BITCOIN Mining met Python

In den beginne...

Bitcoin: A Peer-to-Peer Electronic Cash System

3 Januari 2009
Allereerste block !

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

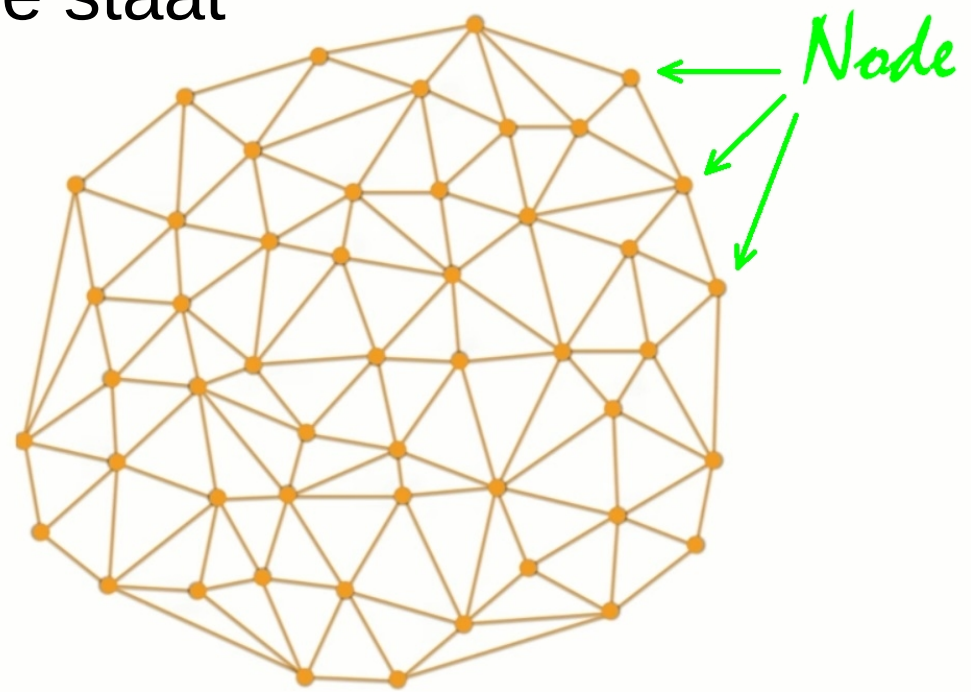
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Fiat geld

- Gecentraliseerd (banken)
- Gewaarborgd en gecontroleerd door de staat
- Ongelimiteerd (men drukt bij)

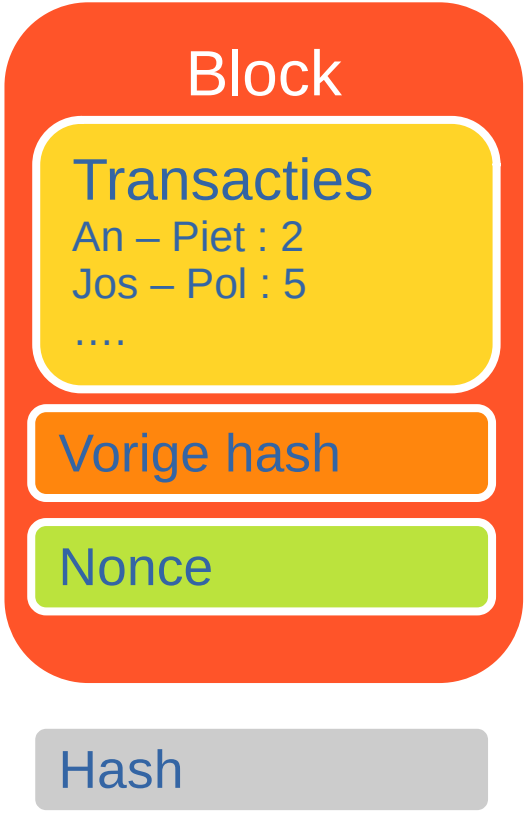
Bitcoin

- Gedecentraliseerd
- Niet onder controle van de staat
- Gelimiteerd
  - 21 miljoen BTC
  - 2140 laatste bitcoin



Ledger

- Grootboek
- Block
  - 1 pagina
  - 1 Mb
  - Miljoenen transacties



Hash?

- Algoritme – resultaat moet uniek zijn!
  - Input: een blok data van willekeurige lengte
  - Output: getal met vast aantal cijfers (hexadecimaal)
  - Zelfde input moet zelfde output geven, maar 1 bit verschil moet een geheel andere output geven!
- $x^2 = 81 \Rightarrow x = 9$ – makkelijk
- $x+y = 5 \Rightarrow x = 0 .. 5, y = 5 .. 0$ – moeilijker
- SHA256(x) = 173fa09b…. – +/- onmogelijk

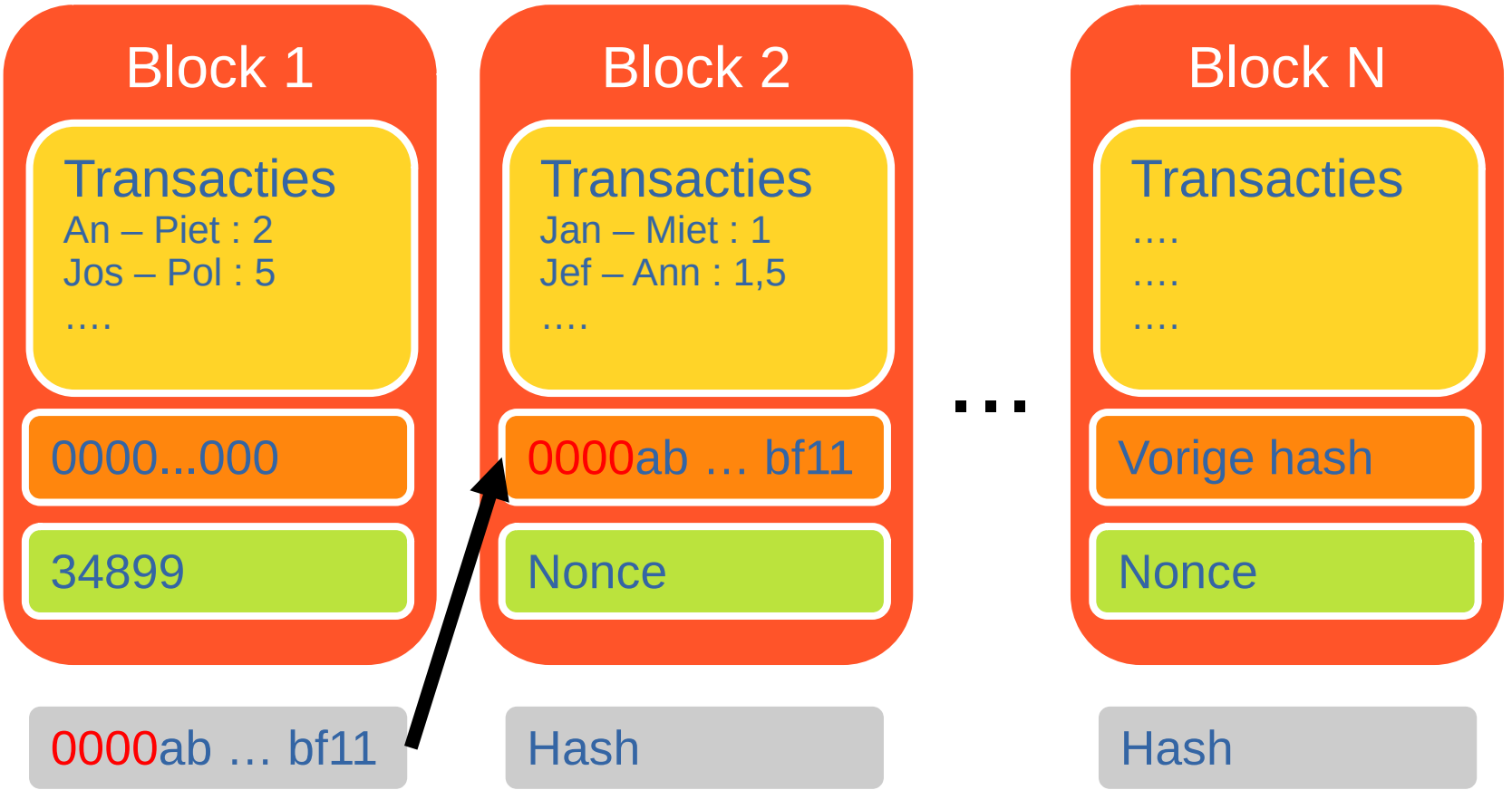
Bitcoin hash

- Moet beginnen met een aantal nullen.
- Moeilijkheidsgraad = aantal nullen.
- Vindt het getal (nonce) dat er voor zorgt dat de hash met x aantal nullen begint.
- Nonce als eerste gevonden? Je krijgt nieuwe bitcoin! Dit is bitcoin mining.

Ledger

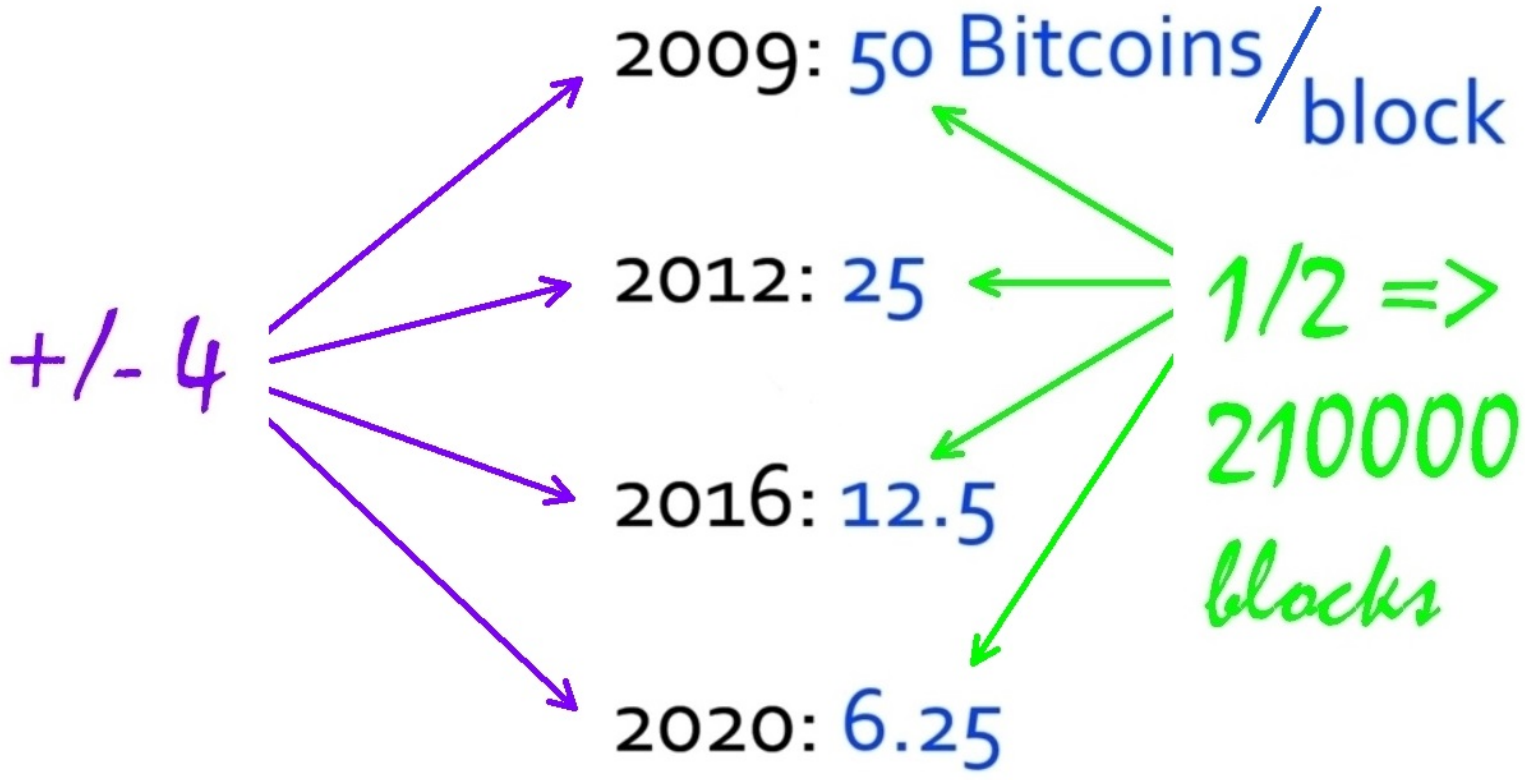

Block 1
Transacties
An – Piet : 2
Jos – Pol : 5
....
Vorige hash
Nonce
Hash
Vorige hash: 000000 … 000
Hash: 7de583 … 58641 => FOUT : 4 nullen
Nonce: 34899
Nieuwe hash: 0000ab78 … 5bf11 => OK

Blockchain


Block 1
Transacties
An – Piet : 2
Jos – Pol : 5
....
0000...000
34899
Block 2
Transacties
Jan – Miet : 1
Jef – Ann : 1,5
....
0000ab … bf11
Nonce
...
Block N
Transacties
....
....
....
Vorige hash
Nonce
0000ab … bf11
Hash
Hash

Show time!!!

Bitcoin mining



Mining evolutie

CPU mining

GPU mining

FPGA mining

ASIC mining

Mining pools