Vakantiecursus 2018

Bitcoin
Een blik onder de motorkap

Boris Škorić
b.skoric@tue.nl
SEC groep
Faculteit Wiskunde en Informatica
TU Eindhoven

TU/e

Inhoud

Bitcoin

- ontwerpprincipes
- technische details
- financiële prikkels
- wijze lessen

Blockchain in het algemeen

- andere cryptovaluta's
- andere toepassingen dan valuta

Waar we het NIET over gaan hebben

NIET:

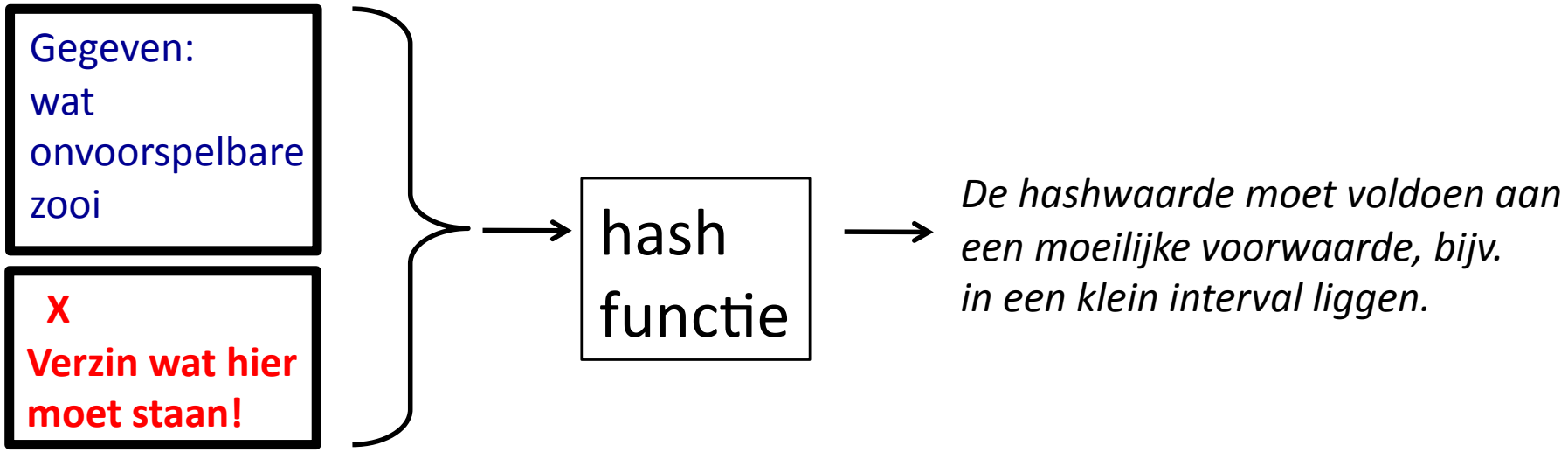
- Geschiedenis van crypto-valuta's
- Economie / politiek
- Criminologie
- Stinkend rijk worden

Wat is Bitcoin?

- Crypto-munteenheid
  - volledig digitaal
  - sleutel geeft toegang tot "rekening"
  - crypto: transacties ondertekenen
  - crypto: nieuw geld maken

- Gedecentraliseerd
  - peer to peer communicatie
  - tijdelijke autoriteit om beslissingen te nemen
- "Block chain"
  - alle transacties openlijk zichtbaar
  - chronologisch aaneengeschakeld

Hashpuzzel



- Een X ***vinden*** kost heel veel pogingen => rekentijd.
- Een X ***checken*** is heel makkelijk!

Bewijs van verrichte arbeid ("Proof of work")

Vereisten

U bent nu een expert in hashes en handtekeningen.

Opdracht: bouw een crypto-munt.

Wat zijn de vereisten?

Welke problemen moet u oplossen?

V1: volledig digitaal

V2: veilig

V3: pseudoniem

V4: geen centrale autoriteit

V5: verifieerbare, eenduidige boekhouding

V6: stabiliteit d.m.v. financiële prikkels

V7: resistent tegen DOS-aanvallen

Anonimiteit versus Pseudonimiteit

Anoniem:
Absoluut geen enkele koppeling tussen observaties en iemands identiteit.

Pseudoniem:
Iedereen heeft een of meerdere pseudoniemen.
Gebeurtenissen mbt dezelfde pseudoniem kunnen aan elkaar gelinkt worden.

Crypto-rekeningen

V1: volledig digitaal
V2: veilig
V3: pseudoniem
V4: geen centrale autoriteit

Stap 1
Publieke sleutel ≡ rekeningnummer
Privé-sleutel geeft toegang tot rekening

Basisidee:

- maak eigen sleutelpaar (**s**,**P**)
- bescherm **s** met je leven
- geef publieke sleutel **P** aan hen die jou geld willen sturen
- ontvang publieke sleutel **Q** van mensen die geld van jou willen ontvangen
- als je een betaling doet naar **Q**, dan onderteken je de transactie met **s**.
- iedereen kan jouw handtekening checken met **P**.

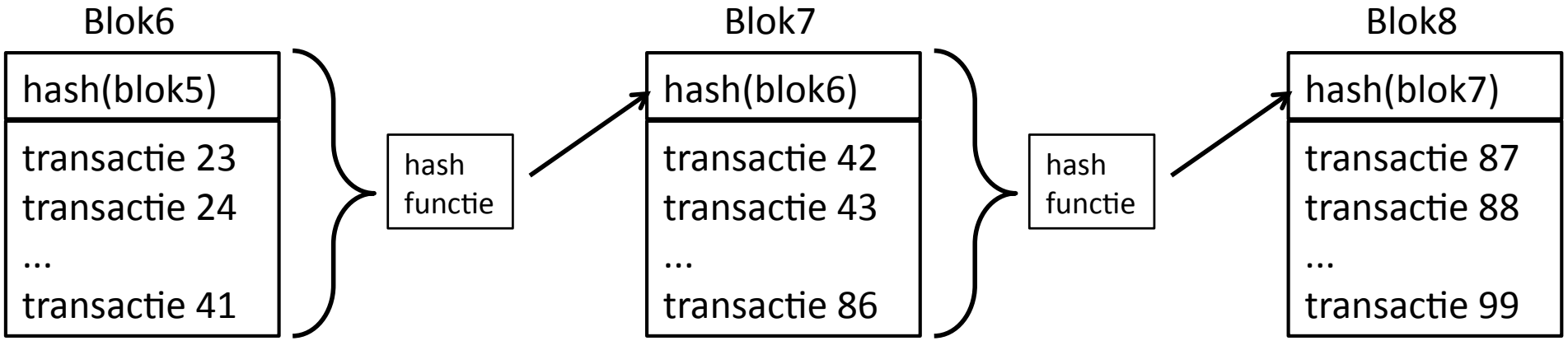
Geen centrale autoriteit nodig.
Maak er zoveel je wilt.

Betalingen aaneenschakelen

Stap 2

Maak een keten.

V4: geen centrale autoriteit
V5: verifieerbare, eenduidige boekhouding



Zet de hele datastructuur op een peer-to-peer netwerk

Voordelen

- niet te vervalsen
- simpele datastructuur

Nadelen

- saldo moet uitgerekend worden
- lastig zoeken in de keten
- de hele keten moet gecheckt worden

Probleem: autoriteit

V4: geen centrale autoriteit
V5: verifieerbare, eenduidige boekhouding
V6: stabiliteit dmv financiële prikkels

Stap 3

Los het autoriteit-probleem op

Wie mag het volgende blok aanplakken?
Hoofdpijndossier!

De oplossing in Bitcoin:
Hashpuzzel oplossen geeft tijdelijk autoriteit, en een geldprijs

Gewone mensen

- kondigen aan welke betalingen ze willen doen
- checken handtekeningen, hashwaardes

"Mijnwerkers"

- verzamelen nog onuitgevoerde betalingen
- proberen de hashpuzzel op te lossen
- kondigen oplossing meteen aan
- de snelste inzending wint, wordt aan de keten geplakt, krijgt de prijs

Mini-quiz

Hebben we nu alle fundamentele problemen opgelost?

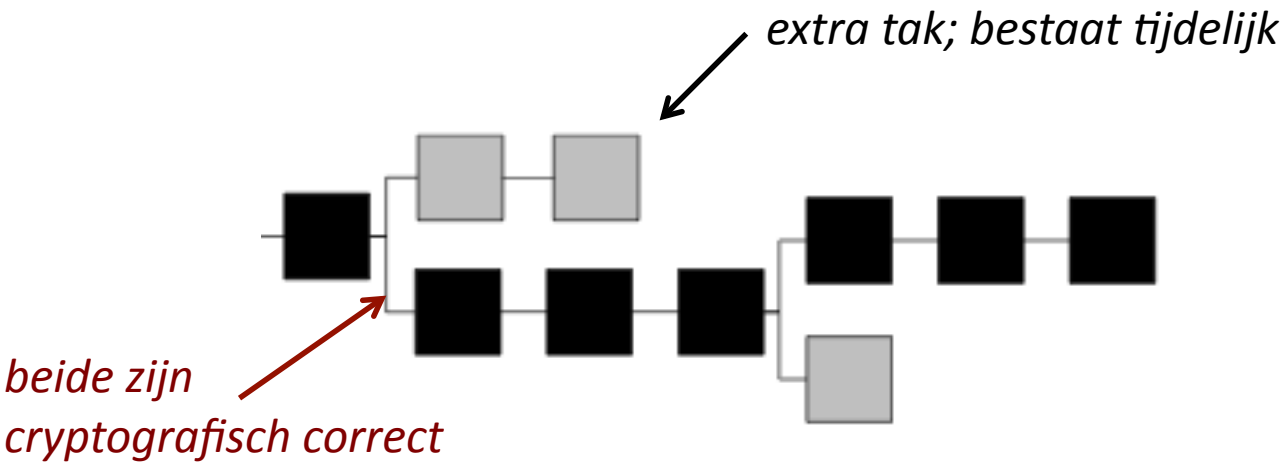
A. Jazeker

B. Absoluut niet

C. Definitely maybe

Probleem: vertakking

Vertakking
- Meerdere miners publiceren tegelijk een geldige oplossing



Consensus: verleng alleen aan de langste tak

Een niet-cryptografische oplossing!

Probleem: motivatie

Motivatie
- Handtekeningen checken is zwaar werk
- Waarom zou een miner jouw transactie in een blok opnemen?

Oplossing: transactiekosten
- Bij iedere transactie blijft er wat geld over
- Dit geld gaat naar de succesvolle miner

Alweer een niet-cryptografische oplossing!

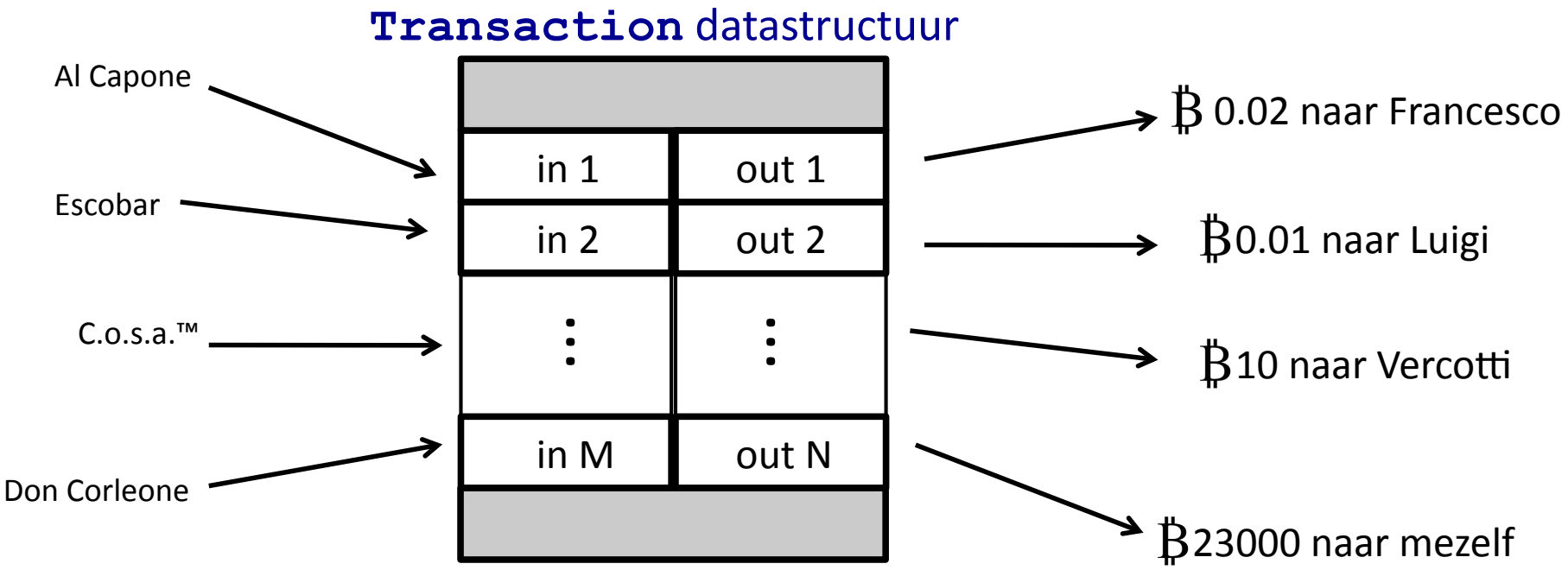
Bitcoin

We begrijpen nu de ontwerpprincipes.

Hoe ziet Bitcoin er precies uit?

- ~~**blokken**~~
- ~~**mining**~~
- **transacties**
- **scripts**
- **transactietypes**

Transacties



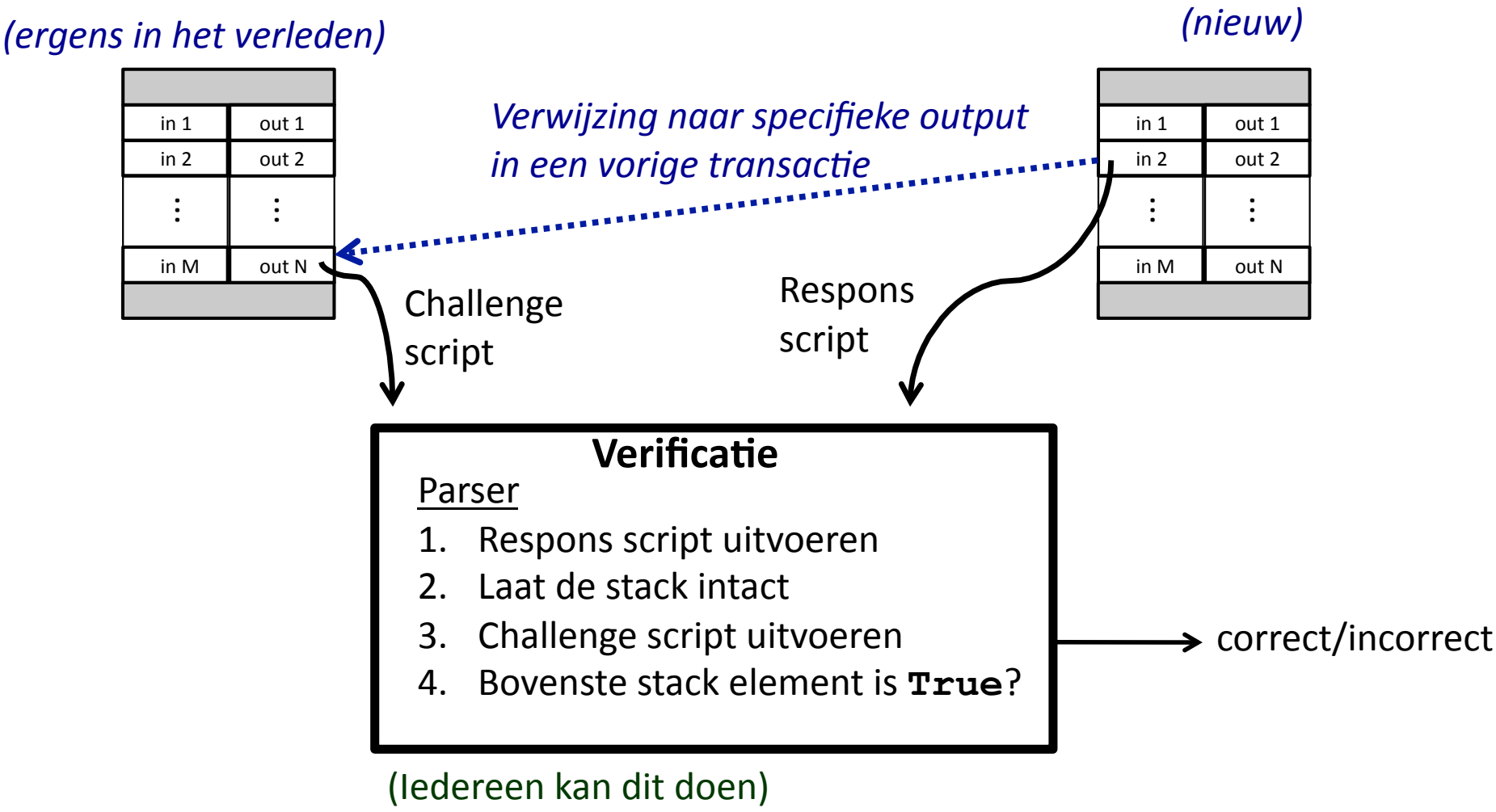
Transactiekosten: ***out < in***

"in" data:

- betalingen aan jou
  - kunnen meerdere publieke sleutels zijn
- iedere "in" bevat een bewijs van eigendom
  - handtekening
- iedere handtekening beslaat ook alle "out" data

BITCOIN
SPEC

Scripts



Standaard scripts

Beperkt aantal toegestane scripts

- Pay-to-Pubkey (P2PK)
- Pay-to-PubkeyHash (P2PKH) *[meest gebruikt]*
- Pay-to-ScriptHash (P2SH)
- Multisig

PubkeyHash adres

- alfanumeriek, 27-34 karakters
- hash van een publieke sleutel

Pay-to-PubkeyHash

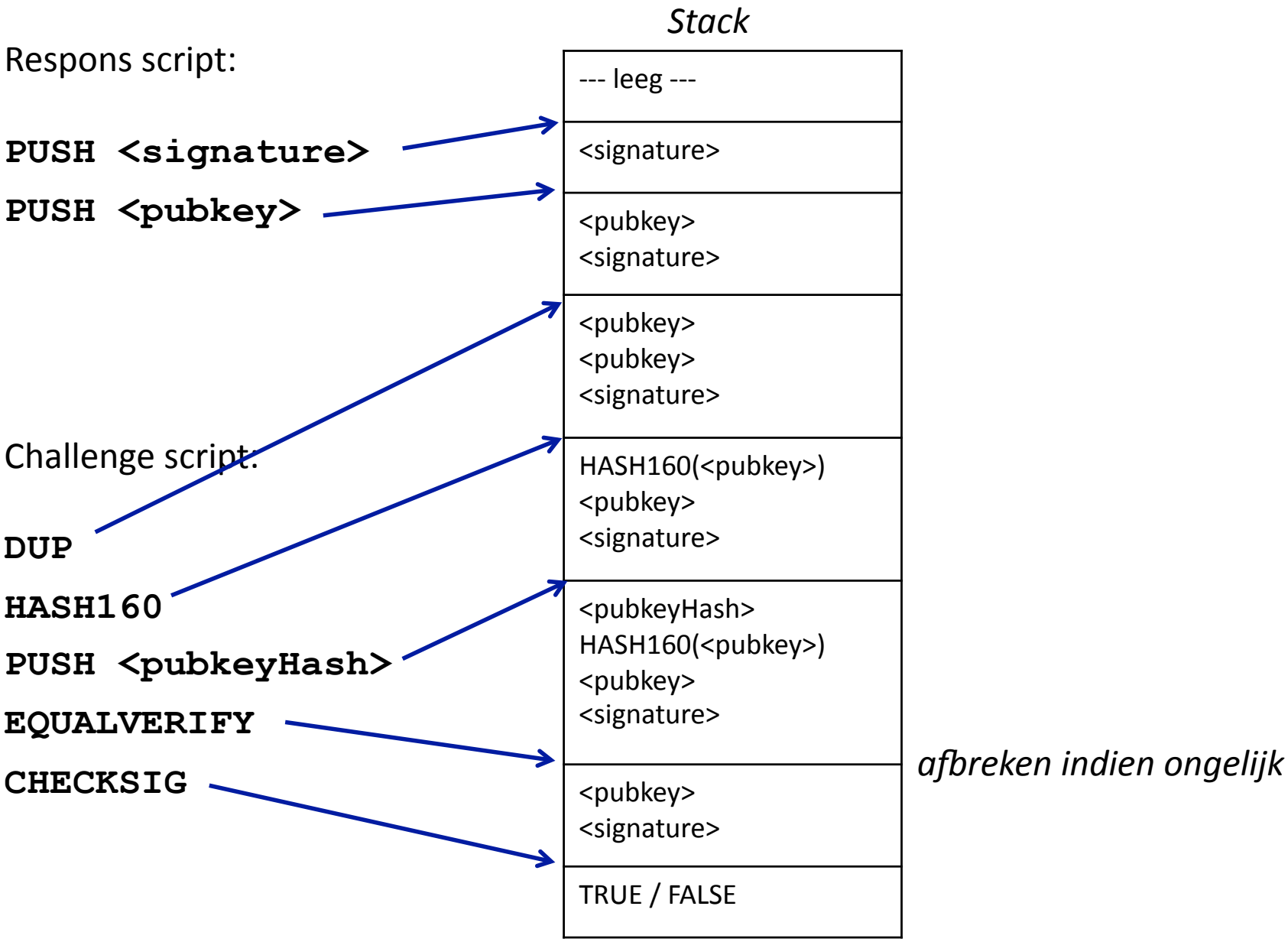
Respons script:

```
PUSH <signature>
PUSH <pubkey>
```

Challenge script:

```
DUP
HASH160
PUSH <pubkeyHash>
EQUALVERIFY
CHECKSIG
```

Pay-to-PubkeyHash



Multisig

m van de n partijen moeten tekenen

Respons script:

```
PUSH <sig_1>
...
PUSH <sig_m>
```

Challenge script:

```
PUSH m
PUSH <pubkey_1>
...
PUSH <pubkey_n>
PUSH n
CHECKMULTISIG
```

Multisig

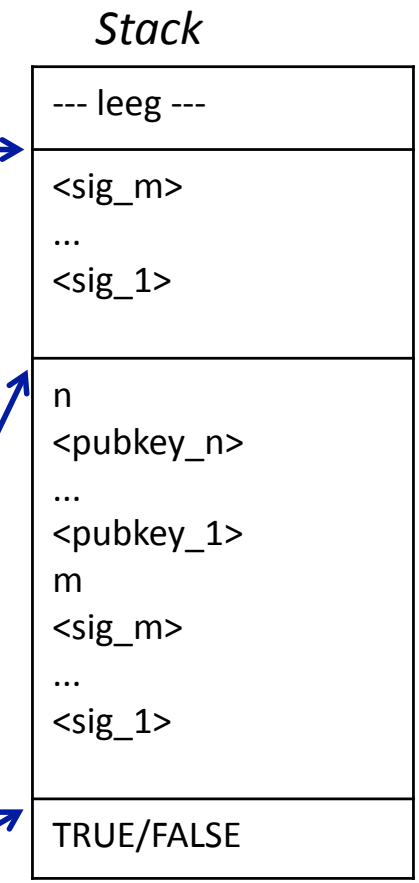
m van de n partijen moeten tekenen

Respons script:

```
PUSH <sig_1>
...
PUSH <sig_m>
```

Challenge script:

```
PUSH m
PUSH <pubkey_1>
...
PUSH <pubkey_n>
PUSH n
CHECKMULTISIG
```



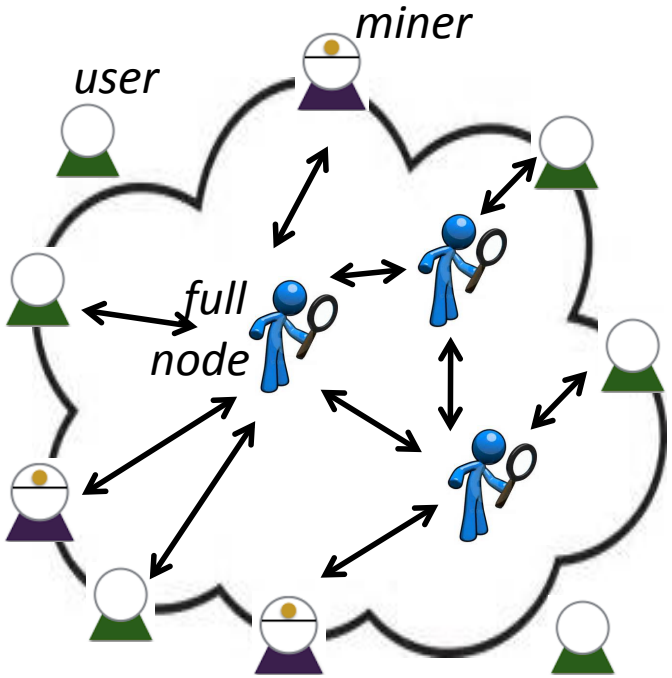
Denk niet in termen van bankrekeningen.

Collectief jongleren: grijp een bal en gooi ballen omhoog.
De blockchain bevat alle ballen die ooit in de lucht gegooid zijn.

Het netwerk

Bitcoin communicatie

- gewone deelnemer: lichtgewicht netpunt
  - weinig opslag, weinig checks
- volledig netpunt:
  - bevat complete blockchain (166 GB)
  - doet alle checks op transacties en blocks (crypto, consensusregels, double spending)
  - stuurt alleen correcte data door
- miners:
  - draaien typisch een volledig netpunt
  - kiezen welke transacties ze meenemen



Waarvoor worden hashfuncties gebruikt in Bitcoin?

Privacy
- tijdelijk verbergen van rekeningnummers

Eerlijke mining
- onvoorspelbare puzzels
- voor iedereen even moeilijk

Dingen aan elkaar knopen
- onbreekbare keten van transacties

Efficientie
- korte representatie van data

Een groots experiment

Bitcoin is in veel opzichten een groot succes

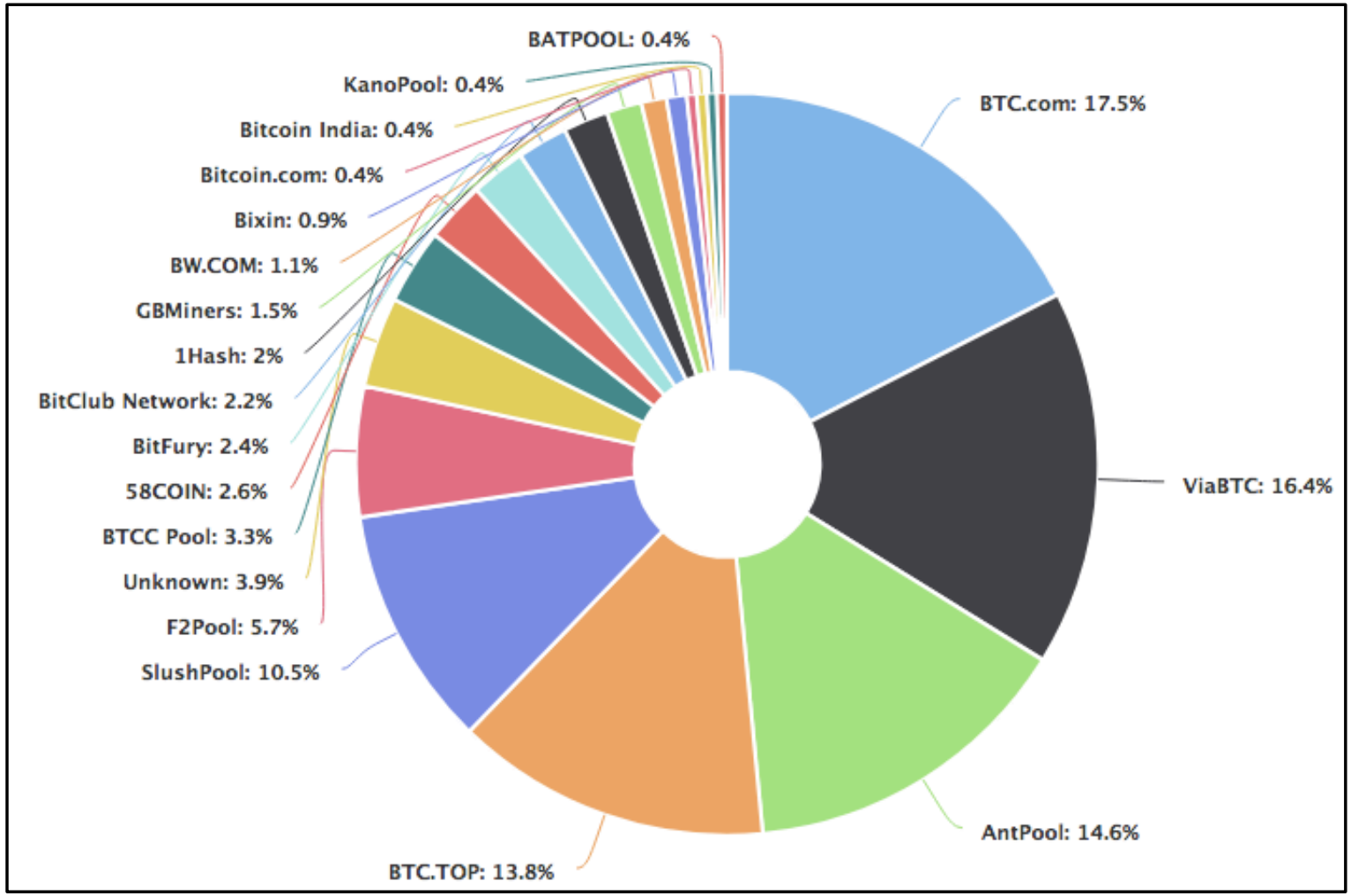
- eerste crypto-valuta
- goed doordachte&geïmplementeerde crypto
- mechanisme voor tijdelijke autoriteit
- mechanisme om nieuw geld aan te maken
- goed gebalanceerde prikkels
- onvervalsbaar
- zeer populair (en gehype't)
- steeds meer regelgeving

WIJZE
LESSEN

Decentralisatie?

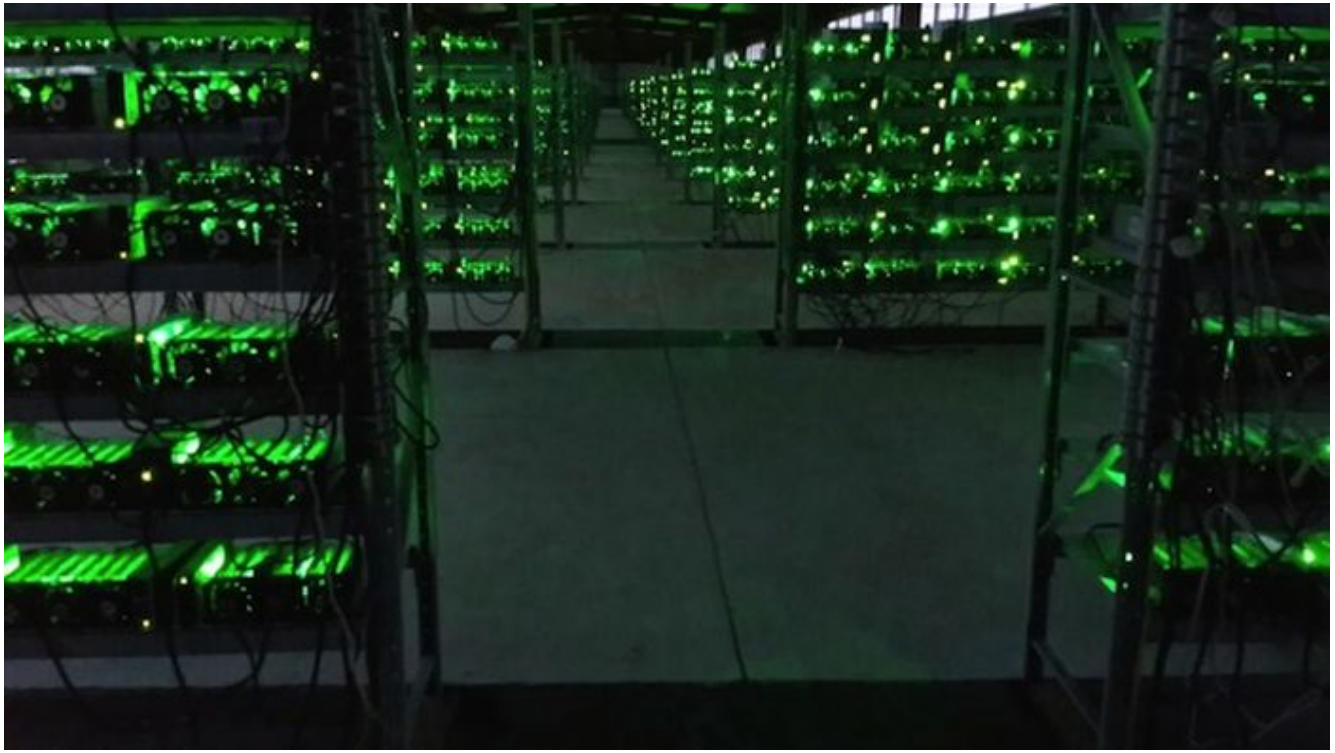
Wie heeft het mining-vermogen?

- **In 2014 had ghash.io bijna 50%**
- **Juni 2017: Mining in China 71%**



https://blockchain.info/pools

GROOTSCHALIGE MINING

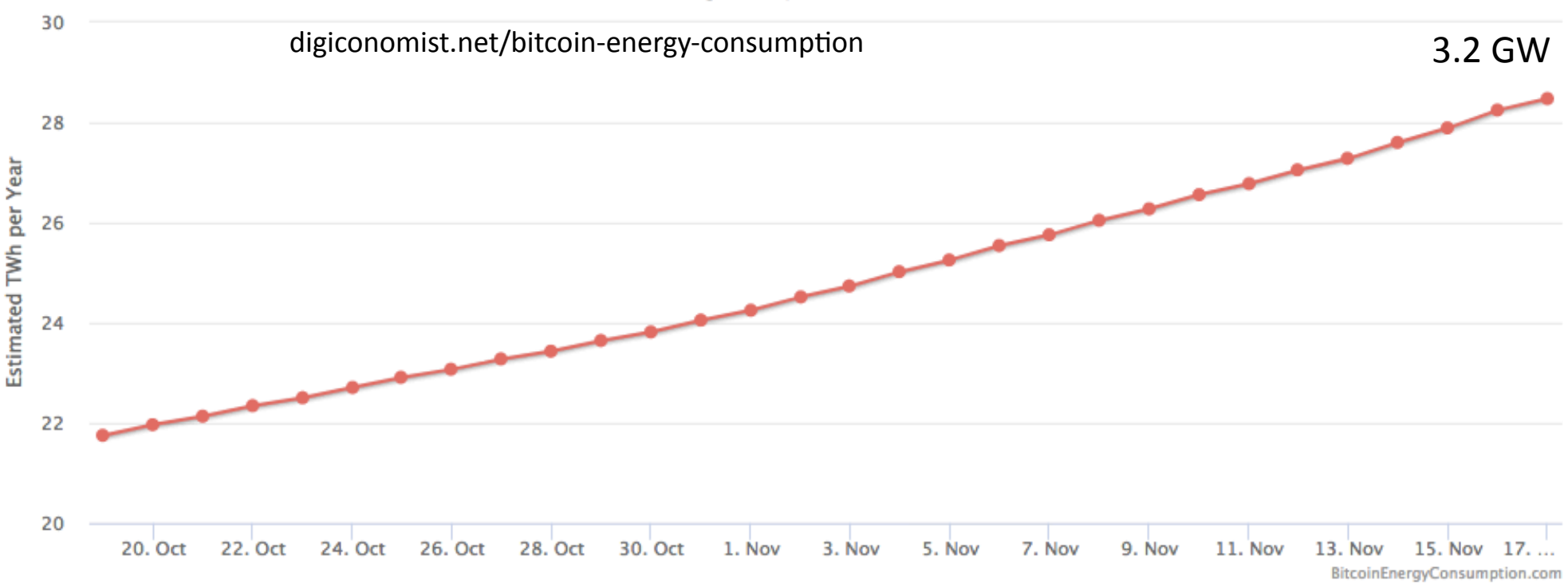


WIJZE LESSEN

Het grote mining probleem

digiconomist.net/bitcoin-energy-consumption

3.2 GW



Annualized global mining revenues	$7,676,196,838
Annualized estimated global mining costs	$1,423,794,674
Country closest to Bitcoin in terms of electricity consumption	Slovak Republic
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.13%
Number of U.S. households that could be powered by Bitcoin	2,636,657
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	9.36

Alternatieven voor mining

(Bewijs van belang) "Proof of stake"

Opties:

- loterij
  - alleen "actieve" accounts doen mee
  - kans evenredig met totaalbezit of leeftijd van de coins
- stemmen

Andere valuta's (inmiddels vele)

ETHEREUM

- gewone accounts
- contract-accounts. ("agents")
- elk contract-account heeft executeerbare code en een toestand
- transactie naar contract-account
  - wordt uitgevoerd door het contract
  - toestand verandert
  - nieuwe toestand komt in de blockchain
  - betaling nodig ("gas") voor executie
- hash functie die lastig in hardware te implementeren is

ZCASH

- veel betere anonimiteit
- "zero knowledge" crypto

Ander gebruik van blockchains

Namecoin

- 2010
- eerste aftakking van bitcoin
- DNS naamregistratie tegen betaling
- top-level-domain ".bit", onafhankelijk van ICANN
- geldigheidsduur 200 dagen

Guardtime

- 2007, Estonia
- "Keyless Signature Infrastructure"
- dagtekening en integriteit van digitale documenten

Afsluitende opmerkingen

Crypto-valuta

- bijzondere nieuwe toepassing van cryptografie
- Bitcoin, de eerste, is uitzonderlijk goed ontworpen
- mining vreet energie
- we zullen in de toekomst een hoop verbeteringen zien

Blockchain in het algemeen

- gedecentraliseerde datastructuur
- alternatief voor Certificatie-Autoriteiten