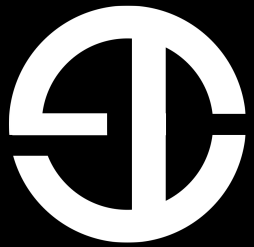
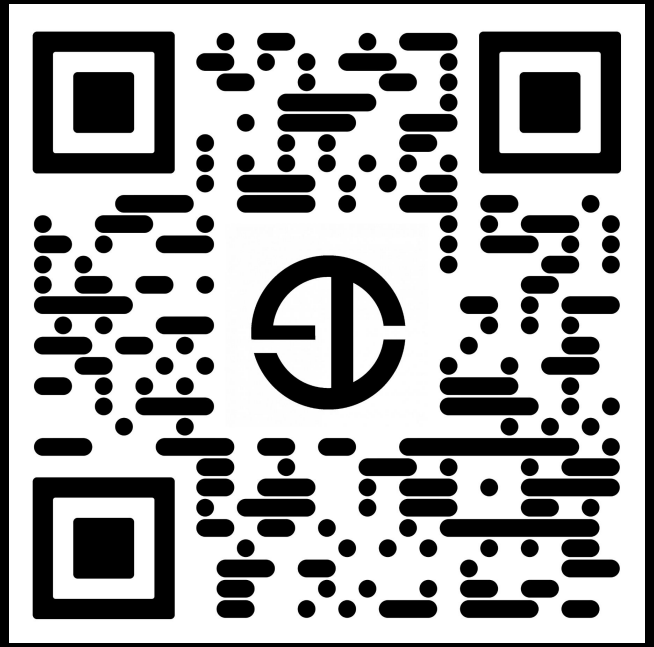


EDUChain

Una blockchain da uno studente, per gli studenti

Abstract

Dove provare l'elaborato su internet?



oppure

http://educhain.altervista.org

Cos'è una blockchain?

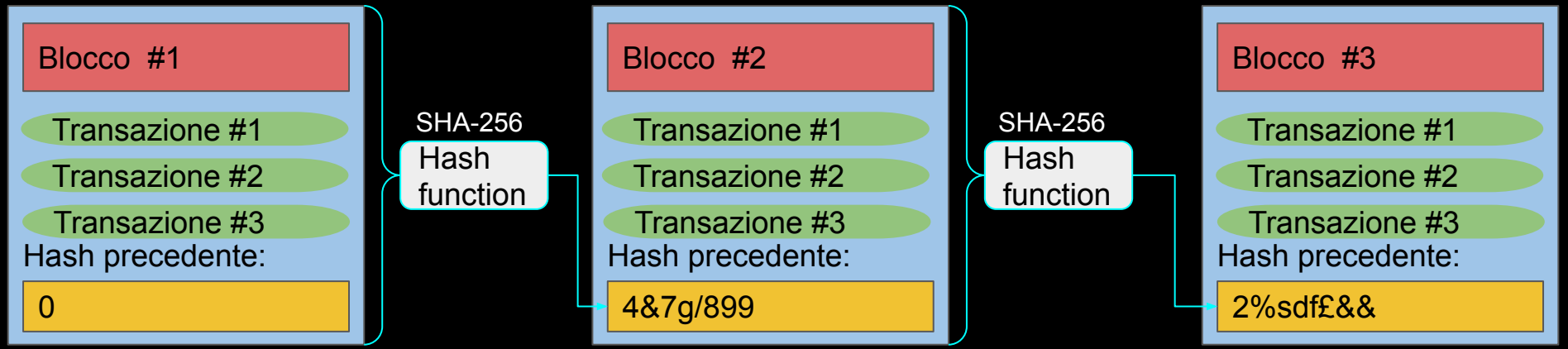
Struttura dati "immutabile" paragonabile ad un registro digitale, le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico la cui integrità è garantita dalla crittografia.

Una volta che qualcosa viene persistito al suo interno:

Non si può più modificare.

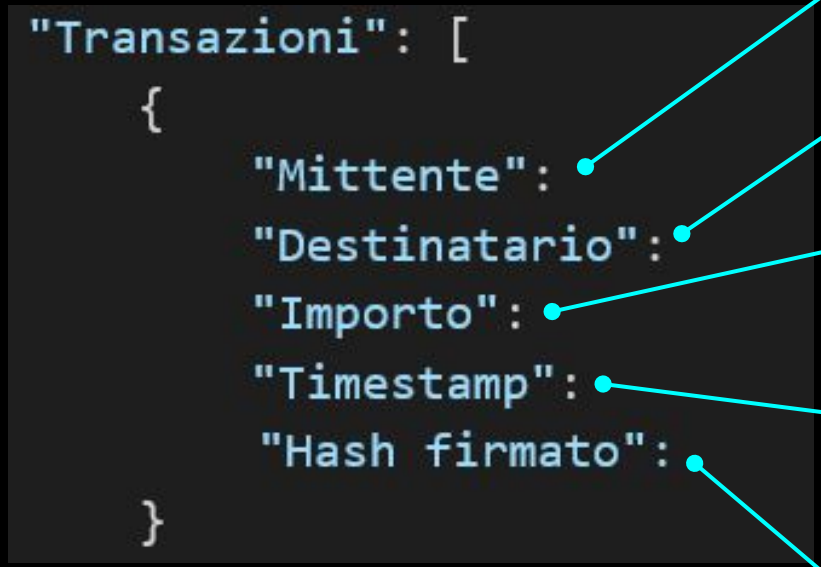
Non si può più eliminare.

Come funziona la mia blockchain?



- La mia blockchain viene salvata in un file di testo;
- Divisa in blocchi da 3 transazioni;
- Ogni blocco può verificare l'integrità del blocco precedente;
- Ogni transazione può verificare la propria integrità grazie a una firma digitale.

Come sono strutturate le transazioni?



Chiave pubblica del mittente

Chiave pubblica del destinatario

Importo della transazione

Numero di secondi dal 1° gennaio 1970 fino ad adesso

Hash dei primi quattro campi della transazione, firmato con la chiave privata del mittente

Cos'è un wallet?

Il wallet di un utente è costituito dall'insieme della chiave privata e chiave pubblica.

Ricavata basandosi sull'algoritmo RSA, utilizzando la generazione di un numero pseudo randomico.

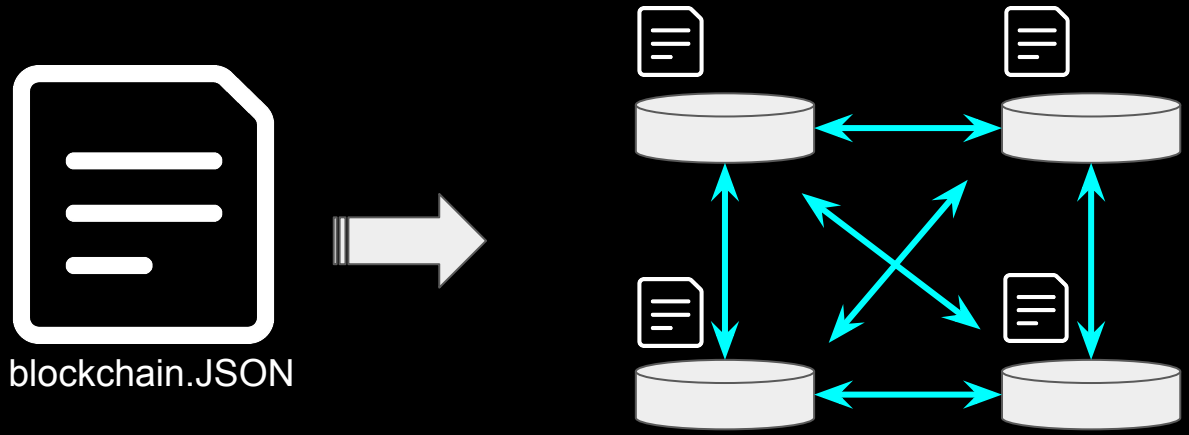
USO: la utilizzo per firmare l'hash della transazione, quando io sono il mittente

Ricavata derivandola dalla chiave privata.

USO:

- La utilizzo per identificarmi, nel caso io sia il destinatario di una transazione;
- La utilizzo per autenticarmi, nelle transazioni dove io sono il mittente.

Dove è conservata la blockchain?

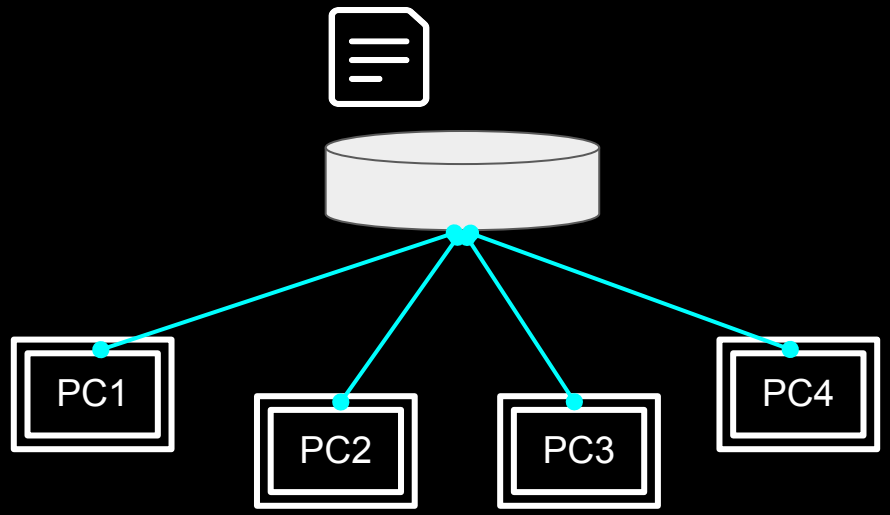


- File condiviso da una rete di nodi;
- Per fare una modifica al file, un nodo deve mandare in broadcast agli altri nodi, la modifica effettuata.

→ In una rete centralizzata, questa modifica deve essere regolata da un protocollo per il consenso.

Dove è conservata la blockchain nel mio progetto?

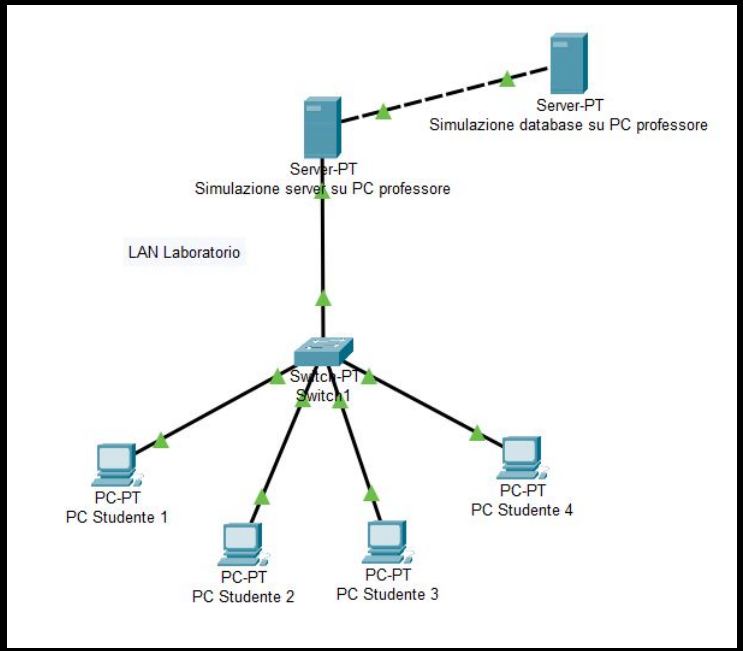
Nel mio caso, l'unico nodo che contiene il file blockchain è il computer del professore.
Avendo questo tipo di struttura si ottengono due vantaggi:



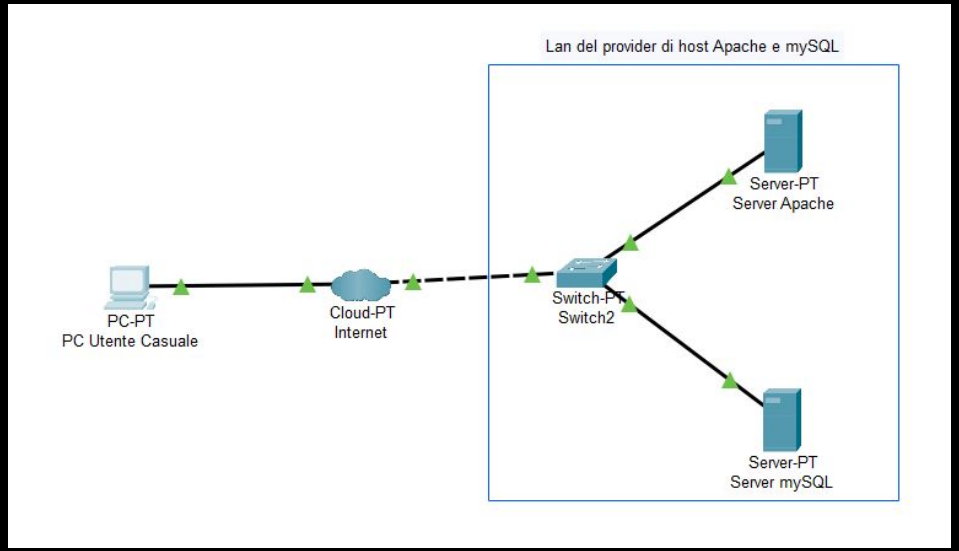
- Non devo gestire il consenso per le modifiche al documento fra i nodi;
- Risparmio, computazionalmente parlando, moltissimi calcoli al server centrale, per la creazione di nuovi blocchi.

Struttura della rete del progetto

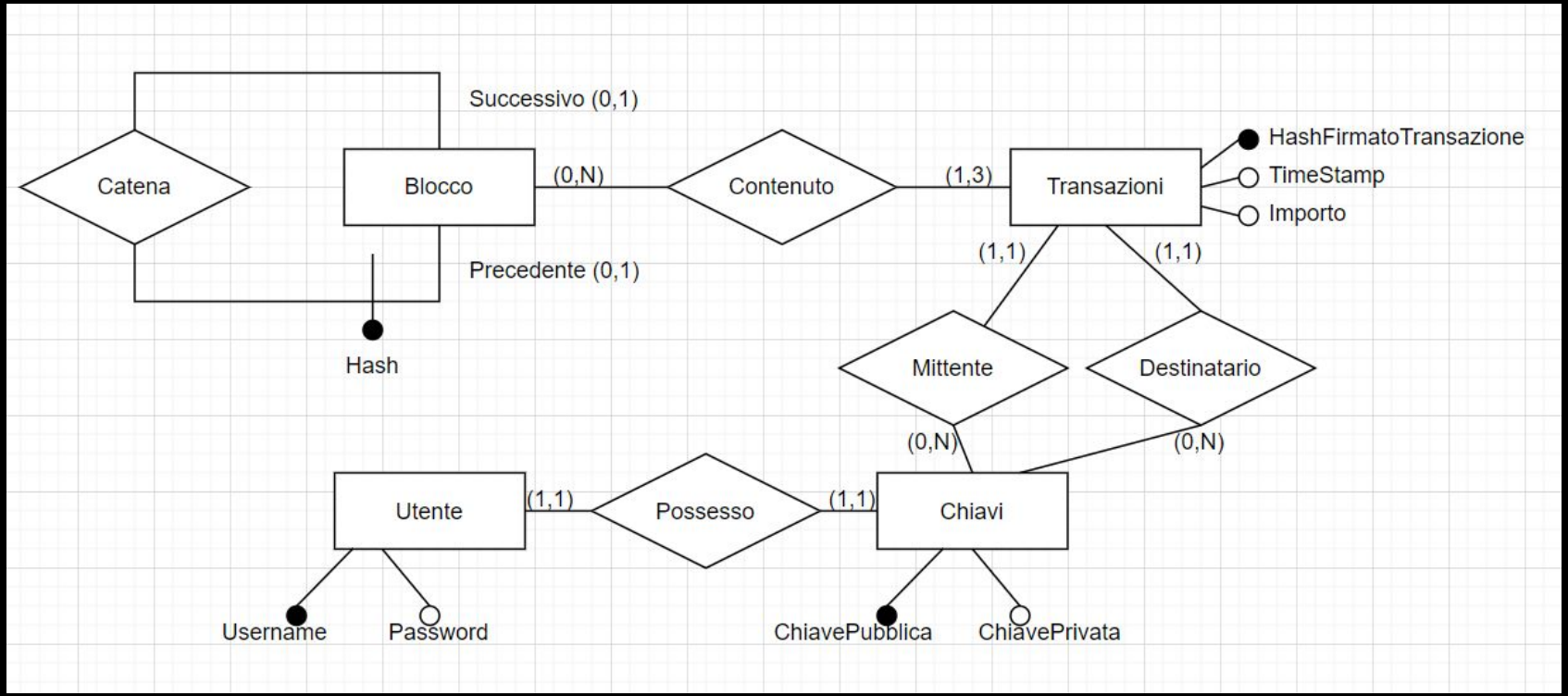
Come sarà usata in laboratorio?



Com'è realmente strutturata in internet?



Struttura della base di dati nel suo complesso



Caratteristiche in comune tra un DBMS e una blockchain?

- Elaborazione di grandi quantità di dati.
- I dati sono condivisi.
- I dati sono persistiti.
- I dati sono protetti in caso di disastro.
- Grande efficienza delle risorse.
- Efficacia nella velocità di diffusione di nuova informazione.