Video utili:  
<https://www.youtube.com/watch?v=BxLSSH_EHjo>

# (Slide 1 - Intro)

Buonasera a tutti,

sono Gabriel Rovesti e sono qui per presentarvi il mio progetto di tirocinio formativo e tesi di laurea. Nel corso del mio lavoro, ho realizzato un progetto che applicasse nel concreto la tecnologia blockchain, verificandone una possibile applicazione all’interno del sito di un cinema applicando degli standard di identità digitale come sistema di verifica, per questo da me denominato VerifiedMovies. Nelle successive slide saranno spiegate le tecnologie usate da un punto di vista teorico ed applicativo, cercando di rendere chiaro il contesto progettuale.

# (Slide 2 - L’azienda)

Per fornire il contesto del mio progetto di tirocinio, desidero presentarvi brevemente l'azienda presso cui ho avuto l'opportunità di lavorare: Sync Lab.

L'azienda offre una vasta gamma di servizi che includono lo sviluppo di applicazioni su misura, la consulenza IT, l'integrazione dei sistemi, la gestione dei dati e l'analisi, l'implementazione di soluzioni di business intelligence e molto altro ancora. Sync Lab ha collaborato con numerose aziende di settori diversi, tra cui banche, assicurazioni, telecomunicazioni e settore pubblico, fornendo soluzioni personalizzate per le loro esigenze specifiche. Sono presenti varie sedi in Italia e sviluppano con metodi agili per meglio soddisfare i propri utenti.

Lo scopo del mio tirocinio è stato quindi di esplorare e studiare la tecnologia blockchain, relativamente nuova e in parte sconosciuta all'azienda. Il mio obiettivo principale era quello di approfondire la conoscenza di questa tecnologia rivoluzionaria e scoprirne possibili applicazioni al di fuori del tradizionale ambito finanziario.

La blockchain è comunemente associata allo scambio di beni economici digitali e alle criptovalute come Bitcoin. Tuttavia, il suo potenziale va ben oltre queste applicazioni. Sync Lab era interessata a comprendere le potenzialità, i limiti e le sfide della tecnologia blockchain in settori diversi, capendo come applicarne i concetti di base da un punto di vista di sicurezza e di implementazione vera e propria.

# (Slide 3 - L’idea del progetto: Blockchain)

Ora spieghiamo meglio la base di questo progetto: la tecnologia blockchain. Essa rappresenta una forma innovativa di struttura dati che offre numerosi vantaggi nell'ambito delle operazioni informatiche e nella gestione dei dati.

La blockchain funziona come una catena di blocchi, dove ogni blocco rappresenta un insieme di dati. Ogni operazione, definita come transazione, viene firmata digitalmente e collegata in modo crittografico alla transazione precedente, creando un collegamento sicuro e immutabile tra i dati. Ciò significa che una volta che una transazione è stata registrata sulla blockchain, non può essere modificata o manipolata senza il consenso della maggioranza dei partecipanti alla rete; infatti, la tecnologia è anche nota come “libro mastro distribuito”, perché valida in modo distribuito e sicuro ogni operazione.

La validazione di ogni transazione viene distribuita tra tutti i partecipanti della rete, definiti nodi, i quali si occupano anche di creare nuovi blocchi, sulla base di un consenso diffuso tra tutti. Una volta che una transazione è stata registrata sulla blockchain, non può essere modificata o manipolata senza il consenso della maggioranza dei presenti.

L'eliminazione degli intermediari nella blockchain porta a una maggiore efficienza e tempi più rapidi nelle operazioni. Le transazioni possono essere eseguite in modo diretto e trasparente tra le parti coinvolte, senza dover fare affidamento su terze parti per la verifica e l'autenticazione.

# (Slide 4 - Obiettivi per il progetto)

Sulla base di questa spiegazione, l'obiettivo principale del mio tirocinio è stato comprendere il contesto della tecnologia blockchain e individuare un caso d'uso reale in cui poter applicare questa tecnologia in modo efficace. Come abbiamo introdotto in precedenza, la blockchain funziona come un libro mastro distribuito, in cui ogni operazione viene tracciata e registrata in modo sicuro, eliminando piattaforme di terze parti per autenticazione e svolgimento delle operazioni stesse.

Durante il mio percorso, ho esplorato come questa tecnologia potesse essere adattata a settori al di fuori dell'ambito finanziario, aprendo la strada a nuove soluzioni in ambito sicurezza. In particolare, mi sono concentrato sull'applicazione della tecnologia blockchain all'interno di una maschera web, al fine di creare un meccanismo di riconoscimento e autenticazione sicuro, che sia conforme agli standard di identità digitale esistenti e applicabili nel contesto blockchain. L'obiettivo era sviluppare una soluzione che garantisse la privacy degli utenti, senza richiedere la divulgazione di informazioni personali legate agli stessi, basato sulla decentralizzazione e crittografia dei dati già presenti all’interno della struttura dati.

# (Slide 5 - Requisiti del progetto)

Passiamo ora ad analizzare i requisiti specifici del progetto. Come menzionato nella slide precedente, l'obiettivo è implementare un sistema di verifica e prenotazione di film soggetti a limiti d'età su un sito web di un cinema immaginario chiamato VerifiedMovies. All’interno di questo, gli utenti dovranno dimostrare la propria età per poter accedere a film adatti all’età affermano di avere.

Per garantire la sicurezza e la privacy durante la fase di verifica dell'età, abbiamo identificato come obiettivo formativo lo studio e la possibile applicazione di Self Sovereign Identity e Zero Knowledge Proof. Questi meccanismi consentono di verificare l'identità senza dover rivelare informazioni personali, evitando così la dipendenza da fornitori di servizi di identità di terze parti, ma dimostrando per certo la validità dei dati dimostrati in quanto considerati alla base affidabili.

Per implementare il meccanismo di riconoscimento descritto, è stato richiesto di utilizzare la blockchain Ethereum. Essendo la seconda più famosa dopo Bitcoin, Ethereum offre la capacità di interagire con la struttura dati blockchain, fornendo un ambiente crittograficamente sicuro, aperto all’interazione esterna, data la sua curva di apprendimento relativamente bassa.

In ultimo, è stato richiesto l’utilizzo del framework web3.js oppure ethers.js, noti per una gestione semplificata del codice su blockchain e la loro interazione con l’ambiente web.

# (Slide 6 - Decentralized Identifiers (DID))

In questa e nelle successive sei slide saranno spiegati e approfonditi i vari standard di identità digitale studiate e da me applicati cominciando dagli Identificatori Decentralizzati, noti anche come Decentralized Identifiers (DID). I DID sono identificatori univoci composti da una stringa alfanumerica, associati a un'entità verificabile secondo lo standard omonimo definito dal consorzio World Wide Web Consortium (W3C) (organizzazione nota per aver standardizzato tecnologie come HTML, CSS, XML, etc.)

I DID sono fondamentalmente una forma di identità digitale che permette a un individuo o un'entità di avere un identificatore unico e verificabile. Ogni DID è associato a un documento chiamato DID Document, che descrive l'entità corrispondente e i metodi di autenticazione utilizzati in modo sicuro.

La caratteristica principale dei DID è che consentono un accesso sicuro senza dipendere da entità di terze parti per la verifica dell'identità. Ogni utente può controllare il proprio DID crittografandolo con la propria chiave privata, associabili e risolvibili ad una persona fisica in modo crittograficamente sicuro. Ciò garantisce un alto livello di sicurezza e autonomia nell'autenticazione e nell'accesso ai servizi. Questo standard è uno dei componenti del meccanismo di verifica realizzato.

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

# (Slide 7 - Verifiable Credentials (VC))

Passiamo poi ad un successivo standard W3C esplorato, nello specifico le Verifiable Credentials (VC), noto anche come Credenziali Verificabili, riferiti ad uno standard ominimo. Queste sono create in formato dati JSON e vengono firmate con la chiave privata dell’utente e la chiave pubblica di un’entità fidata, che ne garantisce la validità.

Ogni credenziale contiene tre componenti principali:

1. Claim (Affermazione): Rappresenta ciò che un'entità afferma con certezza. Ad esempio, potrebbe essere l'informazione sulla data di nascita di un utente.
2. Metadata (Metadati): Include gli attributi base dell'utente che presenta la credenziale, come il nome, l'indirizzo e altri dettagli pertinenti.
3. Proof (Prova): È la prova crittografica di autenticità della credenziale. Questa viene utilizzata per verificare che la credenziale sia stata emessa da un'entità affidabile e non sia stata alterata.

All’interno di queste, l’utente utilizza il proprio DID per dimostrare la propria identità composta dai dati forniti in fase di autenticazione confermandone l’autenticità purché verificate da terze parti note e sicure. In fase di verifica, viene infatti creata una credenziale ogni volta, a fini di sicurezza, contenente l’età ed una prova crittografica di autenticità per consentire la prenotazione previa verifica e successivo accesso ai film appropriati.

# (Slide 8 - Verifiable Presentations (VP))

La credenziale generata dall’utente deve essere poi presentata e per fare ciò esiste un formato stabilito dallo stesso standard W3C precedente chiamato Verifiable Presentations.

Le Verifiable Credentials, come abbiamo visto nella slide precedente, sono credenziali verificabili che contengono informazioni essenziali per l'autenticazione e la verifica dell'identità. Le VP vengono create utilizzando queste credenziali per presentare in modo strutturato e affidabile i dati degli utenti. Queste possono contenere una o più credenziali.

La caratteristica chiave delle VP è la possibilità di esprimere i dati degli utenti in modo tale da consentire una verifica certa attraverso prove comuni di autenticazione che ne garantiscono la non manomissione, chiamate "proofs". Queste vengono utilizzate per dimostrare l'autenticità dei dati presentati nelle Verifiable Credentials e possono associare liberamente vari metodi crittografici.

In questo modo, si ha un meccanismo sicuro per presentare e condividere le informazioni dell'utente, consentendo a terze parti di verificare l'autenticità dei dati senza dover accedere direttamente alle informazioni sensibili dell'utente. Ciò garantisce la privacy e la protezione dei dati personali, consentendo al contempo una verifica affidabile e crittografata.

Una Verifiable Presentation, nel contesto del progetto, rappresentano il passaggio di presentazione della credenziale dell’utente al fine di avviare il meccanismo di verifica dell’identità.

# (Slide 9 - Self Sovereign Identity (SSI))

Fatte le varie premesse, veniamo ora ad uno dei concetti chiave che consente di realizzare quanto descritto in modo opportuno: il modello Self Sovereign Identity, definito anche come “identità auto-sovrana”. Questo rappresenta un modello che dà all'utente il controllo dei propri dati personali, da cui il nome. Si tratta di un'identità digitale che può essere portata tra diversi sistemi, riducendo al minimo lo scambio di dati sensibili.

L'identificazione all'interno di questo modello avviene tramite un Decentralized Identifier (DID), che è un identificatore univoco associato a un'entità verificabile. L'utente può creare e controllare il proprio DID utilizzando le proprie chiavi crittografiche. Questo identificatore viene poi utilizzato all'interno di credenziali immutabili e uniche, che vengono registrate sulla blockchain.

Inoltre, come descritto, tale identificatore univoco viene associato alle informazioni che l’utente sceglie di condividere, presentandole per la verifica al sito del cinema. In questo modo, l’utente ha il pieno controllo dei propri dati personali, decidendo cosa e con chi condividere le proprie informazioni senza affidarsi a servizi di terze parti ed evitare di rivelare dettagli sensibili.

# (Slide 10 - Catena di fiducia)

Per poter realizzare SSI, occorre spiegare precisamente chi sono le parti coinvolte nel processo:

1. La credenziale dell'utente viene emessa da un'entità fidata chiamata "issuer". Questo issuer è responsabile di verificare e certificare i dati personali dell'utente. La credenziale contiene le informazioni essenziali per l'autenticazione e la verifica dell'identità dell'utente, come ad esempio la data di nascita.
2. Nella slide viene rappresentata una "catena di fiducia", che è formata da una serie di issuer fidati (creati a priori all’interno del sito). Questi issuer sono collegati tra loro da una firma digitale proveniente da un'entità superiore, definita "certification authority". Quest’ultimo è l'ente di massima fiducia che garantisce l'autenticità dei dati emessi dai vari issuer. La catena di fiducia parte dalla certification authority e si estende fino all'issuer che emette la credenziale dell'utente.
3. L'utente, in qualità di "holder" della credenziale, fornisce questa credenziale come prova della propria identità. Il sito web di VerifiedMovies assume il ruolo di "verifier" e attiva un meccanismo di verifica interno per confermare l'autenticità della credenziale presentata dall'utente. Il meccanismo di verifica coinvolge il controllo delle firme digitali presenti nella catena di fiducia, assicurandosi che ogni entità coinvolta sia affidabile e che la credenziale sia stata emessa da un issuer fidato.

La citata catena di fiducia è una rete interna che garantisce che l'utente sia univocamente riconosciuto e abbia accesso ai contenuti appropriati sulla piattaforma VerifiedMovies, basata sul meccanismo di verifica con firme digitali spiegati nelle successive slide. Tutti i dati sono salvati in blockchain, che garantisce la non modificabilità delle informazioni purché opportunamente criptate.

# (Slide 11 - Zero Knowledge Proof (ZKP))

Il concetto chiave della prova dell'identità utilizza anche il concetto di Zero Knowledge Proof, o Prove a conoscenza zero. Si tratta di un metodo crittografico che permette a un'entità di dimostrare a un'altra entità di conoscere un certo valore senza rivelarlo effettivamente, ma dimostrando di avere il possesso di una determinata informazione attraverso una prova indiretta che coinvolge enti fidati.

Nel contesto di questa presentazione, il concetto di Zero Knowledge Proof si collega direttamente alla catena di fiducia descritta precedentemente. In questo caso specifico, l'utente deve provare di avere un'età superiore a quella richiesta per la prenotazione di un film, senza dover fornire esplicitamente la propria età anagrafica. Invece, l'utente presenta una prova crittografica che dimostra la sua appartenenza a uno schema comune di fiducia, ovvero la catena di fiducia menzionata in precedenza.

Durante la verifica, vengono controllate le firme digitali delle credenziali presentate, in modo da verificare che siano state emesse da un'entità fidata e che siano corrette. Questo processo avviene attraverso uno standard specificamente progettato per garantire la non ripudiabilità delle prove.

# (Slide 12 – Tecnologie del progetto)

Qui presenti le tecnologie da me utilizzate in fase di codifica del prodotto, composto da due parti.

La parte front-end presenta React come libreria grafica, basandosi sulla creazione di tipi usando il linguaggio TypeScript, riducendo gli errori e garantendo il pieno controllo sui dati forniti, in particolare delle credenziali e della loro presentazione. L’interazione con blockchain è realizzata secondo la libreria web3.js, che permette di comunicare in modo semplice tra la parte grafica e logica fornita dal contratto, permettendone la generazione e l’invocazione delle specifiche funzioni. Inoltre, si è usato Jest per realizzare i vari tipi di test, passando dai singoli test di unità fino ai test di accettazione del prodotto finale.

La parte back-end utilizza come collegamento Node.js, ambiente di esecuzione lato server per lo scambio sicuro dei dati, basato sulla comunicazione con lo smart contract libreria scritto in linguaggio Solidity e basando il tutto su un framework che avvia sulla rete locale la compilazione ed esecuzione delle transazioni, chiamato Hardhat.

# (Slide 13 – Le caratteristiche del progetto)

Sulla base di tutte queste tecnologie innovative, ho creato il progetto VerifiedMovies, una piattaforma che sfrutta le prove dell'identità e Zero Knowledge Proof per offrire un'esperienza di prenotazione cinematografica sicura e privata.

VerifiedMovies offre una funzionalità di registrazione e login che si basa su un meccanismo challenge-response. Durante la fase di registrazione, viene creato un Decentralized Identifier (DID) univoco per ogni utente e la relativa chiave privata viene associata sulla blockchain. L'obiettivo principale è garantire l'accesso ai contenuti riservati, in particolare per i film che hanno limiti di età.

Il meccanismo challenge-response richiede all'utente di firmare digitalmente un numero casuale generato dal sistema. Questa firma dimostra che l'utente è in possesso della chiave privata associata al suo DID. Successivamente, l'utente può effettuare il login utilizzando solo il suo identificatore, senza dover inserire ulteriori dati.

Per implementare questo meccanismo, VerifiedMovies fa uso di uno smart contract (cioè, un programma che definisce le operazioni su rete blockchain) che realizza il concetto di Self Sovereign Identity, seguendo gli standard introdotti dal W3C. Questo è stato sviluppato da Alessio De Biasi, un laureando magistrale in Informatica presso Ca’ Foscari. Il suo codice, scritto in Solidity, il linguaggio di programmazione per smart contract, doveva essere utilizzato come requisito obbligatorio e serve per garantire la creazione del DID, la gestione del documento di identità digitale e l'interazione con la blockchain.

Nella prossima slide, approfondiremo il meccanismo di verifica dell'età dell'utente, che si basa sui limiti d'età dei film e l'utilizzo di credenziali con Zero Knowledge Proof.

# (Slide 14 - Verifica dell’età)

Qui i punti salienti del meccanismo di verifica dell’età, che considera in modo coerente gli standard descritti e segue l’ordine previsto.

* Il processo di verifica inizia con la creazione di una Verifiable Credential. Utilizzando la chiave pubblica dell’issuer, firmiamo la credenziale e generiamo un numero casuale e un valore di firma. Questi elementi sono poi utilizzati per creare una prova di correttezza della firma. Questa procedura ci consente di certificare che l'utente sia in possesso di una credenziale valida senza rivelare i dati contenuti al suo interno.
* Successivamente, generiamo una Verifiable Presentation che contiene la Verifiable Credential creata precedentemente. La presentazione viene firmata digitalmente utilizzando la firma CLSignature2019 e la prova di correttezza generata in precedenza. Questo passaggio ci consente di incapsulare la credenziale all'interno di uno schema comune e verificare la sua validità senza rivelare informazioni sensibili sull'utente realizzando Zero Knowledge Proof e aumentando la scalabilità della rete, grazie ad un meccanismo autocontenuto di verifica.
* Nel processo di verifica, utilizziamo la chiave pubblica dell’issuer per verificare la firma digitale immessa e la prova di correttezza associata. Questo ci permette di garantire che le credenziali siano state emesse da un'autorità affidabile e che la firma sia valida.
* Il concetto di Self Sovereign Identity permette di stabilire che le credenziali sono valide grazie all’emissione da parte di un issuer fidato della credenziale, firmata a catena da un insieme di emittenti figli della stessa autorità di certificazione e garantendo l’autenticità di tutte le credenziali.

## Appunti di contorno su CLSignature2019 venissero giustamente fatte domande su questo

La tecnica di firma digitale utilizzata in questo contesto è chiamata CLSignature2019. Questo meccanismo è stato scelto per diversi motivi. Innanzitutto, permette di implementare un concetto chiamato "Zero Knowledge Proof", che si basa sulla standardizzazione e sulle specifiche descritte in . Questo significa che i dati dell'utente vengono creati e incapsulati all'interno di uno schema comune, consentendo la verifica della validità della credenziale senza rivelare informazioni riservate sull'utente stesso.

Per generare la firma CLSignature2019, vengono seguiti determinati passaggi. Innanzitutto, viene generata una chiave privata per l'emittente, che viene utilizzata per firmare la credenziale. Successivamente, viene generata una chiave pubblica corrispondente, che verrà utilizzata per verificare la firma. Viene inoltre generato un valore casuale chiamato "nonce", che è utilizzato per creare la prova di correttezza della firma. Questa prova di correttezza viene generata calcolando il valore di impegno (commitment) ottenuto moltiplicando il nonce per la chiave pubblica, e successivamente calcolando il valore di risposta (response) moltiplicando la chiave privata per il valore di impegno. Infine, viene calcolato il valore di firma, che insieme al valore di prova di correttezza costituisce la firma CLSignature2019.

L'utilizzo di questa firma digitale è particolarmente adatto alle soluzioni blockchain di secondo livello, come ad esempio Hyperledger Indy, che si basano sul concetto di self-sovereign identity. In questo contesto, vengono coinvolti tre soggetti: l'emittente (issuer) che crea la credenziale e la firma, il possessore (holder) che detiene la credenziale e ne possiede un identificativo decentralizzato (DID), e il verificatore (verifier) che verifica la validità della credenziale. Nel caso specifico del sistema descritto, il cinema stesso funge da verificatore, verificando la validità della credenziale utilizzando la chiave pubblica dell'emittente.

In sintesi, il meccanismo CLSignature2019 è stato utilizzato per implementare un processo di verifica dell'età all'interno dell'applicazione. Questo meccanismo permette di creare e verificare le credenziali in modo sicuro e privato, senza rivelare informazioni sensibili sull'utente. La scelta di CLSignature2019 si basa sulle sue capacità di realizzare Zero Knowledge Proof e sulla sua adozione nelle soluzioni blockchain di secondo livello, garantendo un elevato livello di affidabilità e sicurezza nel contesto specifico.

# (Slide 15 - Conclusioni e resoconto)

In conclusione, il tirocinio è stata un’esperienza certamente formativa e che si è conclusa con la realizzazione degli obiettivi obbligatori, concernenti lo studio e l’analisi di blockchain e degli standard di identità digitale e realizzazione del Proof of Concept, ovvero un prototipo che dimostra la fattibilità di questi e dell’uso di blockchain ad un caso d’uso reale come richiesto. Inoltre, sulla base degli obiettivi desiderabili, il prodotto è stato completamente coperto da casi di test e realizzando una UI per l’applicazione creata.

In retrospettiva, l’esperienza è stata certamente utile in quanto l’ambito blockchain è in gran parte sconosciuto sia nell’ambito informatico che no, creando per me una sfida che ho preso sin da subito con piacere e che ho cercato di sfruttare al meglio, basata su tecnologie complesse a livello realizzativo e spesso neanche standardizzate, come capita per Zero Knowledge Proof. Questa tecnologia può avere implicazioni fortissime se usata in ambito sicurezza e autenticazione; esistono infatti diversi progetti anche finanziati da organizzazioni come la UE basati su SSI e ZKP stessa.

Nel progetto sono stato autonomo, che è stato positivo da un punto di vista organizzativo e anche professionale, in quanto ho potuto toccare con mano delle tematiche complesse e molto formative sia da un punto di vista accademico che nel mondo pratico professionale, realizzando un prodotto che ha soddisfatto e superato le mie stesse aspettative.

(Se avete domande, chiedetemi pure, vi ringrazio intanto per l’attenzione)