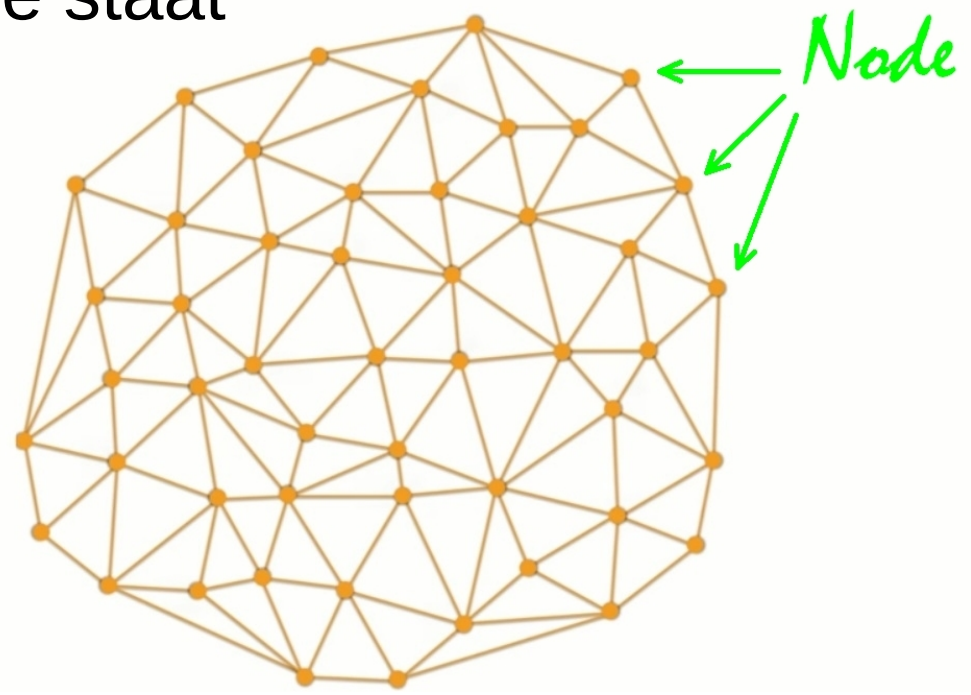
BITCOIN Mining met Python

Fiat geld

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

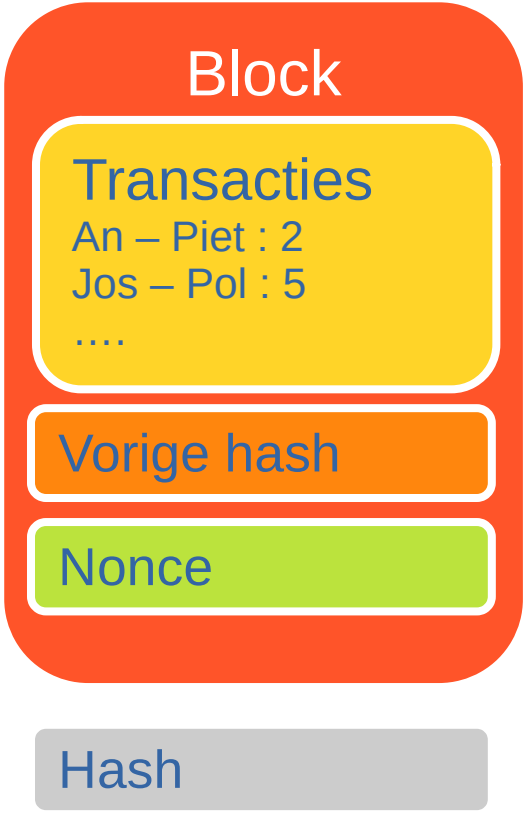
Bitcoin

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



Ledger

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



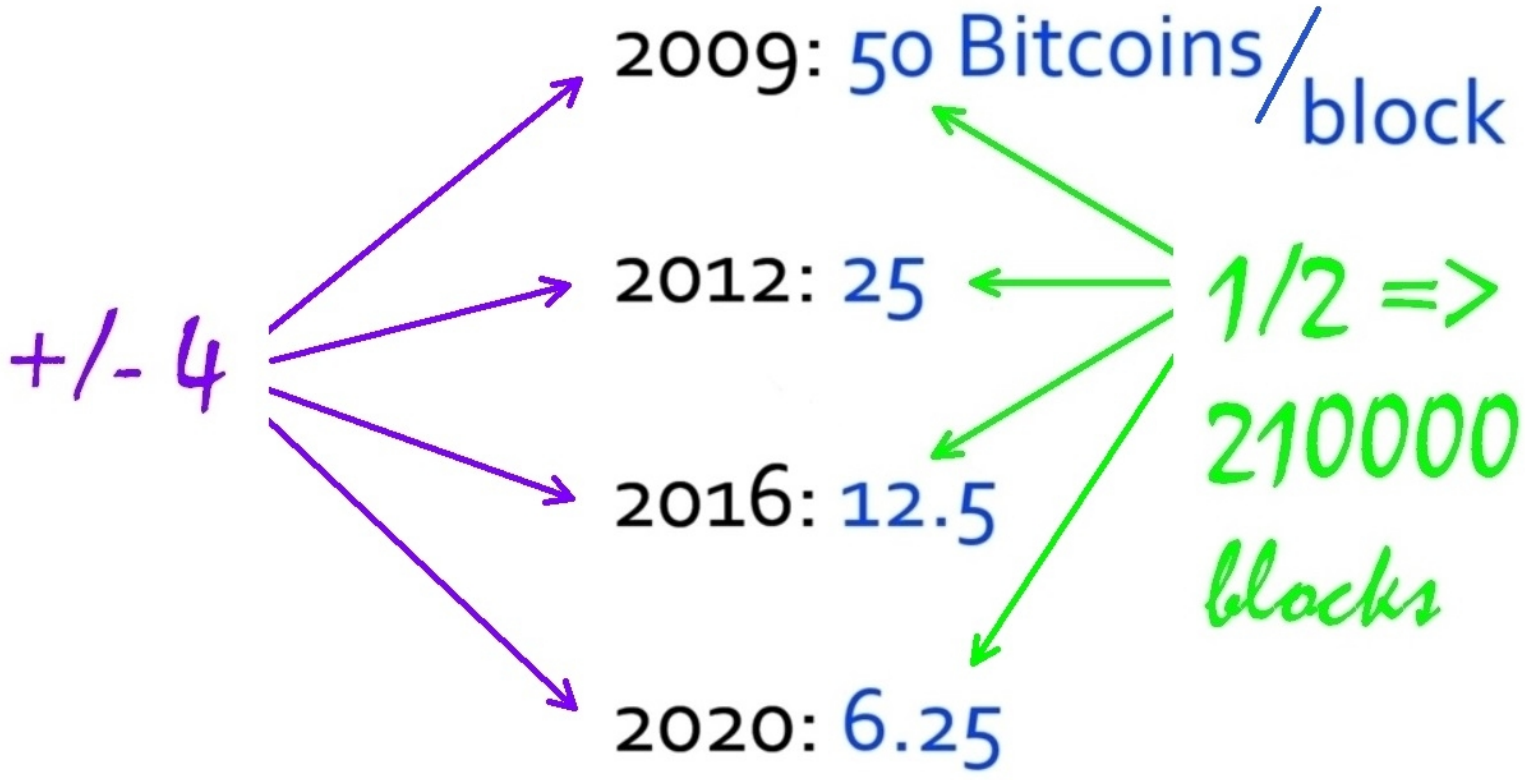
Hash?

- 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.

Bitcoin mining



Ledger

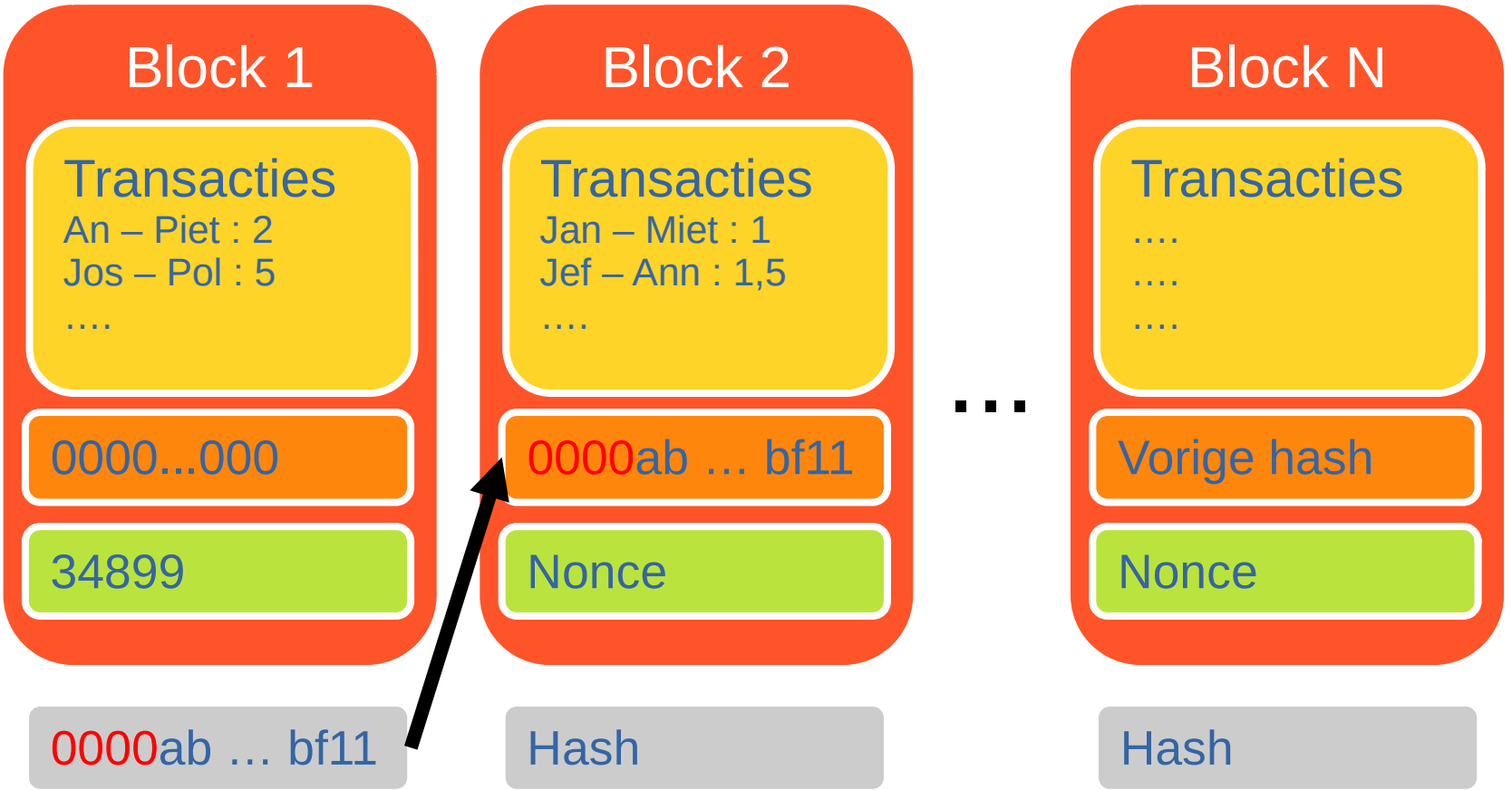
Vorige hash: 000000 … 000

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