Blockchain

Struktura

Obsah

- Co je blockchain?
- Hashing
  - SHA-256 (Bitcoin) / Sha3 - Keccak256 (Ethereum)
  - Crypto adresy
- Proof of Work
- Merkle trees

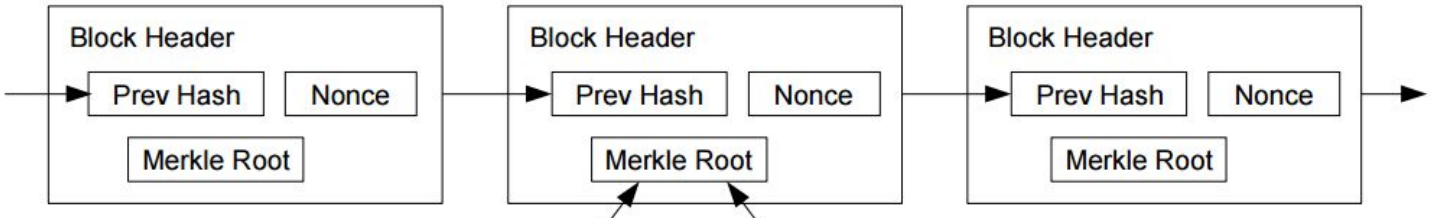
Co je to Blockchain?

Block = soubor dat obsahující relevantní o změnách a interakcí s

- serializovaná transakční data (Alice poslal Bobovi 1 BTC)
- odkaz na parentblock (hash)
- hash současného blocku
- PoW nonce
- Stateroot hash
- blocktime,...

Chain = řetězení bloků odkazem na předchozí block

Blockchain


Block Header
Prev Hash
Nonce
Merkle Root
Block Header
Prev Hash
Nonce
Merkle Root
Block Header
Prev Hash
Nonce
Merkle Root

Co je to Bitcoin?

Bitcoin jsou peníze (jednotka)

Bitcoin je databáze zůstatků

Bitcoin je SW = implementace klienta

Bitcoin je síť = souhrn všech uzlů, na kterých běží Bitcoin klient

Co je to Ethereum?

Ethereum je virtuální stroj (Ethereum Virtual Machine)

Ethereum je databáze stavů (stroje)

Ethereum je SW = implementace klienta

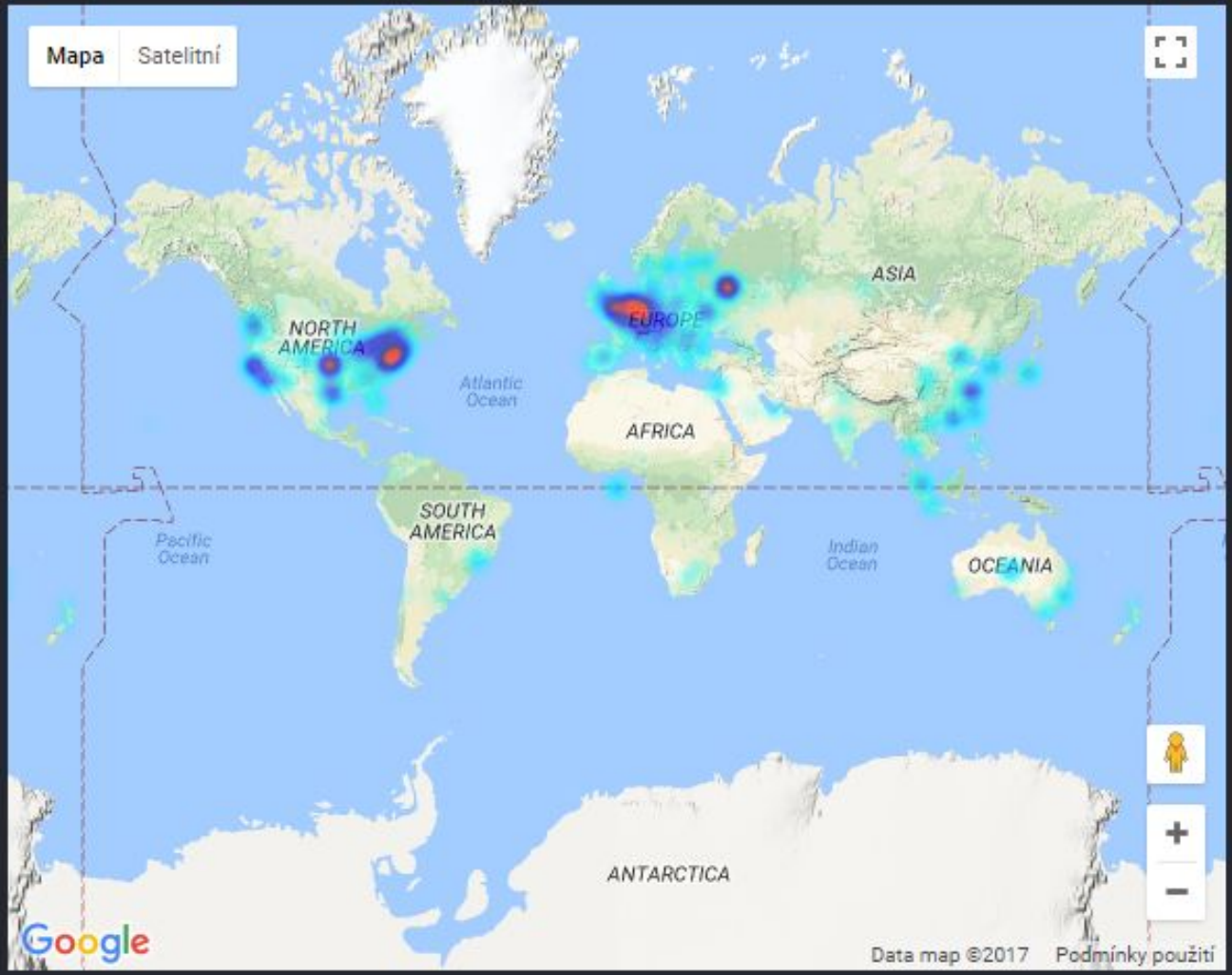
Ethereum je síť = souhrn všech uzlů, na kterých běží Ethereum klienty

vs.

Ether je platidlo, kterým se platí za používání EVM a ukládání dat

COUNTRIES

Total	24419 (100%)
United States	7599 (31.12%)
Germany	1971 (8.07%)
Russian Federation	1736 (7.11%)
China	1203 (4.93%)
Canada	1189 (4.87%)
United Kingdom	1179 (4.83%)
Netherlands	908 (3.72%)
Australia	602 (2.47%)
France	535 (2.19%)
Ukraine	447 (1.83%)



SHA256 / KECCAK256 (SHA3)

Hashovací funkce s velkou “output domain”

- 2^256 -> tj. Hexadecimální číslo o 64 znacích
  - prostě velké číslo 🤷

Cryptoaddresses

Step1:

32 bytes == Private -> 64 bytes == Public key (ECDSA)

Step2:

Keccak256(Public key) == 32 bytes

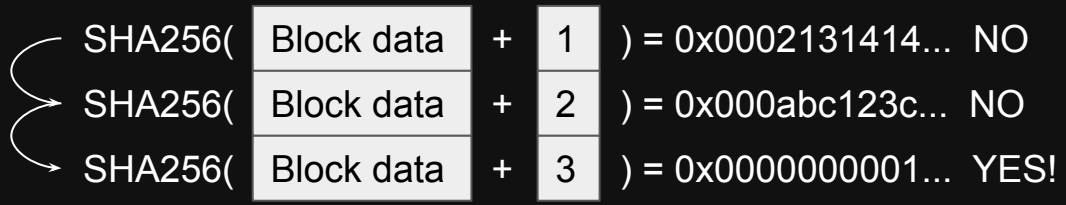
Step3:

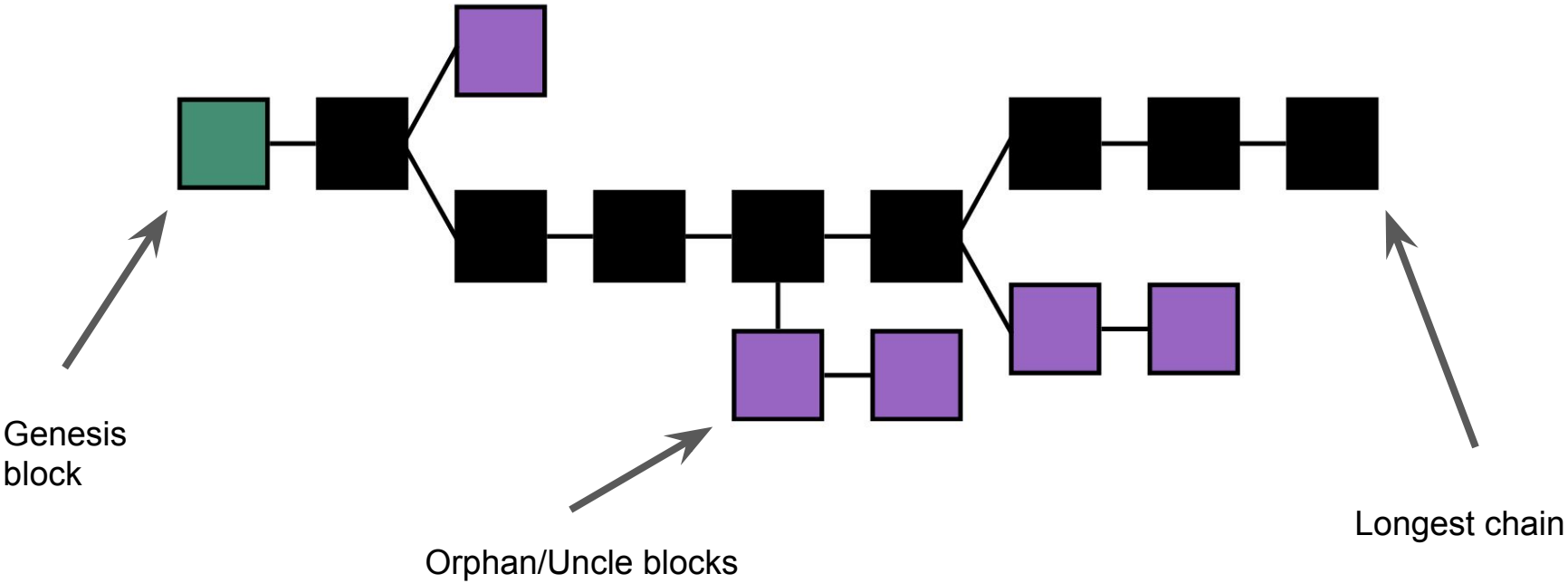
=> vezmi posledních 20 bytes == Ethereum adresa

Proof of Work

Algoritmus vynucující provedení určité výpočetní práce - pomocí hashování.

Mining difficulty - hledání hashe správného tvaru = správný počet nul:




Genesis
block
Orphan/Uncle blocks
Longest chain


coindesk
MINERY
INISIUM MI
About 70 percent of space is filled now, we're still waiting for more miners to come from our partners

Merkle trees

Ověřování velkých stromů pomocí jednoho root hash.

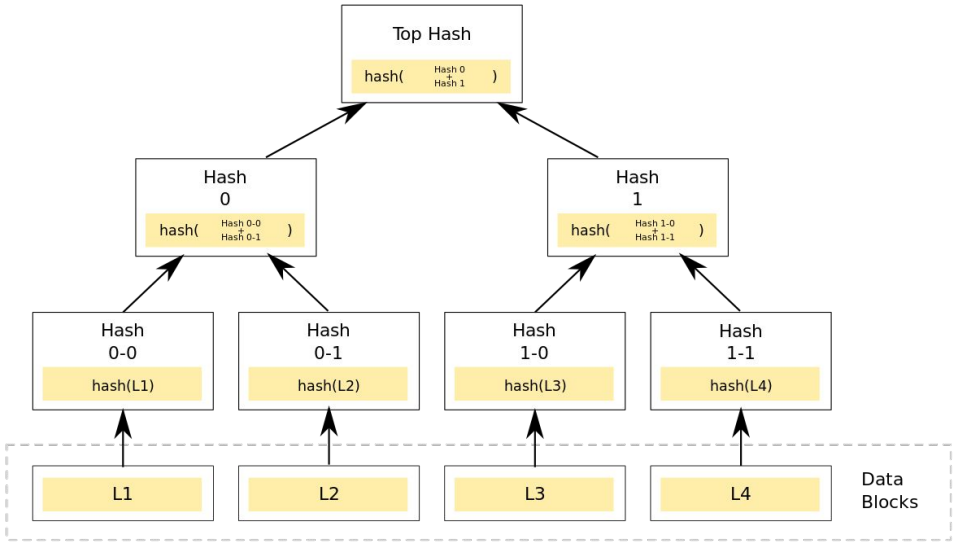
- Dokazování inkluze pomocí Merkle proofs:
  - dodání dat a pouze ostatních hashů vedoucím k merkleroot

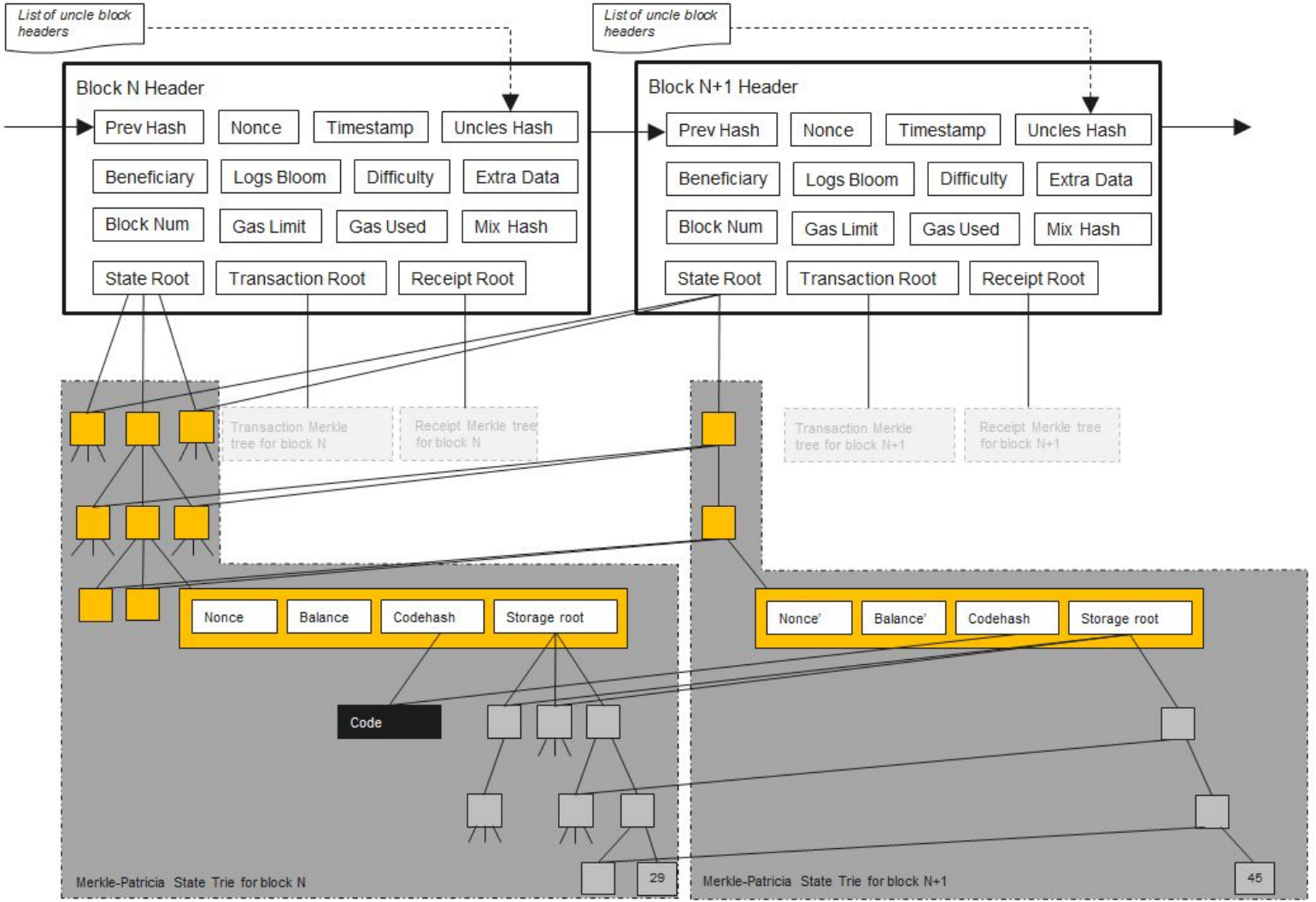
Merkle proof je v podstatě balík dat obsahující:

[samotná data listu, hash leef2, hash(node_k), hash(node_k-1),... hash(node_1)]

-> velikost důkazu je velikost dat = listu + k*32 bytes

Merkle trees




List of uncle block headers
List of uncle block headers
Block N Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Block N+1 Header
Prev Hash
Nonce
Timestamp
Uncles Hash
Beneficiary
Logs Bloom
Difficulty
Extra Data
Block Num
Gas Limit
Gas Used
Mix Hash
State Root
Transaction Root
Receipt Root
Transaction Merkle tree for block N
Receipt Merkle tree for block N
Transaction Merkle tree for block N+1
Receipt Merkle tree for block N+1
Nonce
Balance
Codehash
Storage root
Code
Nonce'
Balance'
Codehash
Storage root
Merkle-Patricia State Trie for block N
29
Merkle-Patricia State Trie for block N+1
45

@JosefJe

Recap