bitcoin.org
paper
genesis block - 3.1.2009
1st transaction 12.1.2009

Protocol

1. new transactions
2. transactions are gathered into blocks
3. find Proof-of-Work (PoW)
4. block is published
5. block is accepted / ignored
6. new block on top of ~~the rec~~eived one

Wallets & Addresses

↓

P/U key

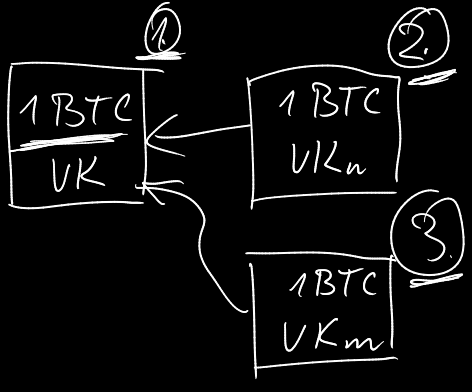
RIPMD-160 (SHA-256(U_k))

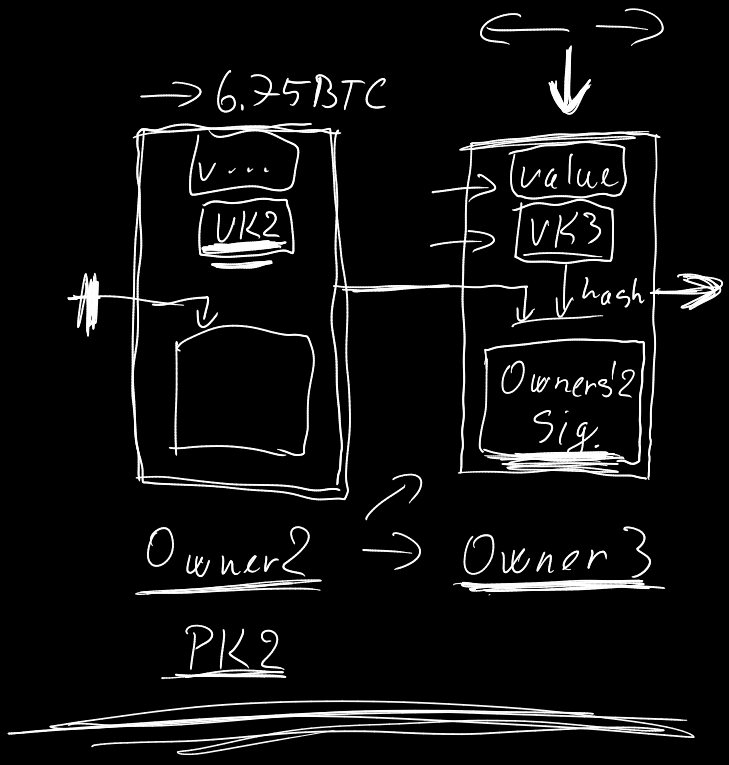
HD

Transactions

- hash
- input
  - prev. transaction
  - signature
- output
  - value
  - receiver's address

Double Spending





ECDSA

↓

ElGamal

↓

DLP

$a, b \in \mathbb{F}_p$ $\quad P = (x, y)$ pre $x, y \in \mathbb{F}_p$

$y^2 \equiv x^3 + ax + b \pmod p$

- secp256k1 $\quad a = 0$, $b = 7$

$\Rightarrow y^2 \equiv x^3 + 7 \pmod p$

BSGS $\Rightarrow O(\sqrt{n})$

$\Rightarrow O(2^{128})$ $\quad (1, n-1)$

$|p| = 256b$

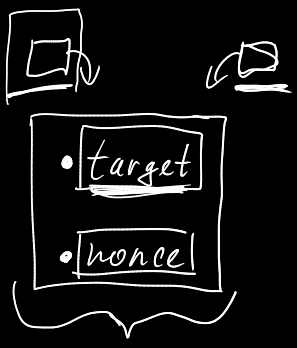
$|n| = 256b$

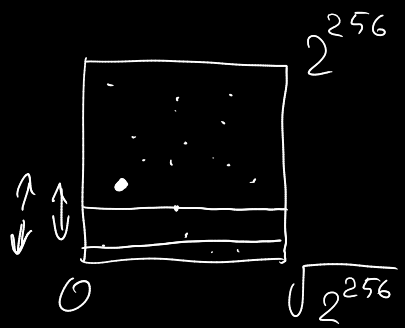
RSADSA $\quad |n| = 3072b$

Chain of Blocks

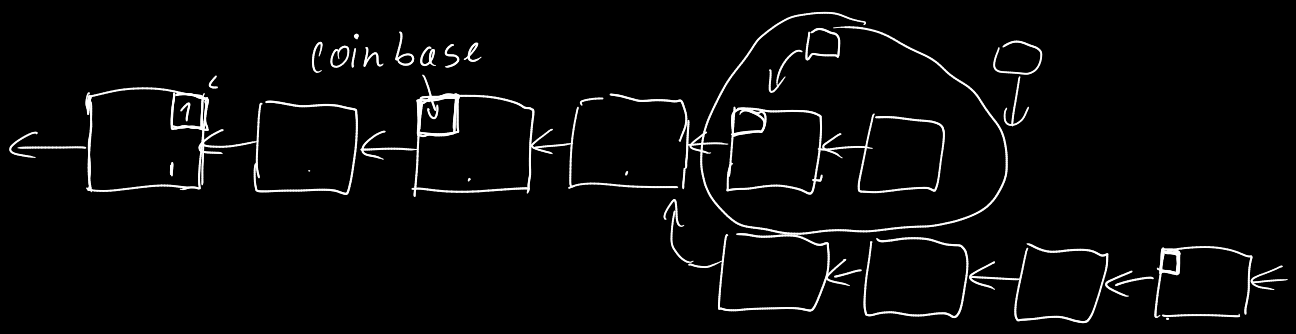
Block:
- transactions
- hash
- prev. block
- timestamp
- target
- nonce

2016 ↓ 10min





hash < target



110 EH/s $\Rightarrow$ 3.56W

51% attack