile normati dallo standard W3C omonimo

- Ad essi è associato un documento che descrive il soggetto associato e i metodi di autenticazione utilizzati in modo sicuro

- 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

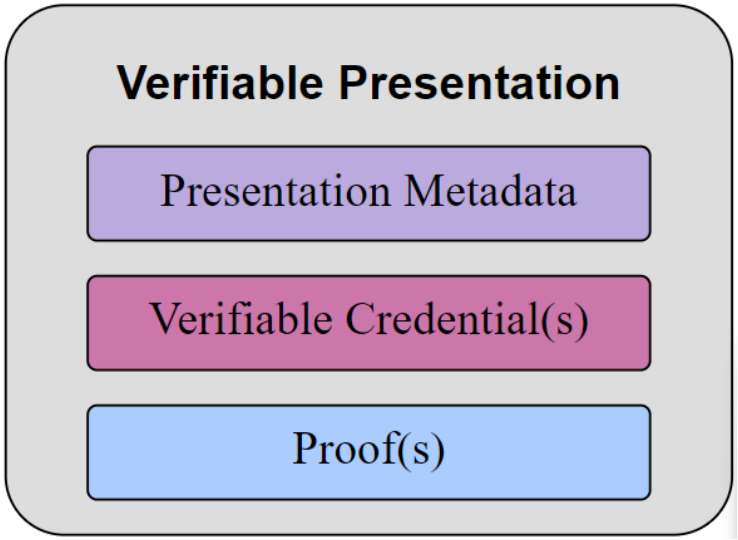
Verifiable Credentials (VC)



- Standard W3C aperto per credenziali digitali firmate digitalmente e verificabili pubblicamente usando il **Decentralized Identifier** dell'utente

- 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 di autenticità (*proof)*

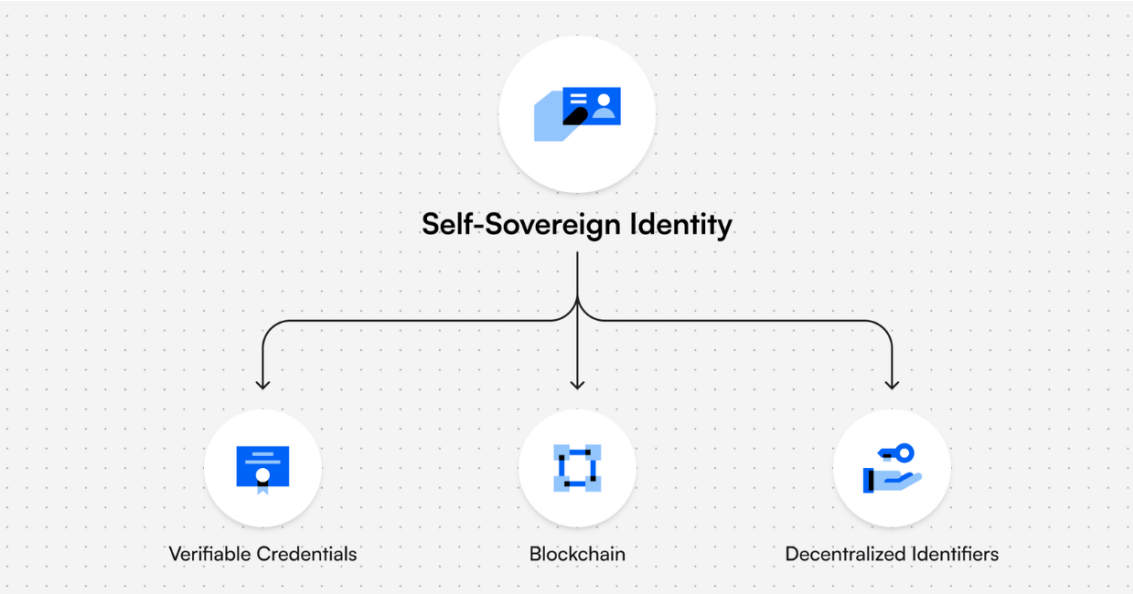
Verifiable Presentations (VP)



- Dati composti da una o più **Verifiable Credentials** che condividono in modo sicuro e verificabile le proprie informazioni (normate nella stessa sezione)

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

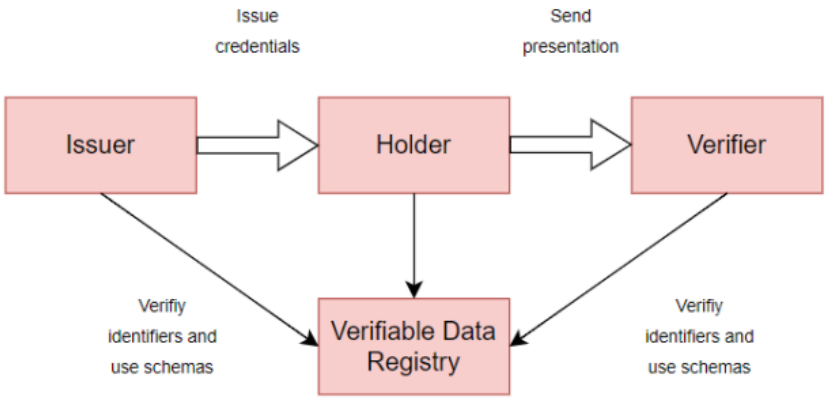
Self Sovereign Identity (SSI)



- 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 le proprie chiavi all'interno di credenziali immutabili e uniche in blockchain

Catena di fiducia



- La credenziale dell'utente viene emessa da un'entità fidata chiamata **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 fornisce questa credenziale come prova in qualità di **holder**
- Il sito attiva un meccanismo di verifica assumendo il ruolo di **verifier**

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 tutte le credenziali sono state firmate da entità fidate e provando la correttezza di ognuna

Il progetto realizzato

VerifiedMovies
PRIVACY MADE EASY

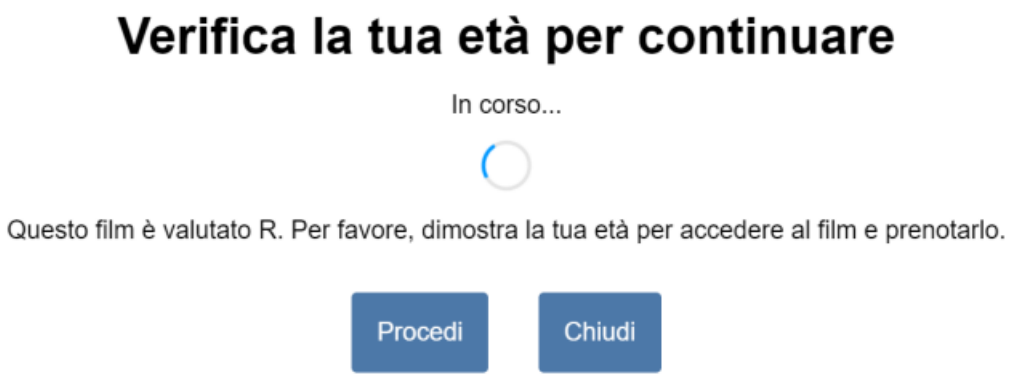
Le caratteristiche del progetto

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

- Implementazione della libreria che realizza **Self Sovereign Identity** usando lo *smart contract* del laureando magistrale in Informatica presso Ca' Foscari Alessio De Biasi

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

Verifica dell'età



1. Creazione di una **Verifiable Credential** sulla base del **Decentralized Identifier** usato in fase di login

2. Creazione di una **Verifiable Presentation** firmato digitalmente secondo lo standard *CLSignature2019* usato per realizzare **Zero Knowledge Proof** e per generare le prove di correttezza della credenziale presentata

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 ma poca presenza e guida sulle attività svolte