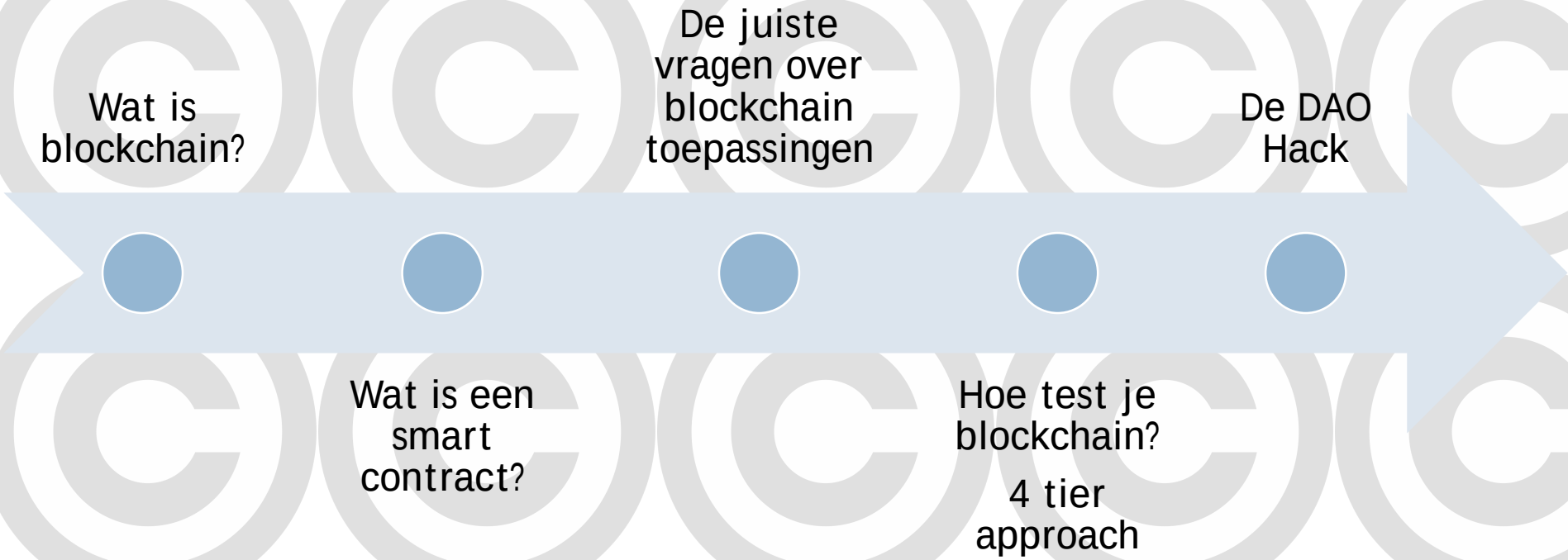
Future-proof Tester: Blockchain

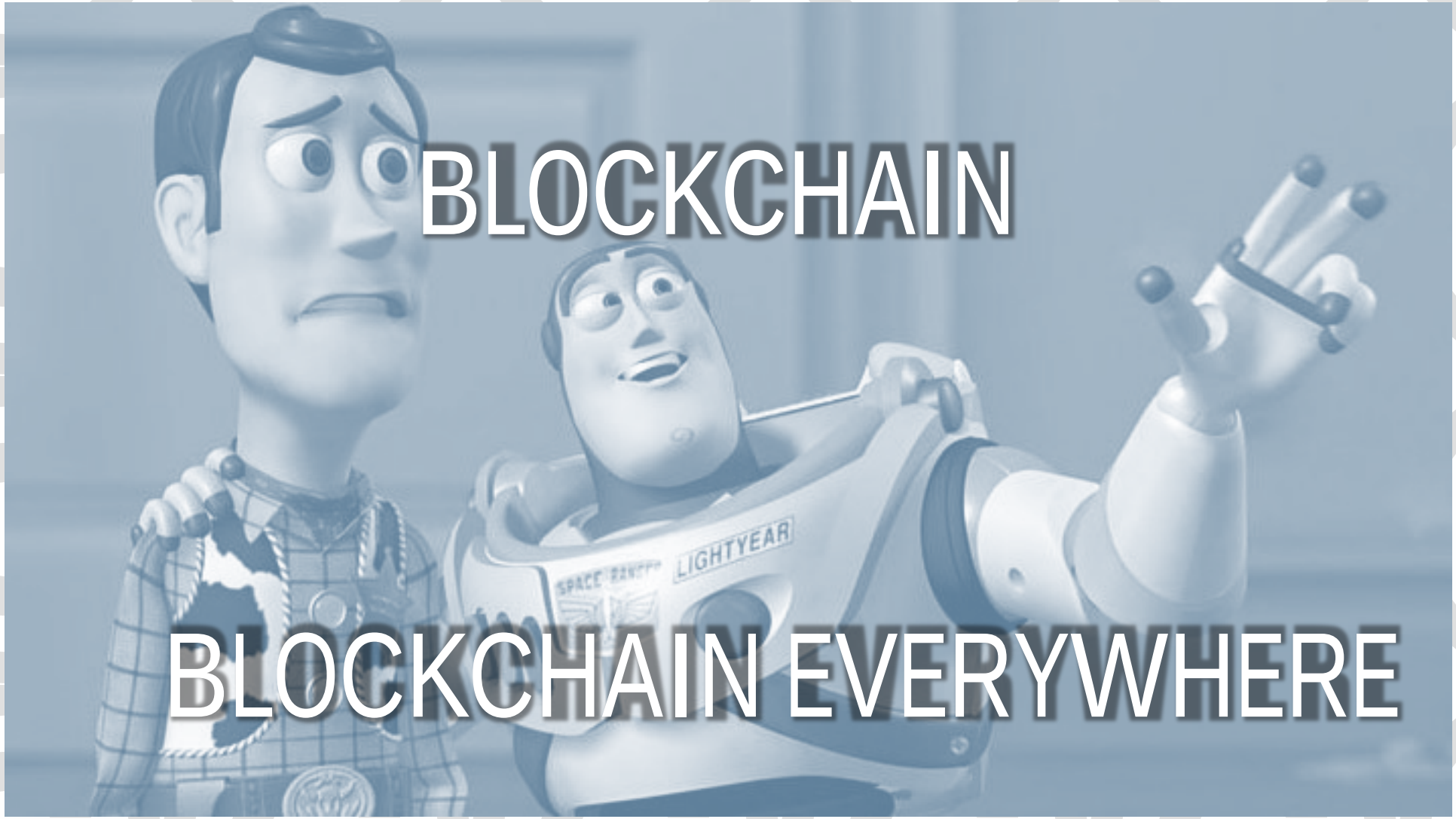
Hoe ga je als tester om met blockchain?

15 mei 2018

Wat we gaan doen:



Krijg ik hier als tester mee te maken?

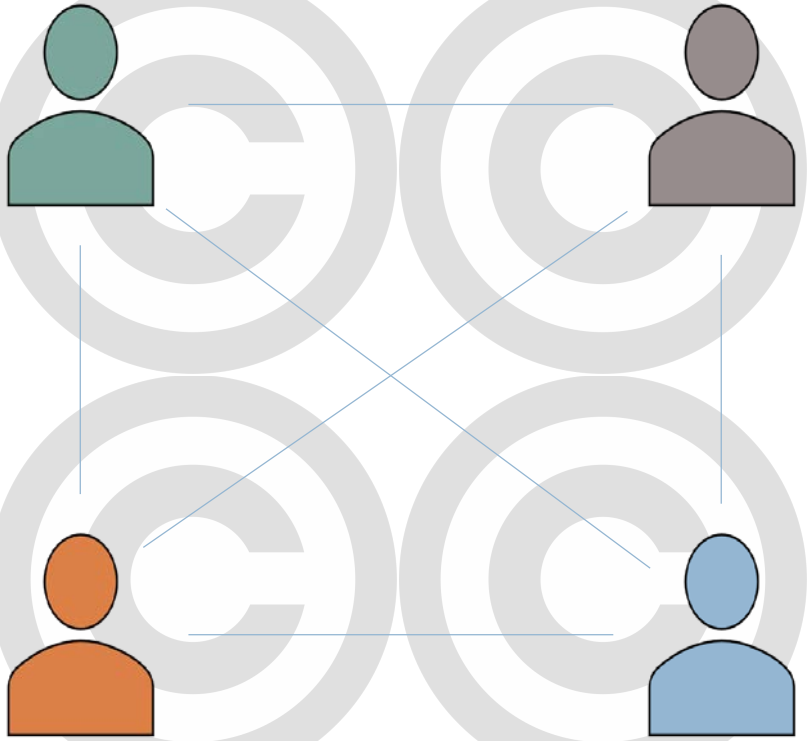


Waar het voor mij begon: 2012

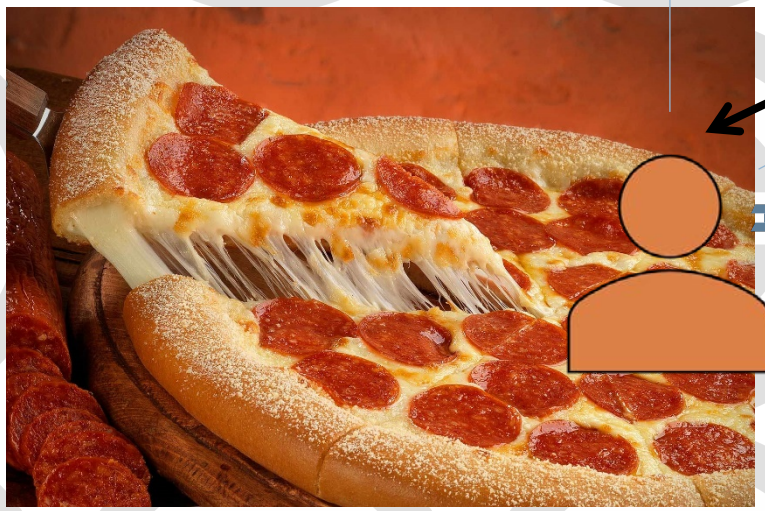
De belangrijkste concepten

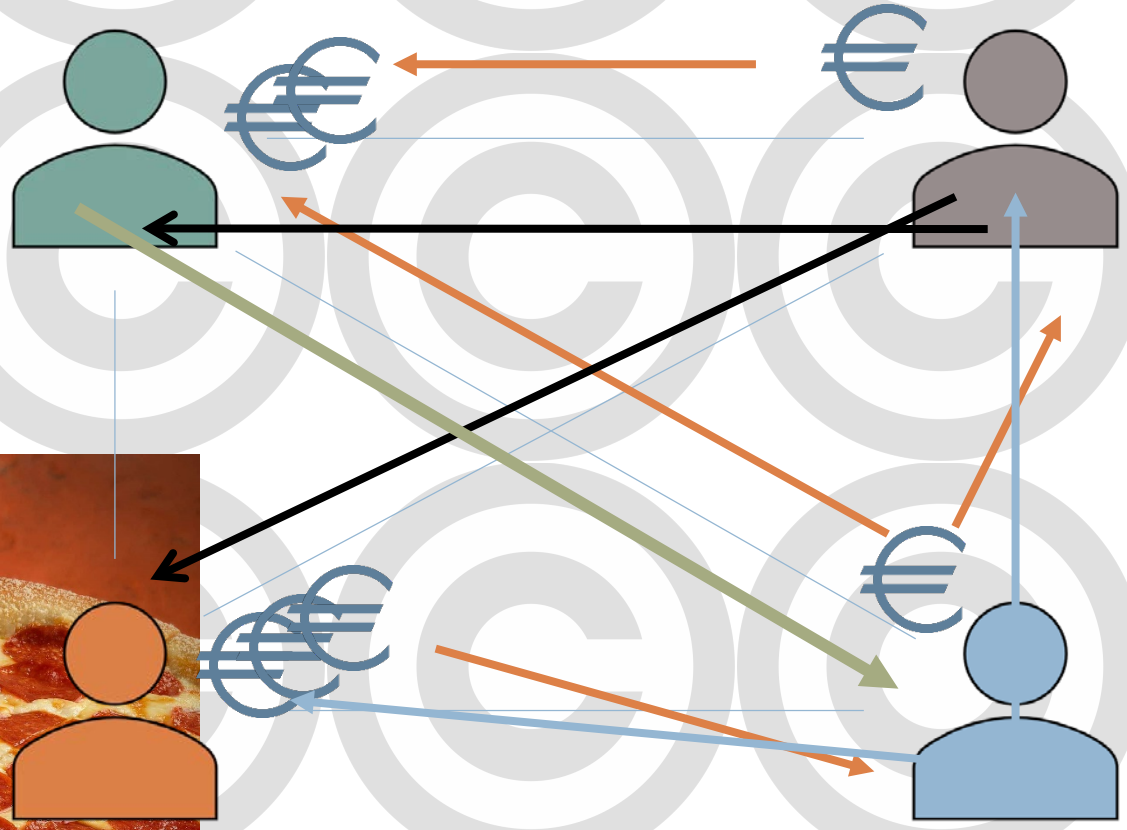
- Digitale handtekeningen
- De transactie geschiedenis
- Gedecentraliseerd
- Proof of Work
- Blockchain

Boekhouding en transacties

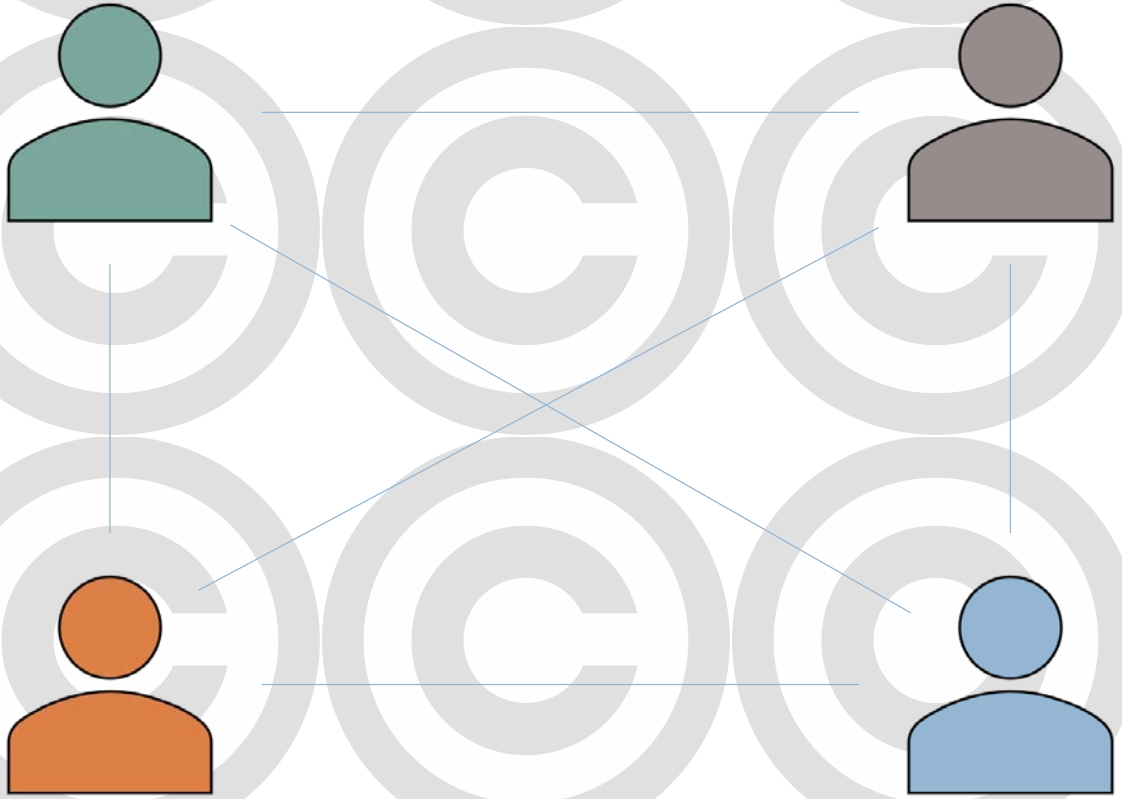


Pizza sessie(s) –wie betaalt wat?

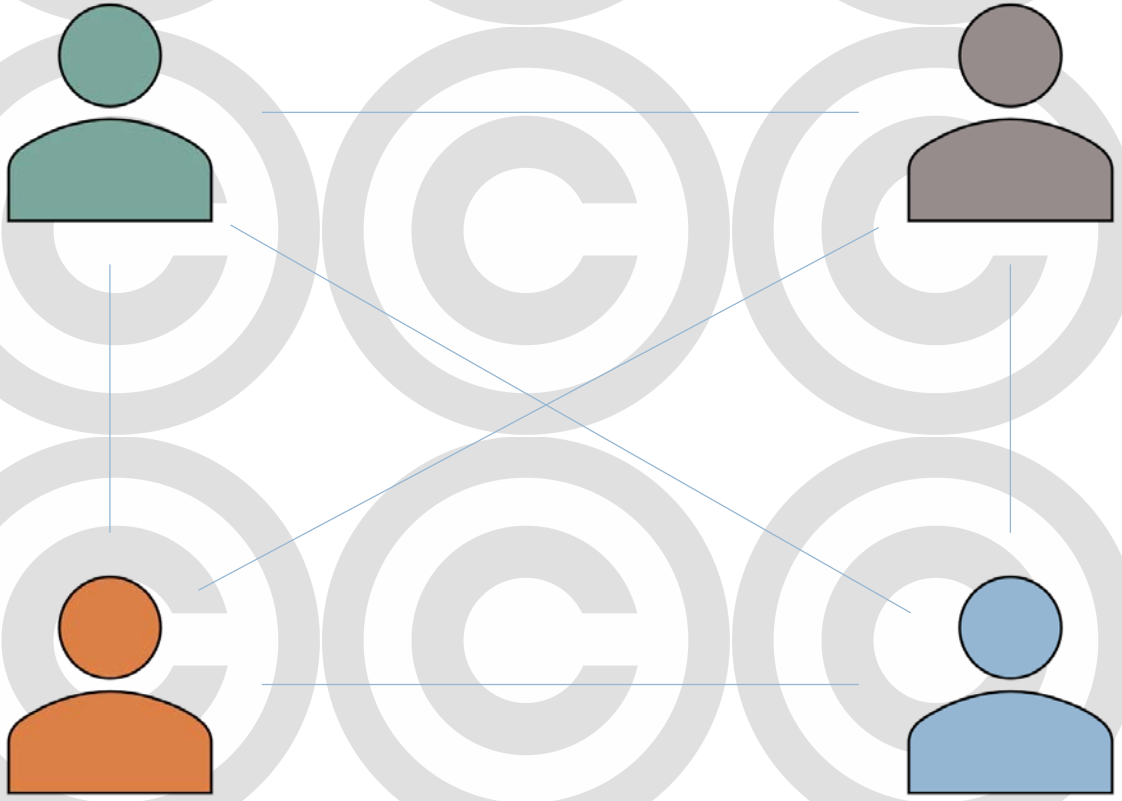


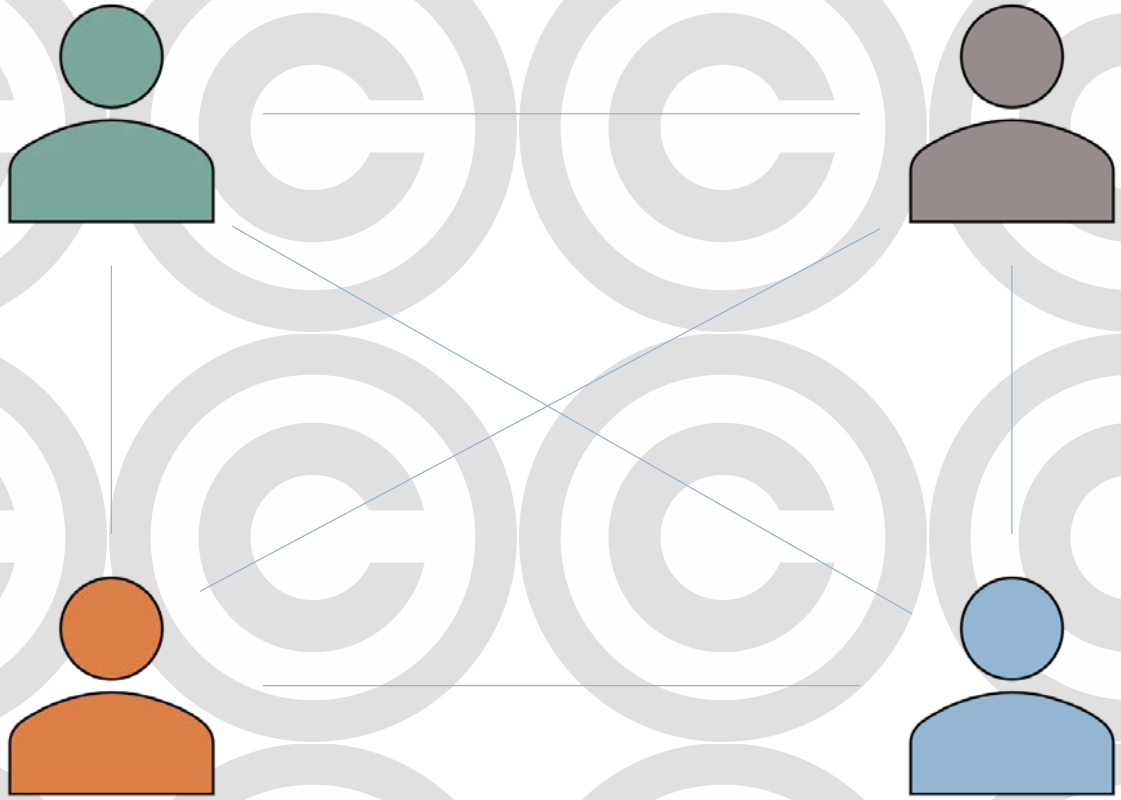


Boekhouden –gedeeld xls op SharePoint



Boekhouden –gedeeld xls op SharePoint





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

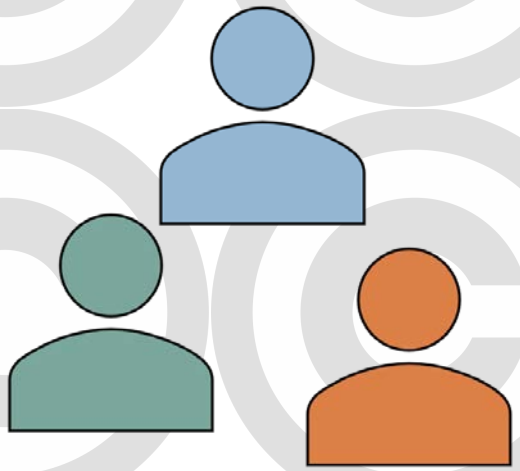
Afspraken voor de gedeelde Excel

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

Eerste probleem: iedereen mag regels toevoegen

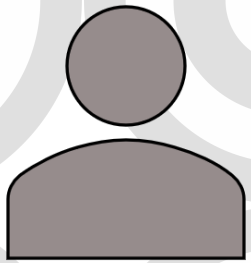
Betaler	Ontvanger	Bedrag
Groen	Grijs	20
Geel	Blauw	50
Blauw	Groen	5
Grijs	Geel	25
Grijs	**Groen**	**100**

Betaler	Ontvanger	Bedrag	Handtekening
Groen	Rood	20	*Groen*
Geel	Blauw	50	*Geel*
Blauw	Groen	5	*Blauw*
Rood	Geel	25	*Rood*



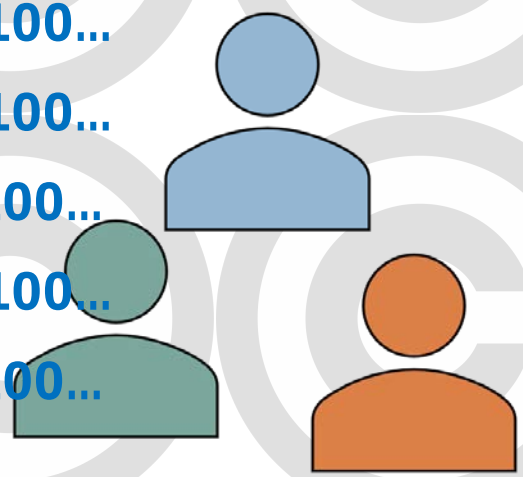
Digitale Handtekeningen

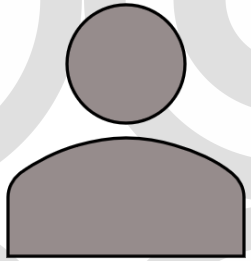
Grijs **01001100…**



Wat voorkomt het kopiëren van een digitale handtekening?

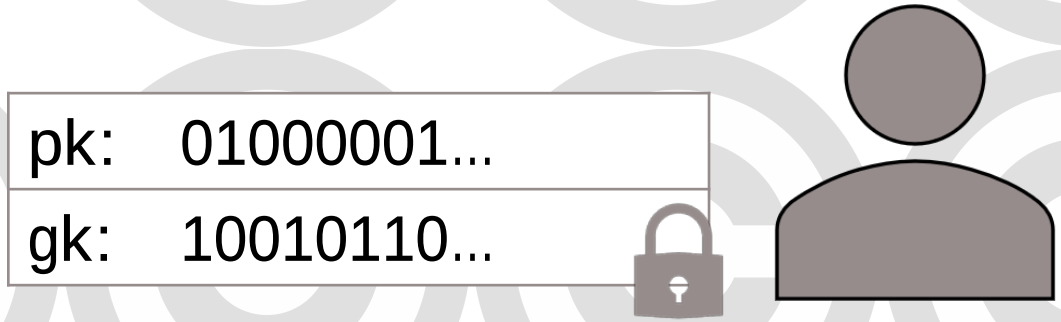
- *Grijs* 01001100…
- COPY + PASTE?
- *Grijs* 01001100…
- *Grijs* 01001100…
- *Grijs* 01001100…
- *Grijs* 01001100…
- *Grijs* 01001100…

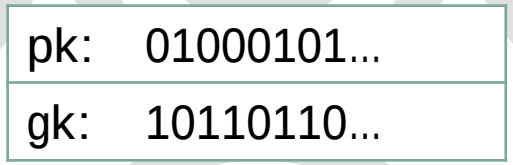


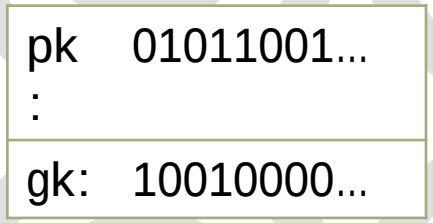


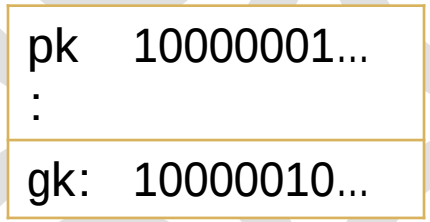
Public key / Private keys*

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





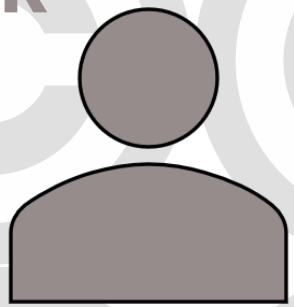


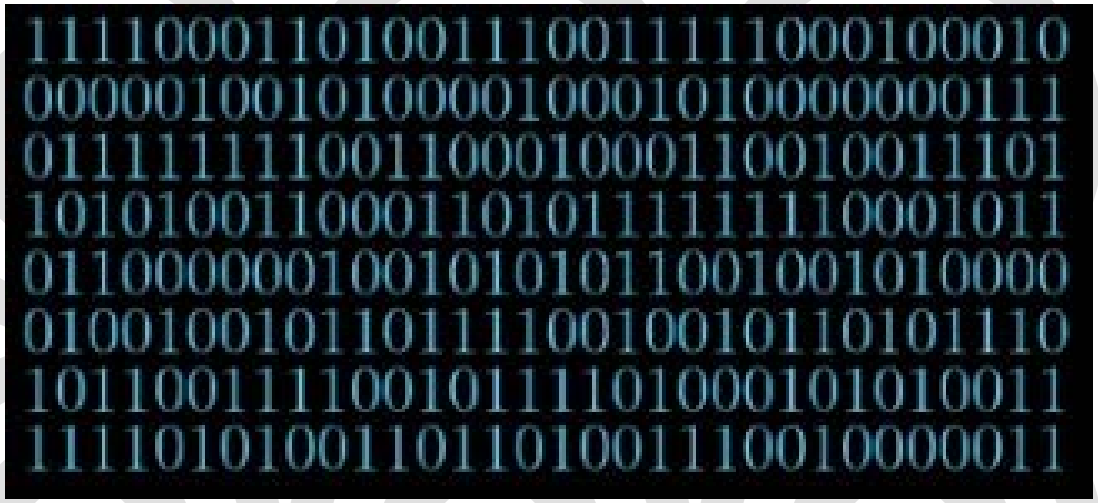


In tegenstelling tot op papier verandert je handtekening per bericht

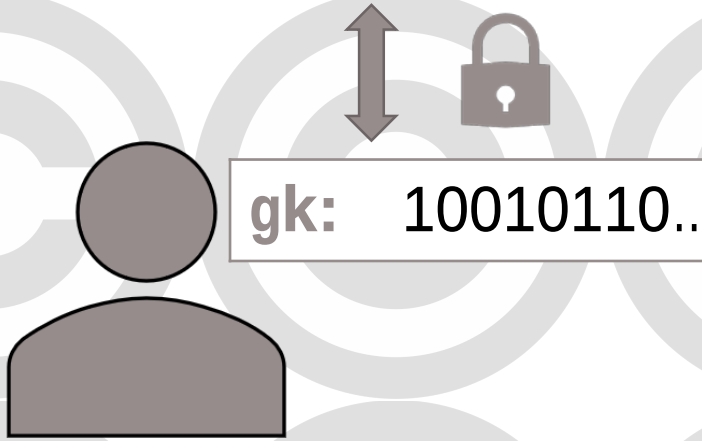
- Sign (message, gk) = signature
- Verify (message, signature, pk) =T/F

Verify (Message, **256 bit signature**, pk) = **True**
alleen als dit ook overeenkomt met de gk



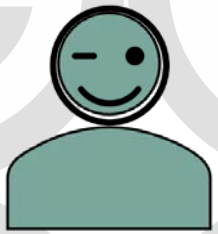


Verify (Message, 256 bit signature, pk) = True



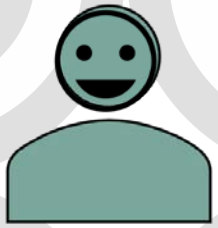
Tweede probleem: dezelfde regel meerdere keren vastleggen

Betaler	Ontvanger	Bedrag	Handtekening
Grijs	**Groen**	**100**	**0 0 1 0 0 1 0 0 1 1…**
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	0 0 1 0 0 1 0 0 1 1…
2	Groen	Rood	100	Nieuwe unieke handtekening
3	Groen	Rood	100	1001100110…
4	Groen	Rood	100	0011110010…



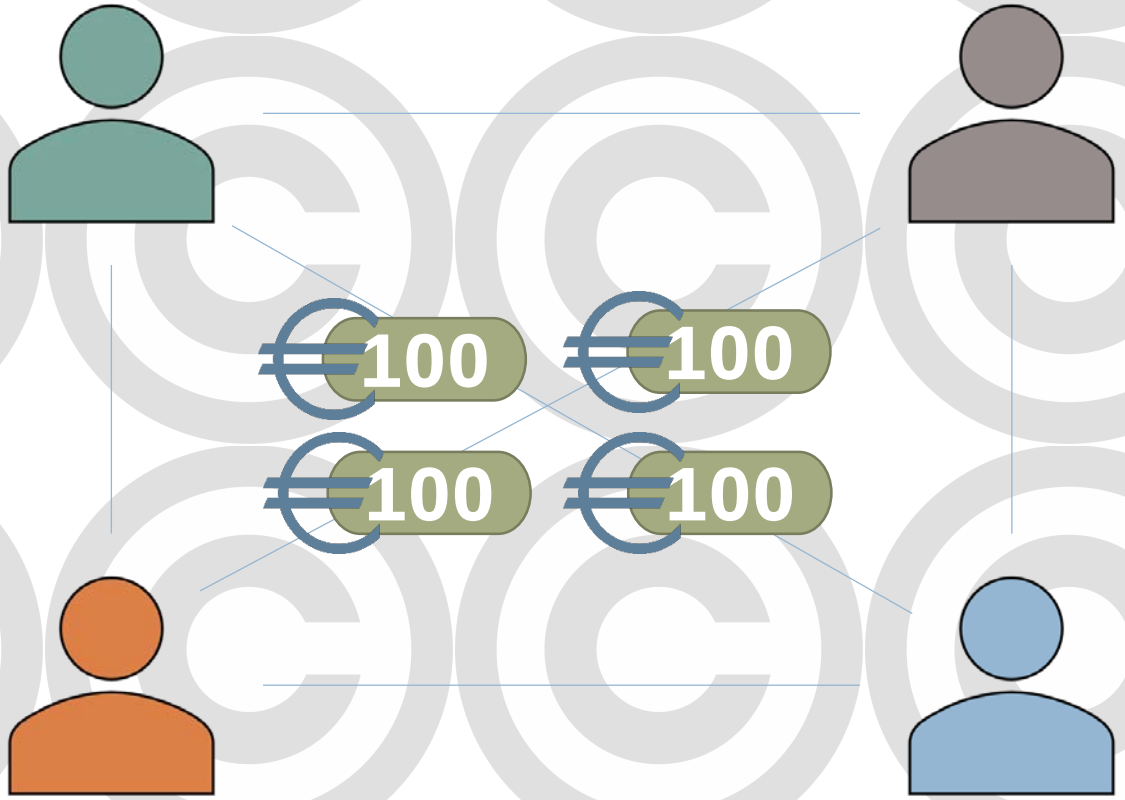
PROTOCOL

- 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	0 0 1 0 0 1 0 0 1 1…
2	Groen	Grijs	20	1001011100…
3	Groen	Grijs	20	1001100110…
4	Groen	Grijs	20	0011110010…

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	0 0 1 0 0 1 0 0 1 1…
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

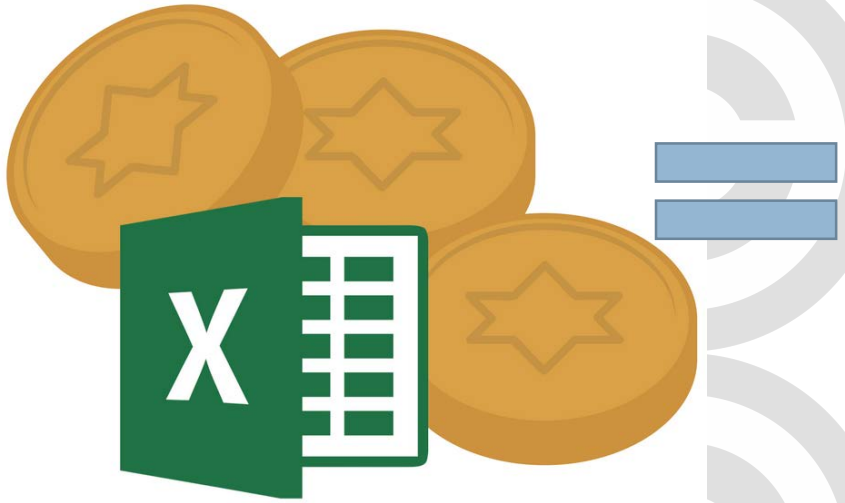
MessageID	Betaler	Ontvanger	Bedrag	Excelcoin
104	Geel	Rood	75	**75**
105	Rood	Groen	100	**100**
106	Groen	Geel	95	**95**
108	Rood	Paars	--	**50**

Je kan immers Pizza kopen met Excelcoin

Euro's omwisselen voor Excelcoin

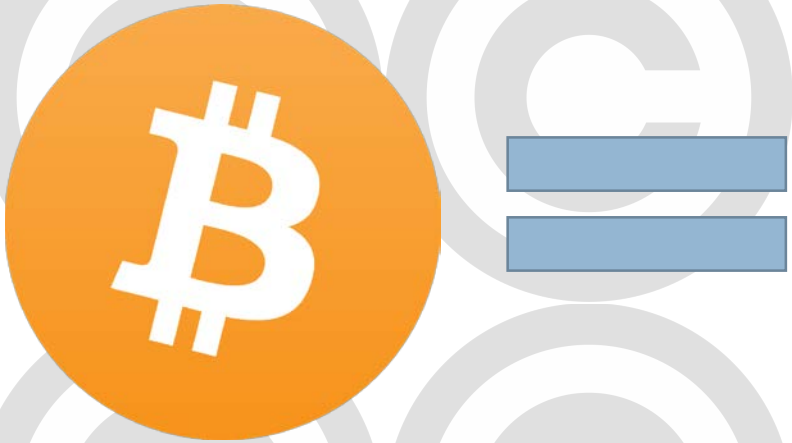
MessageID	Betaler	Ontvanger	Bedrag	Excelcoin
104	Geel	Rood	75	75
105	Rood	Groen	100	100
106	Groen	Geel	95	95
108	Rood	Paars	--	50

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

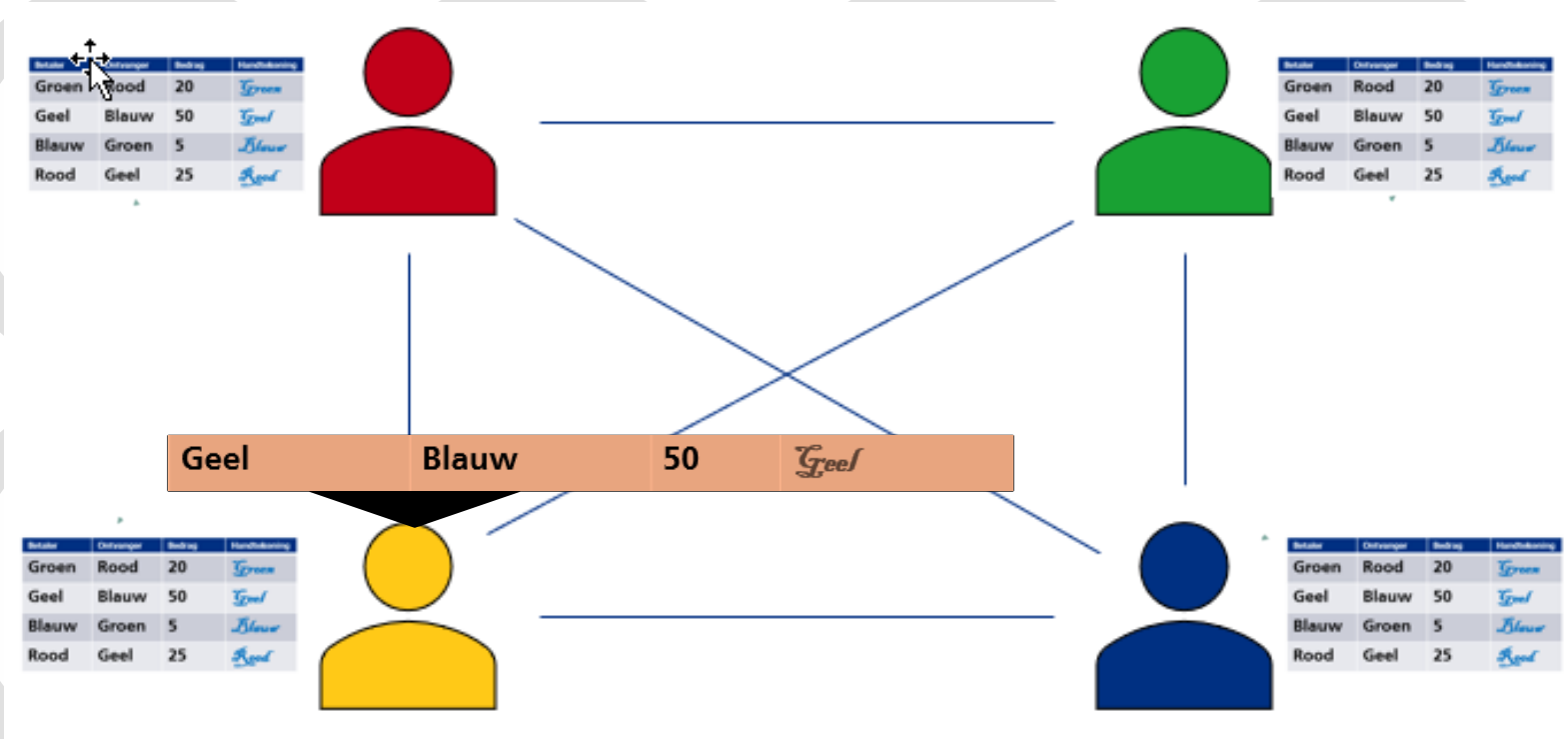


Betaler	Ontvanger	Bedrag	Handtekening
Groen	Rood	20	Groen
Geel	Blauw	50	Geel
Blauw	Groen	5	Blauw
Rood	Geel	25	Rood

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

- Location, location, location

Gedistribueerde boekhouding transacties



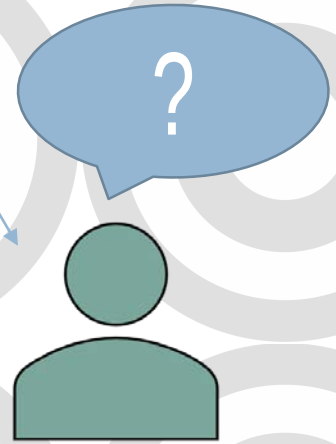
Probleem 4: Hoe weet je dat wat je aan transacties ontvangt hetzelfde is als de anderen?

Groen	Rood	20	Groen

Rood	Geel	25	Rood

Geel	Blauw	50	Geel

Blauw	Groen	5	Blauw



Betaler	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

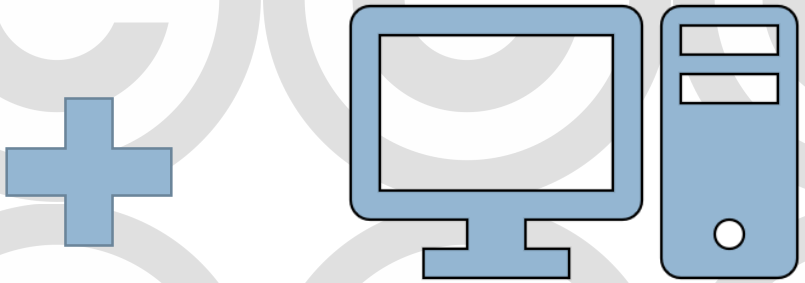
PROTOCOL

- 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

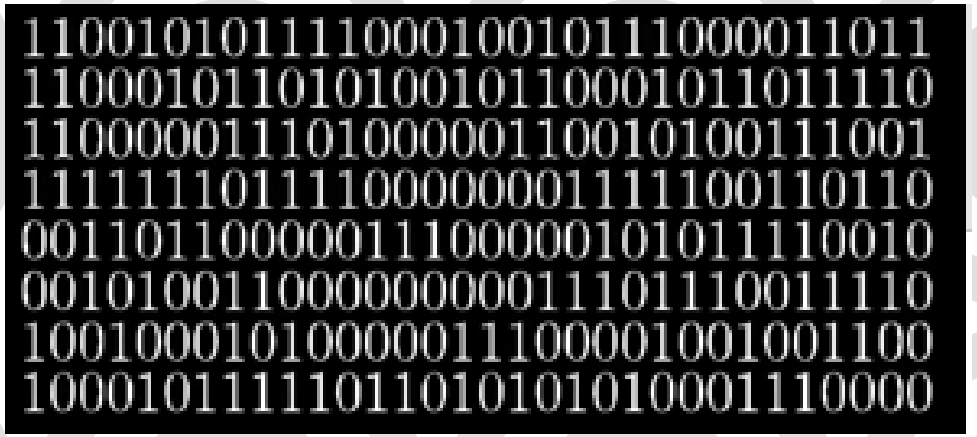
Bitcoin protocol: Geloof de boekhouding waar het meeste rekenwerk in zit.

Betaler	Ontvanger	Bedrag	Handtekening
Groen	Rood	20	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



Cryptografische Hash Functies

HASH



SHA-256(*message/file*)=

Inverse bijna onmogelijk

Bitcoin protocol

PROOF OF WORK

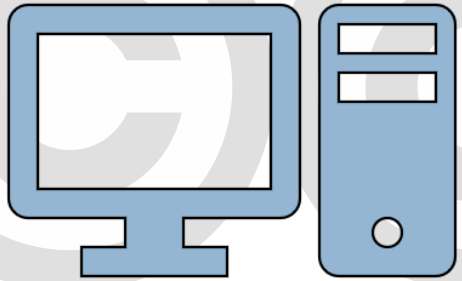
30 nullen

```
00000000000000000000000000000011
11000101101010010110001011011110
11000001110100000110010100111001
11111110111100000001111100110110
00110110000011100000101011110010
00101001100000000011101110011110
10010001010000011000010010011100
10001011111011010101010001110000
```

1234567809

Betaler	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

SHA-256



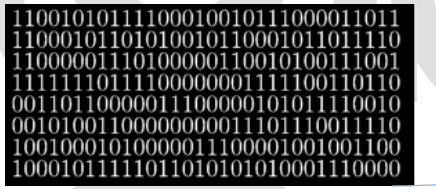
Rekenwerk via een cryptografisch hash functie

Blocks

1234567809

Betaler	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

SHA-256



1230067809

Betaler	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

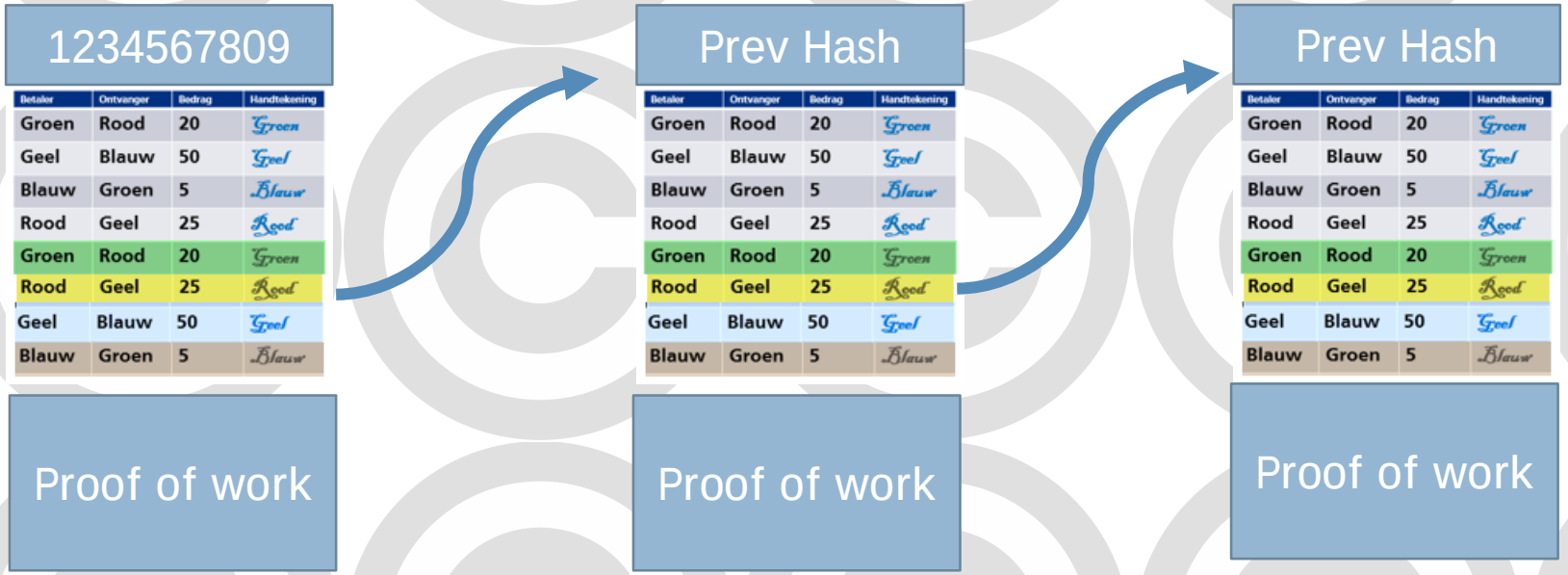
Proof of work

1034547809

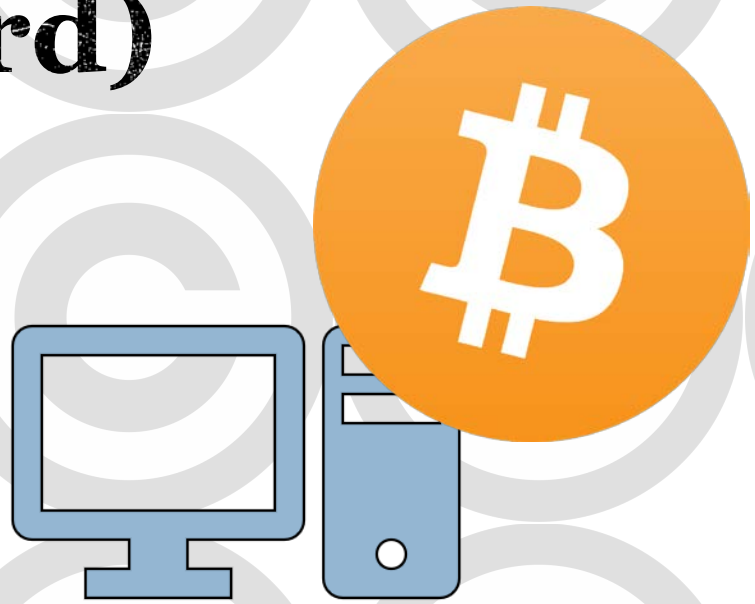
Betaler	Ontvanger	Bedrag	Handtekening
Groen	Rood	20	Groen
Geel	Blauw	50	Geel
Blauw	Groen	5	Blauw
Rood	Geel	25	Rood
Groen	Rood	20	Groen
Rood	Geel	25	Rood
Geel	Blauw	50	Geel
Blauw	Groen	5	Blauw

Proof of work

Blockchain


1234567809
Betaler 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
Prev Hash
Betaler 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
Prev Hash
Betaler 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

Bitcoin beloning voor rekenwerk (aka mining reward)



12,5 bitcoin

Zo ziet dat er in het echt uit

Bitcoin nodes aka bitcoin's r

GLOBAL BITCOIN NODES DISTRIBUTION

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

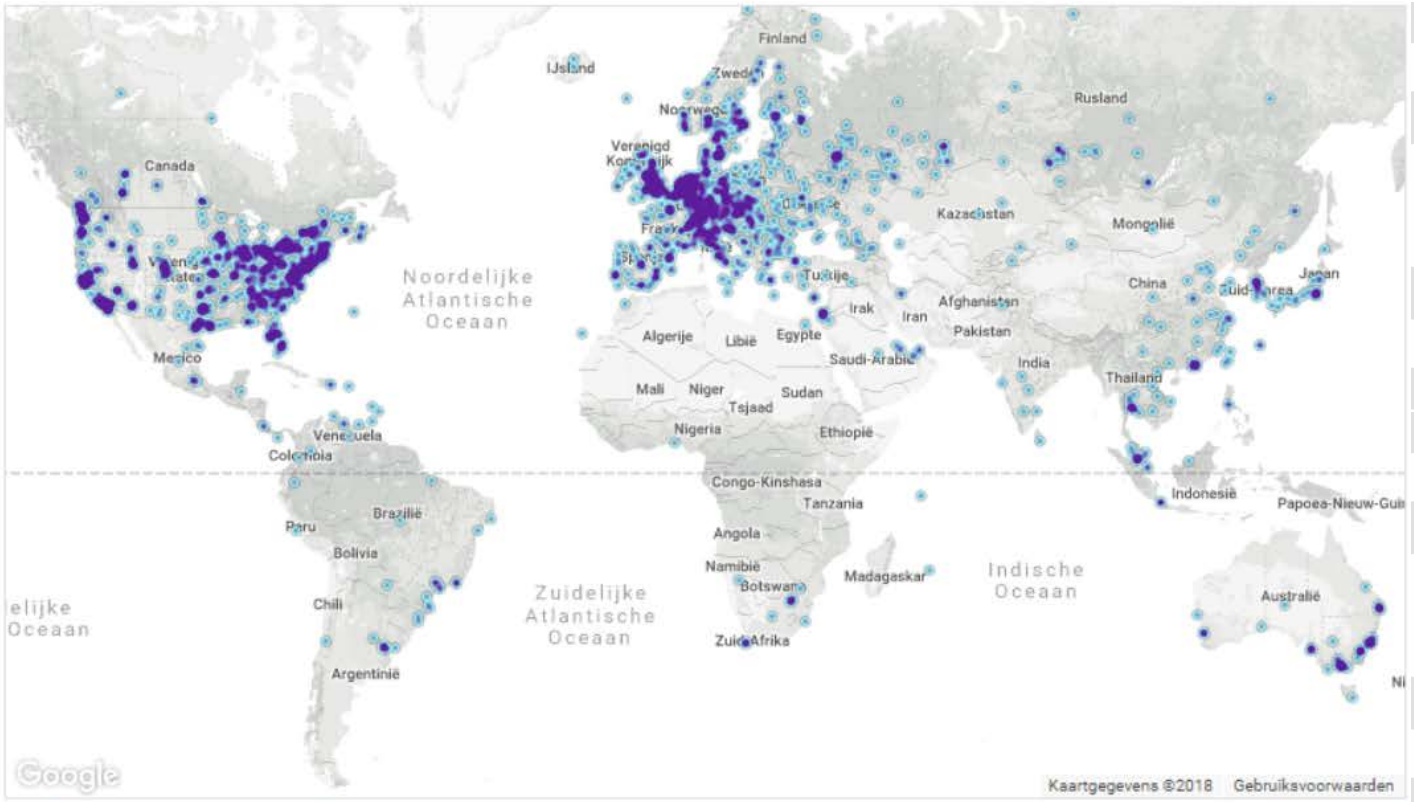
11364 NODES

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%)

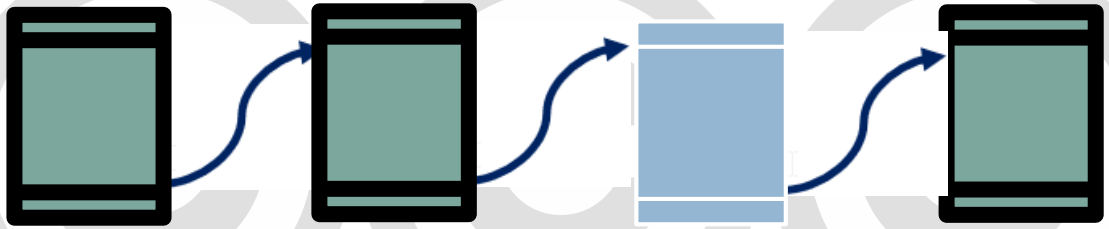
More (104) »

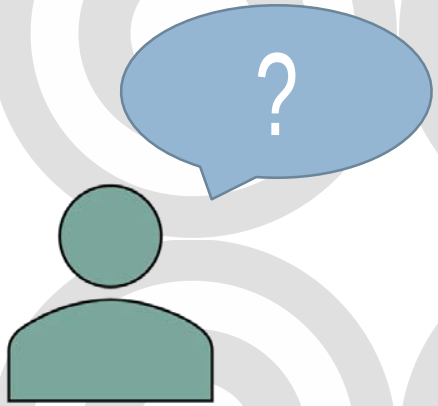


Map shows concentration of reachable Bitcoin nodes found in countries around the world.

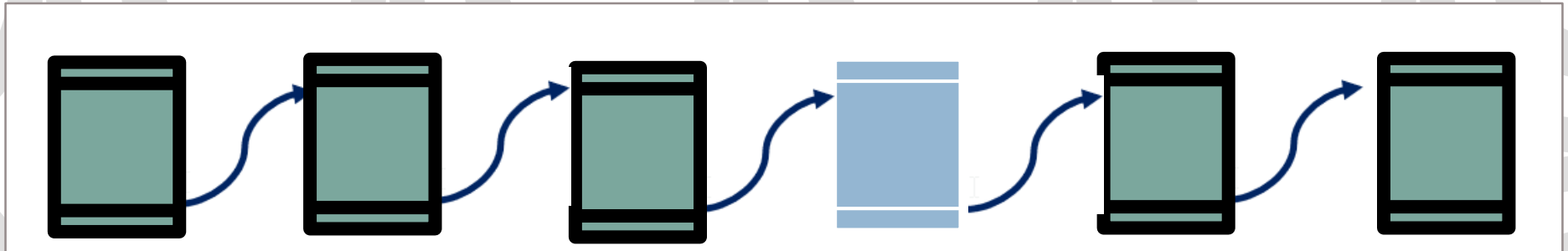
LIVE MAP

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

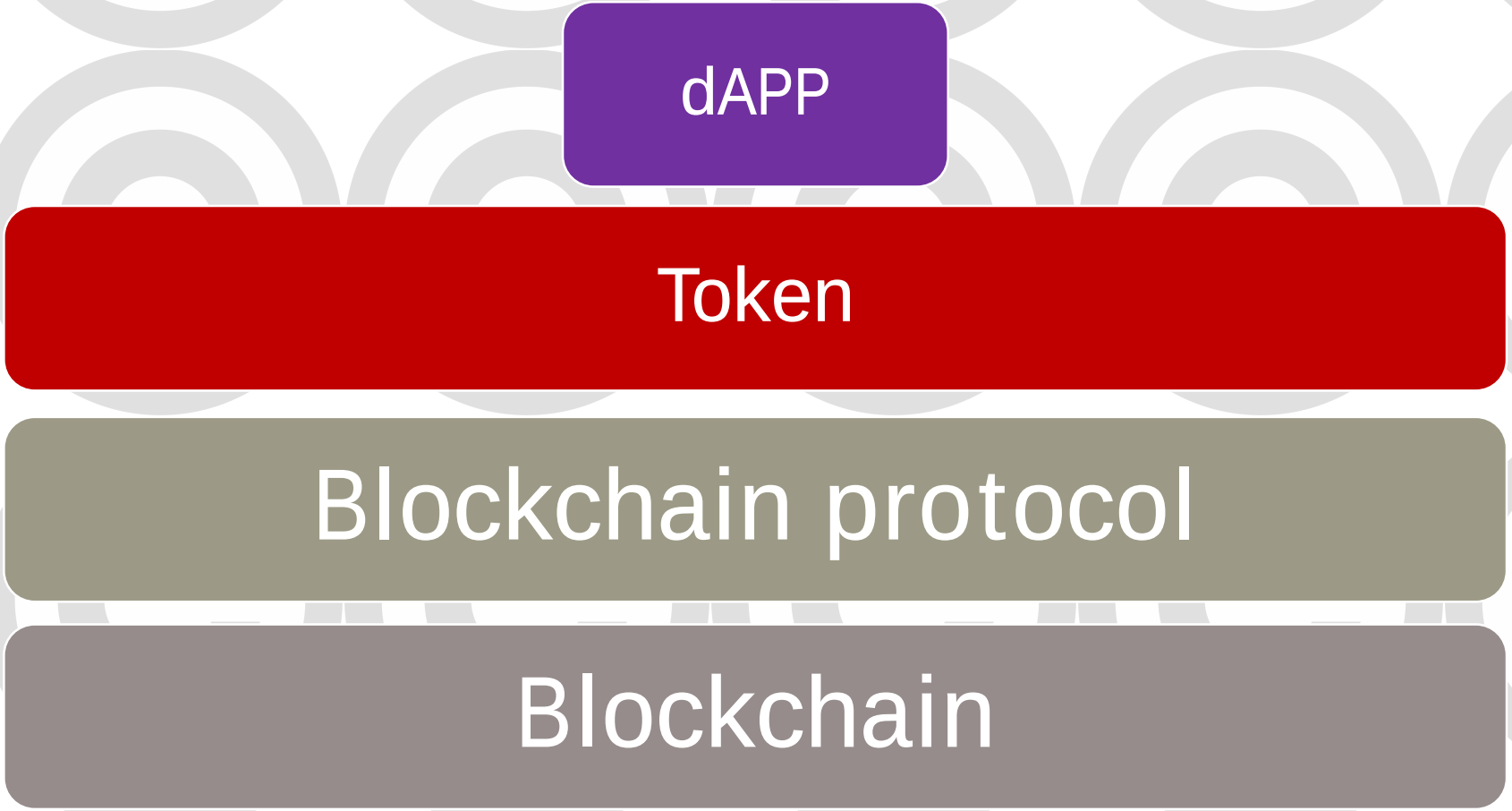
Blockchain

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

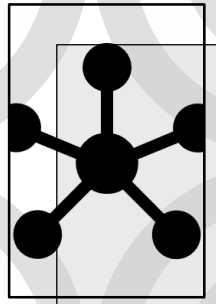


Private Blockchains

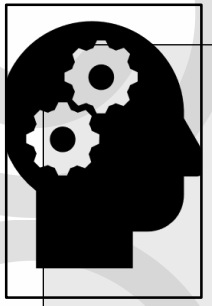
Testing Blockchain

Voor je begint: 6 vragen

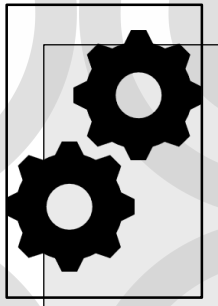
Vertrouw je de ketenpartners?



Kan dit ook in een centrale db?

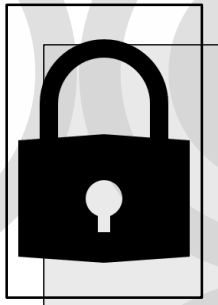


Potentiële toepassing of échte oplossing



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


The End.