

# Future-proof Tester: Blockchain

Hoe ga je als tester om met blockchain?

# Wat we gaan doen:

Wat is  
blockchain?

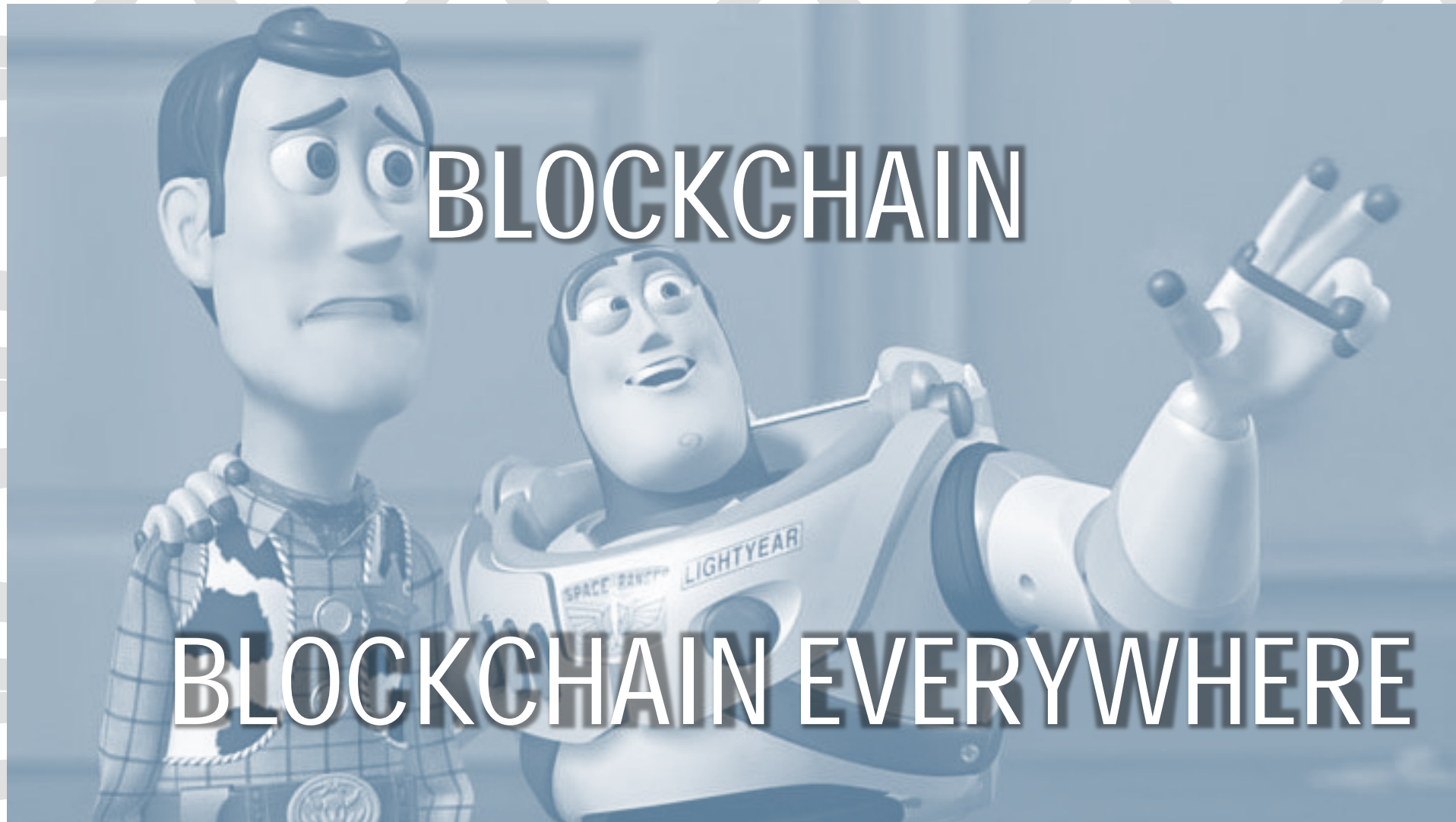
De juiste  
vragen over  
blockchain  
toepassingen

De DAO  
Hack

Wat is een  
smart  
contract?

Hoe test je  
blockchain?  
4 tier  
approach

**Krijg ik hier als tester mee te maken?**



# Waar het voor mij begon: 2012





# De belangrijkste concepten

Digitale handtekeningen

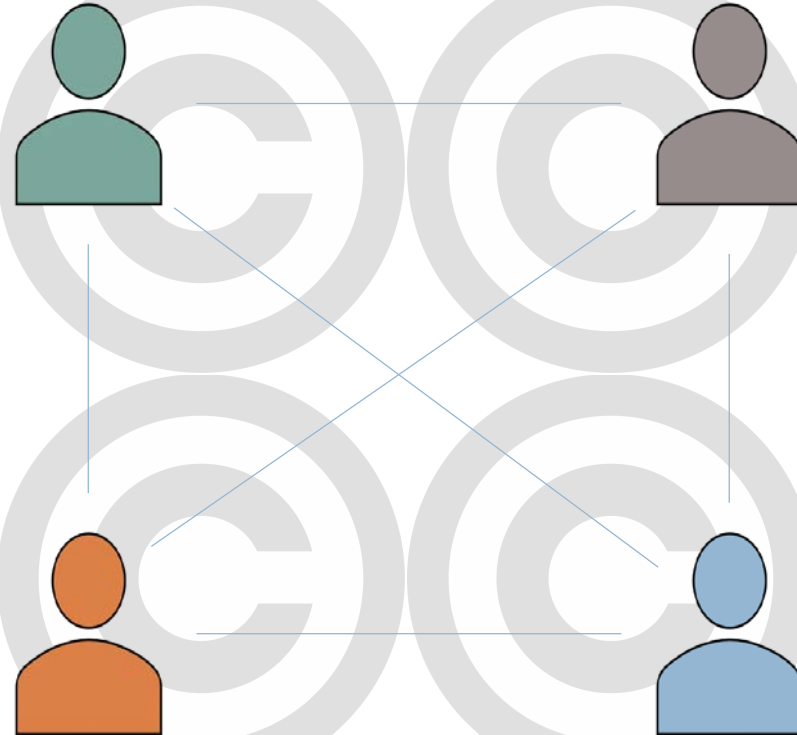
De transactie geschiedenis

Gedecentraliseerd

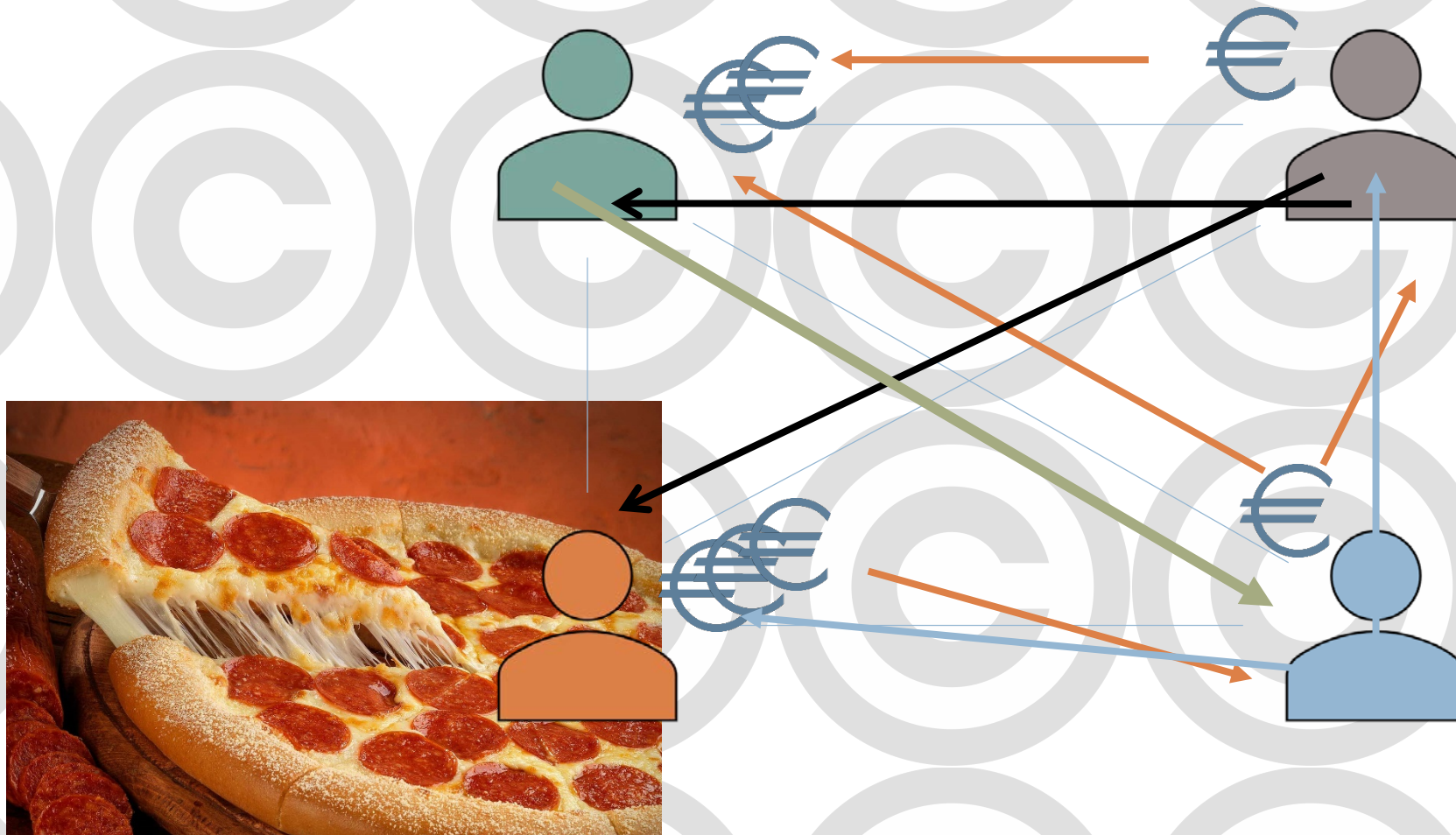
Proof of Work

Blockchain

# Boekhouding en transacties



# Pizza sessie(s) – wie betaalt wat?



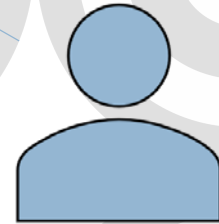
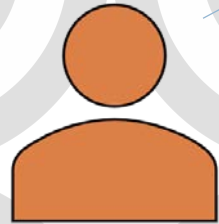
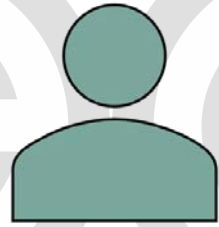
# Boekhouden – gedeeld xls op SharePoint





# Boekhouden – gedeeld xls op SharePoint





| Betaler | Ontvanger | Bedrag |
|---------|-----------|--------|
| Groen   | Rood      | 20     |
| Geel    | Blauw     | 50     |
| Blauw   | Groen     | 5      |
| Grijs   | Geel      | 25     |

# Afspraken voor de gedeelde Excel

- Iedereen mag regels toevoegen
- Aan het einde van de maand wordt door iedereen (in echte euro's) afgerekend.

PROTOCOL



# Eerste probleem: iedereen mag regels toevoegen

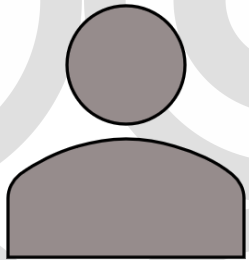
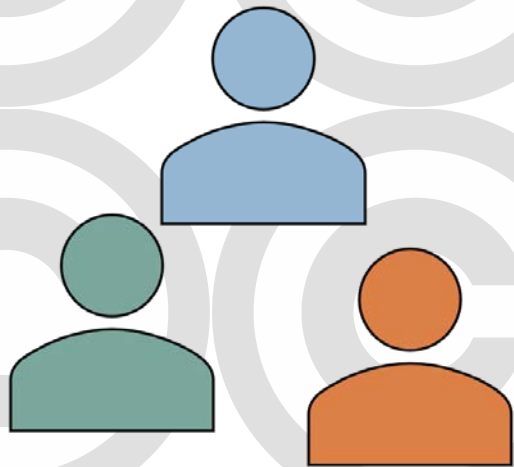
| Betaler | Ontvanger | Bedrag |
|---------|-----------|--------|
| Groen   | Grijs     | 20     |
| Geel    | Blauw     | 50     |
| Blauw   | Groen     | 5      |
| Grijs   | Geel      | 25     |
| Grijs   | Groen     | 100    |





| Betaler | Ontvanger | Bedrag | Handtekening |
|---------|-----------|--------|--------------|
| Groen   | Rood      | 20     | <i>Groen</i> |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |

Digitale  
Handtekeningen  
*Grijs* 01001100...



# Wat voorkomt het kopiëren van een digitale handtekening?

▪ *Grijs* 01001100...

▪ **COPY + PASTE?**

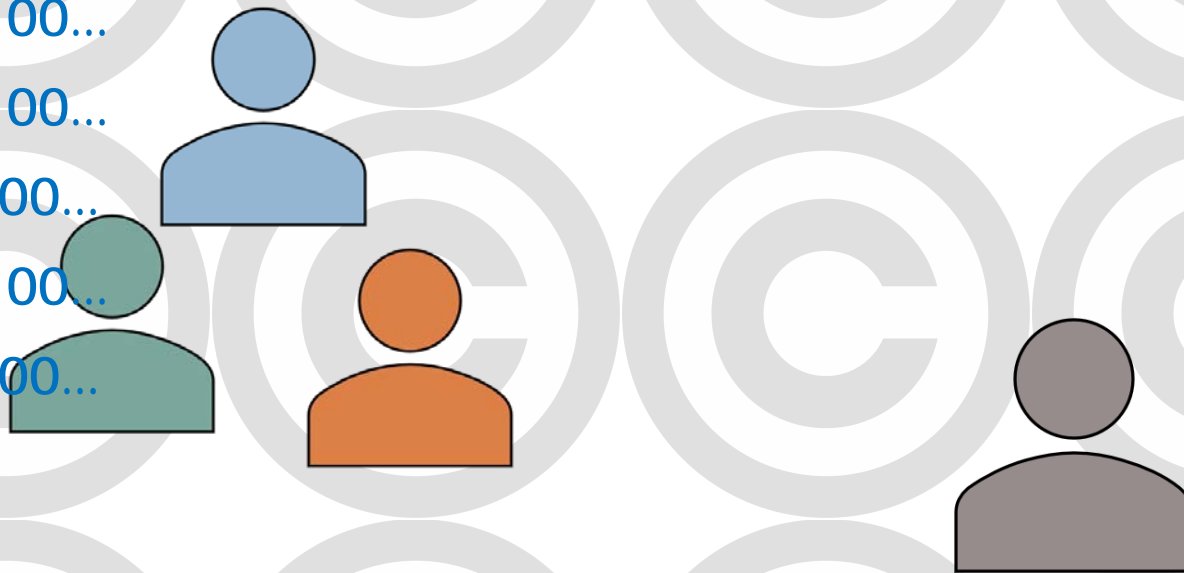
▪ *Grijs* 01001100...

▪ *Grijs* 01001100...

▪ *Grijs* 01001100...

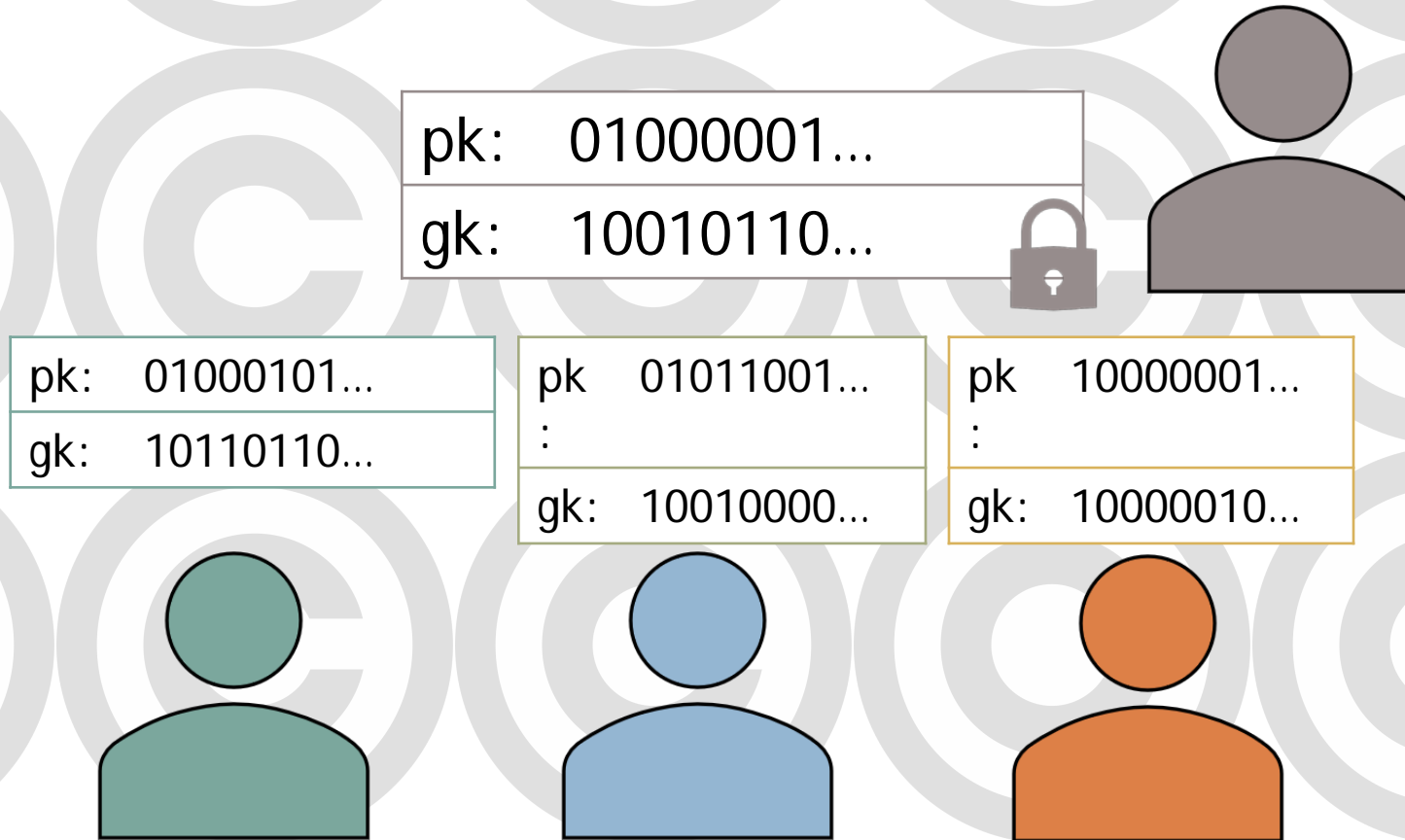
▪ *Grijs* 01001100...

▪ *Grijs* 01001100...



# Public key / Private keys\*

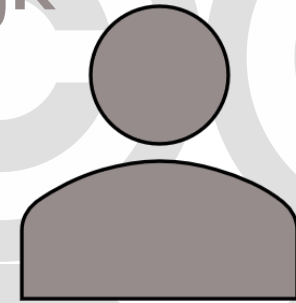
- (private key noemen we voor het gemak even geheime key) gk



# In tegenstelling tot op papier verandert je handtekening per bericht

- $\text{Sign}(\text{message}, gk) = \text{signature}$
- $\text{Verify}(\text{message}, \text{signature}, pk) = \text{T/F}$

$\text{Verify}(\text{Message}, 256 \text{ bit signature}, pk) = \text{True}$   
alleen als dit ook overeenkomt met de  $gk$





```
11110001101001110011111000100010
00000100101000010001010000000111
01111111100110001000110010011101
1010100110001101011111110001011
01100000010010101011001001010000
01001001011011110010010110101110
10110011110010111101000101010011
11110101001101101001110010000011
```



**Verify (Message, 256 bit signature, pk) = True**



gk: 10010110..

# Tweede probleem: dezelfde regel meerdere keren vastleggen

| Betaler | Ontvanger | Bedrag | Handtekening         |
|---------|-----------|--------|----------------------|
| Grijs   | Groen     | 100    | <b>0010010011...</b> |
| Grijs   | Groen     | 100    | 0010010011...        |
| Grijs   | Groen     | 100    | 0010010011...        |
| Grijs   | Groen     | 100    | 0010010011...        |



# Tweede probleem: oplossing MessageID toevoegen

| MessageID | Betaler | Ontvanger | Bedrag | Handtekening               |
|-----------|---------|-----------|--------|----------------------------|
| 1         | Groen   | Rood      | 100    | 0010010011...              |
| 2         | Groen   | Rood      | 100    | Nieuwe unieke handtekening |
| 3         | Groen   | Rood      | 100    | 1001100110...              |
| 4         | Groen   | Rood      | 100    | 0011110010...              |



# PROTOCOL

- Iedereen mag regels toevoegen
- Aan het einde van de maand wordt door iedereen (in echte euro's) afgerekend.
- Alleen regels met een geldige handtekening worden opgenomen.



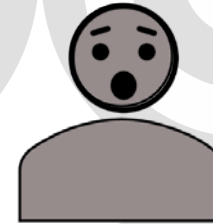
# Derde probleem: wordt er maandelijks wel echt afgerekend?

| MessageID | Betaler | Ontvanger | Bedrag | Handtekening  |
|-----------|---------|-----------|--------|---------------|
| 1         | Groen   | Grijs     | 20     | 0010010011... |
| 2         | Groen   | Grijs     | 20     | 1001011100... |
| 3         | Groen   | Grijs     | 20     | 1001100110... |
| 4         | Groen   | Grijs     | 20     | 0011110010... |

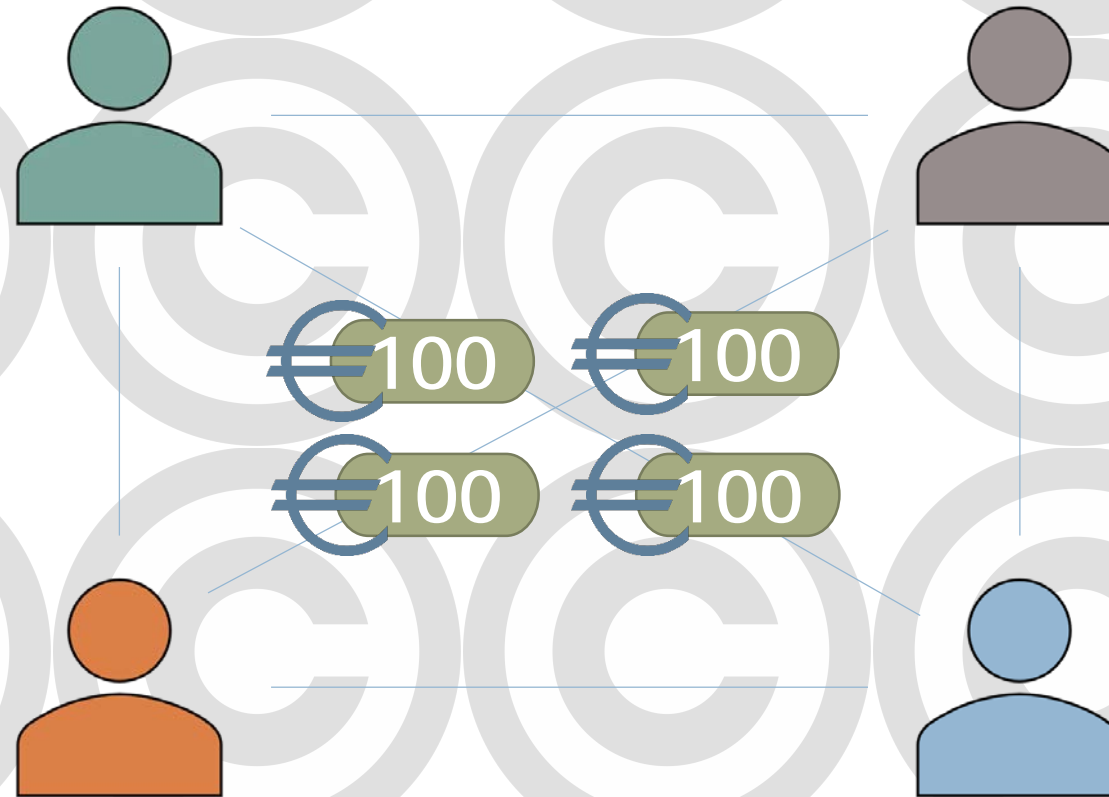
Ik betaal niks!



Hey!



# Derde probleem: oplossing (deel 1) eerst allemaal evenveel inleggen



# Probleem 3: oplossing (deel 2)

- Niemand mag meer uitgeven dan ze bezitten volgens de regels in de gedeelde excel

| MessageID | Betaler | Ontvanger | Bedrag | Handtekening         |
|-----------|---------|-----------|--------|----------------------|
| 1         |         | Rood      | 100    | <b>0010010011...</b> |
| 2         |         | Groen     | 100    | 1001011100...        |
| 3         |         | Geel      | 100    | 1001100110...        |
| 4         |         | Blauw     | 100    | 0011110010...        |
| 5         | Rood    | Groen     | 120    | 0110000001...        |

# PROTOCOL

- Iedereen mag regels toevoegen
- ~~Aan het einde van de maand wordt door iedereen (in echte euro's) afgerekend.~~
- Iedereen legt eerst 100 euro in, en niemand mag meer uitgeven dan ze 'bezitten' volgens de regels in de excel.
- Alleen regels met een geldige handtekening worden opgenomen.

# Dit vereist ook dat je transacties gaat bewaren

- Omdat je wil weten dat er niet meer wordt uitgegeven dan is toegestaan moet je de geschiedenis van alle transacties bijhouden.

| MessageID | Betaler | Ontvanger | Bedrag | Rood heeft: |
|-----------|---------|-----------|--------|-------------|
| 1         |         | Grijs     | 100    | 100 ✓       |
| 2         |         | Groen     | 100    |             |
| 3         |         | Geel      | 100    |             |
| 4         |         | Blauw     | 100    |             |
| 5         | Grijs   | Groen     | 50     | 50 ✓        |
| 6         | Grijs   | Blauw     | 50     | 0 ✓         |
| 7         | Grijs   | Geel      | 20     | -20 ✗       |

# ...verbinding met euro's vervaagt onderling afrekenen in Excelcoin

| MessageID | Betaler | Ontvanger | Bedrag | Excelcoin |
|-----------|---------|-----------|--------|-----------|
| 104       | Geel    | Rood      | 75     | 75        |
| 105       | Rood    | Groen     | 100    | 100       |
| 106       | Groen   | Geel      | 95     | 95        |
| 108       | Rood    | Paars     | --     | 50        |

Je kan immers Pizza kopen met Excelcoin



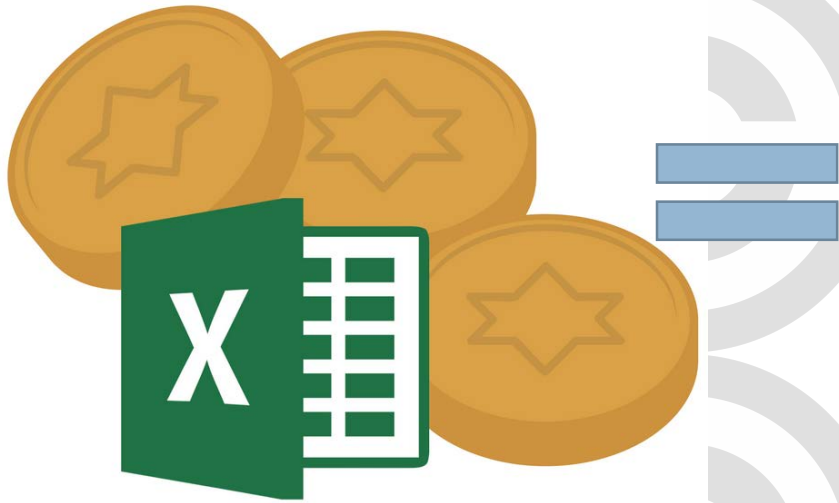


# Euro's omwisselen voor Excelcoin

| MessageID | Betaler | Ontvanger | Bedrag | Excelcoin |
|-----------|---------|-----------|--------|-----------|
| 104       | Geel    | Rood      | 75     | 75        |
| 105       | Rood    | Groen     | 100    | 100       |
| 106       | Groen   | Geel      | 95     | 95        |
| 108       | Rood    | Paars     | --     | 50        |

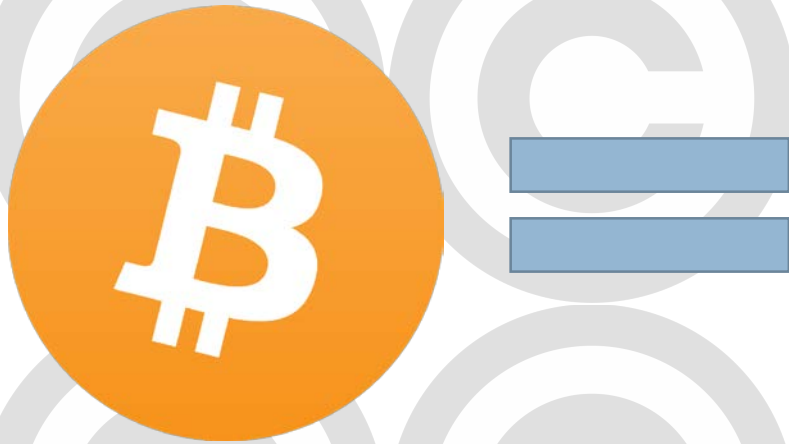


# Excelcoin is nu een cryptovaluta



| ID  | Betaler | Ontvanger | Excelcoin |
|-----|---------|-----------|-----------|
| 104 | Geel    | Rood      | 75        |
| 105 | Rood    | Groen     | 100       |
| 106 | Groen   | Geel      | 95        |
| 108 | Rood    | Paars     | 50        |

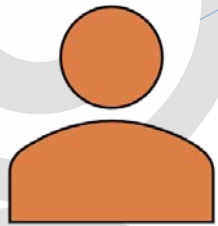
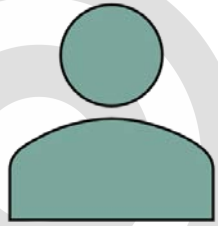
# Blockchain heeft te maken met opslag van de transactie geschiedenis



| Betaler | Ontvanger | Bedrag | Handtekening |
|---------|-----------|--------|--------------|
| Groen   | Rood      | 20     | <i>Groen</i> |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |

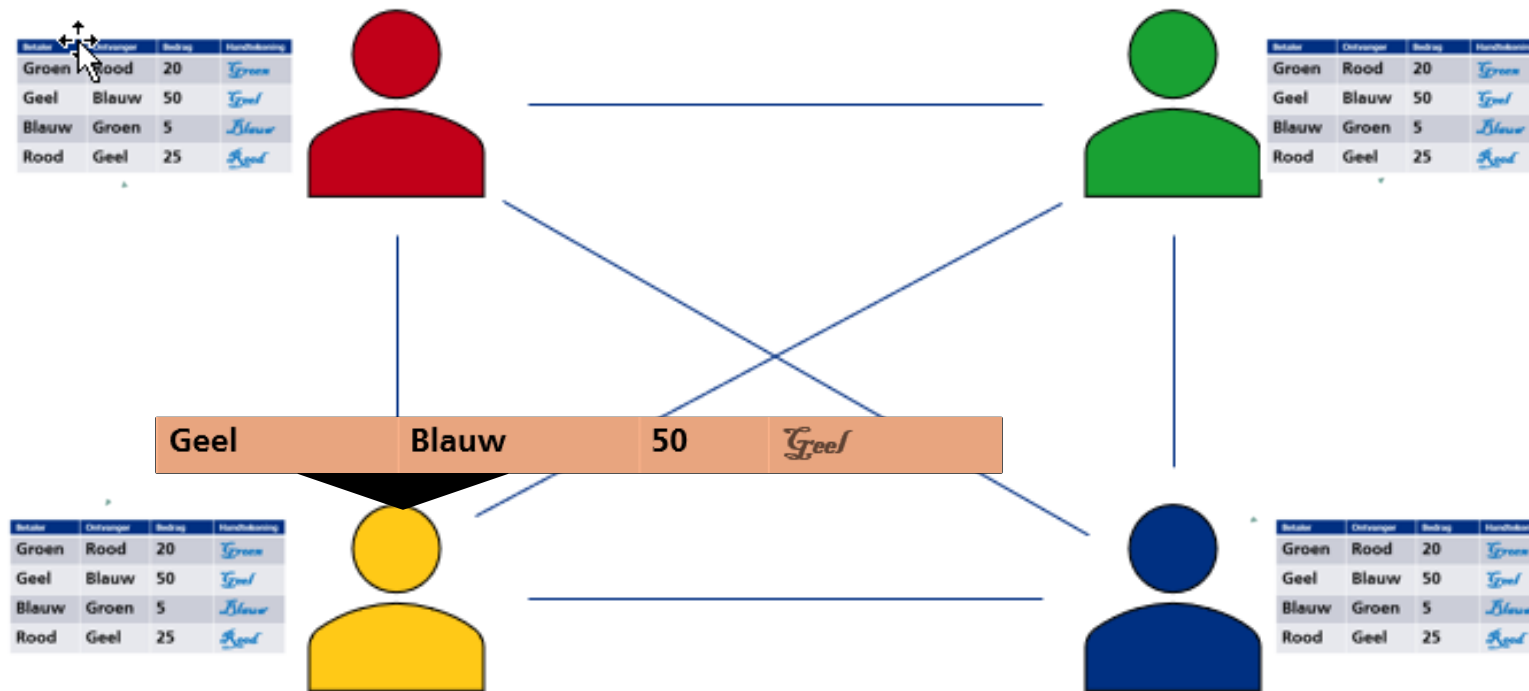
# In dit voorbeeld is er nog 1 groot verschil tussen Bitcoin en Excelcoin...

- Location, location, location

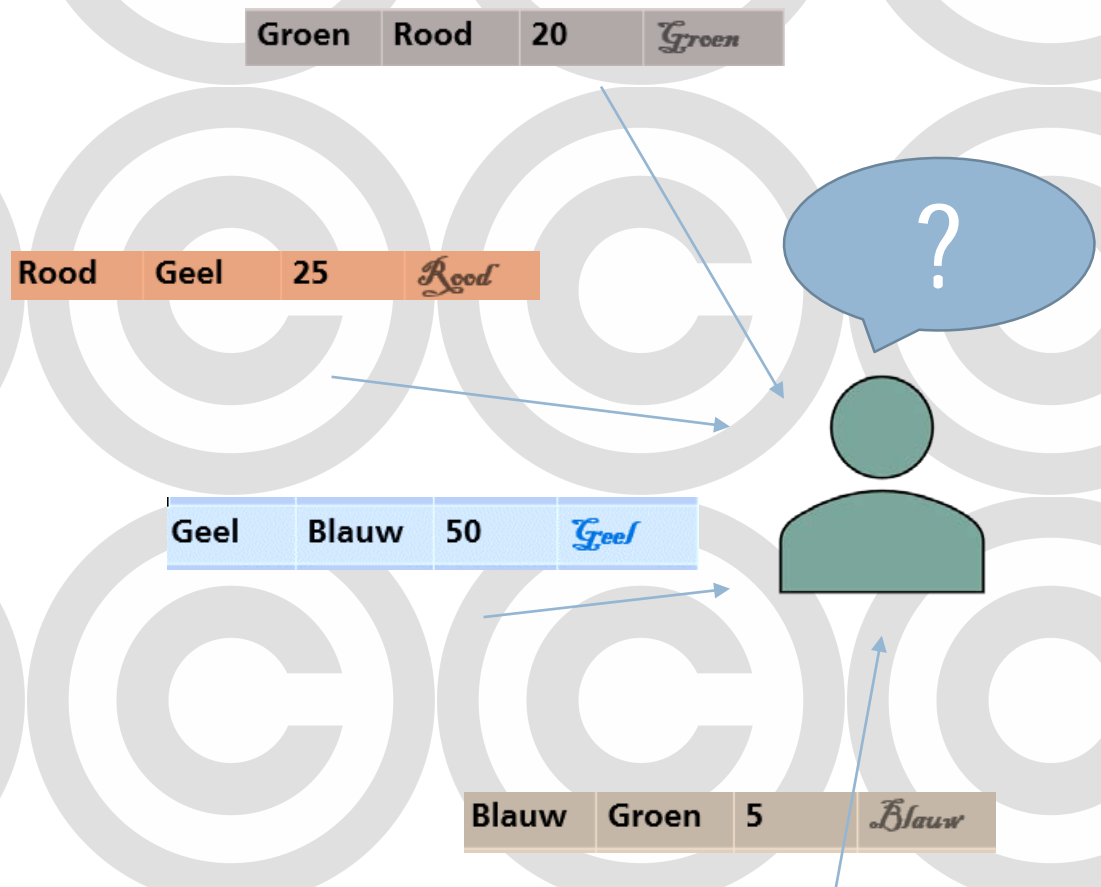


**CENTRAAL  
OPGESLAGEN**

# Gedistribueerde boekhouding transacties



# Probleem 4: Hoe weet je dat wat je aan transacties ontvangt hetzelfde is als de anderen?



| Betaler | Ontvanger | Bedrag | Handtekening |
|---------|-----------|--------|--------------|
| Groen   | Rood      | 20     | <i>Groen</i> |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |
| Groen   | Rood      | 20     | <i>Groen</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |



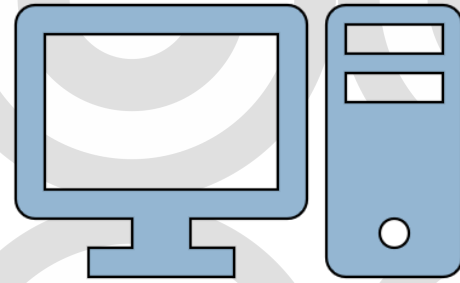
# PROTOCOL

- Iedereen mag regels toevoegen mits ze publiekelijk gedeeld worden
- Niemand mag meer uitgeven dan ze bezitten.
- Alleen regels met een geldige handtekening worden opgenomen.

▪ BITCOIN WHITEPAPER

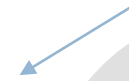
# Bitcoin protocol: Geloof de boekhouding waar het meeste rekenwerk in zit.

| Betaler | Ontvanger | Bedrag | Handtekening |
|---------|-----------|--------|--------------|
| Groen   | Rood      | 20     | <i>Groen</i> |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |
| Groen   | Rood      | 20     | <i>Groen</i> |
| Rood    | Geel      | 25     | <i>Rood</i>  |
| Geel    | Blauw     | 50     | <i>Geel</i>  |
| Blauw   | Groen     | 5      | <i>Blauw</i> |



# Cryptografische Hash Functies

HASH



```
11001010111100010010111000011011
11000101101010010110001011011110
11000001110100000110010100111001
11111110111100000001111100110110
00110110000011100000101011110010
00101001100000000011101110011110
10010001010000011100001001001100
10001011111011010101010001110000
```

SHA-256(*message/file*)=

Inverse bijna onmogelijk

# Bitcoin protocol

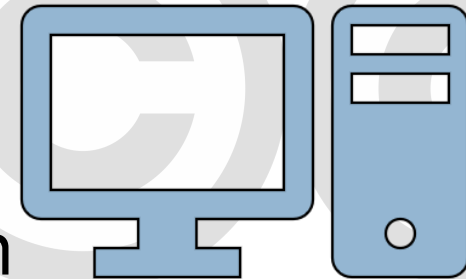
## PROOF OF WORK

30 nullen

| 1234567809 |           |        |              |
|------------|-----------|--------|--------------|
| betaler    | ontvanger | bedrag | handtekening |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |

SHA-256

```
000000000000000000000000000000000000000000000000000000000000000000000000000000000000011  
11000101101010010110001011011110  
11000001110100000110010100111001  
11111110111100000001111100110110  
00110110000011100000101011110010  
00101001100000000011101110011110  
10010001010000011100001001001100  
1000101111101101010101010001110000
```



Rekenwerk via een  
cryptografisch hash functie

# Blocks

| 1234567809 |           |        |              |
|------------|-----------|--------|--------------|
| Betaler    | Ontvanger | Bedrag | Handtekening |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |

| 1230067809 |           |        |              |
|------------|-----------|--------|--------------|
| Betaler    | Ontvanger | Bedrag | Handtekening |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |

| 1034547809 |           |        |              |
|------------|-----------|--------|--------------|
| Betaler    | Ontvanger | Bedrag | Handtekening |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Groen      | Rood      | 20     | <i>Groen</i> |
| Rood       | Geel      | 25     | <i>Rood</i>  |
| Geel       | Blauw     | 50     | <i>Geel</i>  |
| Blauw      | Groen     | 5      | <i>Blauw</i> |

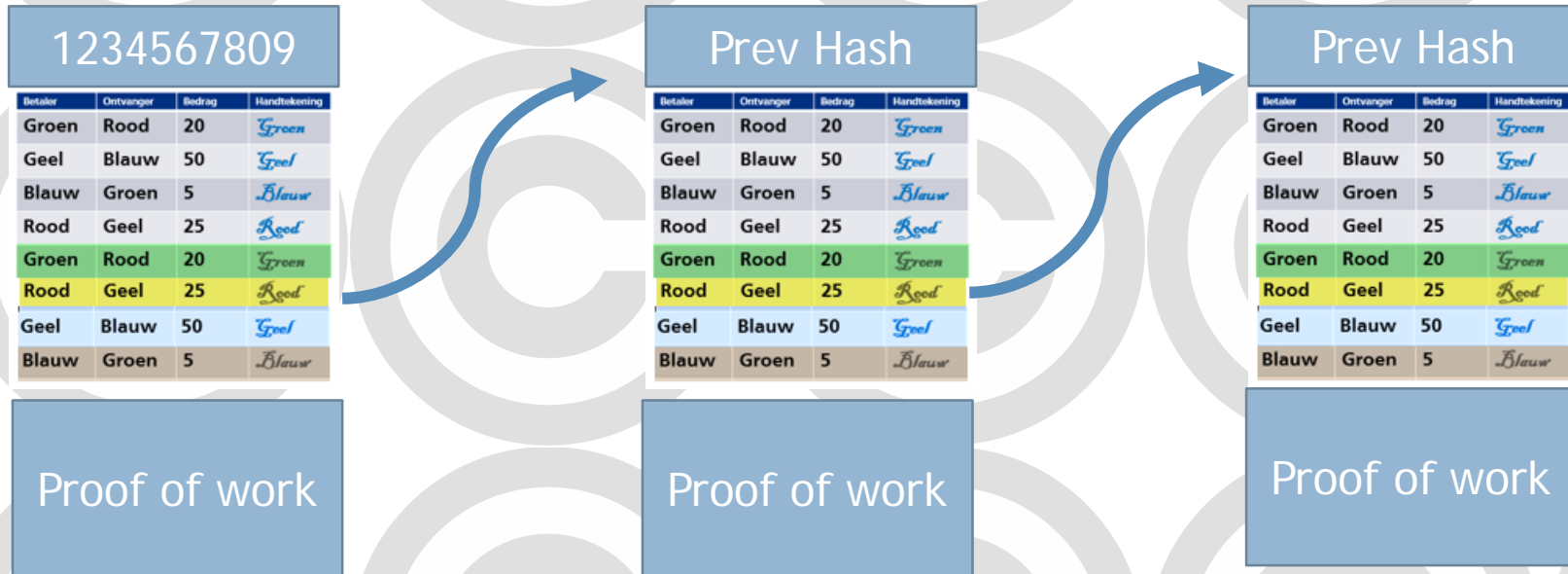
SHA-256

```
11001010111100010010111000011011
110001011010100101100010110111110
11000001110100000110010100111001
11111110111100000001111100110110
00110110000011100000101011110010
00101001100000000011101110011110
10010001010000011100001001001100
10001011111011010101010001110000
```

Proof of work

Proof of work

# Blockchain

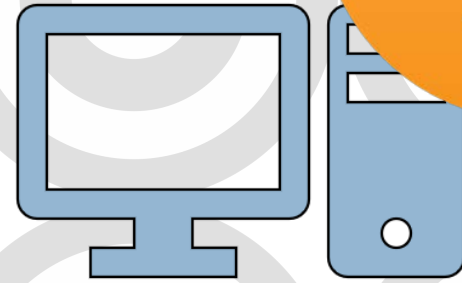




# Bitcoin beloning voor rekenwerk (aka mining reward)

| Prey Hash |           |        |              |
|-----------|-----------|--------|--------------|
| Beleider  | Ontvanger | Bedrag | Handtekening |
| Groen     | Rood      | 20     | Groen        |
| Geel      | Blauw     | 50     | Geel         |
| Blauw     | Groen     | 5      | Blauw        |
| Rood      | Geel      | 25     | Rood         |
| Groen     | Rood      | 20     | Groen        |
| Rood      | Geel      | 25     | Rood         |
| Geel      | Blauw     | 50     | Geel         |
| Blauw     | Groen     | 5      | Blauw        |

Proof of work



12,5 bitcoin

# Zo ziet dat er in het echt uit



# Bitcoin nodes aka bitcoin's

re

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Feb 22 2018  
16:25:01 GMT+0100 (Central Europe Standard Time).

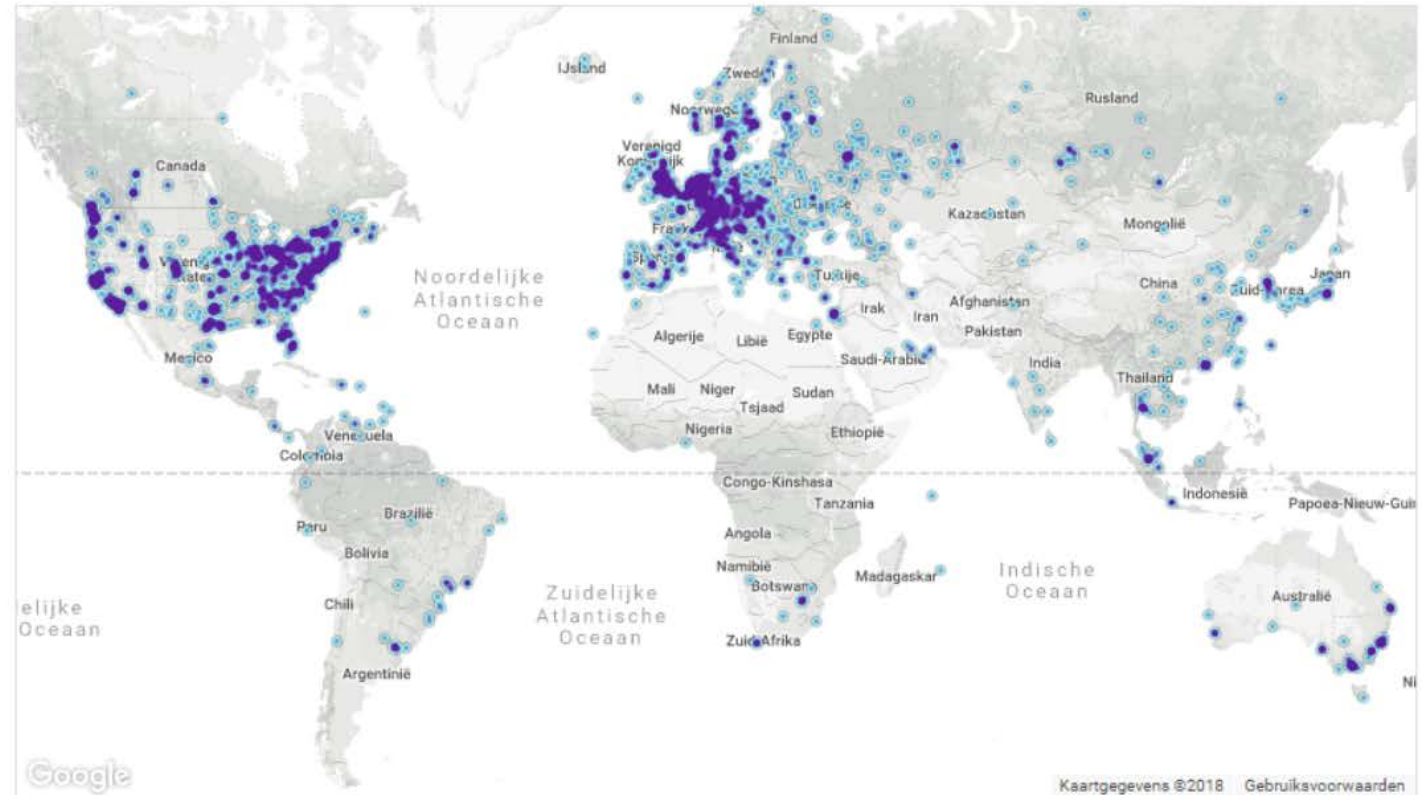
### 11364 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY            | NODES         |
|------|--------------------|---------------|
| 1    | United States      | 2888 (25.41%) |
| 2    | Germany            | 2059 (18.12%) |
| 3    | China              | 927 (8.16%)   |
| 4    | France             | 746 (6.56%)   |
| 5    | Netherlands        | 518 (4.56%)   |
| 6    | Canada             | 431 (3.79%)   |
| 7    | Russian Federation | 381 (3.35%)   |
| 8    | United Kingdom     | 378 (3.33%)   |
| 9    | n/a                | 289 (2.54%)   |
| 10   | Japan              | 222 (1.95%)   |

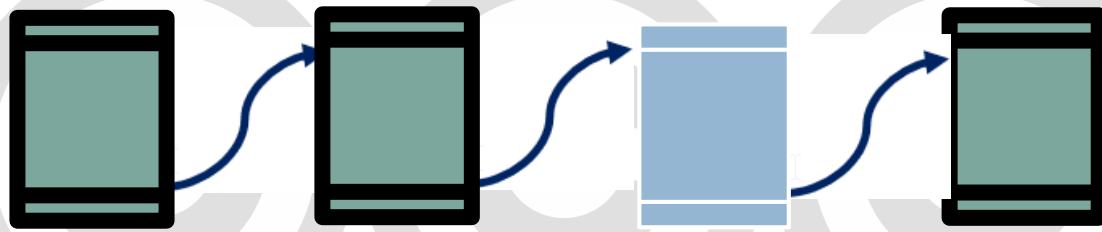
More (104) »



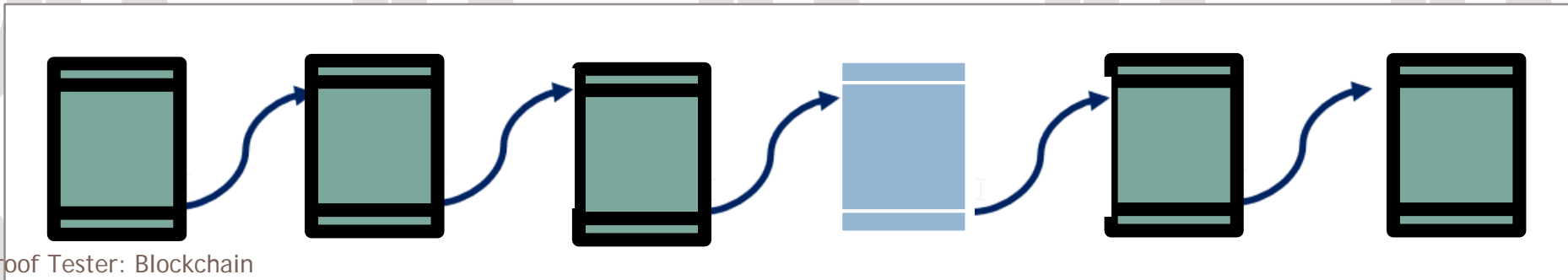
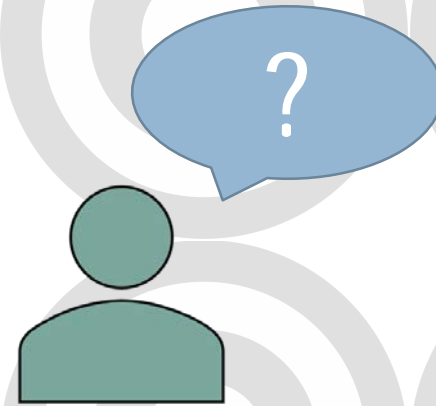
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

# Nog één toevoeging: de waarheid zit in de langste ketting



CONFLICT?







# PROTOCOL

- Iedereen mag regels toevoegen mits ze publiekelijk gedeeld worden
- Niemand mag meer uitgeven dan ze bezitten.
- Alleen regels met een geldige handtekening worden opgenomen.
- **Vertrouw de bloks met het meeste rekenwerk**
- **Vertrouw de langste ketting blokken**
- **Is er geen langste blok? Wacht dan tot er één de langste is**

# Samenvattend de belangrijkste concepten

- Digitale handtekeningen
- De transactie geschiedenis op de blockchain, de token is de cryptovaluta
- Gedecentraliseerd
- Proof of Work
- Block Chains



# Cryptovaluta & Blockchain

Token

(Excelcoin of Bitcoin)

Blockchain protocol

Blockchain

# Ethereum: Smart contracts

- Op Ethereum heten dit decentralized Apps (dApps)
- Bij de message komt een stuk code die ook wordt uitgevoerd bij het uitrekenen van een block.

| MessageID | Betaler | Ontvanger | Ether | Smart contract |
|-----------|---------|-----------|-------|----------------|
| 104       | Geel    | Rood      | 75    | Code           |
| 105       | Rood    | Groen     | 100   | Code           |
| 106       | Groen   | Geel      | 95    | Code           |
| 108       | Rood    | Groen     | 50    | Code           |

# Cryptovaluta + Smart Contract

dAPP

Token

Blockchain protocol


Blockchain

# Private Blockchains



**DIGITAL ASSET HOLDINGS**

accenture IBM BNP PARIBAS  
Goldman Sachs DTCC ABN-AMRO  
ASX PNC ICAP citi  
CME Group J.P.Morgan Broadridge  
Santander InnoVentures



**HYPERLEDGER PROJECT**

accenture ANZ London Stock Exchange IBM bloq  
STATE STREET Digital Asset Holdings r3. SBERBANK WELLS FARGO  
BNP PARIBAS DTCC BLOCKCHAIN Broadridge  
CME Group SWIFT J.P.Morgan  
BNY MELLON CISCO



**R3 CEV**

Bank of America Nordea RBC ACORD RBS UBS  
Hana Financial Group INTESA SANPAOLO  
SMBC SUMITOMO MITSUI BANKING CORPORATION BMO Financial Group  
Danske Bank MIZUHO BNP PARIBAS  
ING ING VYSYA BANK WELLS FARGO SOCIETE GENERALE BBVA BARCLAYS  
CommonwealthBank Deutsche Bank Westpac citi  
THOMSON REUTERS HSBC MUFG TD Bank J.P.Morgan  
BNY MELLON Scotiabank CREDIT SUISSE



**RIPPLE**

CIBC  
Standard Chartered  
nab UBS  
Westpac Santander  
UniCredit Group ATB Financial



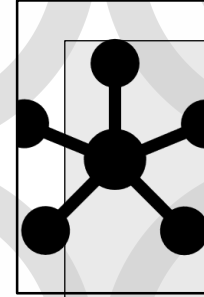
# Testing Blockchain



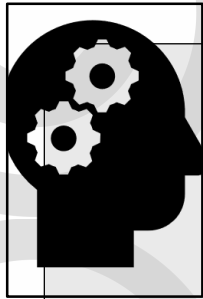
# Voor je begint: 6 vragen



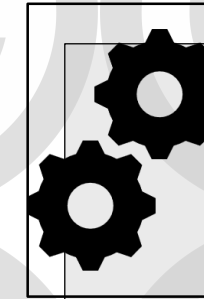
Vertrouw je de ketenpartners?



Kan dit ook in een centrale db?



Potentiële toepassing of échte oplossing



Zijn er werkende voorbeelden?



Hoe ga je opschalen?



Hoe regel je de beveiliging

# 4 tier testing

Smart Contract

Token

Blockchain protocol

Blockchain



# Hoe nu verder?

Graag samen ontdekken...



[sanne.visser@gmail.com](mailto:sanne.visser@gmail.com)



The End.