VerifiedMovies

Rovesti Gabriel – matricola 2009088

Sommario

[Introduzione 2](#_Toc135238061)

[Descrizione 3](#_Toc135238062)

[Analisi delle tecnologie 4](#_Toc135238063)

[Protocolli di identità digitale 4](#_Toc135238064)

[Zero Knowledge Proof 4](#_Toc135238065)

[Self Sovereign Identity 4](#_Toc135238066)

[Tecnologie di firma 4](#_Toc135238067)

[Problematiche e soluzioni 5](#_Toc135238068)

[Sfide e limiti 6](#_Toc135238069)

[Scenari futuri 7](#_Toc135238070)

[Conclusioni 8](#_Toc135238071)

# Introduzione

Il seguente documento fornisce una panoramica del progetto di stage e dello sviluppo di un'applicazione decentralizzata (dApp) chiamata VerifiedMovies. Lo stage mirava a esplorare e implementare le tecnologie blockchain, i protocolli di identità digitale e i concetti di identità auto-sovrana nel contesto di un'applicazione pratica.

Gli obiettivi principali dello stage erano molteplici:

* Acquisire esperienza pratica nello sviluppo di applicazioni decentralizzate utilizzando la tecnologia blockchain.
* Esplorare il potenziale dei protocolli di identità digitale e dell'identità sovrana per migliorare la privacy e la sicurezza dei dati.
* Implementare una dApp che sfrutti i concetti di blockchain e identità decentralizzata per un caso d'uso specifico.

Durante lo stage, l'attenzione si è concentrata sullo sviluppo di VerifiedMovies, una dApp progettata per fornire una piattaforma sicura e trasparente per la verifica e l'autenticazione dei film. Questo documento fornirà una descrizione dettagliata della dApp, delle tecnologie utilizzate, delle sfide incontrate e delle soluzioni implementate.

Il progetto, infatti, descrive l’implementazione di una piattaforma di un cinema basata sugli standard W3C Decentralized Identifier e Verifiable Credentials, usando Zero Knowledge Proof per la verifica sicura delle informazioni trasmesse senza divulgare alcuna informazione sullo stesso.

Lavorando su VerifiedMovies, lo stage ha avuto l'obiettivo di promuovere una comprensione più approfondita delle tecnologie blockchain, dei protocolli di identità digitale e delle potenziali applicazioni dei sistemi decentralizzati. Il progetto ha offerto l'opportunità di esplorare l'intersezione tra blockchain, identità digitale e industria dell'intrattenimento, con l'obiettivo di contribuire al progresso di piattaforme sicure e affidabili.

Le sezioni successive approfondiranno i dettagli della dApp, le tecnologie utilizzate, i problemi affrontati durante lo sviluppo, le sfide incontrate e i potenziali scenari futuri per le implementazioni blockchain e le applicazioni decentralizzate. Il documento si concluderà con una sintesi delle attività svolte durante lo stage e delle competenze acquisite durante il processo.

Basato sullo studio autonomo delle tecnologie blockchain e della loro base, la piattaforma offre un insieme semplificato di funzioni connesse al sito di un cinema, comprendenti una registrazione, un accesso e una gestione del proprio profilo, permettendo l’accesso sicuro ai contenuti qualora univocamente dimostrato. Il contesto della blockchain serve a garantire la sicurezza e l’univocità delle informazioni trasmesse.

# Descrizione

VerifiedMovies è un'applicazione decentralizzata (dApp) sviluppata durante lo stage, con l'obiettivo di fornire una piattaforma sicura e trasparente per la verifica e l'autenticazione dei film. La dApp sfrutta la tecnologia blockchain, i protocolli di identità digitale e i concetti di identità auto-sovrana per garantire l'integrità e l'autenticità dei dati dei film.

Le funzionalità implementate in VerifiedMovies includono:

* Registrazione e Accesso: VerifiedMovies offre agli utenti la possibilità di registrarsi e accedere alla piattaforma in modo sicuro e affidabile. Durante il processo di registrazione, agli utenti viene richiesto di fornire alcuni dati personali, come il nome utente, l’e-mail, la password e la data di nascita. Questi dati vengono criptati e associati in modo univoco a un Decentralized Identifier (DID) all'interno della blockchain. Durante il processo di accesso, VerifiedMovies genera un numero casuale unico e lo presenta all'utente, che deve firmare digitalmente questo numero utilizzando la propria chiave privata associata al DID. La firma viene verificata sulla blockchain e se corrisponde, all'utente viene concesso l'accesso alla piattaforma.
* Integrazione dell'identità digitale: il progetto implementa i protocolli di identità digitale, come Self-Sovereign Identity (SSI), per consentire agli utenti di creare e gestire le proprie identità in modo sicuro e rispettoso della privacy. Ogni utente ha il controllo completo sui propri dati personali e può divulgare selettivamente le informazioni quando necessario. Utilizzando i Decentralized Identifier (DID), VerifiedMovies associa un identificatore univoco a ciascun utente, consentendo loro di presentare e verificare la propria identità attraverso l'uso di Verifiable Credential e Verifiable Presentation. Questo meccanismo garantisce l'autenticità e l'integrità delle informazioni senza dover divulgare dati personali sensibili.
* Interazione con l'utente: La dApp fornisce un'interfaccia utente intuitiva che permette agli utenti di sfogliare e cercare film, visualizzarne i dettagli e interagire con la piattaforma. Gli utenti possono lasciare recensioni e valutazioni per i film, migliorando l'engagement della comunità e fornendo informazioni utili agli altri utenti nella scelta dei film da guardare. Questa interazione facilita una comunità dinamica e partecipativa all'interno della piattaforma.

Le tecnologie utilizzate per sviluppare VerifiedMovies includono piattaforme blockchain, come Ethereum, che forniscono un registro decentralizzato e immutabile per la verifica dei film. Inoltre, VerifiedMovies sfrutta i protocolli di identità digitale basati su Self-Sovereign Identity (SSI) per consentire una gestione sicura e rispettosa della privacy dell'identità degli utenti. Inoltre, VerifiedMovies fa uso di tecniche di Zero Knowledge Proof (ZKP) per garantire la privacy dei dati, consentendo agli utenti di dimostrare determinate affermazioni senza rivelare informazioni sensibili.

Nel complesso, la piattaforma rappresenta una soluzione innovativa che sfrutta le tecnologie blockchain basate su un caso d’uso comune e reale; gli approcci di identità digitale auto-sovrana garantiscono la piena sicurezza delle informazioni trasmesse, costruendo una piattaforma sicura e trasparente per la verifica e l'autenticazione dei film, accedendo ai contenuti solo previa verifica specifica. La decentralizzazione, l'integrità dei dati e la privacy dell'identità degli utenti sono al centro del progetto, offrendo per quanto possibile un’esperienza semplice e sicura.

# Analisi delle tecnologie

Nel capitolo dell'Analisi delle tecnologie, esploreremo in dettaglio le tecnologie utilizzate per implementare VerifiedMovies, concentrandoci sui protocolli di identità digitale, le Zero Knowledge Proof (ZKP) e l'identità auto-sovrana.

## Protocolli di identità digitale

I protocolli di identità digitale svolgono un ruolo fondamentale in VerifiedMovies per garantire una gestione sicura e rispettosa della privacy dell'identità degli utenti. Uno dei protocolli chiave utilizzati è il concetto di Self-Sovereign Identity (SSI), che permette agli utenti di avere il controllo completo dei propri dati personali e di autenticare la propria identità senza dipendere da terze parti centralizzate.

Nel contesto di VerifiedMovies, i protocolli di identità digitale vengono implementati utilizzando i Decentralized Identifier (DID), che forniscono identificatori univoci a ciascun utente. Questi identificatori vengono utilizzati per associare e verificare le identità degli utenti all'interno della blockchain. Inoltre, VerifiedMovies utilizza i concetti di Verifiable Credential e Verifiable Presentation per consentire agli utenti di presentare e convalidare le proprie informazioni di identità in modo sicuro e criptograficamente firmato.

(aggiungere spiegazioni di dettaglio vere e proprie)

## Zero Knowledge Proof

Le tecniche di Zero Knowledge Proof (ZKP) vengono utilizzate in VerifiedMovies per migliorare la privacy dei dati degli utenti. Una ZKP consente a una parte di dimostrare la validità di un'affermazione senza dover rivelare informazioni sensibili. In questo contesto, VerifiedMovies potrebbe utilizzare ZKP per consentire agli utenti di dimostrare che soddisfano determinati criteri per accedere a determinati film, senza dover rivelare dettagli specifici sulla loro identità o preferenze personali.

Ad esempio, un utente potrebbe voler dimostrare di avere l'età legale per guardare un determinato film senza dover rivelare la sua data di nascita effettiva. Utilizzando ZKP, l'utente potrebbe generare una prova criptografica che dimostra che ha un'età superiore a un certo limite senza dover rivelare il suo valore effettivo di data di nascita. Questo garantisce la privacy dell'utente mentre soddisfa i requisiti per accedere al film.

(aggiungere spiegazioni di dettaglio vere e proprie usando questo come base)

## Self Sovereign Identity

L'identità auto-sovrana è un concetto chiave implementato in VerifiedMovies per consentire agli utenti di avere il controllo completo sui propri dati personali e sull'identità. L'identità auto-sovrana permette agli utenti di autenticarsi in modo sicuro senza dover affidarsi a terze parti centralizzate, come governi o aziende.

Con l'identità auto-sovrana, VerifiedMovies consente agli utenti di creare, gestire e controllare le proprie identità digitali in modo sicuro. Gli utenti possono decidere quali informazioni condividere e con chi, mantenendo la privacy e il controllo sui propri dati personali. Questo approccio decentralizzato all'identità consente agli utenti di interagire con VerifiedMovies in modo sicuro e affidabile, senza dover rinunciare al controllo dei propri dati personali.

## Tecnologie di firma

(aggiungere spiegazioni di dettaglio vere e proprie sulle firme utilizzate, just for reference)

# Problematiche e soluzioni

# Sfide e limiti

• Discussione di problemi e sfide relativi all’utilizzo della SSI in applicazioni decentralizzate su blockchain Ethereum

• Implicazioni e limitazioni dell’uso delle soluzioni di second layer in ambito blockchain;

• Primo studio delle vulnerabilità principali della blockchain Ethereum.

# Scenari futuri

# Conclusioni