// Verifiable Presentation + Verifiable Credentials + Zero Knowledge Proof del DID che viene presentato dall'utente

// Definirmi l'insieme degli issuer che possono rilasciare la VC

/\*

(1) Creazione del DID implicitamente (chiamata da una pagina a caso; si assume che l'utente ce l'abbia già) 🡪 fatto

(2) Meccanismo di challenge-response di generazione di prova: numero casuale che viene cifrato con la chiave privata dell'utente e che viene decifrato con la chiave pubblica

(decidere se mandare un "riferimento" alla chiave pubblica utilizzata per la cifratura oppure se dall'altra parte li prova tutti) con inserimento dei dati anagrafici e successiva aggiunta del DID (si assume che l’utente abbia già il suo DID in fase di ) - Registrazione

(3) In fase di login, l'utente accede al sito presentando solo il DID e attivo il meccanismo challenge-response nuovamente (accesso con identità digitale)

(4) Quando voglio vedere un certo contenuto (es. più di 14 anni), l'utente deve presentare la VC (che contiene l'età) e la prova che è lui (che è il DID)

La Verifiable Credential ha un certo issuer; qui viene verificata l'intera catena di fiducia e si verifica che mi fido di almeno uno di questi nella catena

// Successivamente, capire se l'informazione blockchainAccountId è bastevole per dimostrare secondo ZKP è valida o meno e se

// la tipologia di firma EcdsaSecp256k1RecoverySignature2020 è prevista dallo standard ZKP; vedere e capire lo standard ZKP

All’avvio dell’applicazione

1. Prendo un account qualsiasi da quelli di test e registro il DID chiamando createDid() o eventualmente un nuovo account

Meccanismo di registrazione (protocollo) – da 2 a 8 è l’effettiva autenticazione

1. Inserisco i dati e il DID del passo prima
2. Recupero l’account dell’utente tramite web3 accounts (utente)
3. Cifro il numero con il sign di Web3 (utente):
   1. <https://web3js.readthedocs.io/en/v1.9.0/web3-eth.html#sign>
4. Genero una prova contenente il metodo di verifica, un valore di proof e il proof purpose con valore “authentication” (utente):
   1. <https://w3c.github.io/vc-data-integrity/#example-a-dataintegrityproof-example-using-a-nist-ecdsa-2022-cryptosuite>
5. L’utente invia tutto ciò
6. Mi recupero per verifica da verificationMethod mi recupero il didUrl
   1. <https://w3c.github.io/vc-data-integrity/#example-a-dataintegrityproof-example-using-a-nist-ecdsa-2022-cryptosuite>
7. Con questo didUrl chiamo il metodo getAuthentication di SSI.sol
8. Ciò che ritorna è un oggetto contenente blockchainAccountId
9. Uso poi recover con parametri il numero di prima, come signature il campo proof di quanto ha inviato l’utente (attenzione: NON è prefissato di suo) (massimo metti false)
   1. <https://web3js.readthedocs.io/en/v1.9.0/web3-eth-accounts.html#recover>
10. Confronto il risultato che ritorna recover con il blockchainAccountId
11. Se sono uguali, riesco ad entrare/fare la registrazione

Per tutti gli issuer, mi dovrò certamente creare degli account di test da cui dipende l’emissione delle VC (la root o il DID viene fatta nello stesso modo dell’utente normale), mentre tutti gli altri enti che fanno riferimento all’altro come root, verranno creati con childTrustedDid; il processo è ricorsivo, partendo dalla root, andando avanti e quindi, nel campo from specifico di volta in volta l’address.

Appunti fase (2):

Per implementare un sistema di identità digitale basato su un meccanismo di chiave privata/chiave pubblica, ci sono diverse opzioni tra cui scegliere. Una delle opzioni più comuni è l'utilizzo di blockchain, in particolare di una blockchain pubblica decentralizzata come Ethereum.

In questo tipo di sistema, ogni utente ha un'identità digitale rappresentata da un indirizzo sulla blockchain, che è associato a una coppia di chiavi crittografiche: una chiave privata e una chiave pubblica. La chiave privata viene utilizzata per firmare le transazioni e le richieste di autenticazione dell'utente, mentre la chiave pubblica viene utilizzata per verificare le firme.

Quando un utente si registra, viene generata una coppia di chiavi crittografiche e viene salvata l'identità digitale sulla blockchain. Per il meccanismo di challenge-response di generazione di prova, si potrebbe generare un numero casuale, cifrarlo con la chiave privata dell'utente e inviarlo all'utente stesso. L'utente dovrebbe decifrare il numero casuale con la sua chiave pubblica e inviarlo come prova di identità.

Per quanto riguarda l'inserimento dei dati anagrafici, si potrebbe utilizzare un sistema di smart contract sulla blockchain per gestire l'aggiornamento dei dati dell'utente. Quando l'utente si registra, potrebbe fornire i suoi dati anagrafici, che vengono salvati sullo smart contract. Successivamente, se l'utente vuole aggiornare i suoi dati, potrebbe inviare una transazione firmata con la sua chiave privata per aggiornare i dati sullo smart contract.

In generale, l'implementazione di un sistema di identità digitale basato su blockchain richiede una certa conoscenza tecnica e la scelta di una piattaforma specifica sulla quale costruire il sistema. Tuttavia, una volta implementato, un sistema di questo tipo può offrire molti vantaggi in termini di sicurezza, privacy e controllo dell'utente sui propri dati.