ETHERCHAIN2DB

Un framework per la memorizzazione e l'analisi integrata della blockchain di Ethereum tramite un database relazionale.

BLOCKCHAIN E MINING

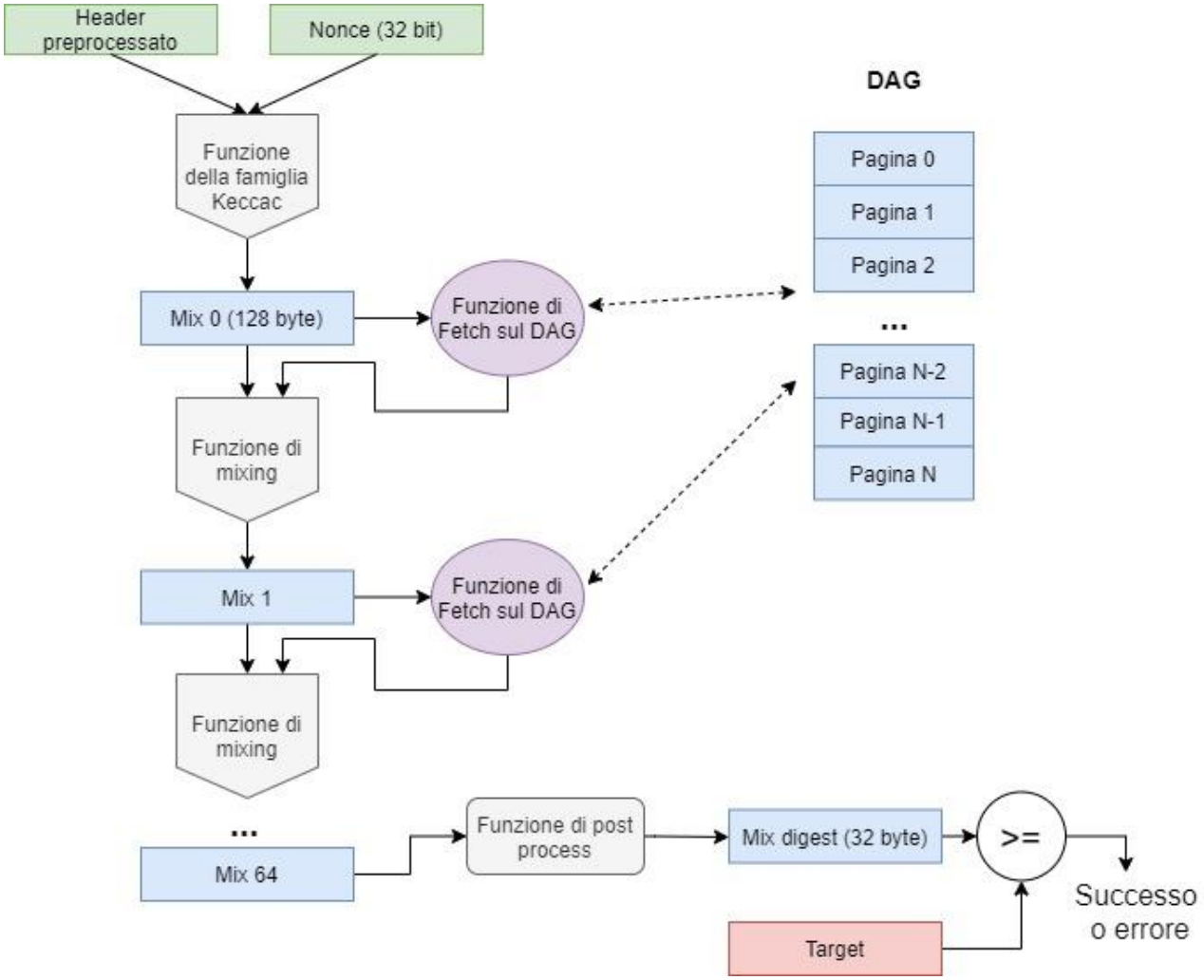
- Struttura dati usata per la gestione e memorizzazione di transazioni divisa in blocchi
- BLOCCO: registro che raccoglie transazioni
- Distribuita e replicata tra più nodi
- Utilizzo di crittografia a chiave privata per lo scambio di criptovalute

- La creazione del blocco avviene attraverso il concetto di mining
- Caratterizzato dal Proof of Work: insieme di operazioni che dimostrano che si è speso del tempo per creare un blocco
- Ogni minatore genera un nonce, questo valore aggiunto con i dati del blocco deve generare un hash minore di un determinato target
- Gli altri utenti possono verificare facilmente la veridicità del nonce
- A volte ci possono essere casi di blocchi validi generati contemporaneamente.

ETHEREUM

- Blockchain popolare creata tra il 2013 e il 2014 da Vitalik Buterin
- Diversa dalle altre Blockchain per l'utilizzo degli smart contracts e gli oracoli
- Permettono di effettuare transazioni solo nel caso in cui il vincolo del contratto si avveri nella realtà
- La moneta di Ethereum è l'Ether, ma anche il Gas è essenziale per il funzionamento dei contratti
- Per pubblicare uno Smart Contract occorre una determinata quantità di Gas
- Il creatore decide il valore del Gas e sta al minatore scegliere se inglobare il contratto nel suo blocco

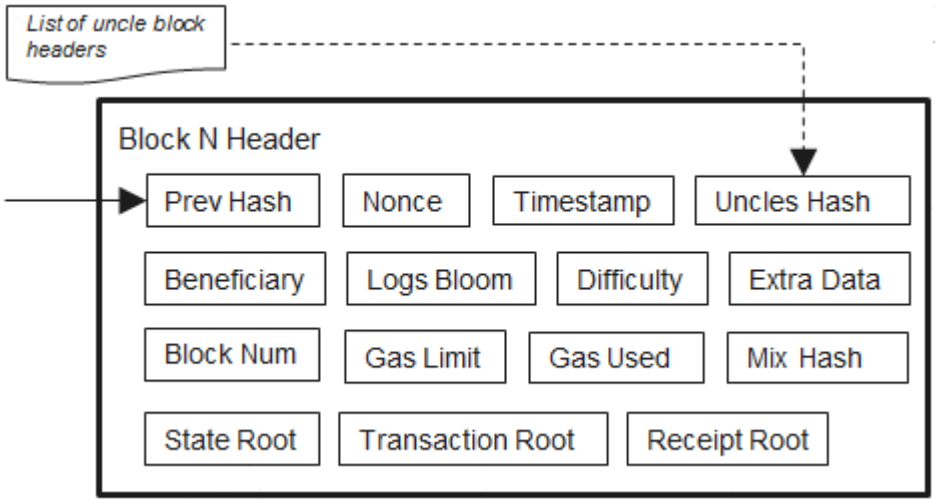
MINING SU ETHEREUM



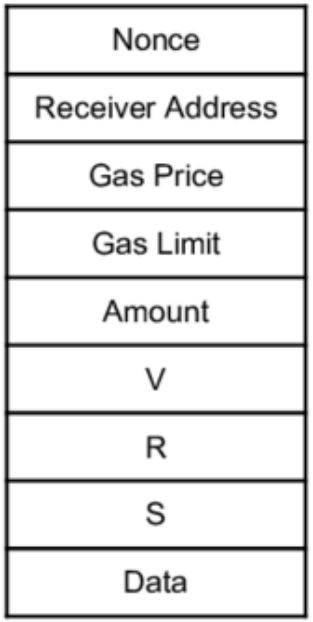
UPDATE DELLA TECNOLOGIA BLOCKCHAIN

- Con alcuni update la ricompensa fissa si è abbassata da 5 a 2 Eth
- Gli sviluppatori stanno cercando di migliorare la blockchain attraverso una nuova versione, Serenity, portando aggiornamenti volta per volta
- Plasma: separazione delle transazioni riguardanti gli smart contracts su una catena laterale per ridurre il traffico della blockchain primaria
- Sharding: divisione della rete in sezioni, in modo da operare in modo quasi indipendente
- Passaggio da Proof of Work a Proof of Stake
- Per creare un blocco non serve più avere potenza di calcolo, ma attraverso una ‘scommessa’ e da quanto tempo la scommessa è stata piazzata
- Ciò previene l’attacco del 51% e ridurre il consumo elettrico tipico della PoW

STRUTTURA DEL BLOCCO

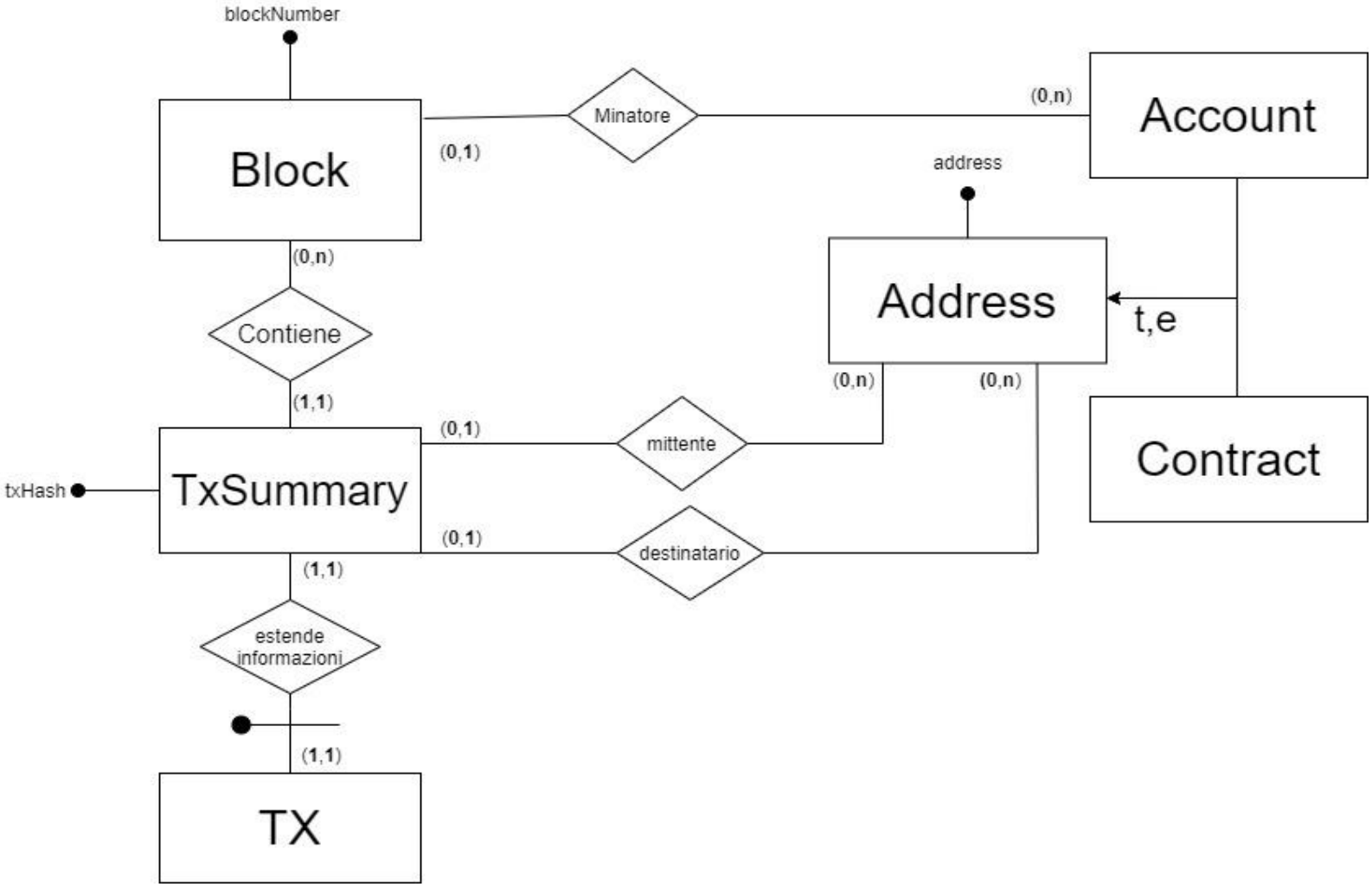


Schema dell'header



Schema di una transazione

MODELLO ER


blockNumber
Block
Minatore
(0,n)
(0,1)
Account
address
Address
t,e
(0,n)
(0,n)
(0,n)
Contiene
(1,1)
(0,1)
mittente
txHash
TxSummary
Contract
(0,1)
destinatario
(1,1)
estende informazioni
(1,1)
TX

CAMPI PRINCIPALI TABLES

- **BLOCK**: *BlockNumber*, blockHash, miner, parentHash, size, timestamp, dollarquote, totalFee;
- **SUMMARYTX**: *txHash*, blockNumber, sender, receiver, value;
- **TX**: *txHash*, gas, gasPrice, gasUsed, contractAddress, fee;
- **ACCOUNT**: *Address*, balance, txCount;
- **CONTRACT**: *Address*, codeSize, functionNumber, tokenTotalSupply;

PROGRAMMA

- Programma scritto in Python
- Si collega la libreria web3 alla rete della blockchain
- Viene impostata la quantità di blocchi da caricare e deciso il punto di partenza della blockchain e inizializzata la base di dati
- Il programma entra in un loop e inizia a estrarre le info riguardanti l'n-esimo blocco e a scriverle sul file SQL
- Ogni 100 blocchi il programma si collega attraverso psycopg2 alla base di dati e carica i dati salvati sul file
- Alla fine il programma carica i blocchi rimanenti e salva il numero dell'ultimo blocco caricato

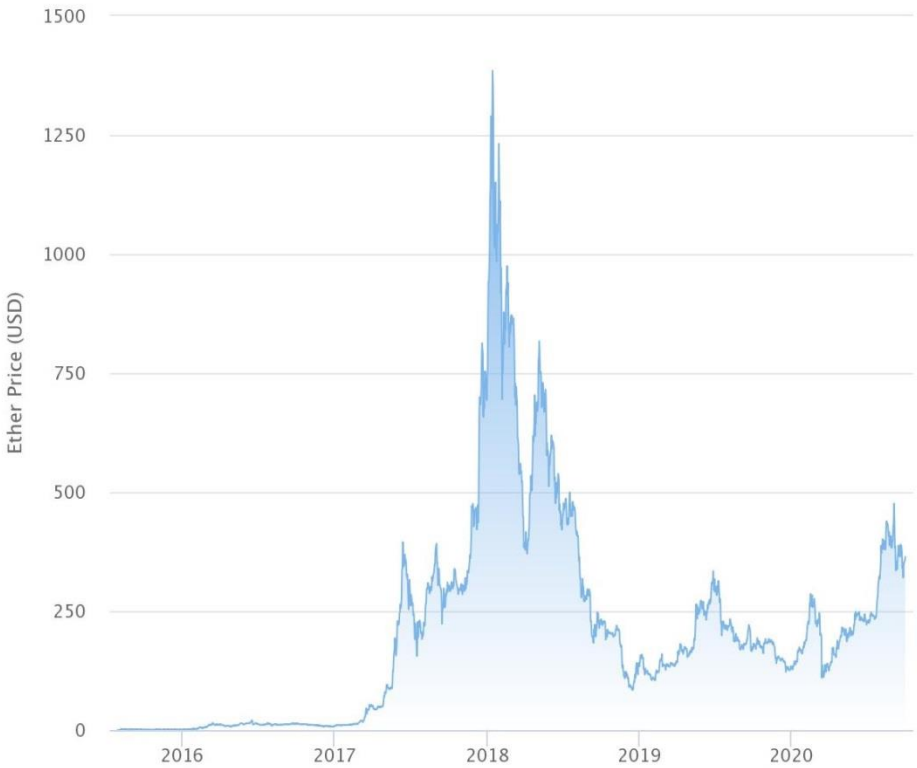
STATISTICHE SUI BLOCCHI

- Numeri piuttosto costanti
- I cali sono dovuti alla ‘Difficulty Bomb’
- Serviva per il passaggio da PoW a PoS
- Il tempo di mining era raddoppiato e il timer è stato resettato
- La dimensione dei blocchi è aumentata nel tempo
- È stato aumentato il gas limit

Blocchi creati giornalmente

VALORE DELL'ETHER

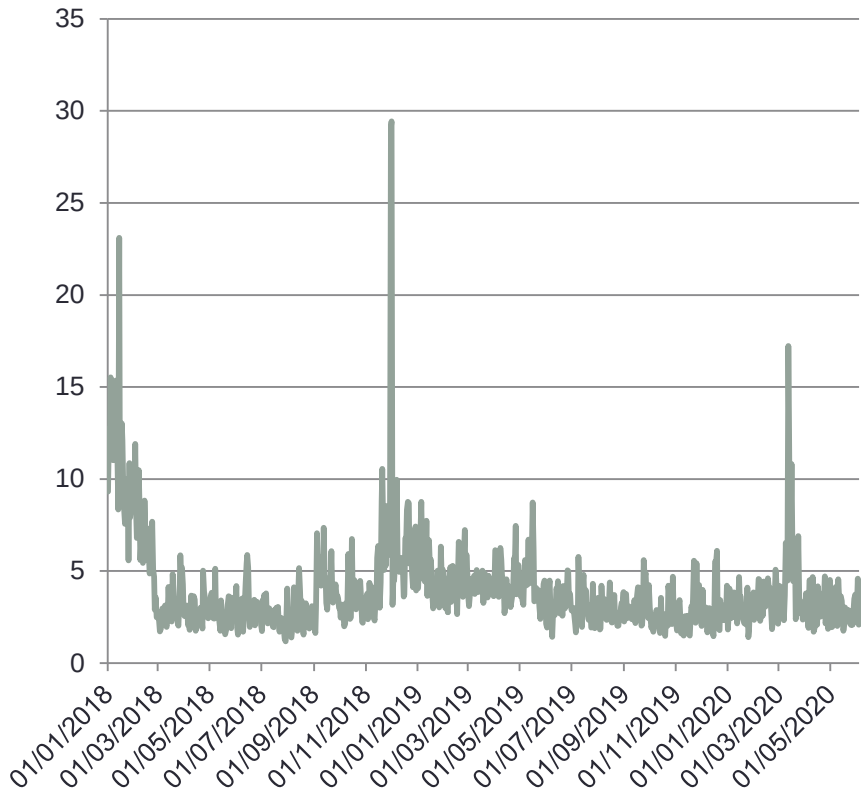
- Valuta molto instabile
- Fino al 2017 1 ETH = 10 $
- Picco nel gennaio 2018 a 1300$
- Sceso nuovamente e risalito a 700$
- Molte criptovalute simili hanno avuto un picco in quel periodo
- Le cause possono essere un aumento di popolarità delle blockchain o una manipolazione del mercato.



Valore dell'Ether in Dollari

STATISTICHE SULLE TRANSAZIONI

- Picco di transazioni avvenuto nello stesso momento della valuta
- Nonostante l'aumento delle dimensioni dei blocchi il numero di transazioni per blocco non aumenta
- Dovuto all'aumento di smart contracts
- Transazioni più complesse = più gas richiesto e fee maggiori
- Media del valore di transazioni costante



Media di valore di transazioni giornaliera