Tesi di laurea triennale in Informatica

CryptoCorso: progettazione e sviluppo di una collezione di NFT sulla blockchain di Ethereum tramite smart contract

Riccardo Corsini

Università degli studi di Verona

11/10/2024

Introduzione

1. Blockchain
   - Cos'è la blockchain
   - Ethereum e smart contract
   - Protocollo di consenso Proof-of-Stake(PoS)
   - Ciclo di vita di una transazione in Ethereum
2. Non-fungible token(NFT)
   - Standard ERC-721
3. CryptoCorso
   - Tecnologie utilizzate
     - InterPlanetary File System(IPFS)
     - Web3
   - Casi d'uso

Indice

Cos'è la blockchain

- La prima blockchain introdotta nel 2009 da Satoshi Nakamoto con l'obiettivo di fungere da "libro mastro" della valuta digitale Bitcoin.
- È una tecnologia che consente di gestire e aggiornare un registro distribuito e immutabile senza la necessità di averene un'entità centrale di controllo e verifica(consenso decentralizzato).
  - È una catena di blocchi contenenti le informazioni sulle transazioni eseguite.
- Esistono due tipologie di blockchain:
  - pubbliche
  - private

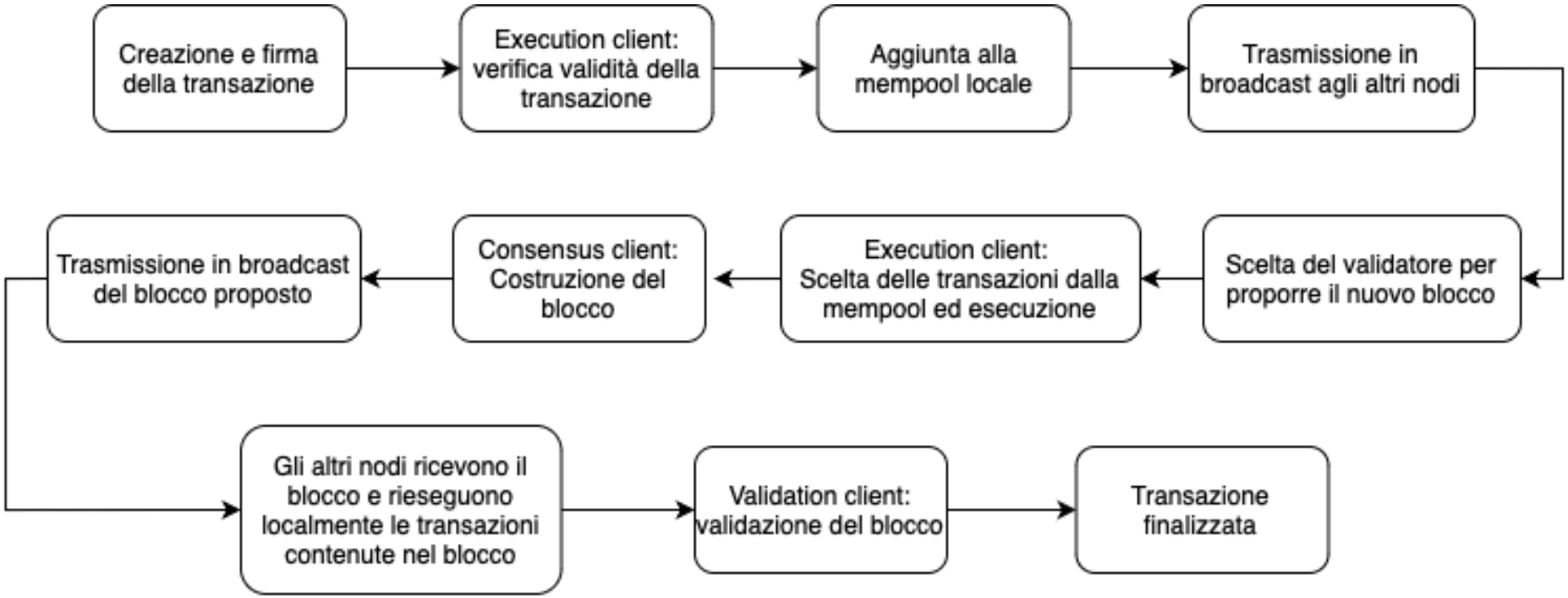
Ethereum e smart contract

- È stato il primo progetto che ha implementato il concetto di smart contract in una blockchain.
  - Uno smart contract è un programma compilato memorizzato all'interno della blockchain che viene eseguito sulla Ethereum virtual machine di ogni nodo automaticamente quando si verifica un evento specifico.
- Ethereum può essere inteso come una macchina a stati ("infiniti") deterministica.
  - Una transazione rappresenta un cambiamento all'interno di una memoria distribuita globalmente.
- Per controllare la quantità massima di risorse che una transazione può consumare durante la sua esecuzione Ethereum utilizza un'unità di scambio detta Gas.

Proof-of-Stake(PoS)

- Il protocollo di consenso usato da Ethereum è il protocollo Proof-of-Stake(PoS).
  - si basa sul fatto che nella blockchain ci sono dei nodi validatori che hanno il compito di andare a validare il contenuto dei blocchi prodotti:
    - Per partecipare alla rete Ethereum come validatore, un utente deve mettere 32ETH in un contratto di deposito.
    - A turno i validatori propongono e votano il prossimo blocco valido.
    - La decisione nel determinare se un blocco è valido richiede il 66% degli ethereum messi in stack.
  - i validatori sono forzati a comportarsi onestamente attraverso un sistema di ricompense e punizioni:
    - Possono perdere i propri depositi bloccati se il blocco che propongono è rigettato dalla maggioranza degli altri validatori.
    - Ricevono una ricompensa, proporzionale al loro deposito, per ogni blocco che viene accettato dalla maggioranza.

Ciclo di vita di una transazione in Ethereum



- execution client: esegue le transazioni localmente
- consensus client: crea nuovi blocchi e li trasmette alla rete
- validator client: testa la validità dei blocchi

Indice

Non-fungible token(NFT)

Fungibilità

Quando diciamo che un oggetto è fungibile, significa che questo può essere interscambiato con un altro oggetto identico e con le stesse proprietà.

- Un NFT è un oggetto digitale non fungibile che viene memorizzato sulla blockchain.
  - Un oggetto è non-fungibile quando è unico e possiede proprietà individuali che lo distinguono da tutti gli altri.
  - Un NFT può rappresentare qualsiasi oggetto unico sia nel mondo reale che in quello digitale.
- Grazie alla blockchain tutte le transazioni che riguardano un token vengono resgitrate, ciò ci permette di avere una dichiarazione permanente di autenticità che può essere visualizzata e accessibile da chiunque.

Standard ERC-721

- Gli NFT possono essere creati attraverso uno smart contract che segue determinate regole dettate dallo standard ERC-721.
- Lo standard definisce l'interfaccia minima che uno smart contract deve implementare per permettere di creare, gestire e tener traccia della proprietà di un NFT.
- Ogni NFT viene identificato da un id univoco all'interno dello smart contract

Indice

CryptoCorso

- Consiste nello sviluppo di una raccolta di NFT, basata sullo standard ERC-721.
- Ogni NFT rappresenta un corso della laurea triennale di informatica e può essere richiesto dagli studenti solo dopo aver superato l'esame corrispondente.
- Tutti i token sono composti da un identificativo univoco, da un'immagine e da un modello 3D contenente la matricola, la data e la valutazione con cui si è superato l'esame.

InterPlanetary File System(IPFS)

- È una rete peer-to-peer per l'archiviazione e la condivisione di dati in un file system distribuito.
- Ogni tipo di dato che viene caricato su IPFS viene identificato da un hash univoco chiamato IPFS Content Identifier(CID).
- Ciò permette di:
  - avere una "ricerca per contenuto"
  - garantire che un file non venga modificato
- IPFS è stato usato nel progetto per poter archiviare e condividere i file riguardanti gli NFT, in modo che quest'ultimi siano sempre raggiungibili e garantendo ai possesori che non vengano modificati.

Web3

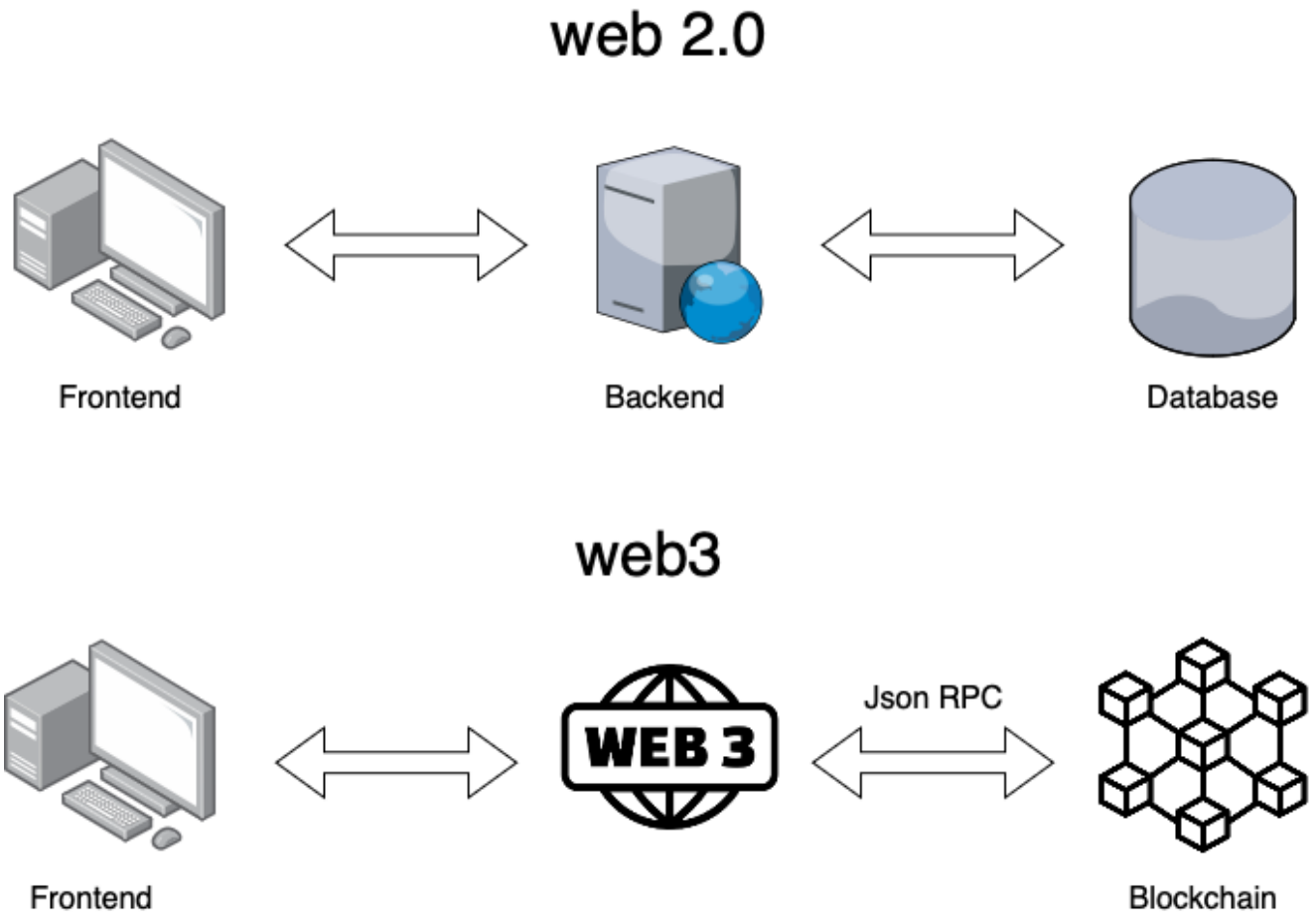
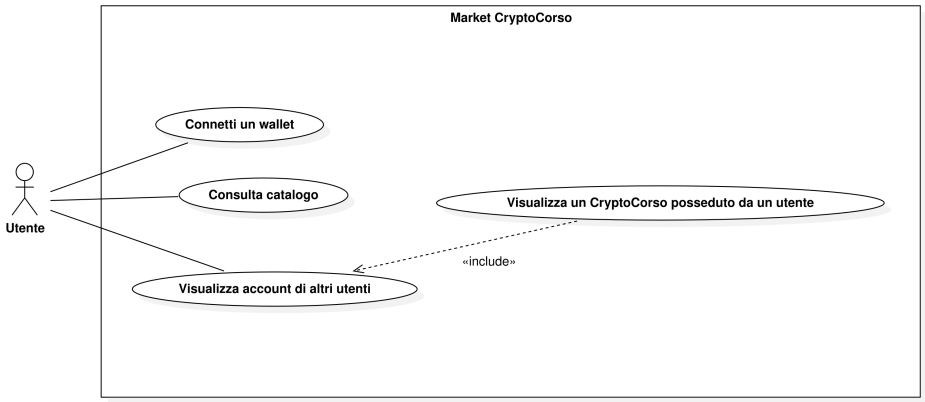


Figure: Dal web 2.0 al web3

Casi d'uso



Caso d'uso: Connetti wallet
Attori: utente, studente, segreteria
Precondizioni: 1. L'attore deve aver installato un wallet 2. L'attore deve aver creato un indirizzo
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore accede all'interfaccia per connettere il wallet
Postcondizioni: 1. L'attore accede al proprio account

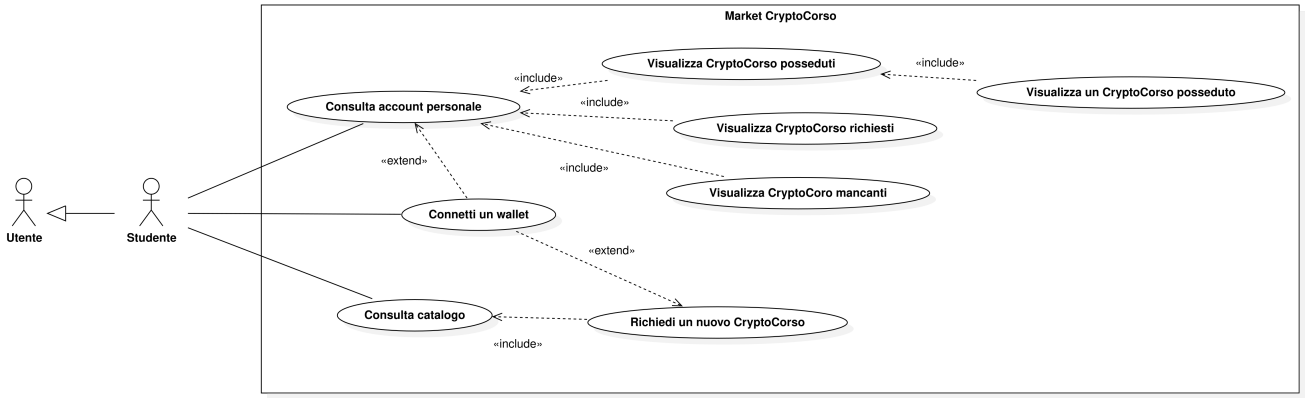
Caso d'uso: Consulta catalogo
Attori: utente, studente, segreteria
Precondizioni:
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore accede al catalogo 3. Se l'attore seleziona un CryptoCorso 3.1 Il sistema visualizza il dettaglio del token che può essere richiesto
Postcondizioni:

Caso d'uso: Visualizza account di altri utenti
Attori: utente, studente, segreteria
Precondizioni: 1. Il sistema deve aver memorizzato almeno un utente
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore dalla home visualizza i 5 utenti con maggior numero di CryptoCorso 3. Se l'attore preme su un indirizzo 3.1 Visualizza l'account dell'utente corrispondente 3.2 Se l'attore preme su un CryptoCorso posseduto dall'utente visualizza il dettaglio di quel token
Postcondizioni:

Caso d'uso: Visualizza un CryptoCorso posseduto da un utente
Attori: utente, studente, segreteria
Precondizioni: 1. Il sistema deve aver memorizzato almeno un utente
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore visualizza l'account di uno studente 3. Se l'attore preme su un CryptoCorso posseduto dallo studente 3.1 L'attore viene introdotto alla pagina del catalogo dedicata al CryptoCorso corrispondente
Postcondizioni:

Figure: Casi d'uso utente

Casi d'uso



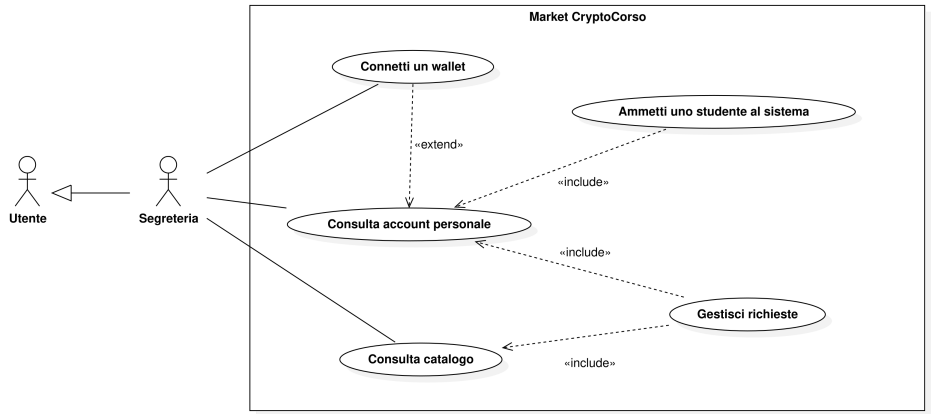
Caso d'uso: Consulta account personale
Attori: studente
Precondizioni: 1. L'attore deve aver connesso un wallet
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore premendo sul suo indirizzo accede all'account personale
Postcondizioni: 1. L'attore accede al proprio account e può visualizzare i CryptoCorso posseduti, richiesti e mancanti

Caso d'uso: Visualizza un CryptoCorso posseduto
Attori: studente
Precondizioni: 1. L'attore deve aver connesso un wallet 2. L'attore deve possedere il CryptoCorso
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. Se l'attore accede alla sezione dell'account personale e preme su un CryptoCorso posseduto 2.1 L'attore viene introdotto alla pagina del catalogo dedicata al CryptoCorso posseduto 3. Se l'attore accede al catalogo 3.1 Premendo su un CryptoCorso, accede alla pagina del catalogo dedicata al token posseduto
Postcondizioni:

Caso d'uso: Richiedi CryptoCorso
Attori: studente
Precondizioni: 1. L'attore deve aver connesso un wallet 2. L'attore non deve aver già richiesto il CryptoCorso 3. L'attore non deve possedere il CryptoCorso
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. Se l'attore accede alla sezione dell'account personale e preme su un CryptoCorso mancante 2.1 L'attore viene introdotto alla pagina del catalogo dedicata al CryptoCorso 2.2 L'attore premendo sul bottone apposito può richiedere il CryptoCorso 3. Se l'attore accede al catalogo 3.1 Premendo su un CryptoCorso, accede alla pagina del catalogo dedicata al token mancante 3.2 L'attore premendo sul bottone apposito può richiedere il CryptoCorso
Postcondizioni: 1. Il sistema registra la richiesta

Figure: Casi d'uso studente

Casi d'uso



Caso d'uso: Consulta account personale
Attori: segreteria
Precondizioni: 1. L'attore deve aver connesso un wallet
Sequenza degli eventi: 1. L'attore è introdotto alla home del sito web 2. L'attore premendo sul suo indirizzo accede all'account personale
Postcondizioni: 1. L'attore accede al proprio account e può gestire le richieste pendenti

Caso d'uso: Gestisci richieste
Attori: segreteria
Precondizioni: 1. L'attore deve aver connesso un wallet
Sequenza degli eventi: 1. L'attore deve verificare la validità della richiesta 2. Se l'attore accetta la richiesta 2.1 Deve creare l'NFT richiesto(Json, immagine e modello 3D) 2.2 Deve caricare L'NFT su IPFS 2.3 Deve inserire il cid corrispondente 2.4 Il sistema crea il token e lo assegna allo studente che l'ha richiesto 3. Se l'attore rifiuta la richiesta 3.1 Il sistema rimuove la richiesta
Postcondizioni: 1. Se l'attore ha accettato la richiesta, viene creato un nuovo token

Caso d'uso: Ammetti uno studente al sistema
Attori: segreteria
Precondizioni: 1. L'attore deve aver connesso un wallet 2. Lo studente deve aver fornito alla segreteria il proprio indirizzo
Sequenza degli eventi: 1. L'attore è introdotto alla schermata home 2. L'attore accede al proprio account personale 3. L'attore inserisce l'indirizzo e la matricola dello studente da ammettere al sistema tramite l'apposito form
Postcondizioni: 1. Lo studente viene ammesso al sistema e può richiedere i CryptoCorsi

Figure: Casi d'uso segreteria