Introductie Blockchain

Presentatie werkgroep betalingsverkeer

6 september 2017

Erwin den Bak / Harry Offermans

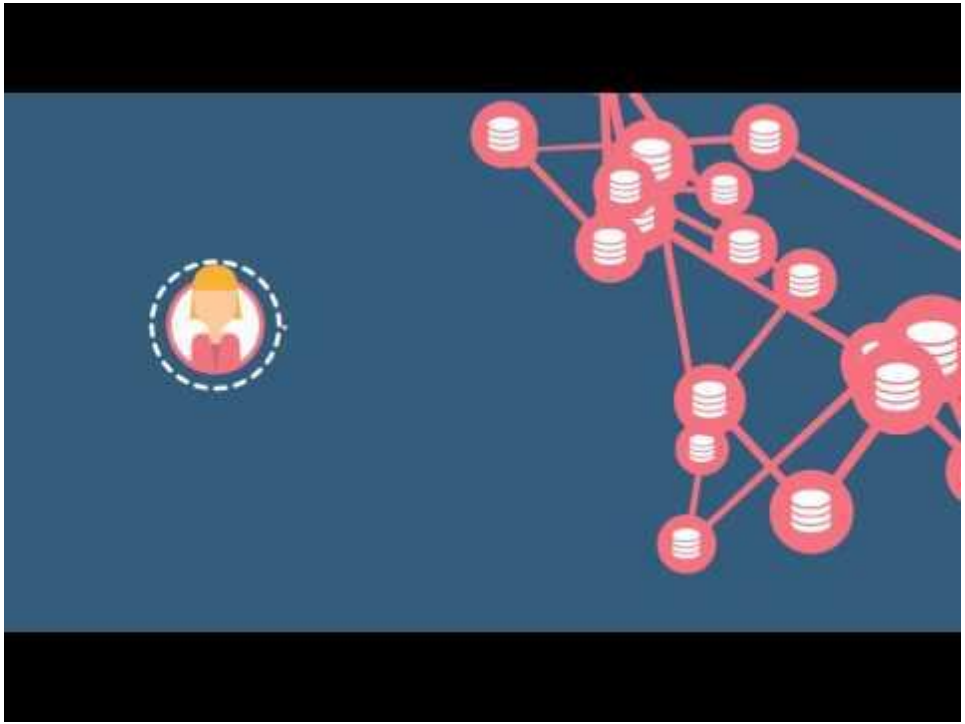
Doelstelling voor vanavond

Inzicht in het concept en de toepassingsmogelijkheden van blockchain

- Hoe werkt blockchain
- Blockchain uitgelegd
- Case-voorbeelden
- Auditimplicaties / relativering / meenemen
- Demo “Hoe werkt Blockchain” (blockchain generator)

Deze presentatie bevat materiaal van: Prof.dr. Eddy Vaassen RA (Tilburg University, BDO, Erasmus Universiteit Rotterdam) en Ivo Luijendijk (Worldline)

Hoe werkt blockchain - een animatie filmpje



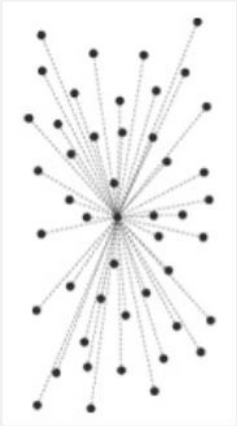
http://www.blockchainpilots.nl

Blockchain uitgelegd - IT ontwikkeling

Blockchain uitgelegd - Soorten netwerken

Centralised network

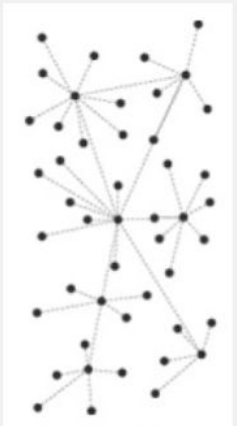
Network with a single point of contact, a server for all the connected nodes



Example
Equens (pre-SEPA)
between the Dutch banks

Federated network
(decentralised)

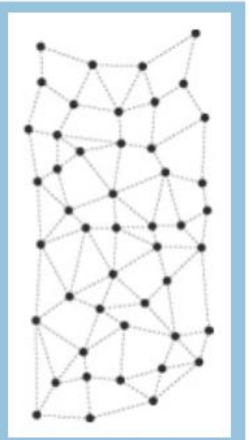
Network of equal servers, that connect child-nodes to the network



Example
Airport network
local & global airports

Distributed Network
(peer-to-peer)

Network of interconnecting nodes, without authority, for peer-to-peer connectivity

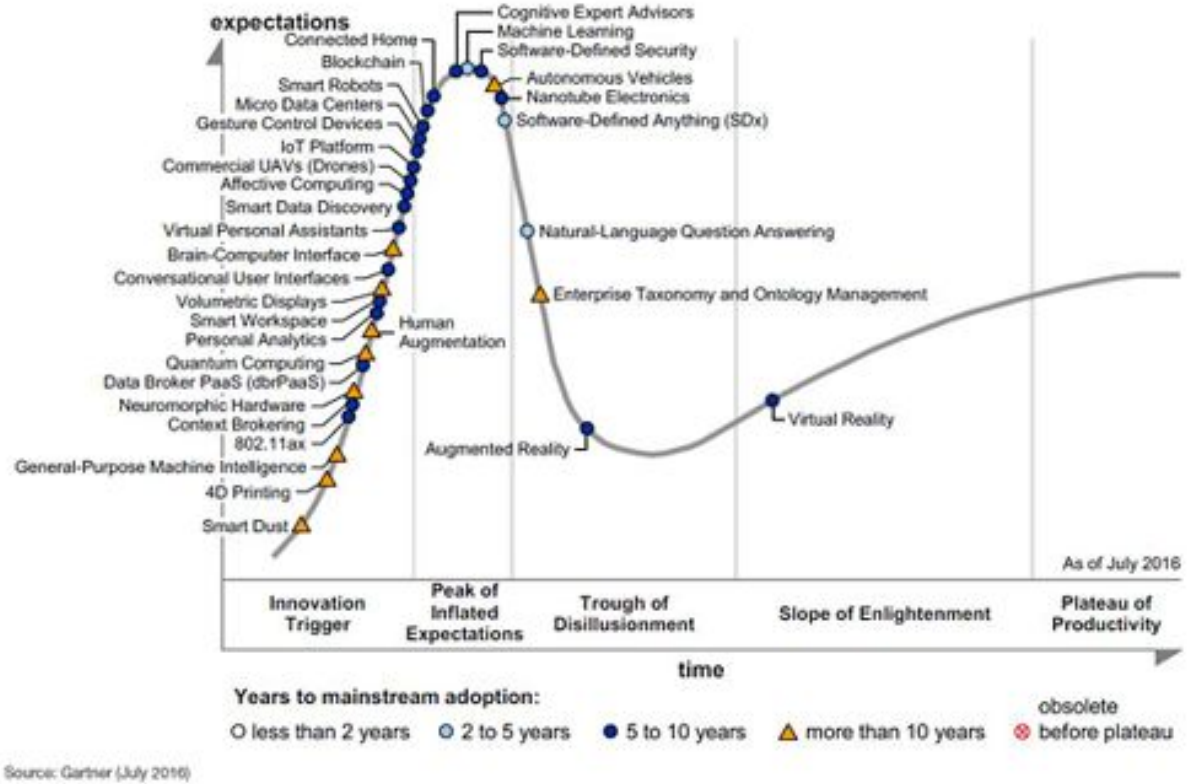


Example
WWW
Information sharing (IP protocol)

Blockchain uitgelegd - Wat is de blockchain ?

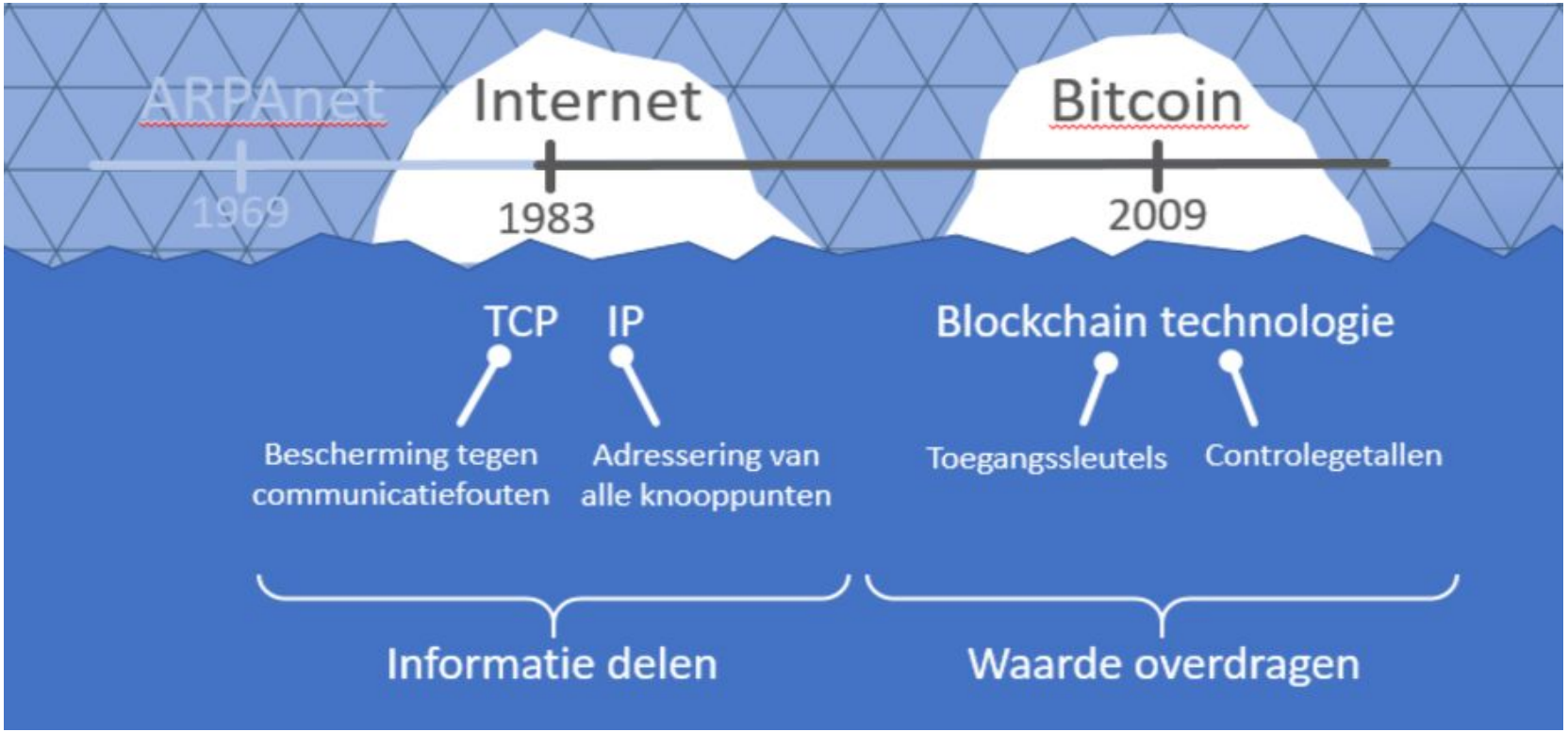
- De blockchain is een keten van transacties die onderling verbonden zijn en waarin die transacties worden gecontroleerd, geautoriseerd en geaccordeerd
- Een transactie kan slechts worden vastgelegd in de blockchain als zij is geaccordeerd door een meerderheid van de nodes in de blockchain (Proof of Work)
- Als een transactie eenmaal is vastgelegd in de blockchain kan ze niet meer worden gewijzigd of verwijderd
- De blockchain is de technologie achter de Bitcoin en andere cryptovaluta
- De blockchain is géén substituut voor informatiesystemen als ERP, CRM, SCM, BI, ..

Blockchain uitgelegd - Gartner hype cycle 2016



Source: Gartner (July 2016)

Blockchain uitgelegd - Wat is de blockchain ?



Redundantie mbt communicatie

Redundantie mbt opslag

Blockchain uitgelegd - Wat is de blockchain ?

Shared ledger

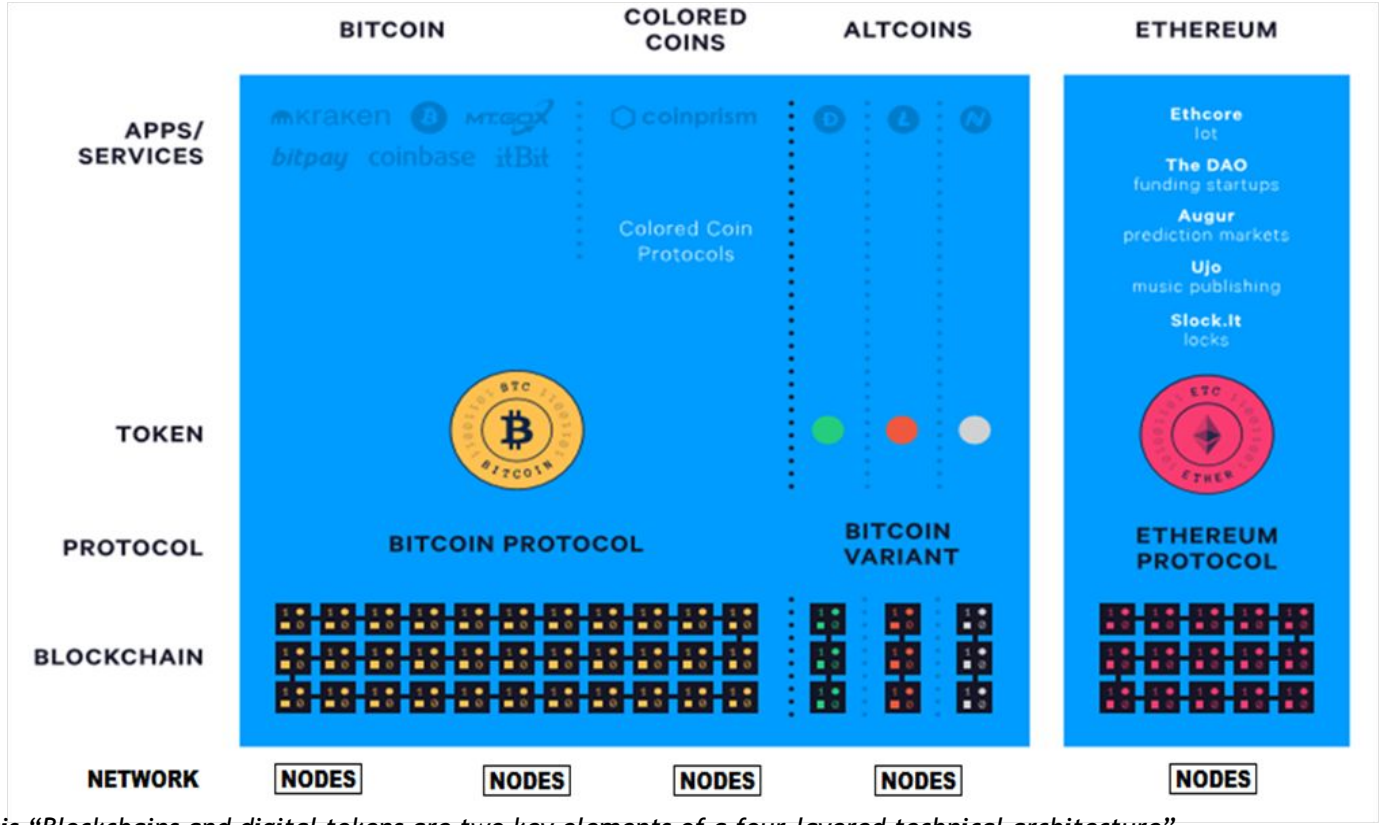
A business network

Privacy and confidentiality

Smart contracts

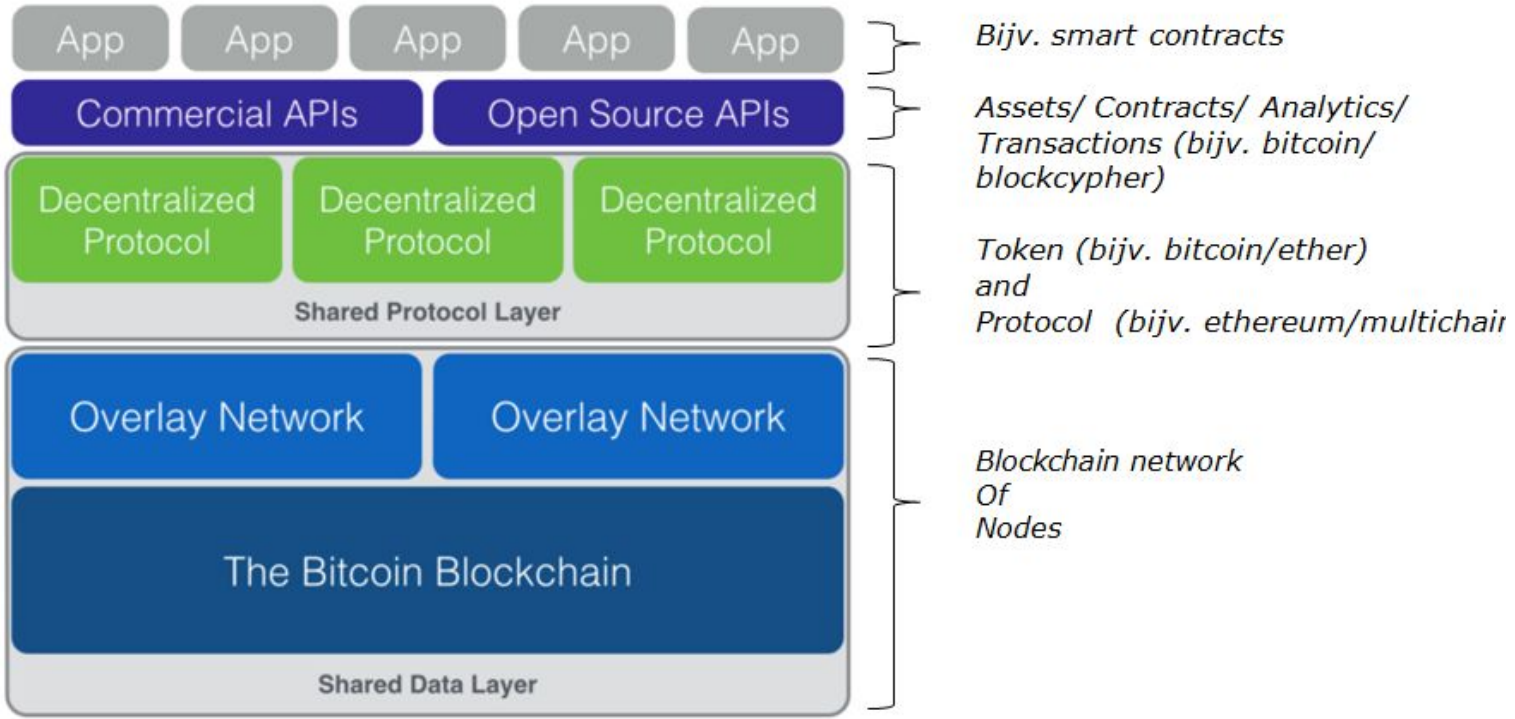
Concensus

Blockchain uitgelegd - Stack architectuur /1



Bron: BCG Analysis "Blockchains and digital tokens are two key elements of a four-layered technical architecture"

Blockchain uitgelegd - Stack architectuur /2

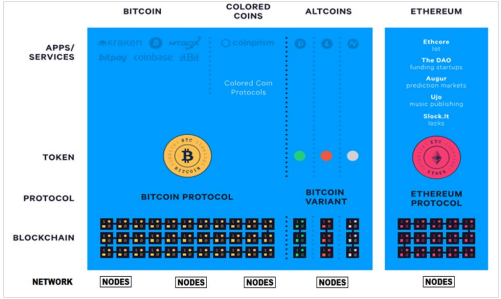


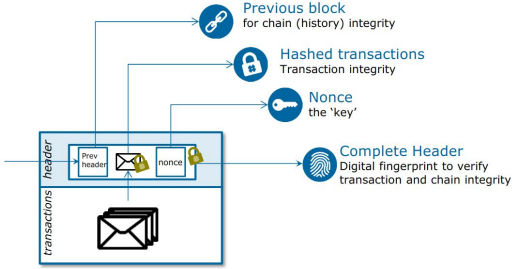
Bron: The Blockchain Application Stack - Joel Monegro

Blockchain uitgelegd - De gebruikte termen

Terminologie:

- Cryptografie
- Hashes
- Publieke en private sleutels
- Peer-to-peer netwerk
- Gedistribueerde databases
- Mining
- Nodes
- Smart contracts
- Proof-of-work
- Trust protocol (bijv. Ethereum)
- Open source software





Blockchain uitgelegd - Het verhaal

- We staan aan de vooravond van een revolutie in internal control en auditing
- Ging het bij Business Process Modeling nog om automatisering van processen, bij continuous auditing vindt controle op de processen en de uitkomsten daarvan geautomatiseerd plaats
- Data-analyse ondersteunt zowel de bedrijfsvoering als de audit; process mining (een vorm van data-analyse) laat zien hoe die processen feitelijk verlopen, maakt conformance checking mogelijk, en kan leiden tot procesverbetering
- De echte revolutie zit in het geheel zonder menselijke tussenkomst laten communiceren van computers met elkaar en die computers ook te laten leren (AI)
- De communicatie als zodanig wordt de kern van het interne beheersingssysteem
- Bij blockchain verlopen de transacties geheel geautomatiseerd en een ‘trusted third party’ is niet meer nodig (want die rol is overgenomen door een ‘trust protocol’ in de blockchain)
- Via ‘tokenization’ van waarde wordt de brug geslagen tussen de echte en de virtuele wereld
- Informatiebeveiliging wordt een steeds belangrijker element van de interne beheersing en het werk van de auditor

Bron: Vaassen

Blockchain uitgelegd - Auditability

- Het verbeteren van de IT systemen van de auditee om een goede basis te creëren voor het verzamelen van controle informatie
- De auditee wordt er beter van omdat de kwaliteit van zijn data verbetert, hij heeft daardoor ook een betere business intelligence, wat leidt tot betere besluitvorming
- De auditor wordt er beter van omdat de audit efficiënter wordt, wat leidt tot hoger gekwalificeerd werk (taakverrijking) en het beschikbaar komen van meer tijd die kan worden besteed aan lange termijn waardetoevoegende activiteiten zoals innovatie

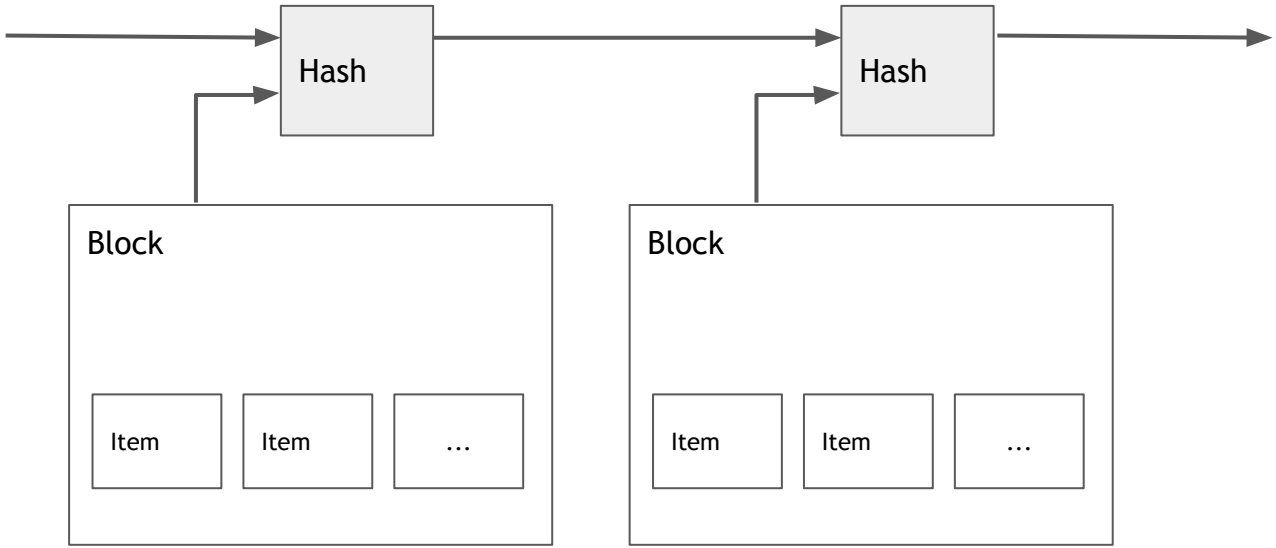
Bron: Vaassen

Blockchain uitgelegd - Deelnemers ecosystemen

Deelnemers kunnen bijvoorbeeld zijn:

- Klanten
- Toeleveranciers
- Dienstverleners (waaronder cloud service providers)
- Banken
- Concurrenten
- Overheidsinstellingen

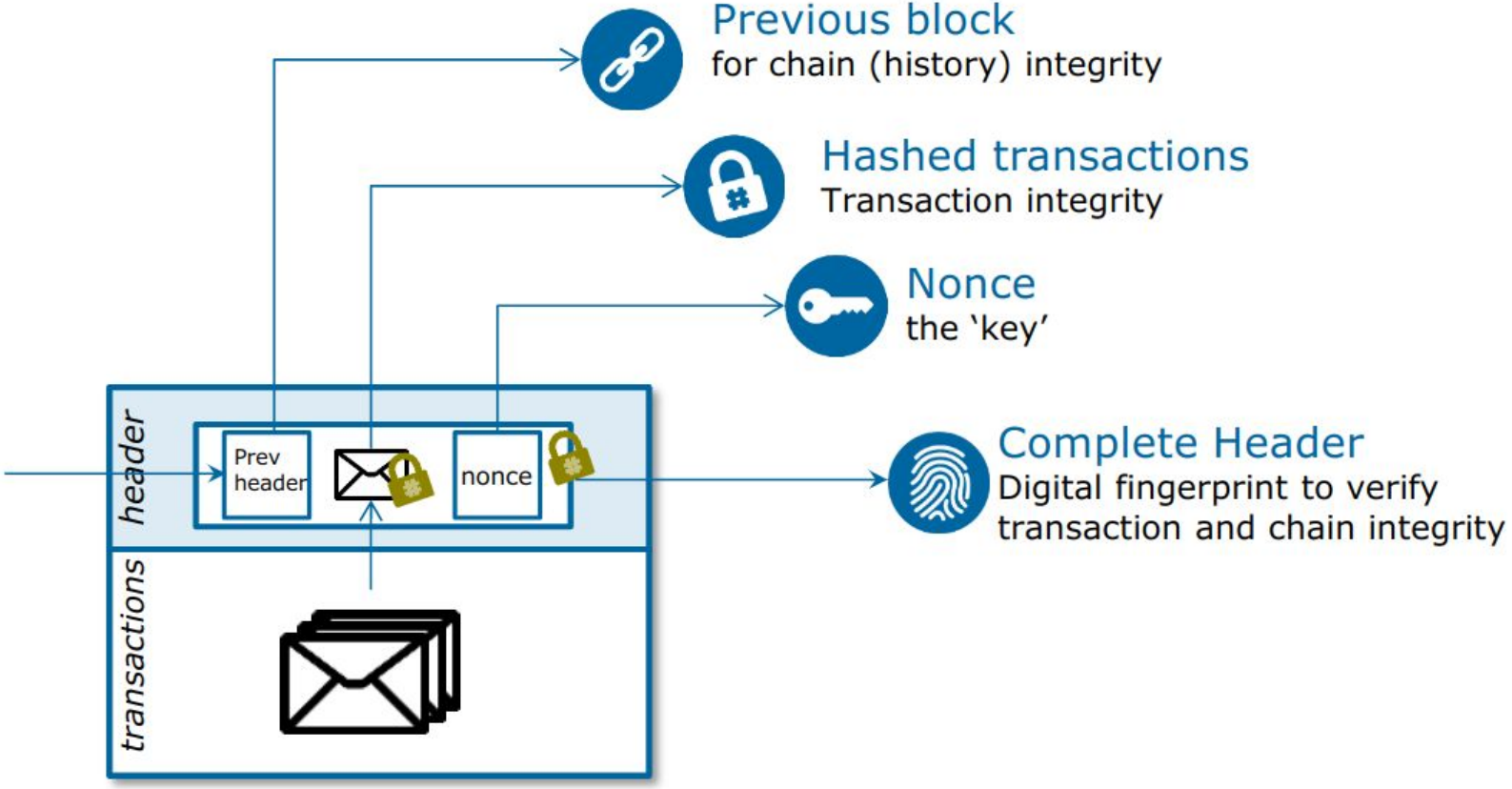
Blockchain uitgelegd - Hashes in de blockchain



**Zie ook deel over demo blockchain generator tool later in de presentatie*

Bron: Vaassen

Blockchain uitgelegd - Hashes in de blockchain



Bron: Luijendijk

Blockchain uitgelegd - Hashes

Berekening:

1. *Neem het identificatienummer*
   Voorbeeld:
   RABO 0123456789
2. *Zet hier de landcode achter*
   Voorbeeld:
   RABO 0123456789 NL
3. *Vervang alle letters door hun positie in het alfabet plus negen (A=10; B=11;…; Z=35)*
   Voorbeeld:
   RABO 0123456789 NL wordt 2710112401234567892321
4. *Voeg hier achteraan 00 toe*
   Voorbeeld:
   271011240123456789232100
5. *Deel deze uitkomst door 97*
   Voorbeeld:
   271011240123456789232100 / 97 = 27939303105511009199 18,5567010309278351
6. *Neem de decimalen achter de komma en vermenigvuldig dit met 97.*
   Voorbeeld:
   0,5567010309278351 x 97 = 54
7. *Trek dit getal af van 98*
   Voorbeeld:
   98-54=44
8. *Dit is het controlegetal, de HASH !*
   Het IBAN nummer is dus: NL44RABO0123456789

Bron: Vaassen

Blockchain uitgelegd - Waarom blockchain ?

- **Veilig:** de aard van de blockchain als gedistribueerde database maakt het moeilijk en duur om als individuele partij veranderingen aan te brengen, simpelweg doordat er te veel kopieën bestaan
- **Betrouwbaar:** de blockchain legt van alle transacties vast wat is overgedragen en voor welk bedrag dat is gebeurd; de blockchain is de ‘shared single source of truth’ die altijd geautomatiseerd gecontroleerd zal worden; hierdoor zal een officieel document of geldeenheid nooit méér dan eenmaal kunnen worden gebruikt als officieel bewijs dan wel betaling
- **Efficiënt:** de transacties in de blockchain vinden rechtstreeks plaats tussen aanbieder en afnemer waardoor deze snel en tegen lage kosten kunnen worden uitgevoerd
- Alle transacties worden gedaan volgens het trust protocol wat vergelijkbaar is met een rule-based code (bijvoorbeeld een gedragscode met gedetailleerde voorschriften of een business rule engine in BPM) die altijd wordt gevolgd
- Verbeterde voorspelbaarheid van processen doordat in work-flows niet meer op personen hoeft te worden gewacht om een bepaalde processstap af te handelen

Bron: Vaassen

Case voorbeelden

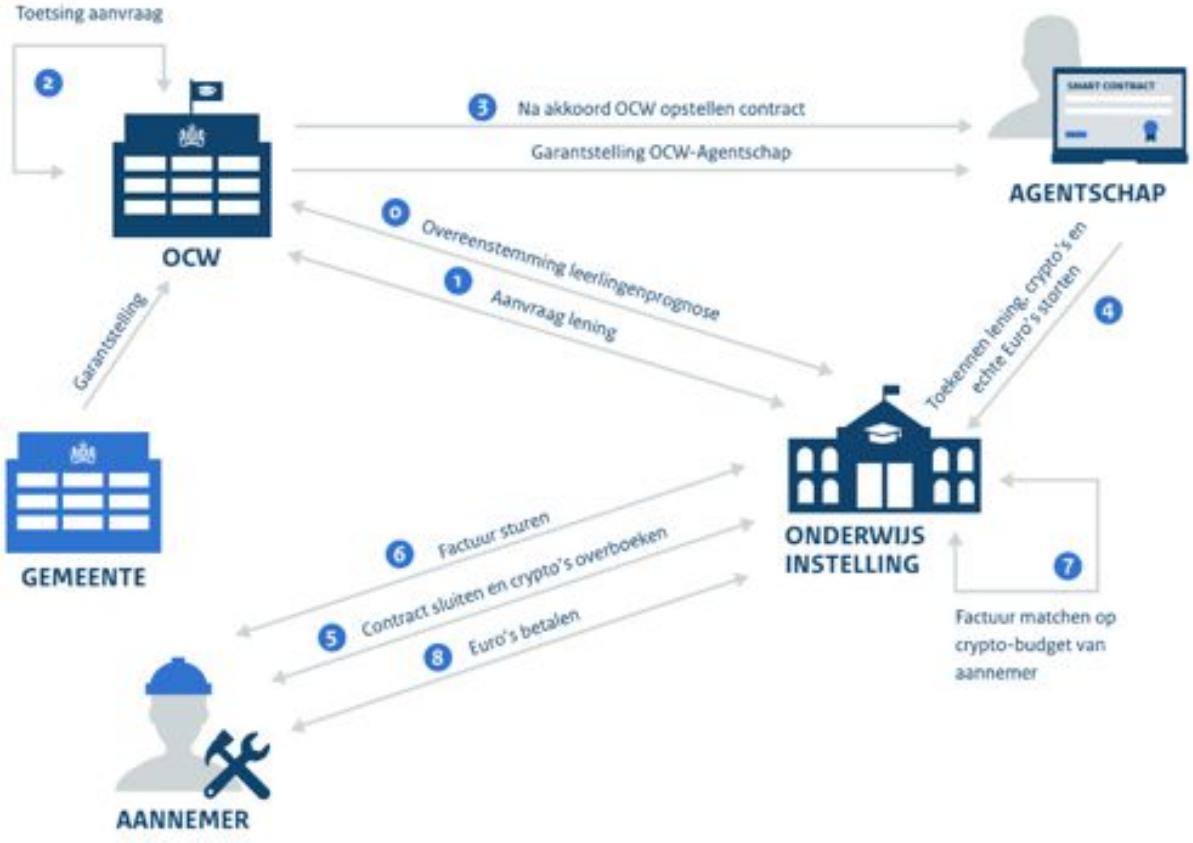
- Schatkistbankieren (Ministerie van Financiën)
- Transport van afvalstoffen (Inspectie voor Leefomgeving en Transport)

Maar ook:

- Kadaster
- Tickets (concerten, voetbalwedstrijden)
- Spaarpunten
- Verkiezingen
- Track & Trace supply chain (agri, fairtrade, diamanten)
- Veilig kopen van onbekenden
- Muziek luisteren en direct betalen aan de artiest
- Veilig documentenverkeer
- Broodfonds verzekeringen
- Persoonsgebonden budget
- Microbetalingen via internet
- Digitale identiteit
- Vergunningen
- Parkeerkaart
- OV-chipkaart
- Elektronisch patiëntendossier
- Handel in e-books en andere digitale goederen
- Energie

http://www.blockchainpilots.nl

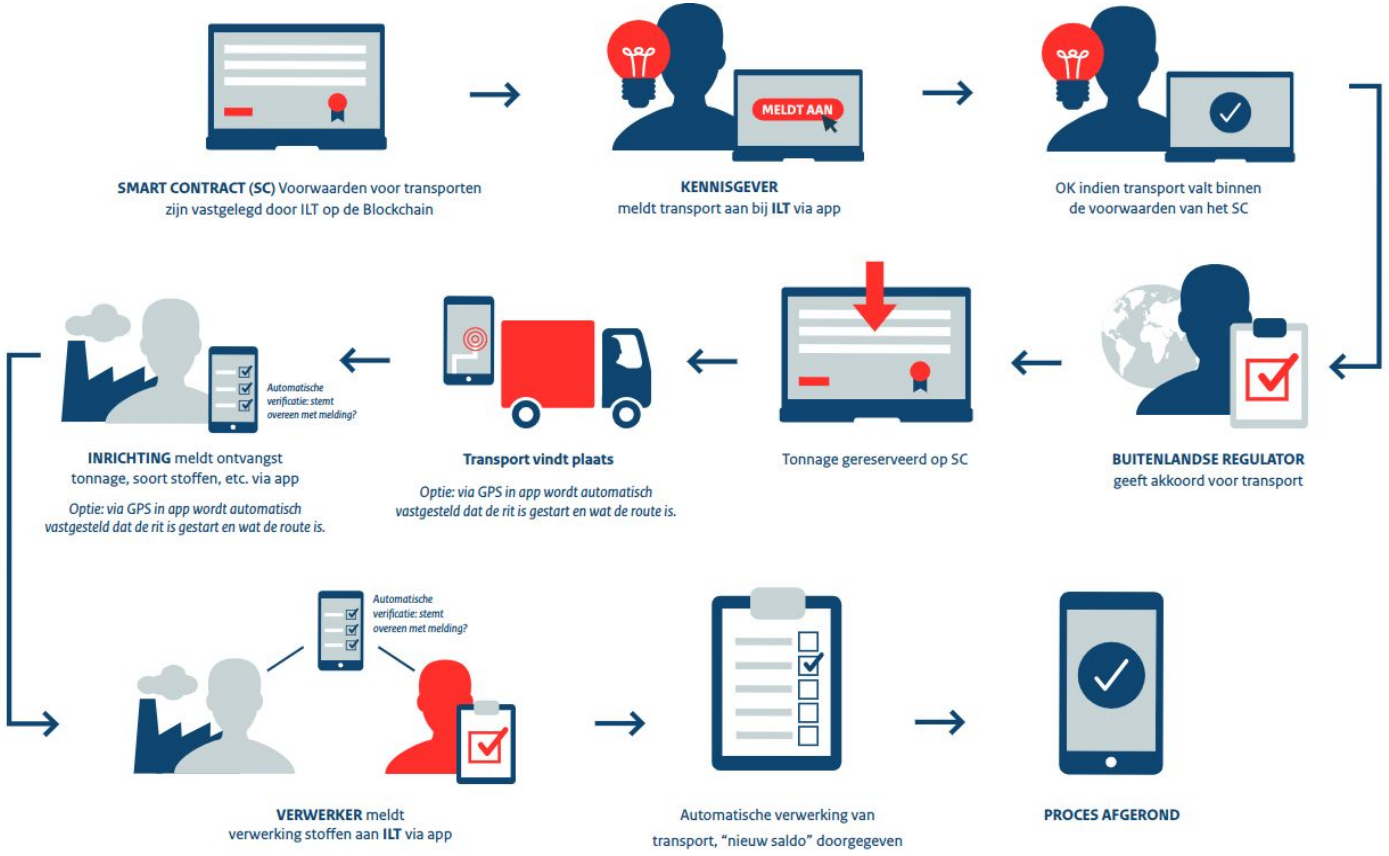
Case #1 - Schatkistbankieren (MinFin)



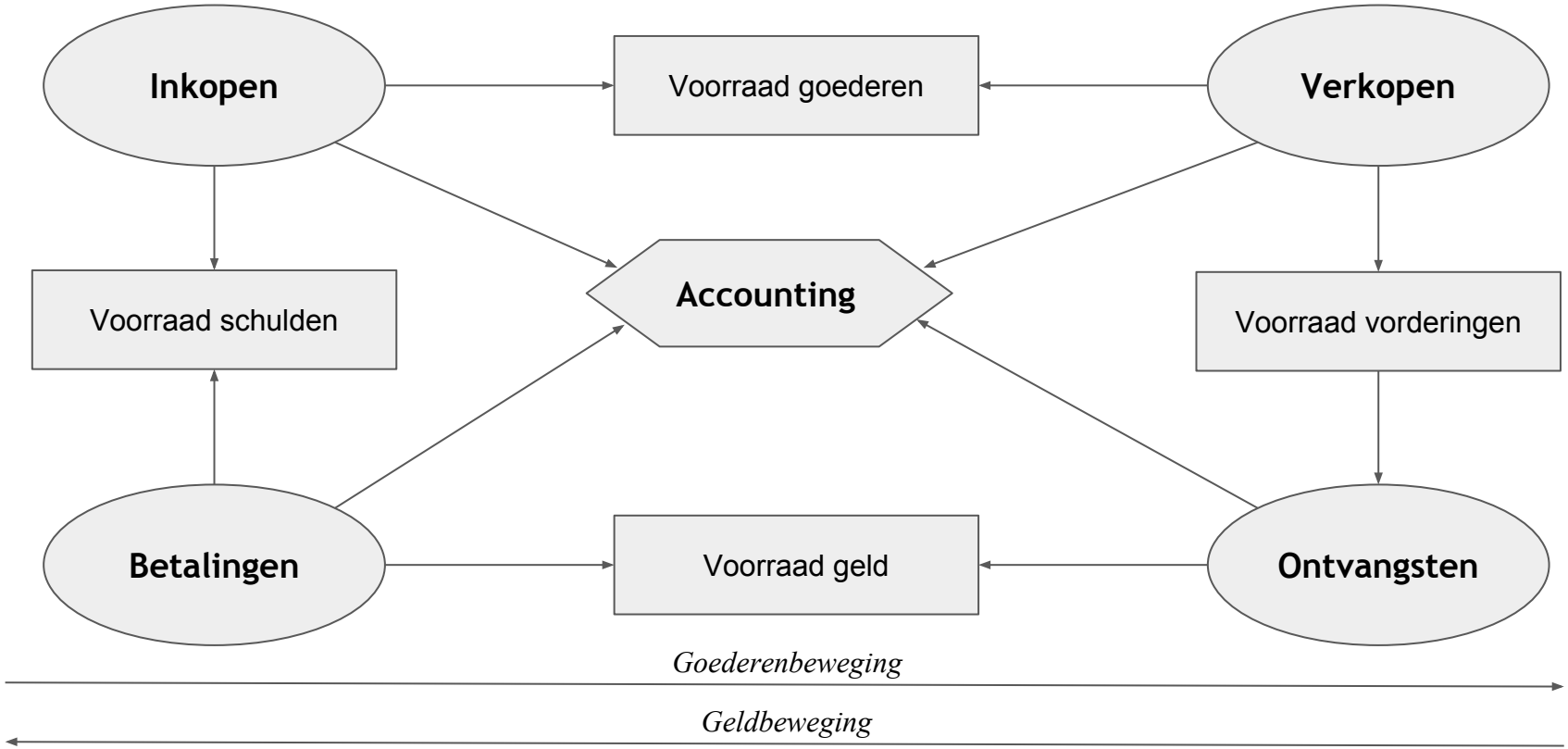
Case #1 - Schatkistbankieren (MinFin)

- Stap 1: Onderwijsinstelling vraagt OCW om een lening voor de realisatie van een *nieuw schoolgebouw*.
- Stap 2/3: Na goedkeuring door OCW wordt het agentschap gevraagd om het contract op te stellen.
- Stap 4: Het agentschap kent de lening toe, cryptovaluta en euro's worden overgeboekt.
- Stap 5: De onderwijsinstelling sluit een overeenkomst met een aannemer.
- Stap 6/7: De factuur van de aannemer wordt getoetst aan het cryptobudget van de onderwijsinstelling.
- Stap 8: De factuur van de aannemer wordt voldaan in euro's.

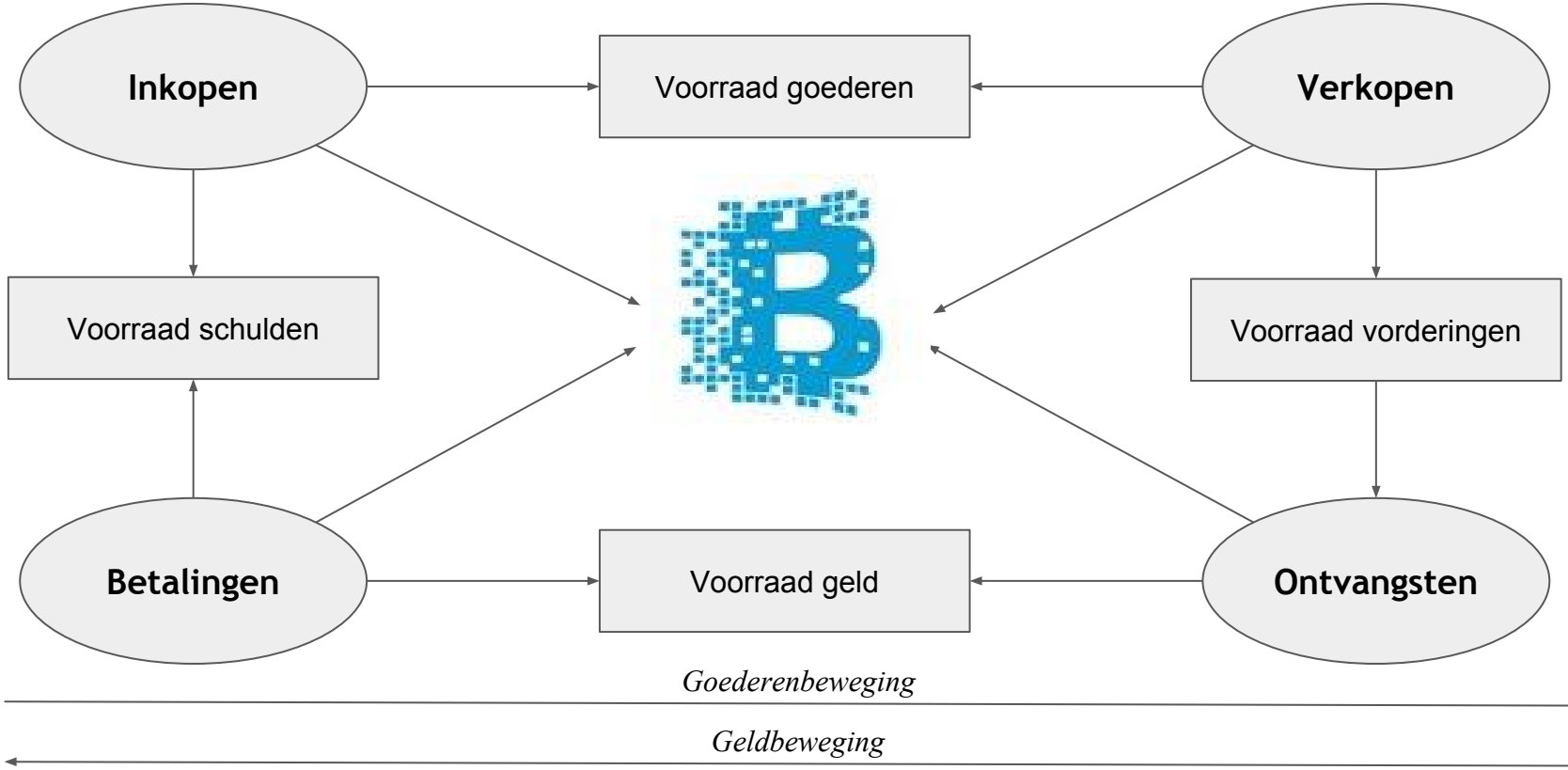
Case #2 - Transport van afvalstoffen (ILT)



Accounting - Nu



Accounting - Toekomst ?



Auditimplicaties

- Bijv. journaalposten worden automatisch door middel van hashes in de blockchain vastgelegd waardoor deze niet gewijzigd of verwijderd kunnen worden in de ERP systemen waarin ze zijn gemaakt
- De blockchain als zodanig kan en hoeft niet ge-audit te worden omdat cryptografie hier een voldoende preventieve werking heeft
- Het probleem zit in de smart contracts, de constructie van bedrijfsregels, de primaire invoer, de exchanges, de apps, de wijze waarop de echte wereld en de blockchain wereld via ‘tokenization’ met elkaar worden afgestemd, en andere systemen die gebruik maken van de blockchain om transacties te verifiëren
- De controlerende functie wordt overgenomen door trust protocols, dus audit van de trust protocols
- Data level assurance en reliability by default d.m.v. blockchain i.c.m. continuous auditing moet worden ingebouwd als systeem bij de auditee waardoor de audit zich op de AO/IB rondom dat systeem zal richten (NIET op de blockchain zélf)
- De audit zal ook gebruik maken van de controle van het werk en de systemen van IT dienstverleners
- De auditor kan een node worden in een private chain bij de auditee

Bron: Vaassen

Relativering

- Naarmate de populariteit en het gebruik van de blockchain toenemen, zal het systeem steeds meer kenmerken gaan vertonen van traditionele transactiesystemen waarin vertrouwde derde partijen tussen aanbieder en vragen in staan (voorbeeld Bitcoin)
- Het systeem vereist een enorme computerkracht bij de ‘miners’ met dienovereenkomstige investeringen maar ook energieverbruik
- Momenteel is de belangrijkste toepassing de Bitcoin; als die faalt, dan wordt dat ook gezien als een falen van de blockchain
- Alle systemen zullen op de schop moeten en het is maar de vraag of de huidige kennis daartoe toereikend is en of de baten hiervan tegen de kosten opwegen
- Samenwerking in ecosystemen is cruciaal; dit betekent dat voortdurend in gezamenlijke belangen van partijen in waardeketens moet worden gedacht; dit vereist een andere manier van denken

Bron: Vaassen

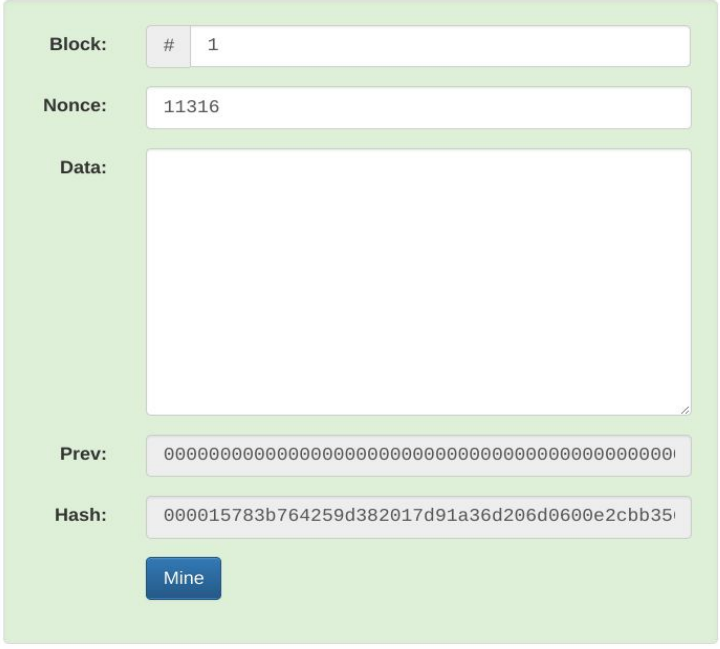
Meenemen

- Er is momenteel veel aandacht voor blockchain, wellicht zelfs over hyped
- Blockchain heeft grote mogelijkheden bij het verbeteren van de betrouwbaarheid van informatie en het bewaken van waarden
- Traditionele control en audit systemen zullen geheel op de schop moeten
- Er zijn veel mogelijke toepassingen van blockchain, maar wat tot nu toe is geïmplementeerd is zeer beperkt en zit veelal in de pilotfase
- Vraag je bij elk proces dat niet soepel verloopt af of de blockchain hier een mogelijke oplossing kan bieden, met daarbij de vraag of aan de vijf randvoorwaarden van toepassing van blockchain is voldaan:
    1. Er is een database
    2. Er zijn meerdere partijen die gegevens moeten kunnen schrijven naar die database
    3. Die partijen zitten in verschillende juridische dan wel economische entiteiten
    4. Er is géén vertrouwen tussen die partijen doordat ze elkaar niet kennen of het economisch niet zinvol is om in continuïteit informatie over elkaar te verzamelen die dit vertrouwen zou moeten geven
    5. De inschakeling van een vertrouwde derde partij is niet mogelijk of wenselijk

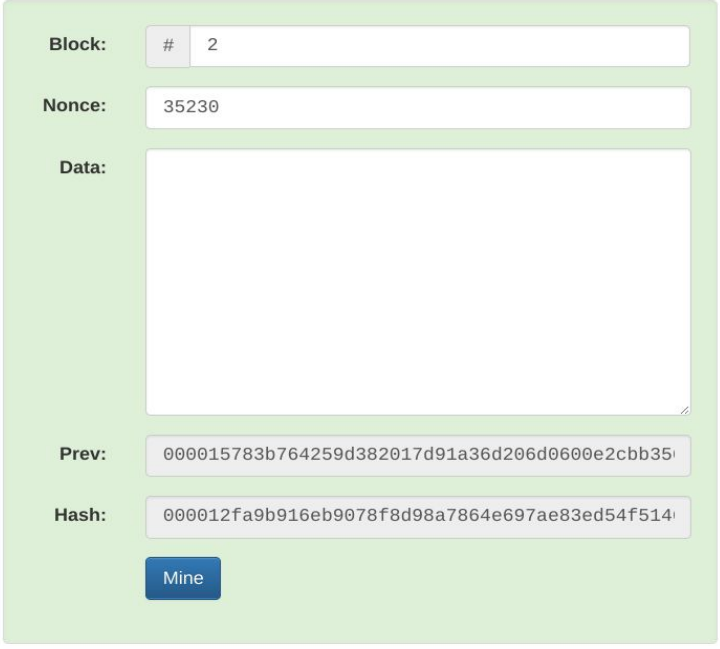
Bron: Vaassen

Demo “Hoe werkt blockchain” (generator)

> blockchain generator tool



> full youtube version



Bron: https://anders.com/blockchain/blockchain.html

https://www.youtube.com/watch?v=_160oMzblY8

Bron:

Dank u