Per il mio tirocinio devo creare una piattaforma di verifica delle identità che comunica con un progetto di Alessio De Biasi riguardo un meccanismo di verifica a catena basato su blockchain (SSI) e non dimostrando di possedere alcun dato tramite Zero Knowledge Proof. Il suo codice è uno smart contract (chiamato SelfSovereignIdentity.sol) che segue lo standard W3C su Self Sovereign Identity e comunica con la mia applicazione.

Caso concreto: film vietati a minori di 18 anni e controllo dell’età con verifiche.

Appunti di Alessio

Non può essere l'applicazione a creare un DID per l'utente, in quanto al DID è associato almeno un account Ethereum e deve essere un account in possesso dell'utente. Pertanto, dev'essere l'utente a generare il DID chiamando createDID e, poi, presenta questo DID all'applicazione.

Il collegamento può essere fatto off-chain utilizzando semplicemente un'applicazione TypeScript che va a richiamare lo smart contract SelfSovreignIdentity per avere le informazioni.

Pagine e funzionalità (frontend)

* Registrazione e login

La registrazione e il login sono i primi passi per accedere alla piattaforma. Puoi creare una pagina di registrazione per raccogliere le informazioni degli utenti e verificare che le credenziali siano univoche. Successivamente, l'utente potrà accedere alla piattaforma con il proprio nome utente e password.

* Verifica dell'età

Dopo che l'utente si è autenticato, la piattaforma può richiedere la verifica dell'età. In particolare, si verifica l’età immessa in fase di registrazione e salvata localmente. Questo richiama localmente il contrato di Alessio e fa cose verificando.

* Accesso ai film

Se l'utente ha superato la verifica dell'età, potrà accedere ai film. Puoi mostrare i film sulla homepage della piattaforma, oppure puoi creare una pagina separata per visualizzare i film. Qui occorrerà implementare un sistema di ricerca o di navigazione per aiutare gli utenti a trovare i film che desiderano.

* Controllo dell'accesso ai film

Per evitare che i minori accedano ai film vietati per la loro età, occorrerà implementare un controllo dell'accesso ai film. Questo si può fare creando una lista di film vietati ai minori e impedendo l'accesso a tali film agli utenti che non hanno superato la verifica dell'età.

Film salvati su un DB locale, usando MongoDB.

Per ChatGPT

Questo il codice del contratto (SelfSovereignIdentity.sol):

Fonti standard

* DID: <https://www.w3.org/TR/did-core/>
* VC: <https://www.w3.org/TR/vc-data-model/>

La generazione del DID dovrebbe avvenire prima del login, in modo che l'utente possa presentare il suo DID all'applicazione durante il processo di login. Ciò significa che l'utente dovrebbe generare il suo DID tramite la funzione `createDID` prima di accedere all'applicazione.

Il processo di generazione del DID potrebbe essere avviato quando l'utente preme il bottone di connessione a Metamask. Una volta che l'utente ha generato il suo DID e ha ricevuto una conferma dallo smart contract SelfSovereignIdentity, l'applicazione può permettere all'utente di accedere, a patto che abbia superato i controlli di età necessari per accedere ai contenuti riservati agli adulti.

Per effettuare i controlli di età, l'applicazione può richiamare direttamente lo smart contract per verificare se l'utente ha superato l'età minima richiesta per accedere ai contenuti. È importante notare che l'applicazione non deve avere accesso ai dati personali dell'utente per effettuare questi controlli, ma può utilizzare il DID dell'utente per verificare l'età con il supporto dello smart contract.

In sintesi, il processo sarebbe il seguente:

1. L'utente preme il bottone di connessione a Metamask.

2. L'utente genera il suo DID tramite la funzione `createDID`.

3. Lo smart contract SelfSovereignIdentity conferma la creazione del DID e lo restituisce all'utente.

4. L'utente presenta il suo DID all'applicazione durante il processo di login.

5. L'applicazione richiama lo smart contract per verificare se l'utente ha superato l'età minima richiesta per accedere ai contenuti.

6. Se l'utente ha superato l'età minima, l'applicazione permette all'utente di accedere ai contenuti riservati agli adulti.