1 Ente presso cui è stato svolto il lavoro di stage

Il lavoro di stage è stato svolto internamente al Dipartimento di Informatica dell'Università degli Studi di Milano, in particolare sotto la supervisione del Dott. Andrea Visconti.

2 Contesto iniziale

La nascita e l'evoluzione del Web 3.0 stanno portando il controllo e la proprietà delle informazioni in transito su Internet nelle mani di chi effettivamente lo utilizza: l'approccio decentralizzato di gestione dei dati sta creando un sistema più equo e autonomo per gli utenti di Internet, rimuovendo gradualmente il necessario controllo esterno delle grandi aziende caratteristico dell'approccio centralizzato del Web 2.0.
Termini come criptovalute, blockchain, finanza decentralizzata, token, NFT, metaverso e app decentralizzate sono concetti oramai diffusi, consolidati e ben noti ai più, e ci stiamo rendendo conto di quanto questi strumenti, se utilizzati in maniera intelligente, siano veramente molto potenti e possano dare una grande mano nell'evoluzione della società contemporanea.

3 Obiettivo del lavoro

L'obiettivo è stato di ideare un sistema per garantire protezione ad un qualsiasi bene materiale, come ad esempio una scultura, una giacca di lusso o una bottiglia di un liquore pregiato, utilizzando i potenti strumenti del Web 3.0 e le tecniche crittografiche apprese durante il mio percorso di studi.
Cosa significa "garantire protezione" ad un bene? Immaginiamo una generica operazione di vendita tra un venditore ed un acquirente. Il nostro obiettivo è assicurare che in questo processo siano rispettate delle proprietà fondamentali:

- Il venditore e l'acquirente siano realmente chi dicono di essere e non dei truffatori;
- Il venditore possegga veramente il bene che sta provando a vendere all'acquirente;
- Il bene venduto dal venditore all'acquirente sia autentico e non un falso.

4 Descrizione del lavoro svolto

Il sistema da ideare coinvolgerà la blockchain e gli NFT.
Il ***primo passo***, quindi, è stato scegliere la blockchain da utilizzare. Nello specifico mi sono basato su due criteri di selezione:

- **Compatibilità con EVM**: riguarda la capacità di una blockchain di eseguire l'EVM, ossia la virtual machine che svolge tutte le operazioni e le transazioni sulla blockchain di Ethereum. Questo dà notevoli vantaggi: essendo Ethereum una delle blockchain più popolari, è molto più semplice trovare online la soluzione ad eventuali problemi riscontrati durante lo sviluppo del sistema, nonché eventuali plugin ed estensioni.
- **Ecosostenibilità**: riguarda il consumo elettrico e le emissioni di CO2.

La scelta, quindi, è ricaduta sulla blockchain Polygon.

Il ***secondo passo*** è stato decidere l'approccio con cui creare gli NFT e, di conseguenza, associarli agli oggetti fisici, in particolare nel caso in cui esistano diverse copie di un bene. La scelta è stata tra l'approccio 1:N, ossia creare un unico NFT e associarlo a tutte le copie dell'oggetto, e l'approccio 1:1, cioè creare un NFT per ogni oggetto effettivo. Dopo aver analizzato i pro e i contro di entrambi gli approcci, la scelta è stata l'approccio 1:1.

Il ***terzo passo*** è stato definire un metodo concreto per creare gli NFT sulla blockchain scelta al passo 1 e secondo l'approccio deciso al passo 2. Nello specifico, i sottopassi necessari sono stati i seguenti:

1. **Definire un documento di specifica per il cliente**: contiene tutte le informazioni che il cliente deve produrre ed esibire affinché si possa creare un NFT rappresentante un bene materiale di sua proprietà.
2. **Creare uno smart contract**: sarà lo strumento con cui creare gli NFT successivamente.
3. **Verificare lo smart contract**: per far fronte a errori nella compilazione o a manipolazioni malevole. Consiste nel confrontare il codice sorgente originale del contratto con il bytecode compilato che viene effettivamente eseguito sulla blockchain.
4. **Creare gli NFT**: usando lo smart contract si creano gli NFT rappresentanti i beni da proteggere.
5. **Trasferire gli NFT al cliente**: si trasferisce la proprietà degli NFT creati al cliente, che potrà visualizzarli nel proprio crypto wallet.

Il ***quarto ed ultimo passo*** è stato fornire alcune idee di utilizzo degli NFT creati e trasferiti al cliente durante il passo precedente.
In particolare mi sono concentrato su 3 punti:

- **Come associare l'NFT all'oggetto fisico**: l'idea proposta è di utilizzare un QR code, eventualmente insieme ad un chip integrato per una doppia autenticazione. Questo perché l'approccio 1:1 scelto è sufficiente ad impedire una grande quantità di truffe di contraffazione.
- **Come presentare l'NFT**: l'idea proposta è di utilizzare uno store virtuale come OpenSea per mostrare l'NFT. Questo perché questi strumenti sono molto user-friendly e permettono di visualizzare graficamente l'NFT e la sua storia in modo semplice e comodo.
- **Come vendere il bene**: l'idea fornita per un sistema finale di vendita dei beni si basa principalmente sul principio di creare gli NFT dinamicamente con il primo acquisto e non staticamente a priori.

5 Tecnologie coinvolte

Durante lo sviluppo del sistema sono state utilizzate diverse tecnologie e strumenti.
Ecco un elenco delle principali: blockchain, con funzioni hash e hash pointers; smart contract; NFT; crypto wallet, con firma digitale; Solidity; JavaScript; Alchemy; Hardhat; Pinata; PolygonScan e OpenSea; QR code.

6 Competenze e risultati raggiunti

È stato creato un sistema per la protezione di un qualsiasi bene materiale. Inoltre, sono state fornite una serie di idee di utilizzo.
Durante questa esperienza ho compreso a fondo quanto le tecnologie del Web 3.0 siano importanti e, se impiegate in modo corretto, possano risolvere problemi della vita quotidiana in modo molto semplice.
Il maggiore problema riscontrato durante il lavoro è stato comprendere come implementare concretamente il sistema a livello di codice, che tuttavia è stato risolto grazie all'aiuto di informazioni e codici d'esempio trovati online.

7 Bibliografia

Ecco un elenco delle principali fonti di informazione utilizzate durante lo sviluppo del sistema:

- *On the cryptography of Distributed Ledger Technology - 1. Hash Functions*
  URL: `https://www.finriskalert.it/wp-content/uploads/visconti.pdf`
  (visitato il 14/03/2024)
- *Blockchain Merkle Trees*
  URL: `https://www.geeksforgeeks.org/blockchain-merkle-trees/`
  (visitato il 14/03/2024)
- *What is blockchain?*
  URL: `https://opensea.io/learn/blockchain/what-is-blockchain`
  (visitato il 14/03/2024)
- *What is a smart contract?*
  URL: `https://opensea.io/learn/blockchain/what-is-a-smart-contract`
  (visitato il 15/03/2024)
- *What is an NFT?*
  URL: `https://opensea.io/learn/nft/what-are-nfts`
  (visitato il 16/03/2024)
- Adeniyi E. A., Falola P. B., Maashi M. S., Aljebreen M., Bharany S.
  Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions (consultato il 17/03/2024)
- *What is a crypto wallet?*
  URL: `https://opensea.io/learn/web3/what-is-crypto-wallet`
  (visitato il 17/03/2024)
- *What is Etherscan?*
  URL: `https://opensea.io/learn/blockchain/what-is-etherscan`
  (visitato il 18/03/2024)
- *What are EVM Compatible Blockchains? A Guide to the Ethereum Virtual Machine*
  URL: `https://tinyurl.com/2w56cppp`
  (visitato il 10/03/2024)
- *Update Report: Energy Efficiency and Carbon Footprint of the Polygon Blockchain*
  URL: `https://carbon-ratings.com/dl/polygon-update-2022`
  (scaricato il 12/10/2023)