

Università degli Studi di Verona

Facoltà di Scienze e Ingegneria

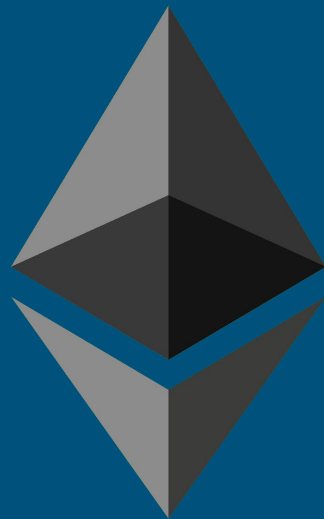


Tesi di Laurea

“EtherContracts2DB: Un framework per la
memorizzazione e l'analisi degli Smart Contract
di Ethereum tramite un database relazionale”

Introduzione

- **Ethereum** : piattaforma decentralizzata basata su un sistema peer to peer
- **La Blockchain** : struttura dati condivisa e immutabile
- **Gli Smart contracts** : un programma la cui esecuzione e i cui risultati sono garantiti dalla blockchain
- **Token** : gettone virtuale con un dato valore
- **Gas** : unità che misura la potenza di calcolo necessaria per eseguire un'azione sulla blockchain di Ethereum



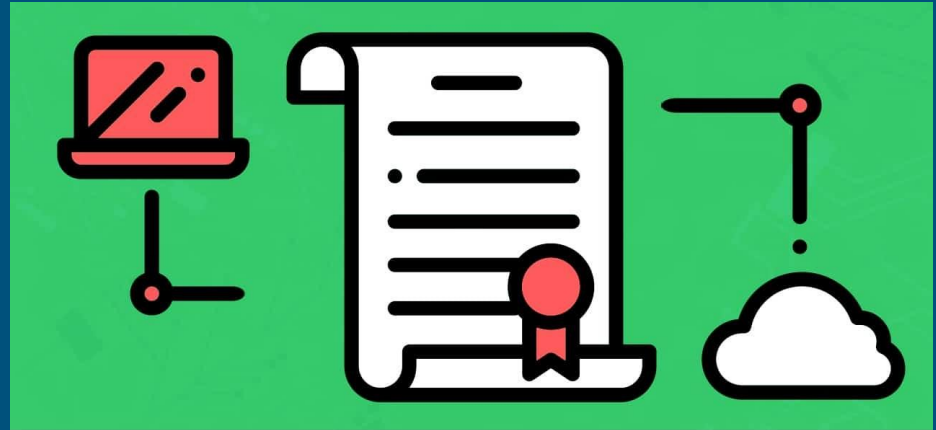
Smart Contract

Codice che viene salvato sulla blockchain

Un contratto è immutabile

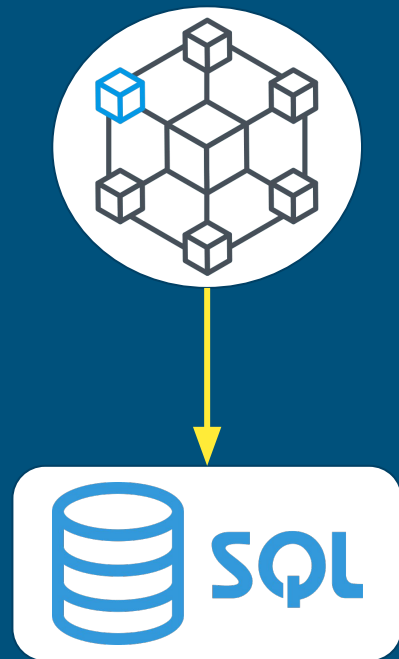
Funziona come un normale contratto tra individui, senza necessità di un intermediario

Codice viene eseguito da ogni nodo di Ethereum

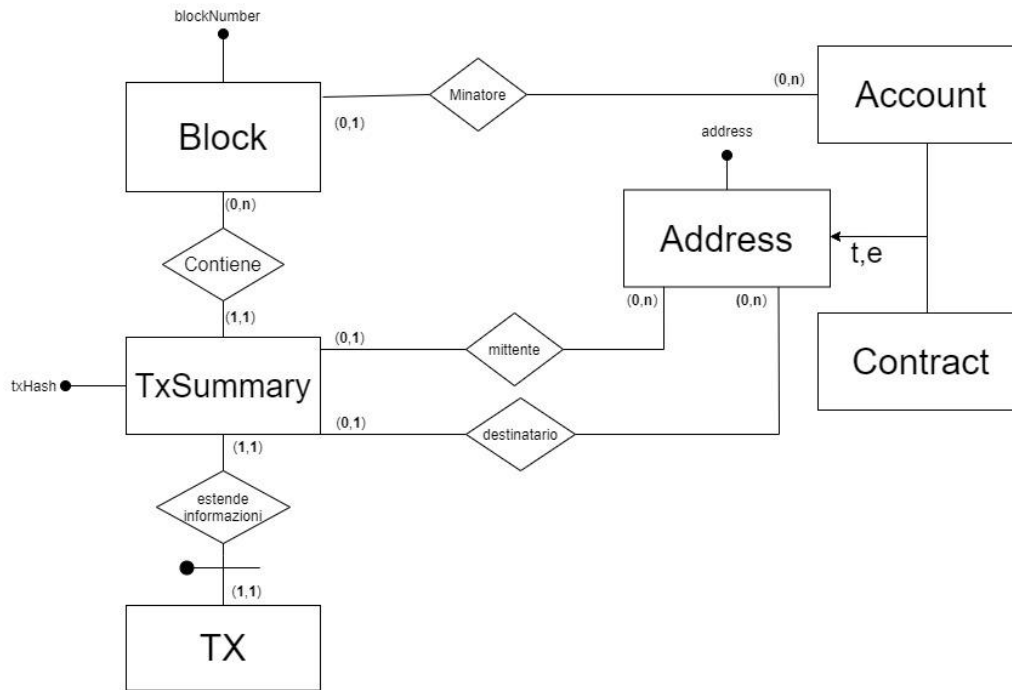


Scopo della tesi

1. Sviluppare un Framework che permetta di trasferire tutta o parte della blockchain di Ethereum su un database relazionale in PostgreSQL
2. Lanciare interrogazioni in sql sul database ed osservarne i risultati



Modello E/R



Attributi principali delle tabelle

Block : BlockNumber, Timestamp, Difficulty , Nonce , dollarQuote

TXSummary : TxHash, Sender , Receiver

Tx : Gas , GasPrice , GasUsed , input, Status

Contract : Address , codeSize , functionNumber , TokenTotalSupply

Account : Address, balance, TxCount

Framework

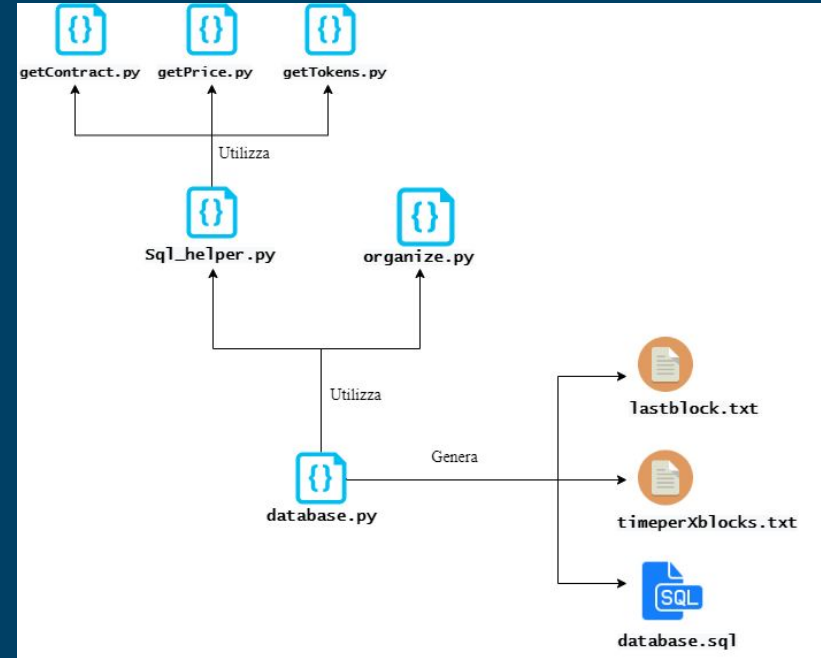
Librerie scartate

- Web3j
- Web3js
- Presto
- Quick Blocks

Librerie utilizzate

- web3.py
- psycpg2

Struttura della libreria sviluppata

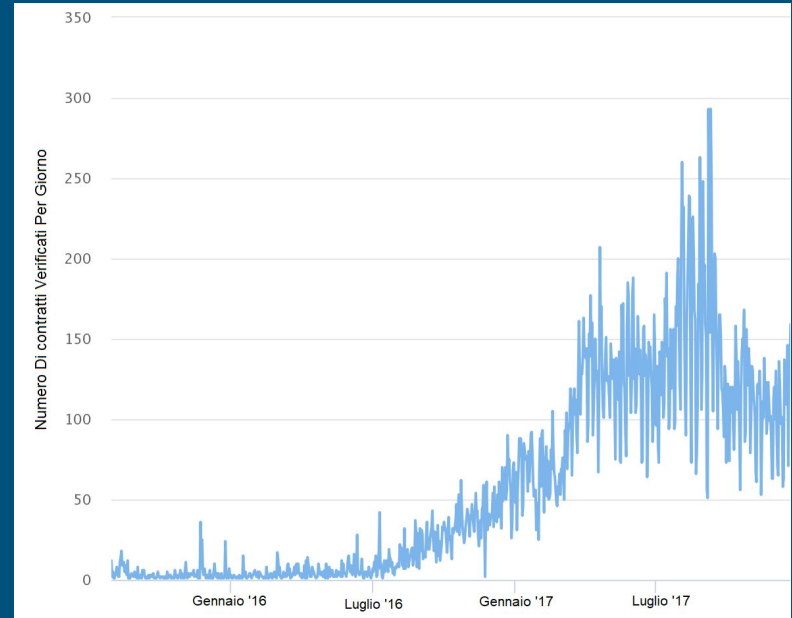


Analisi statistica dei dati

Numero di contratti pubblicati per giorno

La crescita inizia a metà 2016 ed è riconducibile al fatto che sempre più utenti e aziende abbiano iniziato a far uso di Ethereum

Il picco che si nota nel maggio del 2017 è dato dal fatto che un gruppo di società chiamato EEA(Enterprise Ethereum Alliance) abbia deciso di investire nello sviluppo di progetti per la piattaforma Ethereum



Query lanciata sul database

La seguente interrogazione calcola la media per giorno delle forniture totali di token da parte dei contratti

Vengono considerati solo Token
Contract

La query fa uso di una tabella virtuale data_contratto che contiene indirizzo e data di un contratto

```
SELECT    DC.data::DATE ,    AVG(C.tokenTotalSupply),count(*)
FROM      Contract C
          JOIN  data_contratto DC ON DC.address = C.address
WHERE     C.tokenTotalSupply <> 0
GROUP BY  DC.Data::DATE
```

Risultato

Data	Token	numero
02-08-2016	$5028219084126572 * 10^{60}$	13
03-08-2016	$19281831982520778 * 10^{60}$	13
20-07-2018	$767694516834294 * 10^{60}$	401

Grazie per l'attenzione