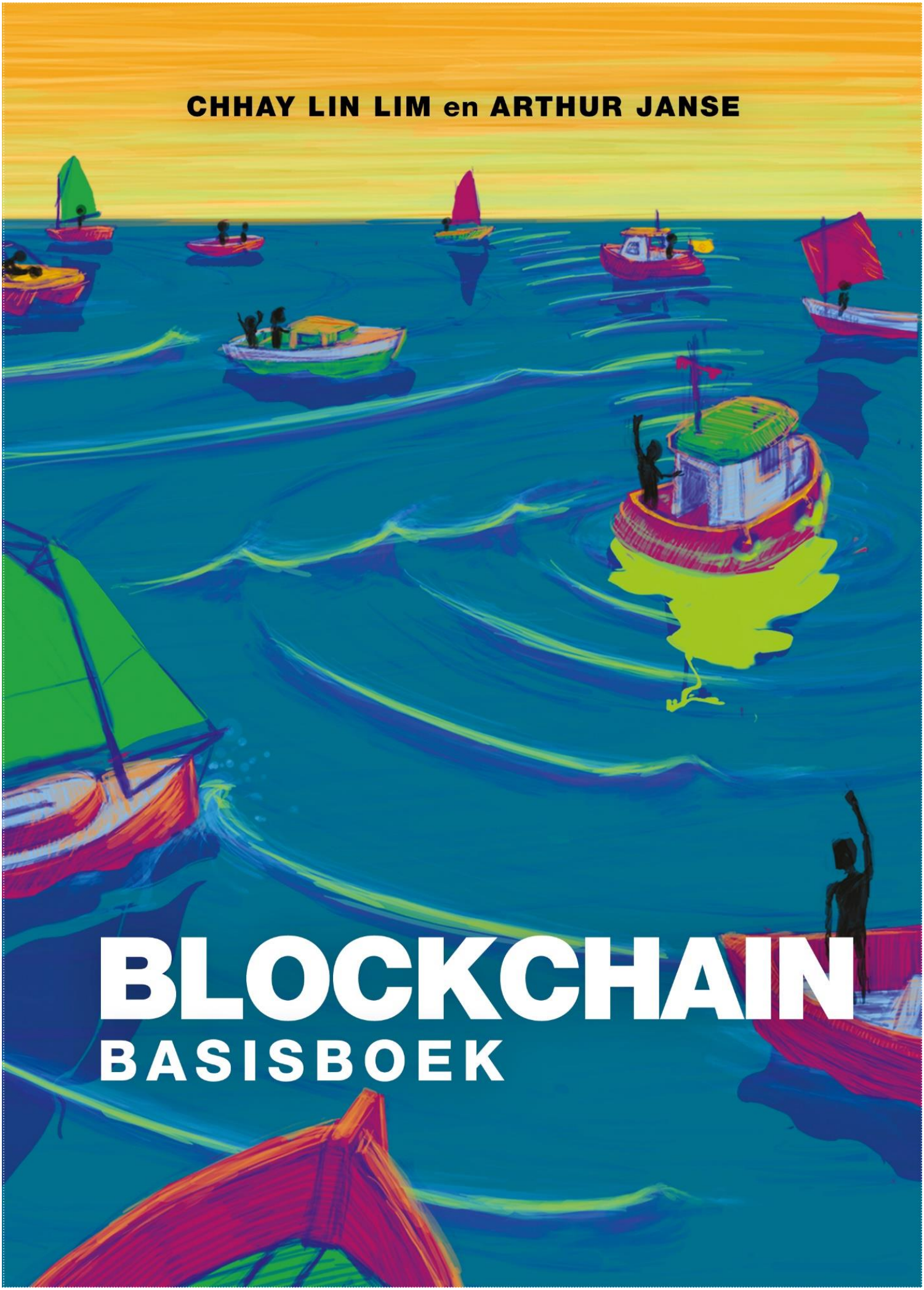
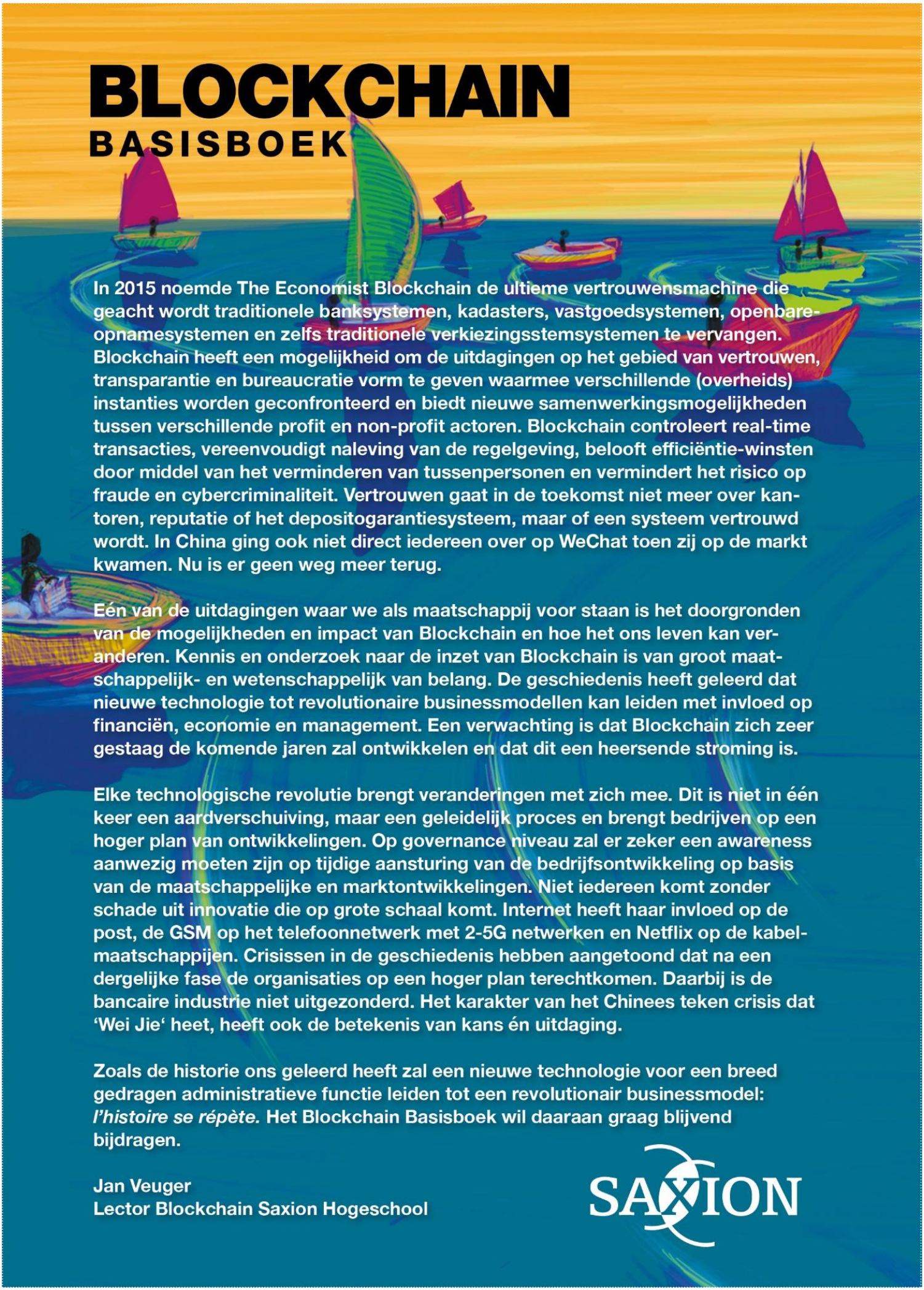
CHHAY LIN LIM en ARTHUR JANSE



BLOCKCHAIN
BASISBOEK

BLOCKCHAIN
BASISBOEK



In 2015 noemde The Economist Blockchain de ultieme vertrouwensmachine die geacht wordt traditionele banksystemen, kadasters, vastgoedsystemen, openbare-opnamesystemen en zelfs traditionele verkiezingsstemsystemen te vervangen. Blockchain heeft een mogelijkheid om de uitdagingen op het gebied van vertrouwen, transparantie en bureaucratie vorm te geven waarmee verschillende (overheids) instanties worden geconfronteerd en biedt nieuwe samenwerkingsmogelijkheden tussen verschillende profit en non-profit actoren. Blockchain controleert real-time transacties, vereenvoudigt naleving van de regelgeving, belooft efficiëntie-winsten door middel van het verminderen van tussenpersonen en vermindert het risico op fraude en cybercriminaliteit. Vertrouwen gaat in de toekomst niet meer over kantoren, reputatie of het depositogarantiesysteem, maar of een systeem vertrouwd wordt. In China ging ook niet direct iedereen over op WeChat toen zij op de markt kwamen. Nu is er geen weg meer terug.

Eén van de uitdagingen waar we als maatschappij voor staan is het doorgronden van de mogelijkheden en impact van Blockchain en hoe het ons leven kan veranderen. Kennis en onderzoek naar de inzet van Blockchain is van groot maatschappelijk- en wetenschappelijk van belang. De geschiedenis heeft geleerd dat nieuwe technologie tot revolutionaire businessmodellen kan leiden met invloed op financiën, economie en management. Een verwachting is dat Blockchain zich zeer gestaag de komende jaren zal ontwikkelen en dat dit een heersende stroming is.

Elke technologische revolutie brengt veranderingen met zich mee. Dit is niet in één keer een aardverschuiving, maar een geleidelijk proces en brengt bedrijven op een hoger plan van ontwikkelingen. Op governance niveau zal er zeker een awareness aanwezig moeten zijn op tijdige aansturing van de bedrijfsontwikkeling op basis van de maatschappelijke en marktontwikkelingen. Niet iedereen komt zonder schade uit innovatie die op grote schaal komt. Internet heeft haar invloed op de post, de GSM op het telefoonnetwerk met 2-5G netwerken en Netflix op de kabelmaatschappijen. Crisissen in de geschiedenis hebben aangetoond dat na een dergelijke fase de organisaties op een hoger plan terechtkomen. Daarbij is de bancaire industrie niet uitgezonderd. Het karakter van het Chinees teken crisis dat ‘Wei Jie‘ heet, heeft ook de betekenis van kans én uitdaging.

Zoals de historie ons geleerd heeft zal een nieuwe technologie voor een breed gedragen administratieve functie leiden tot een revolutionair businessmodel: *l’histoire se répète.* Het Blockchain Basisboek wil daaraan graag blijvend bijdragen.

Jan Veuger
Lector Blockchain Saxion Hogeschool

SAXION

BLOCKCHAIN

BASISBOEK

CHHAY LIN LIM

ARTHUR JANSE

Uitleg van de boekomslag door de illustrator

De ongekende mogelijkheden en uitgestrektheid van de oceaan symboliseert het internet. De diversiteit van boten met hun verschillende kleuren representeert de verscheidenheid van mensen die betrokken zijn bij blockchain. De lichtgevende boten zijn de full nodes van de blockchain die gedecentraliseerd van elkaar afliggen. Deze boten staan in verbinding met elkaar en met de andere boten, de gewone gebruikers, via lichtgevende rimpels op het water die lijken op het wifi-icoon. Aan de horizon komt de zon op. Met andere woorden: we staan aan het begin van een nieuwe dag, een nieuw tijdperk dat door blockchain wordt ingeluid.
Cheerted Keo, (Cheertedkeo.com)

Colofon:

Druk	De Boekdrukker Amsterdam
ISBN	978-90-9032191-2
NUR	781
1e oplage	januari 2020
Omslag	De Boekdrukker Amsterdam
Eindredactie	Chhay Lin Lim

Help het boek te vertalen naar het Engels
We willen graag iedereen de kans geven het Blockchain Basisboek te ontvangen en lezen. Daarom verzamelen we geld voor een Engelse vertaling. Vanuit het Engels kan het boek dan verder worden vertaald naar andere talen. Een goede vertaling kost €0,06 per woord dus we proberen in totaal €7.500 op te halen.

Wil jij een paar EUR bijdragen?
De meest transparante, goedkoopste en snelste manier ken je al: via Nederlandse aanbieders van cryptodiensten kun je met iDeal crypto's kopen en versturen naar een publiek blockchainadres. De goedkoopste aanbieders waar je ook kleine bedragen kunt sturen zijn https://www.litebit.eu/nl/kopen en https://anycoindirect.eu/nl.

Als je hier bijvoorbeeld €3,50 stuurt, gaat er netto €3,08 naar het adres toe. Het verschil van €0,42 zijn de administratiekosten van de cryptodienst. Deze diensten staan per 10 januari 2020 onder toezicht van de Nederlandsche Bank.

De publieke blockchain adressen die we hebben aangemaakt en waar je je bijdrage naar toe kunt sturen zijn:

Bitcoin: 1KEJZRuUjhgJtPri9tEDEk7HA2HweMbVgB

Ethereum: 0x5f570e4acb6cb0004218a0f74f334c16aa48befc

Je kunt via https://www.blockchain.com/explorer zien hoeveel geld er naar de rekeningen is gestuurd. Als we €7.500 ophalen brengen we het boek naar een vertaalbureau.
Bedankt!

Chhay en Arthur

Over de schrijvers

Chhay Lin Lim is medeoprichter van Serey, een op blockchain gebaseerde platform met verscheidene applicaties. Het initiële doel van Serey is om creativiteit en meningsuiting te stimuleren in voornamelijk Cambodja. Zo kun je op Serey.io artikelen plaatsen die op de blockchain worden bewaard en daardoor niet gecensureerd kunnen worden. Serey heeft ook een Serey Marktplaats waar mensen hun goederen en diensten kunnen aanbieden. Het doel hiervan is om vrijwillige economische associatie te stimuleren.

Daarnaast is hij docent/onderzoeker aan Saxion Hogeschool en lid aan het Saxion Blockchain Lectoraat. Hij ontwikkelt workshops met betrekking tot Blockchain en geeft les in de vakken Blockchain en Digital Technology (voorheen Financial Technology) binnen de minor Digital Business Models & Blockchain.

Daarvoor was hij werkzaam bij European Merchant Services (EMS), een FinTech-bedrijf in handen van First Data en ABN Amro. Daar verrichtte hij technische integraties van online betaalmethoden (creditcards, PayPal, iDEAL, Klarna, enzovoorts) met webshops.

Hij heeft een academische achtergrond in Economie en Filosofie. Beide onderwerpen zijn nog steeds zijn passie. Hier schrijft hij regelmatig over op Notesonliberty.com en Chhaylinlim.wordpress.com.

Hij ziet het als zijn doel om blockchaintechnologie toe te passen om de (financiële) soevereiniteit van mensen te waarborgen en hoopt ooit de realisatie van seasteads – micronaties op de oceaan – mee te maken.

Chhay Lin Lim
c.l.lim@saxion.nl

Arthur Janse heeft naast de studie Bedrijfswetenschappen aan de Universiteit van Nijmegen tevens de Controllersopleiding afgerond aan de Vrije Universiteit Amsterdam. Van 1997 tot 2014 werkte hij als Financieel Manager bij multinationals AkzoNobel en Hilti. Hij heeft ruim 12 jaar in het Midden-Oosten gewoond en gewerkt, waaronder in Turkije, Egypte en Dubai.

Na zijn terugkeer in 2014 naar Nederland heeft hij zich als docent op Saxion Hogeschool met passie geworpen op de toepassing van digitale technologieën als Big Data, Kunstmatige intelligentie, Robotic Process Automation en Blockchain.

Als kwartiermaker rond het thema Blockchain heeft hij een belangrijke bijdrage geleverd aan de oprichting van het Saxion Lectoraat Blockchain. In zijn rol als docent en onderzoeker werkt hij mee aan de ontwikkeling van Masterclasses voor bedrijven en overheid, organiseert hij workshops en de Saxion Blockchain Hackathon.

Persoonlijk investeert hij in blockchain bedrijven, en was hij zodoende betrokken bij onder andere de oprichting van blockchainbedrijf Blockchain Projects bv.

Arthur is er van overtuigd dat decentraler denken in de digitale wereld een niet te missen kans is; een wereld waar de eigen identiteit en data kunnen worden gebruikt om het initiatief bij het individu zelf te leggen. Als je je wil verdiepen wat dit voor jou en je (toekomstige) organisatie kan betekenen biedt dit basisboek een stevige introductie in de materie.

Arthur Janse
a.j.c.janse@saxion.nl

Voorwoord

In 2015 noemde The Economist blockchain de ultieme vertrouwensmachine die geacht wordt traditionele banksystemen, kadasters, vastgoedsystemen, openbare-opnamesystemen en zelfs traditionele verkiezingsstemsystemen te vervangen. Blockchain heeft een mogelijkheid om de uitdagingen op het gebied van vertrouwen, transparantie en bureaucratie aan te pakken, waarmee verschillende (overheids)instanties worden geconfronteerd en biedt nieuwe samenwerkingsmogelijkheden tussen verschillende profit- en non-profitactoren. Blockchain controleert real-time transacties, vereenvoudigt naleving van de regelgeving, belooft efficiëntiewinsten door middel van het verminderen van tussenpersonen en vermindert het risico op fraude en cybercriminaliteit. Een recente investering van ruim 56 miljoen EURO door ING in de nieuwe Utility Settlement Coin (USC) is een voorbeeld van investeringen in een blockchaintechnologie om het huidige stroperige proces van afwikkelen van financiële transacties te vergemakkelijken. Vertrouwen gaat in de toekomst niet meer over kantoren, reputatie of het depositogarantiesysteem, maar over of een systeem werkt. Bedrijven als bijvoorbeeld Amazon, Google, Apple, Uber en Airbnb bieden sublieme technologische ervaringen, maar kennen ook kritische kanttekeningen. In China ging ook niet direct iedereen over op WeChat toen zij op de markt kwamen. Nu is er geen weg meer terug.

Eén van de uitdagingen waar we als maatschappij voor staan, is het doorgronden van de mogelijkheden en impact van blockchain en hoe het ons leven kan veranderen. Kennis en onderzoek naar de inzet van blockchain met het adagium ‘Is de technologie op zoek naar een probleem of ondersteunt zij juist maatschappelijk ontwikkelingen?’, is van groot belang. De geschiedenis heeft geleerd dat nieuwe technologie tot revolutionaire businessmodellen kan leiden, met invloed op financiën, economie en management. Een grote vraag is hoe snel blockchain zich gaat ontwikkelen, evenals haar toepassingen. Stephen Hawking schreef in zijn laatste boek *Brief answers to the big questions* hoe we de toekomst vorm kunnen geven. Hij schreef:

> “In the same way that the internet, our mobile phones, medical imaging, satellite navigation and social network would have been incomprehensible tot the society of only a few generations ago, our future world beginning to conceive. Information on its own will not take us there, but intelligent and creative use will.” (Hawking 2018: 207)

Met blockchaintechnologie kan een meer duurzame, veilige en betrouwbare digitale infrastructuur worden gebouwd. Dat maakt deze technologie in potentie revolutionair. Maar omdat blockchaintechnologie ook erg complex is en nog in de kinderschoenen staat, kan deze potentie alleen worden gerealiseerd als open wordt samengewerkt. Enerzijds, omdat vanwege de complexiteit het bundelen van kennis nodig is. Anderzijds, omdat het decentrale karakter van blockchain vraagt om nieuwe, decentrale vormen van governance. Een intensieve samenwerking is een vereiste tussen verschillende opleidingen, maar ook in onder andere de Dutch Blockchain Coalition (2018). Wereldwijd groeien in rap tempo blockchains for money (financieel gewin, privaat eigendom) en blockchains for control (vergaren van data, staatscontrole), maar de ontwikkeling van blockchains for good (publiek belang, collectief eigenaarschap) blijven achter.

Elke technologische revolutie brengt veranderingen met zich mee. Hierbij komen er nieuwe businesscases en verdwijnen er bedrijven. Dit is niet in één keer een aardverschuiving, maar een geleidelijk proces en brengt bedrijven als bijvoorbeeld Leica, Wehkamp en Volvo op een hoger plan van ontwikkelingen. Op governanceniveau moet er zeker een awareness aanwezig zijn op tijdige aansturing van de bedrijfsontwikkeling, op basis van de maatschappelijke en marktontwikkelingen. Niet iedereen komt zonder schade uit innovatie die op grote schaal komt. Internet heeft haar invloed op de post, de GSM op het telefoonnetwerk met 2-5G netwerken en Netflix op de kabelmaatschappijen. Crisissen in de geschiedenis hebben aangetoond dat na een dergelijke fase de organisaties op een hoger plan terechtkomen. Daarbij is de bancaire industrie niet uitgezonderd. Het karakter van het Chinese teken voor crisis, dat ‘Wei Jie’ heet, heeft ook de betekenis van kans en uitdaging.

Zoals de historie ons geleerd heeft zal een nieuwe technologie voor een breed gedragen administratieve functie leiden tot een revolutionair businessmodel: l'histoire se répète. De tijd zal het ons vertellen. Dit Blockchain Basisboek wil daaraan graag blijvend bijdragen.

Jan Veuger
Lector Blockchain

Inleiding

Chhay Lin Lim over het boek

Het Blockchain Basisboek dat voor je ligt, is voortgekomen uit een diep verlangen om de filosofische, ethische, economische, technologische en bedrijfskundige relevantie van blockchain op coherente wijze in beeld te brengen voor studenten. Sinds de publicatie van de Bitcoin white paper uit november 2008 door Satoshi Nakamoto is er redelijk wat gepubliceerd over blockchain, maar er is zelden een Nederlandstalig boek op de markt gekomen met een gesubstantieerd holistische blik op dit onderwerp.

De kracht van dit boek is dat blockchain wordt benaderd vanuit een breed scala aan perspectieven. De verwachting is dat de lezer de relevantie van blockchain hierdoor beter kan ontleden en een dieper begrip krijgt van de mogelijkheden van blockchain. Een bijkomend voordeel is dat het Blockchain Basisboek de lezer structuur biedt in zijn leerdoelen. Het zal naar verwachting een aanzienlijke bijdrage leveren aan het structureel verbeteren van de module Blockchain binnen de Saxion minor Digital Business Models & Blockchain. Hoewel het boek is geschreven voor studenten, hebben ook niet-studenten die geïnteresseerd zijn in blockchain profijt van het lezen van dit boek.

Ikzelf heb een diepe persoonlijke reden waarom ik geïnteresseerd ben geraakt in blockchain. Ik kwam voor het eerst in aanraking met blockchain in 2011, toen ik op financieel-economische fora en nieuwssites hoorde over de belofte dat Bitcoin, de eerste applicatie van de blockchaintechnologie, de monopolie op geldproductie van centrale banken kon ontnemen. Niet vermoedende dat Bitcoin een uiterst coherent en revolutionair hoogstandje was, negeerde ik dergelijke artikelen tot eind 2011. Bij het lezen van de achterliggende gedachte van Bitcoin vanaf eind 2011 - begin 2012 begon langzaamaan te dagen dat de technologie wellicht toch tot enorme ontwrichting van de samenleving zou kunnen leiden. Met de bagage van inmiddels acht jaren blockchain, heb ik in vergelijking tot vele anderen een schat aan ervaring – hoewel ik me nog steeds een kind voel binnen de snel veranderende blockchainwereld.

Ik herinner me nog het enthousiasme van de eerste blockchainpioniers die fora vol met geeks en ideologen vulden met poëtische teksten over hoe blockchain de mensheid vrijer zou maken. Dit was een tijd zonder ICO’s en een tijd waarin mensen niet in de blockchainwereld stapten voor het geld, maar om een technologie te helpen introduceren die de samenleving vooruit zou helpen.

Er is voor mij haast geen betere periode geweest om in aanraking te komen met Bitcoin. De financiële crisis was enkele jaren eerder losgebarsten in 2007. De wereld kampte nog met de nasleep, of wellicht beter gezegd met de nog steeds razende storm, die het financieel-economische landschap heeft geroerd. Deze periode heeft aangetoond dat ons financiële systeem zeer fragiel is. Het ziet er inmiddels ook naar uit dat het beleid om de economie op gang te houden door middel van lage rentestanden, het vergroten van de geldhoeveelheid en consumptiestimulansen slechts een kortstondige oplossing van centrale banken en overheden is geweest. Tot de dag van vandaag zijn rentestanden nog historisch laag, in sommige gevalen zelfs negatief. Voor degenen onder ons die nooit hebben geloofd dat zulk beleid goed zou zijn voor onze economie en samenleving, is het aantrekkelijk om verder te kijken naar een alternatieve oplossing die het financieel systeem drastisch zou kunnen veranderen. Een dergelijke oplossing, Bitcoin en de onderliggende blockchaintechnologie, staat centraal in dit boek.

Wat Bitcoin zo interessant maakt, is dat het niet alleen een protest is tegen het huidige financiële systeem, maar ook een protest tegen het intellectuele establishment met zijn vele theoretische aannames van onze economische realiteit. De financiële crisis heeft voor sommige mensen de ogen geopend, dat sommige klassen van bijvoorbeeld macro-economische experts geen experts zijn. Sterker nog, deze gecentraliseerde clubs van experts – centrale bankiers, beleidsmakers bij de overheid, banken, enzovoorts – zijn net als de rest van ons onwetend over de krachten die onze macro-economische realiteit vormgeven. Bitcoin onderkent deze onwetendheid van experts en biedt ons een alternatief waarbij er geen centraal orgaan is die pretendeert te weten hoe ons financiële systeem moet worden ingericht. Het economisch-sociale systeem waar we in leven is voor een centraal orgaan namelijk te complex om te begrijpen, waardoor het onmogelijk is onze samenleving zo in te richten dat er geen ongewenste consequenties uit voort zullen vloeien. Wij zouden, zoals Friedrich Hayek al schreef in *The Constitution Of Liberty* (1960) de limieten van onze eigen kennis met betrekking tot de inrichting van onze samenleving moeten onderkennen:

> "No human mind can comprehend all the knowledge which guides the actions of society."

Bitcoin speelt op drie manieren in op deze epistemologische bescheidenheid. Ten eerste maakt Bitcoin gebruik van een gedecentraliseerd netwerk, waarin alle individuen die willen deelnemen aan het besluitproces van Bitcoin – elk in bezit van hun eigen particuliere kennis –

samen deelnemen aan besluitvorming. Ten tweede is de Bitcoin-code open source. Ten derde wordt de markt van geldproductie opengebroken. Betekent het dat een gedecentraliseerd netwerk waarin consensus moet worden bereikt over de richting die Bitcoin moet inslaan, altijd zal leiden tot de juiste besluiten? Dat niet. Echter, is de Bitcoin-code wel open source waardoor anderen makkelijk de broncode kunnen inzien, kopiëren en bewerken naar eigen inzichten, zodat nieuwe experimenten met andere, wellicht betere vormen van cryptovaluta en andere vormen van consensus kunnen ontstaan. Het heeft de markt van geldproductie geopend, de barrière om deel te nemen aan de industrie van geldproductie verlaagd en de competitie binnen de industrie van geldproductie geïntensiveerd. Met het doorbreken van de monopolie op geldproductie door overheden en centrale banken is er een historische fase gestart waarin elk individu een eigen valuta kan creëren die in potentie kan concurreren met nationale gelden. Hiermee is Friedrich Hayeks visie om geld te denationaliseren en de monopolie op geldproductie te doorbreken, werkelijkheid geworden.

Toch is het niet alleen het financiële systeem dat zal worden beïnvloed door Bitcoin en blockchain. Met name de onderliggende technologie, blockchain, biedt nieuwe technologische mogelijkheden om ook andere industrieën te transformeren.

Tot slot wil ik vermelden dat de komende jaren steeds meer oproepen zullen komen om breed maatschappelijke discussies over cryptovaluta's en blockchain te voeren. Wanneer mensen zeggen dat we de samenleving moeten betrekken bij het bediscussiëren van de ethiek van cryptosystemen, moeten we ons afvragen waarom de samenleving opeens aandacht schenkt aan de grote vorderingen die de cryptowereld maakt. Waar komt de aandacht vandaan?

Terug in 2011, beschouwde de samenleving ons als vreemd en slecht geïnformeerd. Encryptie, digitaal geld, anonieme netwerken, digitale pseudoniemen, Zero-Knowledge, online reputaties, informatiemarkten, zwarte markten en het verval van natiestaten werden openlijk besproken binnen de cryptowereld en het publiek besteedde vrijwel geen aandacht.

6-7 jaren later, nadat Bitcoin heeft aangetoond niet slechts een rage te zijn, volgen sommige groepen in de samenleving de ontwikkelingen van cryptosystemen nauwlettend en proberen ze het discours te leiden 'in het belang van de samenleving'. Wie zijn zij en wat zijn hun belangen? Banken, centrale banken en nationale overheden. Zij proberen het discours rond cryptosystemen te vormen, omdat (a) banken bang zijn dat een deel van hun operaties overbodig worden gemaakt door cryptosystemen, (b) centrale banken vrezen dat ze controle

verliezen op het monetair beleid en (c) nationale overheden angstig zijn dat hun nationale valuta's zullen worden uitgeconcurreerd door cryptovaluta's en ze geen cryptobetalingen meer kunnen traceren. Wanneer zij oproepen tot maatschappelijke discussies over de ethiek en consequenties van cryptosystemen, zullen zij dus eerder geneigd zijn om de discussies te betreden vanuit een positie van angst. Kunnen we dan werkelijk substantiële discussies voeren met deze groepen? Of zullen zij, al gemotiveerd om cryptosystemen te overreguleren, de discussies betreden en alles wat mooi is aan cryptosystemen bederven zodat deze systemen hun modi operandi niet bedreigen?

Het punt dat ik wil maken is dat we voorzichtig moeten zijn en moeten waken voor hen die nobel roepen dat we meer maatschappelijke discussies moeten voeren over cryptovaluta's en blockchain. Ik hoop dat je met de informatie die je in dit boek zult treffen, de fictie en realiteit van blockchain kunt onderscheiden en je met een open blik en sociologische verbeeldingskracht discussies in het maatschappelijk belang zult betreden.

Je zult in het vervolg van het boek meer lezen over de consequenties en mogelijke disrupties die Bitcoin en blockchain teweeg kunnen brengen. Voordat we echter zover zijn om dit te behandelen, bespreken we eerst de basisbeginselen van blockchain.

Chhay Lin Lim
Medeoprichter van Serey.io
Docent/onderzoeker bij Saxion Hogeschool

Arthur Janse over het boek

Toen me als student begin jaren negentig werd verteld dat internet het in de toekomst mogelijk zou maken om vanuit de bank een bioscoopkaartje te bestellen en betalen, ging een wereld voor me open. ‘Onmogelijk’, dacht ik nog. ‘Een revolutie’.

En een revolutie was het. Internet leidde tot een enorme toename van ons welzijn. Niet meer verdwalen met de auto in Parijs omdat je even de nieuwste wegenkaart niet hebt. Niet meer 3 maanden wachten voordat een film ook in Nederland uit is. Niet meer langs een reisbureau voor een netnietwatjezoekt reis, maar zelf achter de pc lekker kiezen wat je wilt.
Snel, eenvoudig en goedkoop. Een echte digitale revolutie mogelijk gemaakt en gebruikt door de generatie veertigers en vijftigers die nu in de maatschappij zoveel invloed uit kunnen oefenen.

Dus toen Bitcoin en blockchain voor het eerst werden genoemd was ik er klaar voor. ‘Stap 2’, dacht ik. ‘Hierop hebben we gewacht om nu echt alles uit internet te halen’. Decentraal vertrouwen, directe uitwisseling van eigendom, vertrouwelijke uitwisseling van ideeën, een potentiële bron van innovatie voor elk individu, macht neerleggen bij het individu. Et cetera, et cetera.

Blockchain is één van de veelbelovende ontwikkelingen die ik zo kan noemen. Naast kunstmatige intelligentie, Internet of Things, biomechanica en andere 4^{e} industriële revolutie ontwikkelingen. Niet alleen de technologie, maar de gedachte erachter en de maatschappelijke kansen die het biedt zijn superspannend. En ze bieden een mooi penseel waarmee je als huidige generatie student de toekomst in kan gaan kleuren over de komende 10-20 jaar. Blockchain is niet voor alles een oplossing. Je koffie gaat het niet zetten. En er is nog genoeg werk aan de winkel. Maar het bestaat, het ontwikkelt zich en jij kunt hieraan meehelpen. Hopelijk biedt dit boek hiertoe een eerste handvat. Succes, en geniet ervan!

Arthur Janse
Docent FinTech bij Saxion Hogeschool
Saxion Blockchain Lectoraat

Leeswijzer

Het boek is opgedeeld in de volgende drie delen:

Deel I: De technische aspecten van blockchain en relevante innovaties die door blockchain zijn geïnitieerd of worden ondersteund.

Deel II: De ontstaansgeschiedenis en economisch-filosofische achtergrond van blockchain.

Deel III: Bedrijfstoepassingen van blockchain.

Binnen deze delen hebben de hoofdstukken een vaste indeling. Elk hoofdstuk begint met leerdoelen en een inleiding in de eerste paragraaf. Vervolgens komt de inhoud aan bod in aparte paragrafen. Als afsluiting heeft elk hoofdstuk een paragraaf met een samenvatting, opmerkingen die je na het lezen van het hoofdstuk uit kunt leggen, een verklarende begrippenlijst en de gebruikte bronnen in dat hoofdstuk.

In de hoofdstukken worden intermezzo's gebruikt voor teksten die niet tot het onmisbare deel horen, maar wel de tekst verder helpen verduidelijken.

Waar in dit boek de aanspreekvorm 'hij' wordt gebruikt, kun je ook 'zij' lezen. In het boek is gekozen voor het mannelijke voornaamwoord.

Bitcoin- en Ethereumeenheden

Aantallen in Satoshi	Aantallen in Bitcoin
1 Satoshi	0,00000001 ₿
10 Satoshi	0,00000010 ₿
100 Satoshi	0,00000100 ₿
1.000 Satoshi	0,00001000 ₿
10.000 Satoshi	0,00010000 ₿
100.000 Satoshi	0,00100000 ₿
1.000.000 Satoshi	0,01000000 ₿
10.000.000 Satoshi	0,10000000 ₿
100.000.000 Satoshi	1,00000000 ₿

Aantallen in Wei	Naam en inspirator
1 Wei	Wei (Wei Dai)
10 Wei	
100 Wei	
1.000 Wei	Babbage (Charles Babbage)
10.000 Wei	
100.000 Wei	
1.000.000 Wei	Lovelace (Ada Lovelace)
10.000.000 Wei	
100.000.000 Wei	
1.000.000.000 Wei	Shannon (Claude Shannon)
10.000.000.000 Wei	
100.000.000.000 Wei	
1.000.000.000.000 Wei	Szabo (Nick Szabo)
10.000.000.000.000 Wei	
100.000.000.000.000 Wei	
1.000.000.000.000.000 Wei	Finney (Hal Finney)
10.000.000.000.000.000 Wei	
100.000.000.000.000.000 Wei	
1.000.000.000.000.000.000 Wei	Ether

DEEL I: TECHNISCHE ASPECTEN VAN BLOCKCHAIN EN RELEVANTE INNOVATIES

Deel I bevat in totaal 12 hoofdstukken en behandelt de technische aspecten en relevante innovaties van blockchain. We beginnen met te kijken naar hoe de Bitcoin blockchain werkt en gaan gedurende het deel over naar andere blockchainprojecten.

In hoofdstuk 1 beginnen we met een korte uitleg van blockchainbeginselen. Hierbij definiëren we wat blockchain is en splitsen we de eigenschappen van blockchain in inherente en emergente eigenschappen. Als je hoofdstuk 1 hebt gelezen, dan zul je merken dat je al direct een gesprekspartner bent over blockchain.

In hoofdstuk 2 behandelen we het huidige betaalproces. De ambitie van Bitcoin is om een peer-to-peerbetaalsysteem te worden. Het is om die reden relevant om te begrijpen hoe het huidige betaalproces werkt, zodat de urgentie van Bitcoin en cryptovaluta beter kan worden toegelicht. In het hoofdstuk kijken we voornamelijk naar iDEAL en creditcardbetalingen.

In hoofdstuk 3 maken we een duidelijker onderscheid tussen de cryptovaluta Bitcoin en het Bitcoin-netwerk. Het consensusmechanisme van Bitcoin, Proof-of-Work, en de verschillen tussen het Bitcoin betaalsysteem en reguliere betaalsystemen komen nadrukkelijk aan bod.

In hoofdstuk 4 bespreken we mijning, nodes, Bitcoin updates en forks. Hierbij behandelen we wat mijners doen, krijgen we meer inzicht waarom het Bitcoin-netwerk zoveel energie kost en begrijpen we ook beter waarom het Bitcoin-netwerk zo veilig is. Daarnaast bespreken we andere typen nodes dan mijners en zien we hoe updates worden doorgevoerd in een gedecentraliseerd netwerk als Bitcoin. We zien ook wat er gebeurt wanneer er onenigheden bestaan in de community en het ene deel een update wel doorvoert en het andere niet.

In hoofdstuk 5 kijken we naar symmetrische, asymmetrische (public key) en Zero-Knowledge cryptografie. Cryptografie is een essentieel element van blockchain, omdat we daarmee de authenticiteit van data kunnen vastleggen en verifiëren. Daarnaast wordt er ook een context geschetst waarin cryptografie werd uitgevonden en hoe cryptografen en digitale rechtenactivisten vanaf de uitvinding van public key cryptografie op gespannen voet staan met overheden die niet willen dat burgers beschikken over onkraakbare communicatie.

In hoofdstuk 6 stappen we over naar Proof-of-Stake, een ander consensusmechanisme dan dat wordt gebruikt bij Bitcoin. We behandelen de verschillende varianten van Proof-of-Stake en zetten de eigenschappen van dit consensusmechanisme af tegen Proof-of-Work. Ook kijken we naar de performance van een blockchain en behandelen we de urgentie om blockchains schaalbaarder te maken. Hierbij bespreken we een aantal potentiële technieken die worden toegepast of onderzocht om de schaalbaarheid te vergroten.

In hoofdstuk 7 kijken we naar 51%-aanvallen en decentralisatie. We behandelen hoe een 51%-aanval werkt bij Proof-of-Work en bij Proof-of-Stake. Daarnaast bespreken we het blockchaintrilemma en werpen we een genuanceerder blik op het concept decentralisatie.

In hoofdstuk 8 behandelen we blockchain 2.0, smart contracts en applicaties die worden gebouwd op een blockchainplatform. Het blockchain 2.0-platform dat we onder de loep nemen is Ethereum. Het is relevant voor ons om te beseffen wat de mogelijke impact gaat worden op ons leven als er meer blockchainapplicaties komen die vertrouwde tussenpartijen eruit halen. Denk hierbij bijvoorbeeld aan een platform als Uber zonder Uberbedrijf of een socialmediaplatform als Facebook, maar dan zonder een Facebookbedrijf.

In hoofdstuk 9 komt blockchain governance aan bod. Binnen een decentraal netwerk waarbij er geen vertrouwde tussenpartijen zijn, is governance een grote uitdaging. Hoe moeten we de blockchain zo inrichten dat mensen worden gestimuleerd om goed gedrag te vertonen? Ook bespreken we besluitvormingsrechten en accountability. De governance ziet er anders uit voor verschillende typen blockchains: publiek, privaat en consortium. Daarnaast kunnen blockchains ook permissionless en permissioned zijn.

In hoofdstuk 10 kijken we naar cryptoeconomics, een nieuwe discipline die is opgekomen door de komst van blockchain. Het houdt zich bezig met de productie, consumptie en welvaartsoverdracht door middel van computernetwerken, toegepaste cryptografie, speltheorie en softwareontwikkeling. Daarnaast kijken we ook naar de verschillende typen cryptografische tokens en hoe ze eventueel kunnen worden ingezet binnen een blockchain.

In hoofdstuk 11 geven we een overzicht van de geschiedenis van het internet. Hierbij komt ook naar voren wat de beloften waren van het internet en hoe we met de komst van blockchain de beloften wellicht kunnen waarmaken.

In hoofdstuk 12 behandelen we tot slot de ontwikkeling in digitale identiteiten. De Self-Sovereign Identity komt nadrukkelijk aan bod. Blockchain maakt het mogelijk om onze digitale identiteit beter te beschermen en ons meer eigenaarschap te geven over onze digitale data.

Na deel I gaan we verder op de grotere achterliggende sociaal-economische en filosofische gedachten die de Bitcoin blockchain hebben beïnvloed.

1. Een korte uitleg van blockchainbeginselen

"Sorry to be a wet blanket. Writing a description for this thing for general audiences is bloody hard. There's nothing to relate it to."

- Satoshi Nakamoto (2010)

1.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Dat blockchain in essentie een gedistribueerd grootboek is, waarin je verschillende data kunt opslaan.
- Blockchain op het laagste en middelniveau kennen aan de hand van het Bitcoin-voorbeeld, zodat je na afloop van het hoofdstuk al een gesprekspartner bent.
- Wat de inherente en emergente eigenschappen zijn van blockchain.
- Wat de verschillen zijn tussen een blockchainnetwerk en een gecentraliseerd netwerk.

Inleiding

Op 31 oktober 2008, werd er onder de naam Satoshi Nakamoto een e-mail uitgestuurd naar een lijst van deelnemers op de Cryptography mailing list.[1] In de mail stond een verwijzing naar een ***white paper*** getiteld *Bitcoin: A Peer-to-Peer Electronic Cash System*. In de e-mail staat dat Satoshi heeft zitten werken aan een nieuw elektronisch geldsysteem dat volledig peer-to-peer is, waar geen 3e partij tussen zit. Dit systeem maakt het mogelijk om online betalingen te verzenden naar een andere partij, zonder dat er een financieel instituut benodigd is. Het betaalmiddel dat hierbij wordt gebruikt, is een totaal nieuwe digitale munteenheid, genaamd Bitcoin.

De belangrijkste eigenschappen van dit geldsysteem zijn volgens Satoshi Nakamoto:

1. Double-spending wordt voorkomen met een peer-to-peernetwerk.
2. Er is geen munthuis of 3e partij die de rol van het munten op zich neemt.
3. Deelnemers kunnen anoniem zijn.

[1] De originele e-mail is te vinden via: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

4. Nieuwe munten komen in omloop door middel van een Proof-of-Work-mechanisme dat lijkt op die van Hashcash.
5. Dit Proof-of-Work-mechanisme drijft ook het netwerk aan om double-spending te voorkomen.

Sleuteltermen als double-spending, peer-to-peernetwerk, Proof-of-Work, Hashcash, timestamps, hashing, digital signatures die in de e-mail naar voren komen, maken het moeilijk voor het algemeen publiek om blockchain te begrijpen. Zeker omdat er nog niet eerder iets was, wat goed met blockchain te vergelijken was. Het is echter wel essentieel om deze termen te begrijpen als we blockchain willen doorgronden.

Dit hoofdstuk begint met een korte laagdrempelige introductie op wat blockchain is (paragraaf 1.2). Dit word in paragraaf 1.3 gevolgd door een uitgebreidere uitleg van belangrijke eigenschappen die een blockchain bezit. Tot slot ronden we het hoofdstuk in paragraaf 1.4 af met een samenvatting, een lijst van belangrijke woorden en een bronnenlijst.

1.2 Blockchain op het eenvoudigste niveau uitgelegd

Een blockchain is op verschillende niveaus uit te leggen. Op het eenvoudigste niveau wordt er vaak een simpele en ongenuanceerde analogie gelegd, met een database of een grootboek dat alle transacties bijhoudt. Een exacte kopie van dit grootboek is verdeeld over verschillende computers die op het netwerk zijn aangesloten. Om het grootboek te hacken, moet je het merendeel van deze verschillende computers tegelijkertijd hacken en op hetzelfde moment dezelfde data wijzigen in dezelfde uitkomsten. De kans dat er zo'n grootschalige[2] hack plaatsvindt, is zeer klein. Dit maakt de blockchain zo betrouwbaar.

De lezer van deze uitleg begrijpt nu dat de blockchain:

1. een database is die te vergelijken is met een grootboek,
2. dat gekopieerd en verdeeld is over verschillende computers,
3. en dat betrouwbaar is, omdat een hack alleen succesvol kan zijn als meerdere van deze computers tegelijkertijd gehackt worden.

[2] Afhankelijk van het aantal aangesloten computers.

1.3 Blockchain op een middelniveau uitgelegd

Het doel van dit boek is dat de lezer blockchain op een hoog niveau begrijpt, waardoor de bovenstaande uitleg voor ons niet voldoet. Om tot dat hoge niveau te komen, is het van belang om het eerst op een middelniveau te begrijpen. Je merkt dat je door beheersing van blockchain op dit niveau al een stevige gesprekspartner kan zijn.

Op het middelniveau, is het het handigst dat we blockchain benaderen door Bitcoin als een voorbeeld te nemen. In principe is een blockchain een database waarin verschillende data kunnen worden opgeslagen. In het geval van de Bitcoin blockchain wordt de hele transactiegeschiedenis van alle Bitcoins bijgehouden en weet de blockchain dan ook exact hoeveel Bitcoin iedereen heeft. Wat de Bitcoin blockchain bijzonder maakt, is dat deze blockchain (of database) wordt onderhouden door een netwerk van servers die in het gunstigste geval allemaal over eenzelfde kopie van de blockchain beschikken. Er wordt hier expliciet “in het gunstigste geval” gezegd, omdat het weleens voorkomt dat de data binnen de blockchains onderling van elkaar kunnen verschillen. Dit is mogelijk als een server bijvoorbeeld tijdelijk is uitgevallen en de blockchain niet volledig is gesynchroniseerd. Het zou ook kunnen dat een kwaadwillend persoon valse informatie in zijn lokale blockchain plaatst. Een server kan een computer zijn, maar is in principe een apparaat waar data op kunnen worden geslagen. Dit kan dus ook een mobiele telefoon of een smart-tv zijn. De servers controleren de blockchaindata op juistheid en synchroniseren de inhoud van hun blockchain met de databases van alle andere servers op het netwerk. Hierdoor delen de servers die aangesloten zijn op het blockchainnetwerk, in het gunstigste geval, altijd eenzelfde kopie van de blockchain.[3]

Wie zijn dan deze servers die aangesloten zijn op het netwerk en een kopie hebben van de blockchain? Ze worden met een technisch term een ***full node*** genoemd. In het geval van de Bitcoin blockchain ligt het Bitcoin-protocol geheel open en is iedereen vrij om zijn computer of server aan te sluiten op het netwerk. De belangrijkste taak van deze **nodes** is om alle mutaties

[3] Het is belangrijk om te beseffen dat er geen eenduidige definitie bestaat van een blockchain. Volgens Webopedia is blockchain een type datastructuur waarbij data wordt gedistribueerd over een netwerk van computers. Daarnaast is deze data makkelijk te identificeren en te volgen, waardoor de blockchain een vertrouwensnetwerk is. Oxford Dictionaires ziet blockchain echter als een digitaal grootboek waarin transacties in Bitcoin of andere cryptovaluta op chronologische wijze publiekelijk worden geregistreerd. Sommige onderzoekers, als bijvoorbeeld Sultan et al. (2018), schrijven weer dat blockchain een gedecentraliseerde database is met opeenvolgende cryptografisch gelinkte datablokken, die worden gesteund door een consensusmodel.

van de blockchain te verifiëren op juistheid en om het netwerk robuust te houden. Niemand weet precies hoeveel Bitcoin full nodes er zijn, omdat sommige nodes achter gesloten poorten zitten en daardoor onzichtbaar zijn voor het netwerk.[4] In december 2019 zijn er ongeveer 10.000 Bitcoin full nodes met open poorten die verspreid zijn over meer dan 100 verschillende landen. Ongeveer een kwart daarvan is gevestigd in de Verenigde Staten en zo'n 5% zit in Nederland (Bitnodes.earn, 2019).[5] Omdat de blockchain een database is die is gedistribueerd over verschillende servers, wordt deze technologie ook wel gezien als een vorm van ***Distributed Ledger Technology*** (DLT) of ***Gedistribueerd Grootboek Technologie*** genoemd. Hierbij kan blockchain dus worden gezien als een DLT, maar andersom hoeft een DLT niet altijd een blockchain te zijn.

1.3.1 Inherente en emergente eigenschappen van de blockchain

Het is belangrijk om onderscheid te maken tussen de ***inherente*** en de ***emergente eigenschappen*** van de blockchain. Deze twee typen eigenschappen worden regelmatig door elkaar gehaald.[6]

Als we de blockchain zien als een database die informatie registreert, dan zijn dit de essentiële inherente eigenschappen van een blockchain:

1. Data zijn gerangschikt in datablokken.
2. De blokken zijn incrementeel oplopend.
3. De data zijn betrouwbaar, omdat ze cryptografisch verifieerbaar zijn.
4. De data zijn digitaal.

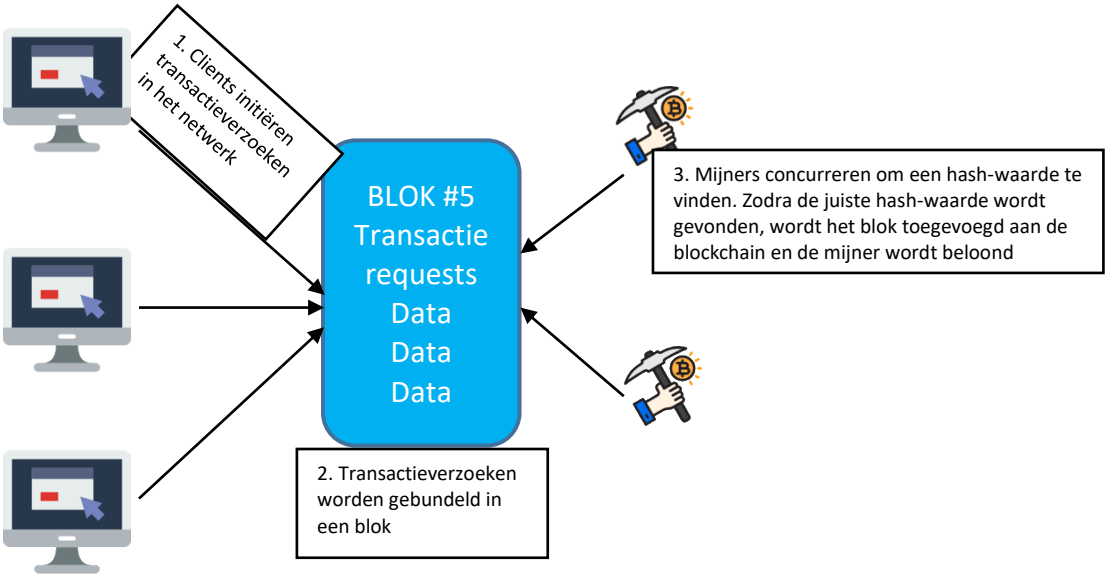
Data zijn gerangschikt in blokken die worden aangeduid met incrementeel oplopende bloknummers. Deze blokken zijn aan elkaar geketend middels cryptografische hash-waarden. Dit klinkt wellicht wat ingewikkeld, maar voor nu is het voldoende om het volgende procesplaatje in beeld te hebben. Een uitgebreidere uitleg hoe de data cryptografisch worden versleuteld in blokken en hoe de blokken aan elkaar worden geketend, volgt in hoofdstuk 3.

---

[4] Nodes met open poorten zijn in staat om blokken te helpen verspreiden naar nieuwe full nodes die deze blokken nog niet hebben. Voor de rest verschillen zij niet van nodes met gesloten poorten.

[5] Zie: www.bitnodes.earn.com voor een overzicht van de distributie van Bitcoin full nodes. Dit zijn wel nodes die achter open poorten zitten en daardoor bereikbaar zijn in het netwerk. Het aantal full nodes varieert van dag tot dag. Nodes kunnen net als computers of servers worden opgestart of gesloten en vereisen ook onderhoud.

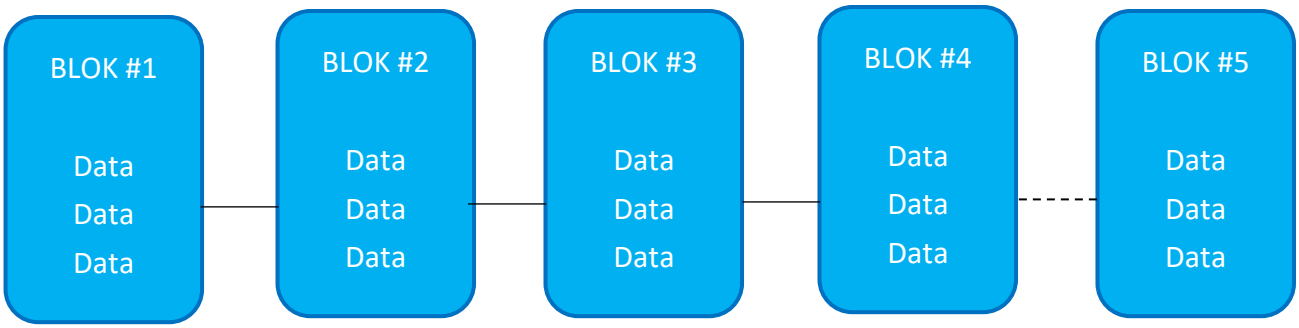
[6] Zie *Blockchain: properties and misconceptions* (2017) van De Leon, Stalick, Jillepalli en Haney met betrekking tot de misconcepties over de eigenschappen van Blockchain.



Afbeelding 1: Een vereenvoudigde weergave van hoe een blok wordt aangemaakt bij de Bitcoin blockchain.

De afbeelding hiervoor legt uit dat clients, apparaten zoals een mobiele telefoon van waaruit Bitcoin transacties worden geïnitieerd, allereerst verzoeken doen om hun transacties toe te mogen voegen aan een nieuw blok. In het voorbeeld worden de verzoeken toegevoegd aan een blok, waarna ***mijners*** aan de slag gaan om dit blok daadwerkelijk te mogen produceren. Volgens het Bitcoin-protocol mag de mijner die als eerste de juiste hash-waarde vindt het blok produceren en een bericht uitzenden naar de full nodes op het netwerk, dat de juiste hash-waarde is gevonden. De nodes controleren of de hash-waarde juist is. Zo ja, dan wordt het blok met de nieuwe transacties toegevoegd aan de blockchain.[7]

[7] Hierbij is het belangrijk om te weten dat een mijner niet hetzelfde is als een full node. Een mijner is één van meerdere typen full nodes. De primaire taak van een mijner is om nieuwe blokken aan te maken, terwijl full nodes een kopie hebben van de blockchain, nieuwe blokken verifiëren en deze toevoegen aan de blockchain. Later in hoofdstuk 4 bespreken we het onderscheid in de verschillende typen nodes.



Afbeelding 2: Block #5 is toegevoegd aan de blockchain.

In het geval van Bitcoin duurt het vinden van de juiste hash-waarde gemiddeld 10 minuten. Dit wordt de ***bloktijd*** van Bitcoin genoemd. De tijd voor het vinden van een juiste hash-waarde kan echter ook langer of korter duren. Je kunt het vinden van de juiste hash-waarde vergelijken met het zoeken naar een willekeurig getal tussen de 0 en 1.000. De mijner probeert dan bijvoorbeeld eerst 0 uit, dan 1, dan 2, dan 3, enzovoorts totdat hij het getal vindt dat juist is.[8] Het vinden van het juiste getal wordt regelmatig uitgelegd als zijnde het oplossen van een ingewikkelde wiskundige puzzel. Soms wordt het getal eerder gevonden en soms wat later. Het uitproberen van de verschillende getallen kost computerkracht. Een mijner met meer computerkracht kan binnen een kortere periode meerdere getallen uitproberen om op die manier sneller het juiste getal – of hash-waarde – te vinden. De beloning voor het vinden van de juiste hash-waarde is momenteel een vaste beloning van 12,5 Bitcoin + de variabele beloning van transactiekosten van de transactierequests in het blok.[9] Het is om deze reden dat er onder mijners een wedloop van computerkracht is ontstaan bij Bitcoin. Het systeem waarbij mijners computerkracht moeten gebruiken om een juiste hash-waarde te kunnen vinden wordt ***Proof-of-Work*** genoemd. Het vinden van de juiste hash-waarde vereist namelijk het bewijs dat er werk in de vorm van computerkracht is geleverd aan het netwerk.

Je kunt je afvragen of het vinden van de juiste hash-waarde niet sneller gebeurt naarmate er betere chiptechnologie wordt ontwikkeld die de computerkracht vergroot. Het antwoord hierop is dat het Bitcoin-protocol de moeilijkheidsgraad voor het vinden van de juiste hash-waarde automatisch aanpast, zodat deze ongeveer om de 10 minuten wordt gevonden en er dus om de 10 minuten ook een nieuw blok wordt geproduceerd.

[8] In werkelijkheid kan de mijner willekeurig een getal kiezen en loopt het bereik van de mogelijke getallen van 0 tot 4.294.967.295. In paragraaf 3.5.2 komen we hierop terug.

[9] Om de vier jaar wordt de vaste beloning gehalveerd. Je kunt hier vinden wanneer de volgende halvering plaatsvindt: www.bitcoinblockhalf.com

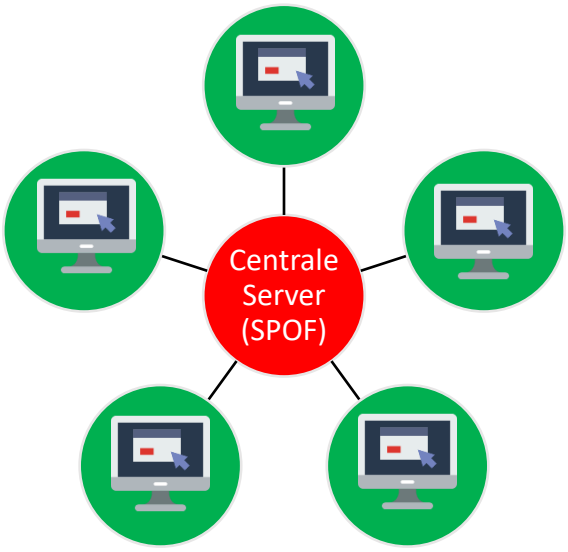
Als we weer even teruggaan naar blockchain vanuit het laagste kennisniveau, en de analogie met een grootboek wat nader bekijken, kunnen we zeggen dat een pagina van het grootboek vergelijkbaar is met de afzonderlijke blokken van een blockchain. Per pagina worden alle transacties die binnen een periode van ongeveer 10 minuten vallen, geregistreerd. Met andere woorden; op pagina 1 worden alle transacties van de eerste 10 minuten geregistreerd, op pagina 2 alle transacties van de volgende 10 minuten, op pagina 3 alle transacties van de daaropvolgende 10 minuten enz. Al deze pagina's vormen op deze manier een coherent grootboek, waarin alle transacties vanaf de eerste 10 minuten zijn bijgehouden.

Wanneer je gebruikmaakt van een gedistribueerd netwerk, leidt dit tot de volgende interessante consequenties die als emergente eigenschappen van de blockchain kunnen worden beschouwd:

1. Er is geen Single Point of Failure (SPOF).
2. Nieuwe data moeten worden bevestigd door andere nodes.
3. Een vorm van consensus is vereist om updates door te voeren en overeenstemming te bereiken over wat de juiste staat van de blockchain is.
4. Een blockchain is moeilijk te hacken.
5. Het bemoeilijkt het censureren of veranderen van de data op de blockchain.
6. Het is een peer-to-peernetwerk, waarbij er geen vertrouwen nodig is in een centrale partij.

Een goed gedistribueerde blockchain heeft geen Single Point of Failure

Een ***Single Point of Failure*** (SPOF) is het deel van een netwerk dat bij uitval de werking van het volledige netwerk stopt. Een SPOF is onwenselijk als je een systeem wil met een hoge beschikbaarheid en betrouwbaarheid.



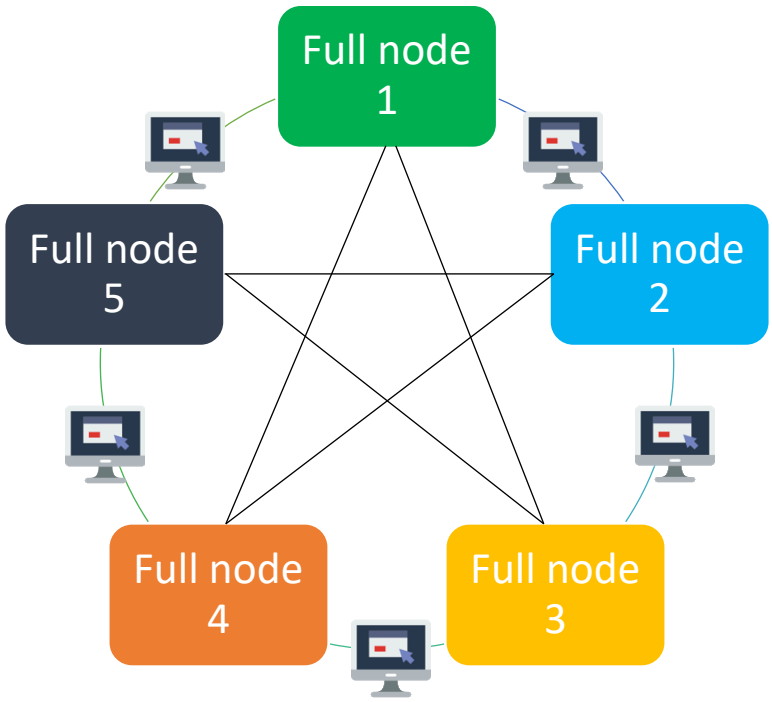
Afbeelding 3: Een weergave van een netwerk met een Single Point of Failure.

Je vindt in afbeelding 3 een weergave van een netwerk met een SPOF, de centrale server waar andere apparaten op aangesloten zijn. Een apparaat aangesloten aan het centrale netwerk kan bijvoorbeeld een computer, een desktop, een printer of een mobiele telefoon zijn.

Wanneer jij met jouw laptop een browser als Safari opent en naar de website Huisdieren.nl gaat, dan vindt er een verbinding plaats tussen jouw browser en de server van Huisdieren.nl, waar alle data van Huisdieren.nl zijn opgeslagen. Onderdeel van de data is bijvoorbeeld de inhoud van de website en de inloggegevens. Als deze centrale server met data uitvalt – wellicht doordat de database is gehackt, of doordat de stroom is uitgevallen – kan je browser niet meer bij deze data en wordt er een Error op je scherm getoond. Deze Error verschijnt niet alleen op je browser, maar op elke apparaat die connectie wil maken met Huisdieren.nl. In het geval van een hack zijn jouw gegevens wellicht gestolen of gewijzigd. Daarnaast, omdat alle data van gebruikers van Huisdieren.nl zijn bewaard op de server, heeft de beheerder van de server de mogelijkheid om jouw inloggegevens te veranderen, jouw account te sluiten en wellicht ook de mogelijkheid om jouw gebruikersgegevens in te zien. Gebruikers van de website moeten de beheerder van de server vertrouwen dat hij zorgvuldig omgaat met hun data. De noodzaak in dergelijke systemen om een centrale partij of beheerder te vertrouwen met je data en om te vertrouwen dat de SPOF niet uitvalt, maakt het model kwetsbaar.

Het zijn niet alleen kleine websites die last hebben van een SPOF design, maar ook grote gerenommeerde bedrijven. In 2015 was er bijvoorbeeld stroomuitval bij een enkel datacenter van PayPal. Als gevolg daarvan konden vele gebruikers de PayPal-website niet meer bereiken, creditcard transacties konden niet meer worden verwerkt, mensen konden geen toegang meer krijgen tot hun persoonlijke accountinformatie, of er werden incorrecte balansen getoond.[10]

Bij blockchain wordt de kwetsbaarheid van een SPOF voorkomen, doordat de blockchain gedistribueerd is over een netwerk van nodes. Doordat elke node een kopie heeft van de blockchain zijn er geen grote gevolgen voor het netwerk wanneer er één uitvalt. Omdat de andere nodes nog steeds een kopie hebben van de blockchain kan er nog steeds worden geverifieerd wat de balansen zijn en welke transacties er in het verleden hebben plaatsgevonden. Sinds de release van de Bitcoin blockchain is het netwerk niet één keer uitgevallen. Dit toont aan hoe robuust gedistribueerde grootboektechnologie kan zijn, mits zij goed is ingericht en wordt onderhouden door voldoende nodes.



Afbeelding 4: Een weergave van een gedistribueerd netwerk, waarbij de blockchain gedistribueerd is over een netwerk van full nodes.

[10] Zie 'Paypal's recent power outage drives bitcon adoption' (Parker, 2015) om meer te lezen over het incident.

Een gedistribueerde blockchain vereist bevestigingen van nieuwe data door andere nodes

Bij een gecentraliseerde server is het relatief gezien eenvoudig om nieuwe data-injecties op te nemen in de database. De nieuwe data hoeven slechts door één enkele partij te worden toegevoegd. Bij een gedistribueerd netwerk als blockchain ligt dit anders. Als de nieuwe data door een mijner worden toegevoegd aan een blockchain, moet deze data nog worden geverifieerd door andere full nodes en dan ook worden opgenomen op de blockchains die tot beschikking staan van de nodes. Er is daardoor altijd een risico dat nieuwe data die nog niet bevestigd zijn door full nodes alsnog worden geweigerd. Om deze reden adviseert Satoshi Nakamoto (2010) Bitcoin-gebruikers om bij een transactie altijd eerst te wachten op enkele bevestigingen, om er zeker van te zijn dat de transactie daadwerkelijk goed is opgenomen in de blockchain. Het is ook goed om, in het geval van Bitcoin, de Bitcoin pas weer uit te geven als je zeker weet dat de Bitcoin die je tot je beschikking hebt al is bevestigd. Hij schrijft:

> "As you figured out, the root problem is we shouldn't be counting or spending transactions until they have at least 1 confirmation. 0/unconfirmed transactions are very much second class citizens. At most, they are advice that something has been received, **but counting them is premature**."[11]

Over het algemeen wordt er aangegeven dat het good practice is om minimaal 4 bevestigingen te krijgen van een transactie, voordat je er zeker van bent dat het is opgenomen op de balans en je deze weer uit kan geven.

Een gedistribueerde blockchain vereist consensus

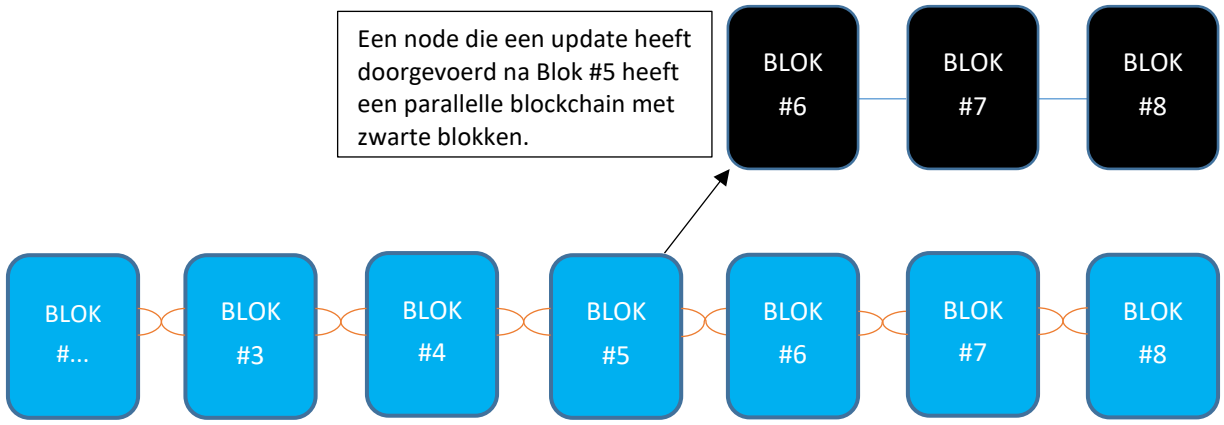
Hoe zit het dan met nieuwe updates van het netwerkprotocol? Een gedistribueerde blockchain vereist consensus om updates door te voeren en overeenstemming te bereiken over de juiste staat van de blockchain. Bij een gecentraliseerde server hoeft één enkele partij slechts de update door te voeren. Als je het volledige gedistribueerde netwerk veilig wil updaten, dan zullen alle nodes de update moeten accepteren en implementeren. Het is echter mogelijk dat sommige nodes de update weigeren te implementeren.

In principe wordt er door de eerste node die de update heeft gedaan, een signaal naar de andere nodes op het netwerk gestuurd dat hij een update heeft gedaan. Omdat deze node een

[11] Satoshi Nakamoto heeft dit commentaar geplaatst op het Bitcoin Forum, 30 september 2010. Zie: https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

iets gewijzigde versie van de blockchain heeft, is er een tijdelijke splitsing van de blockchain, een ***soft fork***. Er is hierbij ook afgesproken dat de andere nodes een x-aantal tijd hebben om de update door te voeren. De tijd wordt hierbij vaak uitgedrukt in het aantal blokken. Om een update van het blockchainprotocol door te voeren, moet bijvoorbeeld twee derde van de nodes de update hebben uitgevoerd, voordat Blok #100 is aangemaakt. Wanneer minder dan twee derde van de nodes de update heeft doorgevoerd binnen die bepaalde tijd, vervalt de update en keren de nodes weer automatisch terug naar de originele blockchain.

Het concept dat er bij een update een tijdelijke splitsing plaatsvindt van de blockchain is een interessante eigenschap. Wij komen hier in hoofdstuk 4.6 nog op terug. Hierbij zullen we ook bespreken wat er gebeurt bij een update die niet tijdelijk, maar permanent is. Ofwel, een update waarbij de blockchain splitst in twee verschillende chains die niet meer met elkaar kunnen communiceren. Dit is wat je een ***hard fork*** noemt.



Afbeelding 5: Illustratie van een fork.

Een onwaarheid omtrent blockchain die veelal circuleert is dat elke node exact dezelfde softwareversie heeft. Dat hoeft niet zolang de softwareversies maar compatibel zijn met elkaar en de full nodes met elkaar kunnen communiceren. Wanneer een full node een softwareversie heeft draaien die niet compatibel is, kan deze node niet meer de nieuwe data op de blockchain verifiëren.

Soft forks en hard forks worden in paragraaf 4.6 in meer details besproken. Voor nu voldoet het om te beseffen dat bij een update van het netwerk consensus moet worden bereikt tussen de full nodes.

Een gedistribueerde blockchain is moeilijk te hacken

Het feit dat een kopie van de blockchain wordt bewaard op verschillende nodes zorgt ervoor dat het lastig te hacken is, omdat de targets – de blockchains – zich op zoveel verschillende plaatsen bevinden. Daarnaast zijn als het goed is ook alle transacties uit het verleden geverifieerd. Hiermee is er duidelijk geregistreerd wie wat bezit op de blockchain. Een wijziging van een balans die niet correspondeert met eerdere gegevens wordt direct opgemerkt. Om controle te hebben over het netwerk, zou je meerdere nodes moeten hacken en diens blockchain moeten wijzigen. Dit is mogelijk middels een ***51%-aanval*** waarbij je, in het geval van Bitcoin, een meerderheid van alle computerkracht moet bezitten.[12]

51%-aanvallen worden in hoofdstuk 7 behandeld. Voor nu is het belangrijk om te weten dat je een Bitcoin tweemaal kan uitgeven middels een 51%-aanval. Het tweemaal uitgeven van een Bitcoin wordt ook wel ***double-spending*** genoemd.

Een gedistribueerde blockchain bemoeilijkt censuur en fraude

Er wordt vaak gezegd van de blockchain dat de data die erop staan, onveranderbaar zijn. Dit is echter niet waar. Het is mogelijk om data te wijzigen of te verwijderen als er consensus bestaat binnen de community om dit te doen. Het is echter lastig om consensus te vinden voor dergelijke acties. Het is dus wel van belang dat wanneer je de voor- en nadelen van een blockchainproject onderzoekt, je ook kijkt hoeveel full nodes er zijn en wie ze beheren. Het is mogelijk dat één enkele partij het merendeel van de nodes in handen heeft, of dat er een oligopolie is in de samenstelling van full nodes, waardoor deze de blockchain gemakkelijk kunnen kapen. Desalniettemin, als we ervan uitgaan dat het blockchainnetwerk goed gedistribueerd is, kunnen we zeggen dat censuur en veranderen van data op de blockchain lastig te bewerkstelligen zijn.[13]

Het is een peer-to-peernetwerk, waarbij er geen vertrouwen nodig is in een centrale partij

De voorgaande vijf emergente eigenschappen leiden ertoe dat er geen vertrouwde tussenpartij nodig is. Beslissingen worden genomen via een consensusmechanisme en transacties op de

[12] Hoewel de 51%-aanval de bekendste is, zijn er ook vele andere aanvallen mogelijk. Ook reguliere aanvallen die plaatsvinden bij gecentraliseerde netwerken zoals het corrumperen van core developers, bugs in onvrijwillig foutief geschreven code, of het stelen van sleutels die toegang geven tot servers komen voor bij blockchains.

[13] Wij gaan momenteel niet verder in op hoe data kan worden gecensureerd en veranderd op de blockchain. Dit komt later in het boek aan bod. Voor nu is het voldoende om te weten dat transacties op de blockchain dus wel kunnen worden gewijzigd met voldoende consensus van de nodes.

blockchain vinden peer-to-peer plaats zonder tussenpartij, wat interessante gevolgen heeft. Een vertrouwde tussenpartij wordt ook wel een ***trusted third party*** (TTP) genoemd.

Een peer-to-peernetwerk is een netwerk van computers (nodes), die gelijkwaardig zijn aan elkaar en die diensten aan elkaar kunnen verlenen. Iedereen heeft toegang tot het Bitcoin-netwerk en is vrij om een node te worden op het netwerk. Elke participant binnen het netwerk volgt het Bitcoin-protocol op een gelijkwaardig niveau en elke node wordt als gelijkwaardig beschouwd. Er zijn geen speciale Bitcoin nodes die worden voorgetrokken of die meer rechten hebben dan andere nodes: een mijner is gelijkwaardig aan elke ander mijner, net zoals elke full node gelijkwaardig is aan elke andere full node. Peer-to-peertransacties zonder tussenpartij betekent dat er geen centrale partij is die jouw transacties kan reguleren, stoppen en bevriezen. Met de uitschakeling van tussenpartijen gaan transacties sneller en goedkoper. Dit staat in contrast met het ***client-servermodel*** (werkstation-servermodel). Een client-servermodel maakt gebruik van een gecentraliseerde server die diensten verleent aan clients, bijvoorbeeld gebruikers van een e-maildienst. De server bevat vaak een database waarin logingegevens als gebruikersnamen en wachtwoorden staan. Clients die eenmaal ingelogd zijn, krijgen dan toegang tot de diensten van de server. Een zwakte van een dergelijk model is dat er een SPOF is. In dit geval is de SPOF de server. Als deze eenmaal wordt uitgeschakeld, hebben de clients geen toegang meer tot de diensten van de server. Daarnaast kan er gevoelige informatie worden buitgemaakt als de server is gecorrumpeerd door bijvoorbeeld hackers. De beheerder van de server kan ook bepaalde gebruikersrechten verlenen aan de clients en hen zowel toegang verlenen als ontzeggen.[14]

In het volgende hoofdstuk zullen we huidige betaalsystemen met banken, Payment Service Providers, card schemes en transactieverwerkers nader bespreken en deze afzetten tegen transactiesystemen op de blockchain.

Nu je min of meer de basis van blockchain begrijpt, kunnen we blockchains makkelijker onderscheiden van andere projecten die ook peer-to-peer zijn, maar toch geen gebruikmaken van blockchaintechnologie. Een dergelijk project dat we nader bespreken is de online dienst om muziek met elkaar te delen, Napster.

[14] In *The Internet of Money* (2016) vergelijkt de Bitcoin-evangelist Andreas Antonopoulos dit model met een meester-slaafrelatie, waarbij de server de meester is en de client de slaaf.

Intermezzo: Napster

In 1999 kwam er een peer-to-peer file sharing dienst op de markt genaamd Napster, opgericht door de tieners Shawn Fanning en Sean Parker. Napster maakte het mogelijk voor mensen om op een gemakkelijke wijze digitale muziekbestanden te delen met en te downloaden van anderen. Het zorgde voor veel commotie, omdat er voor het eerst op grote schaal muziek gratis met elkaar werd gedeeld. Met Napster konden mensen individuele liederen downloaden en beluisteren. Als men voorheen in bezit wilde komen van een liedje, moest men een volledige album aanschaffen. In 2001 werd Napster uiteindelijk na een rechtszaak met de Recording Industry Asssociation of America gesloten, omdat het verspreiden en downloaden van digitale muziekbestanden in strijd werd geacht met copyrightwetgeving. Desalniettemin staat Napster nog steeds bekend als een revolutionaire dienst die de muziekindustrie heeft ontwricht. In de Verenigde Staten bereikte de cd-verkopen zijn piek in het jaar 2000, waarna er een scherpe daling ontstond – mede veroorzaakt door Napster en daaropvolgende diensten als BitTorrent en Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

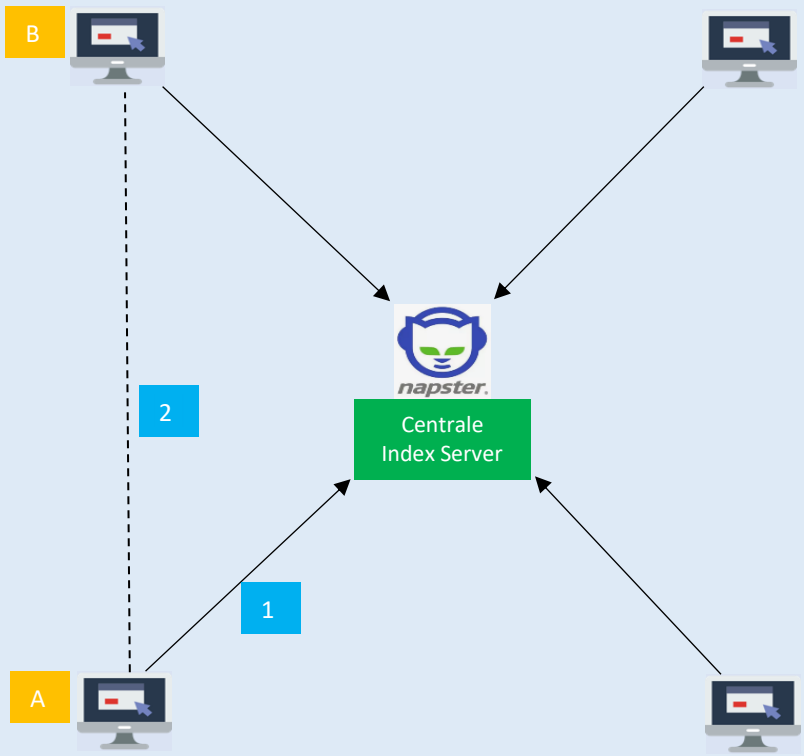
The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Napster staat erom bekend dat het gebruikmaakt van een peer-to-peernetwerk. Hoe komt het dan toch dat autoriteiten in staat zijn geweest om Napster te sluiten, wat vrijwel onmogelijk is met Bitcoin?

Bij het Bitcoin-netwerk bezitten alle full nodes een exacte kopie van de Bitcoin blockchain. Het Bitcoin-netwerk bestaat ongeveer uit 10.000 nodes, die verspreid zijn over de hele wereld, waardoor het lastig wordt om ze allemaal op te sporen en te sluiten. Hoewel het delen van muziekbestanden peer-to-peer plaatsvindt bij Napster, bevat het ook een centraal serverelement.

Napster maakt namelijk gebruik van een centrale index die bijhoudt welke computer welke bestanden heeft om te delen met andere gebruikers. Als een gebruiker (computer A) naar een nummer wil zoeken als bijvoorbeeld Michael Jackson – Billie Jean, dan wordt er een verbinding gelegd met de index en zoekt de index welke computers dit nummer hebben. Als uit de index blijkt dat computer B dit nummer heeft, wordt er een directe peer-to-peerverbinding gelegd tussen computer A en B, waardoor A direct het nummer van B's computer kan downloaden.

Napster is aldus een mixed model van client-server en peer-to-peer. Het centrale indexelement is client-server, maar het downloaden van de daadwerkelijke bestanden gebeurt peer-to-peer. De centrale indexserver is een serieuze achilleshiel gebleken voor Napster, omdat deze gemakkelijk kan worden gesloten, waardoor Napster niet meer werkt. Omdat Napster slechts een centrale indexserver heeft, waarin staat welke computers welke deelbare muziekbestanden heeft, heeft Napster zelf geen muziekbestanden op zijn server. Het heeft alleen gebruikers gefaciliteerd om peer-to-peerconnecties te leggen en muziek met elkaar te delen.



Afbeelding 6: Napster netwerk. (1) Computer A voert een zoekopdracht in Napsters centrale indexserver naar Michael Jackson – Billy Jean. Napsters centrale indexserver zoekt naar computers die aangesloten zijn op het netwerk en die het nummer beschikbaar hebben gesteld op hun harde schijf. (2) Computer B heeft het nummer. Computer A en B leggen een directe peer-to-peerverbinding, waarna computer A het muziekbestand downloadt van computer B.

1.4 Samenvatting, begrippen en bronnen

Samenvatting

Het is belangrijk om te weten dat blockchain in principe een grootboek is en om onderscheid te kunnen maken tussen de inherente en emergente eigenschappen van de blockchain.

Een blockchain is in principe:

1. een database die te vergelijken is met een grootboek,
2. dat gekopieerd en verdeeld is over verschillende servers en
3. dat betrouwbaar is, omdat een hack alleen succesvol kan zijn als meerdere van deze servers tegelijkertijd gehackt worden.

Wat de blockchain bijzonder maakt, is dat het wordt onderhouden door een netwerk van nodes die – in het gunstigste geval, maar het hoeft niet altijd – allemaal over een exacte kopie van de blockchain beschikken. De full nodes synchroniseren hun blockchain namelijk met elkaar. Het is hierbij niet van belang dat nodes de laatste softwareversie draaien. Het belangrijkste is dat zij blokken blijven produceren in het geval dat de full node een mijner is, nieuwe transacties verifiëren en het netwerk helpen onderhouden.

Als we de blockchain zien als een database die informatie registreert, dan zijn dit de essentiële inherente eigenschappen van een blockchain:

1. data zijn gerangschikt,
2. incrementeel,
3. betrouwbaar, doordat de data cryptografisch verifieerbaar zijn, en
4. digitaal.

Wanneer je gebruikmaakt van een gedistribueerd netwerk, leidt dit tot de volgende interessante consequenties, die als emergente eigenschappen van de blockchain kunnen worden beschouwd:

1. Er is geen Single Point of Failure.
2. Nieuwe data moeten worden bevestigd door andere nodes.
3. Een vorm van consensus is vereist om updates door te voeren en overeenstemming te bereiken over wat de juiste staat van de blockchain is.
4. Een blockchain is moeilijk te hacken.
5. Het bemoeilijkt het censureren of veranderen van de data op de blockchain.
6. Het is een peer-to-peernetwerk, waarbij er geen vertrouwen nodig is in een centrale partij.

Opmerkingen die je nu kunt uitleggen

- Blockchains verschillen van traditionele databases.
- Een blockchain is eigenlijk een grootboek die is gekopieerd en gedistribueerd over een netwerk van meerdere computers.
- De reden waarom Napster heeft gefaald is omdat het een SPOF had. Een blockchain, daarentegen, kent geen SPOF en is daardoor lastiger uit te schakelen.
- Een blockchain heeft zowel inherente als emergente eigenschappen. Het zijn voornamelijk de emergente eigenschappen die een blockchain interessant maken.
- Een blockchain is een peer-to-peernetwerk.

Verklarende begrippenlijst

51%-aanval: Een aanval op de blockchain die wordt bewerkstelligd door meer dan 51% van alle computerkracht van het netwerk te verkrijgen.

Bitcoin halvering: De halvering van het aantal nieuwe Bitcoins dat vrijkomt wanneer er een geldige blok wordt geproduceerd door een mijner.

Bloktijd: De gemiddelde tijd waarin er een geldige blok wordt geproduceerd door een mijner. Bij Bitcoin is dit 10 minuten.

Client-servermodel: Het model waarbij clients (gebruiker) verbonden zijn met een server. De server bevat data die relevant zijn voor de clients. De clients maken connectie met de server om toegang te krijgen tot deze data. Hierdoor zijn de clients afhankelijk van de server.

Distributed Ledger Technology (DLT): Gedistribueerd grootboektechnologie.

Double-spending: Het tweemaal uitgeven van een Bitcoin. Dat je bijvoorbeeld 1 Bitcoin hebt, maar daarmee 1 Bitcoin stuurt naar persoon A en 1 Bitcoin naar persoon B.

Emergente eigenschappen van blockchain: Eigenschappen van een blockchain die opkomen wanneer de blockchain is gedistribueerd over een netwerk van computers.

Full node: Een node die een volledige kopie heeft van de blockchain.

Gedistribueerd Grootboek Technologie: Zie Distributed Ledger Technology.

Hard fork: Een permanente splitsing van de blockchain, wanneer een deel van de nodes besluit om niet mee te gaan met een update en afzonderlijk verdergaan met een eigen blockchainversie. Een welbekende Bitcoin hard fork is de hard fork die heeft geleid tot Bitcoin en Bitcoin Cash.

Inherente eigenschappen van blockchain: Eigenschappen die eigen zijn aan een blockchain. Dit zijn eigenschappen die alle blockchains per definitie hebben.

Mijner: Een computer die computerkracht levert om een geldige blok te mogen produceren. Een blok is alleen geldig als hij een nonce vindt die leidt tot een geldige hash-waarde.

Node: Apparaat die is verbonden aan een computernetwerk.

P2P: Zie peer-to-peer.

Peer-to-peer: Een computernetwerk waarbij computers gelijkwaardig zijn aan elkaar en elkaar diensten kunnen aanbieden.

Proof-of-Work: Een consensusmechanisme waarbij mijners computerkracht moeten gebruiken om een juiste hash-waarde te vinden van een nieuwe blok. Door het vinden van een juiste hash-waarde, mogen zij het blok toevoegen aan de blockchain en krijgen zij een beloning.

Single Point of Failure (SPOF): Het deel van een netwerk dat bij uitval de werking van het volledige netwerk stopt.

Soft fork: Een tijdelijke splitsing van de blockchain. Bij een update van de blockchain, kan een deel meegaan met de update en een deel niet. Op die manier krijg je tijdelijk twee verschillende blockchainversies. Bij een soft fork is er afgesproken dat nodes een x-aantal tijd hebben om de update door te voeren. Als er niet voldoende nodes meegaan met de update voor die tijd, dan keert de blockchain automatisch terug naar de oude versie.

SPOF: Zie Single Point of Failure.

Trusted third party (TTP): Vertrouwde tussenpartij.

TTP: Zie trusted third party.

White paper: Een document dat beschrijft hoe een specifiek probleem wordt opgelost. Satoshi Nakamoto heeft in de Bitcoin white paper geschreven hoe Bitcoin het probleem van double-spending oplost in een gedistribueerd netwerk.

Bronnen

Antonopoulos, A. M. (2016). *The Internet of money: talks by*. Merkle Bloom Llc.

Bitcoin Block Reward Halving Countdown. (2019). Geraadpleegd op 23 december 2019, van Bitcoinblockhalf.com website: http://www.bitcoinblockhalf.com

de Leon, D.C., Stalick, A. Q., Jillepalli, A. A., Haney, M. A., & Sheldon, F. T. (2017). Blockchain: properties and misconceptions. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 286–300. https://doi.org/10.1108/apjie-12-2017-034

Nakamoto, S. (2008). Bitcoin P2P e-cash paper. Geraadpleegd op 23 december 2019, van Metzdowd.com website: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, 30 september). Re: I broke my wallet, sends never confirm now. [Online forumcomment]. Bericht geplaatst op https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, 1 november). Paypal's recent power outage drives bitcoin adoption. Geraadpleegd op 23 december 2019, van Bravenewcoin.com website: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. *11th IADIS International Conference Information Systems 2018*, 49–57

Iconen

Computer gemaakt door Prettycons van www.flaticon.com

Mijner gemaakt door Srip van www.flaticon.com

2. Tekortkomingen van het huidige betaalproces

"Money is low bandwidth … You don't need some sort of big infrastructure improvement to do things with it. It's really just an entry in a database."

- Elon Musk (2003)

2.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat Point-of-Sale (POS) en e-commercetransacties zijn.
- Hoe het betaalproces verloopt van reguliere betaalmethoden als creditcards en iDEAL en welke partijen bij dergelijke transacties betrokken zijn.
- Dat het proces van betaling bestaat uit authenticatie, autorisatie en clearing & settlement.
- In welke opzichten blockchaintransacties voordelen bieden ten opzichte van transacties met reguliere betaalmethoden.

Inleiding

Zoals vermeld in hoofdstuk 1 is Bitcoin de eerste applicatie die gebruik heeft gemaakt van Blockchaintechnologie, ontwikkeld als zijnde een nieuw geldsysteem. Voordat we in het volgende hoofdstuk verder ingaan op Bitcoin, is het belangrijk om eerst te begrijpen hoe huidige transactieprocessen werken. Met meer inzicht in hoe transactieprocessen verlopen, wordt het duidelijker wat de relevantie van Bitcoin en blockchain is binnen transactiemodellen.

Oppervlakkig gezien lijkt een transactie simpel. Het is toch slechts de kaartgegevens invoeren of de kaart door een pinautomaat halen en de betaling is gedaan, nietwaar? Echter, is dit technisch gezien toch een vrij complexe procedure, waarin de betaling drie processen doorloopt met meerdere spelers in de transactieketen. Als je doorhebt hoe deze processen verlopen, kun je ook reflecteren op de tekortkomingen van huidige transactiesystemen. In onze uitleg over hoe transacties werken, kijken we in het bijzonder naar hoe de betaalprocessen van creditcards en iDEAL verlopen.

Het is gebruikelijk in de betalingsindustrie om een onderscheid te maken tussen ***Point-of-Sale*** (PoS) betalingen in fysieke winkels en de ***e-commerce***transacties die online plaatsvinden op voornamelijk webshops. In paragraaf 2.2, bespreken we het proces van een PoS-transactie met creditcard. Dit wordt opgevolgd door een bespreking van e-commercetransacties met iDEAL en creditcard in paragraaf 2.3. In paragraaf 2.4, kijken we naar de kosten van deze transacties en zullen we zien dat de kosten aanzienlijk hoog zijn, omdat er veel tussenpartijen betrokken zijn. Dit hoofdstuk eindigt vervolgens in paragraaf 2.5 met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst.

Het meest relevant voor ons is:

1. Om te begrijpen welke spelers actief zijn binnen de transactieprocessen.
2. Om te begrijpen dat elke partij in de transactieketen een deel van de fees opeist.
3. Om te begrijpen wat de snelheid is van clearing & settlement bij transacties.

Clearing & settlement is het verwerkingsproces van een transactie, waarbij het geld van de uitgevende bank daadwerkelijk wordt uitgewisseld en verrekend met de ontvangende bank.

2.2 Point-of-Sale

Een creditcardtransactie in een fysieke winkel doorloopt de volgende drie processen:

1. Autorisatie.
2. Authenticatie.
3. Clearing en settlement.

Voor deze processen is het belangrijk om te weten dat de volgende spelers betrokken zijn binnen het transactieproces:

1. ***Kaarthouder***: degene met de creditcard. In dit geval is het de betalende klant.
2. ***Merchant***: de eigenaar van de winkel.
3. ***Acquire****r/Bank van de Merchant*: financiële instelling die verantwoordelijk is voor het ontvangen van transactieverzoeken van de Merchant en die deze verzoeken weer doorstuurt naar de Issuing Bank. Deze ontvangt en verstuurt het bericht van de Issuing Bank terug naar de Merchant met het antwoord of de betaling is goedgekeurd of niet.
4. ***Acquiring Processor****/Service Provider*: financiële instelling die de dienst en daarmee vaak ook de betaalautomaat aanbiedt aan de Merchant om betalingen te kunnen accepteren. In sommige gevallen wordt deze dienst geboden bij de Acquirer. In ons voorbeeld nemen we voor het gemak aan dat de Acquirer ook deze dienst aanbiedt. Deze dienst

wordt ook weleens aangeboden door een Payment Service Provider die daarnaast ook het contact legt met creditcardnetwerken om Merchants op aan te sluiten.

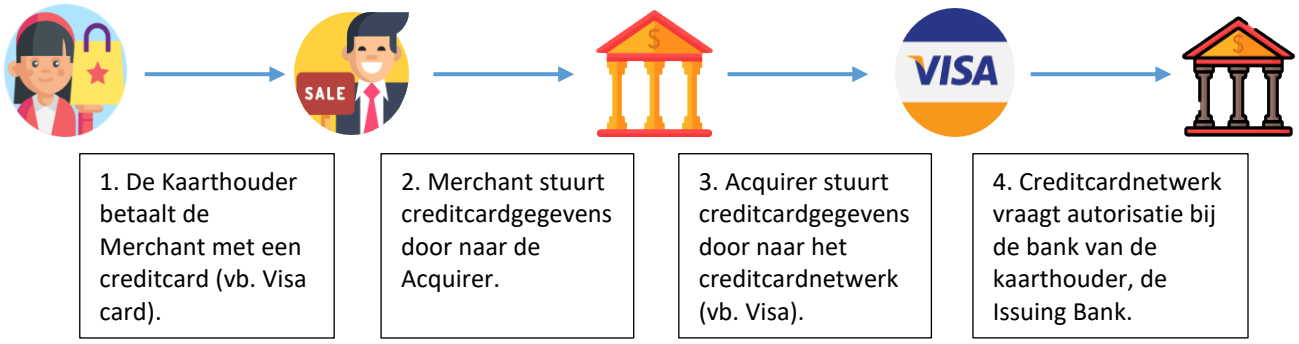
5. ***Creditcardnetwerk***: het netwerk dat creditcardtransacties verwerkt. Voorbeelden zijn Visa, MasterCard, China Union Pay en American Express.
6. ***Issuing Bank***: financiële instelling die de creditcard heeft uitgegeven aan de Kaarthouder. Vaak is dit de bank van de Kaarthouder.

Wij zullen elk van de drie processen in meer detail beschrijven.

2.2.1 Autorisatie

In het autorisatieproces wordt er gevraagd bij de bank van de kaarthouder of de Kaarthouder de transactie mag uitvoeren.

1. De Kaarthouder doet zijn creditcard in een betaalterminal en voert zijn gegevens in, zoals zijn pincode bij het punt van aankoop (Point-of-Sale).
2. De creditcardgegevens worden elektronisch doorgestuurd naar de Acquirer, de bank van de winkelier.
3. De Acquirer stuurt de creditcardgegevens door naar het creditcardnetwerk als bijvoorbeeld Visa, Mastercard, American Express of China Union Pay.
4. Het creditcardnetwerk beoordeelt de betaling en vraagt een transactieautorisatie aan bij de bank van de Kaarthouder. Bij de autorisatie wordt gekeken of de volgende gegevens kloppen:
    a. Creditcardnummer
    b. Creditcardvervaldatum
    c. Factuuradres
    d. Creditcardbeveiligingscode als het CVV wat op de achterkant van de creditcard staat
    e. Betaalbedrag

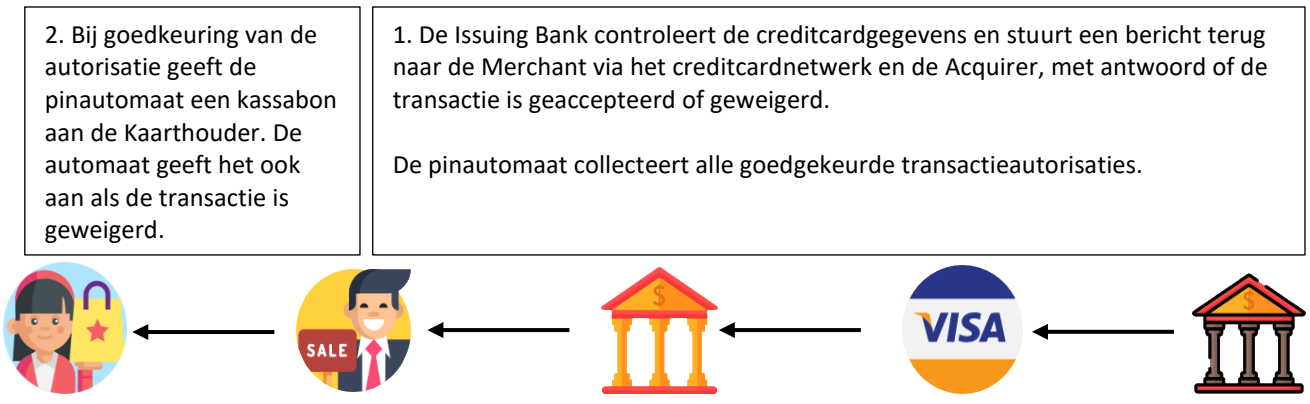


Afbeelding 7: Autorisatieproces van een creditcard bij een Point-of-Salebetaling.

2.2.2 Authenticatie

De bank van de Kaarthouder, de Issuing Bank, verifieert in de authenticatiefase of gegevens ter autorisatie kloppen.

1. De Issuing Bank valideert het creditcardnummer, de vervaldatum, de beveiligingscode, het factuuradres en of er voldoende saldo is op de rekening. Aan de hand van deze authenticatie wordt er een bericht teruggestuurd via dezelfde kanalen naar de Merchant met het antwoord of de Issuing Bank de transactie goedkeurt of weigert.
2. Zodra de Merchant de autorisatie heeft ontvangen, zal de Issuing Bank het transactiebedrag inhouden van de rekening van de Kaarthouder. De Merchant biedt daarnaast een kassabon aan, aan de Kaarthouder, waarmee de aankoop is gecompleteerd. Ook verzamelt de betaalautomaat alle goedgekeurde transactieautorisaties die aan het eind van de dag worden verwerkt in een batch.

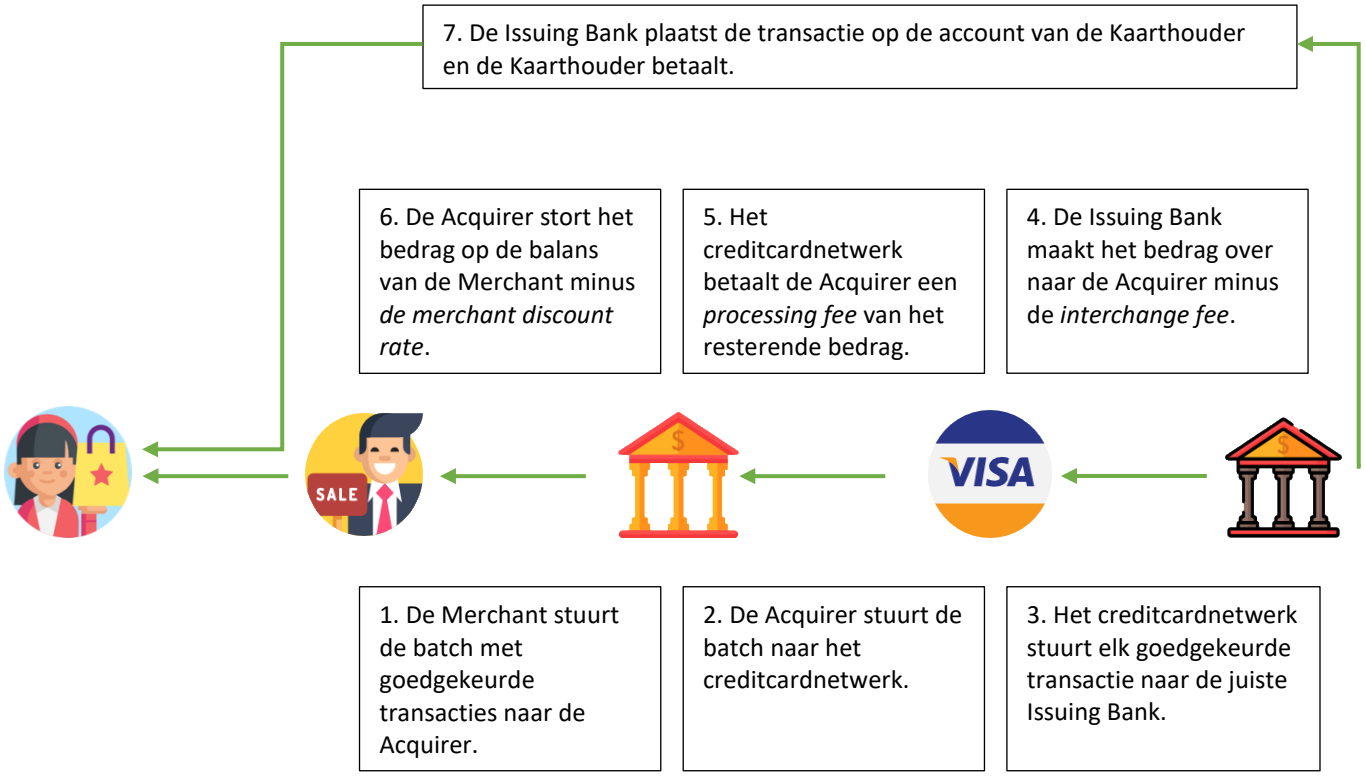


Afbeelding 8: Authenticatieproces van een creditcard bij een Point-of-Salebetaling.

2.2.3 Clearing & Settlement

In het proces van clearing & settlement worden de betalingen daadwerkelijk afgeschreven van de rekening van de Kaarthouder en bijgeschreven bij de rekening van de Merchant.

1. De Merchant – of beter gezegd de betaalautomaat van de Merchant – verstuurt aan het eind van de dag alle goedgekeurde autorisaties in een batch naar de Acquirer.
2. De Acquirer verstuurt de batch naar het creditcardnetwerk voor afhandeling.
3. Het creditcardnetwerk bekijkt de transacties in de batch en stuurt elke goedgekeurde transactie naar de juiste Issuing Bank. Daarnaast krijgt het creditcardnetwerk ook een klein percentage van de betaling, de ***assessment fee***.
4. Normaal gesproken maakt de Issuing Bank het geldbedrag minus ***interchange fees*** naar de Acquirer. De interchange fees zijn fees die worden betaald aan de Issuing Bank.
5. Het creditcardnetwerk betaalt de Acquirer (en de acquiring processor) een percentage van het bedrag voor hun dienstverlening. Dit is de ***processing fee***.
6. De Acquirer stort het bedrag op het account van de Merchant minus de ***merchant discount rate***.
7. De Issuing Bank plaatst de transactie op het account van de Kaarthouder. De Kaarthouder betaalt het bedrag.

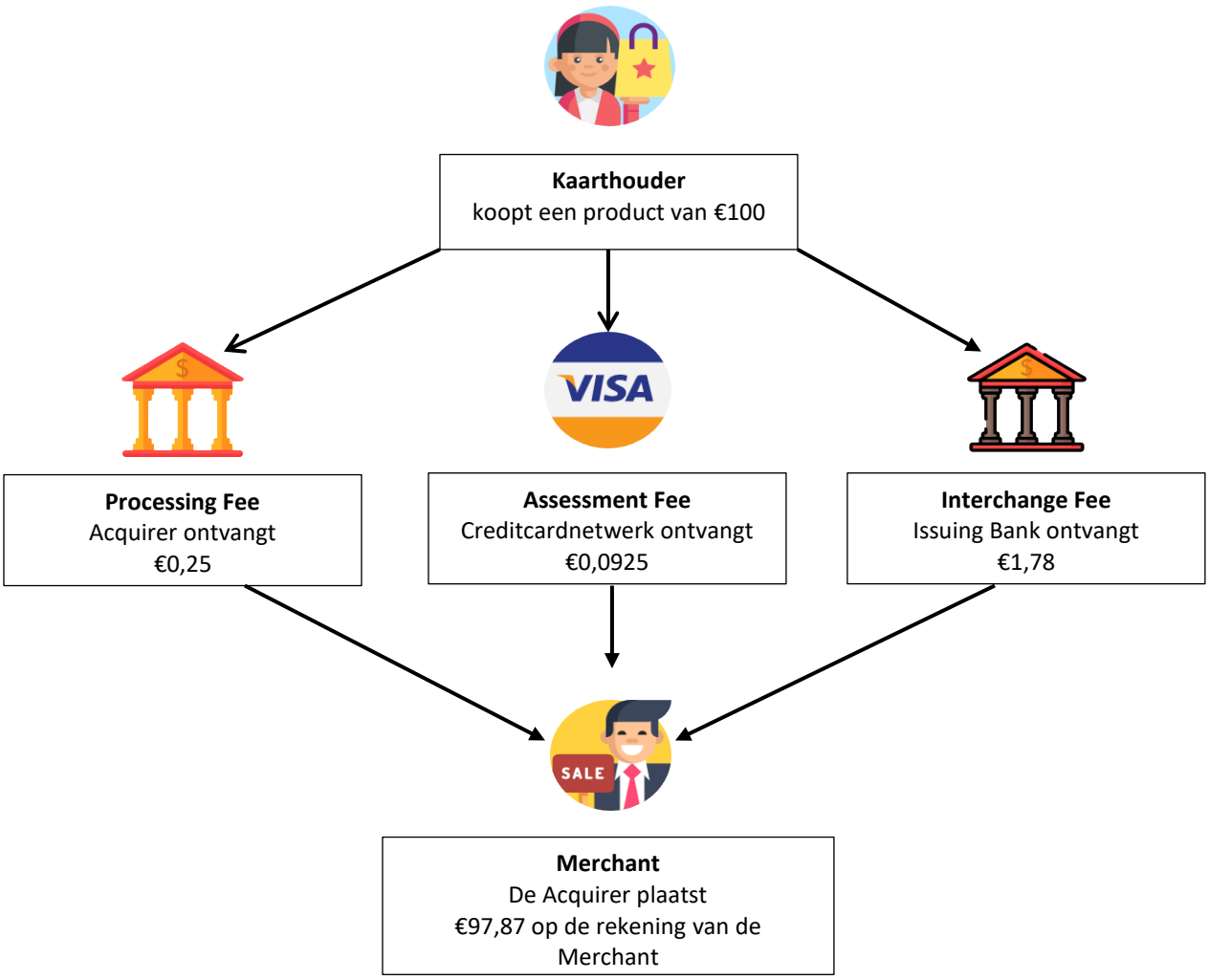


Afbeelding 9: Proces van clearing & settlement van een creditcard bij een Point-of-Salebetaling.

Als we kijken naar de kosten van creditcardtransacties dan zijn er drie kosten die een Merchant maakt op het ontvangen van een transactie:

1. Processing fee voor de Acquirer.
2. Assessment fee voor het creditcardnetwerk.
3. Interchange fee voor de Issuing Bank.

De som van al deze tarieven wordt de ***merchant discount rate*** genoemd. Deze is vaak rond de 2-3%, maar kan ook wel oplopen tot 5%. Hieronder vind je een schematische weergave hoe het bedrag van een aankoop van €100 wordt verdeeld onder de spelers in de transactieketen.



Afbeelding 10: Kostenverdeling van een creditcard bij een Point-of-Saletransactie.

2.3 E-commerce

Bij e-commercetransacties spelen ook dezelfde spelers een rol. Het grote verschil is dat de transactie online plaatsvindt, vaak in een webwinkel.

In het geval van een iDEAL-betaling is er geen creditcardnetwerk als Visa en MasterCard, maar zijn ook hier een Issuing Bank en een Acquirer of Payment Service Provider. De laatste speelt de rol van een Acquirer en legt voor de Merchant de verbinding met het iDEAL-betaalplatform. In Nederland wordt het platform gedragen door banken. Tot op heden zijn er 11 banken die een licentie hebben om als Issuing Bank te fungeren voor iDEAL.[15]

De Acquirers en Payment Service Providers zorgen ervoor dat het geld dat is betaald vanuit de Kaarthouder bij de accounts van Merchants komt. In Nederland zijn er momenteel 8 Acquirers en tientallen Payment Service Providers.[16]

2.3.1 iDEAL (e-commercetransactie)

Het transactieproces van iDEAL is als volgt:

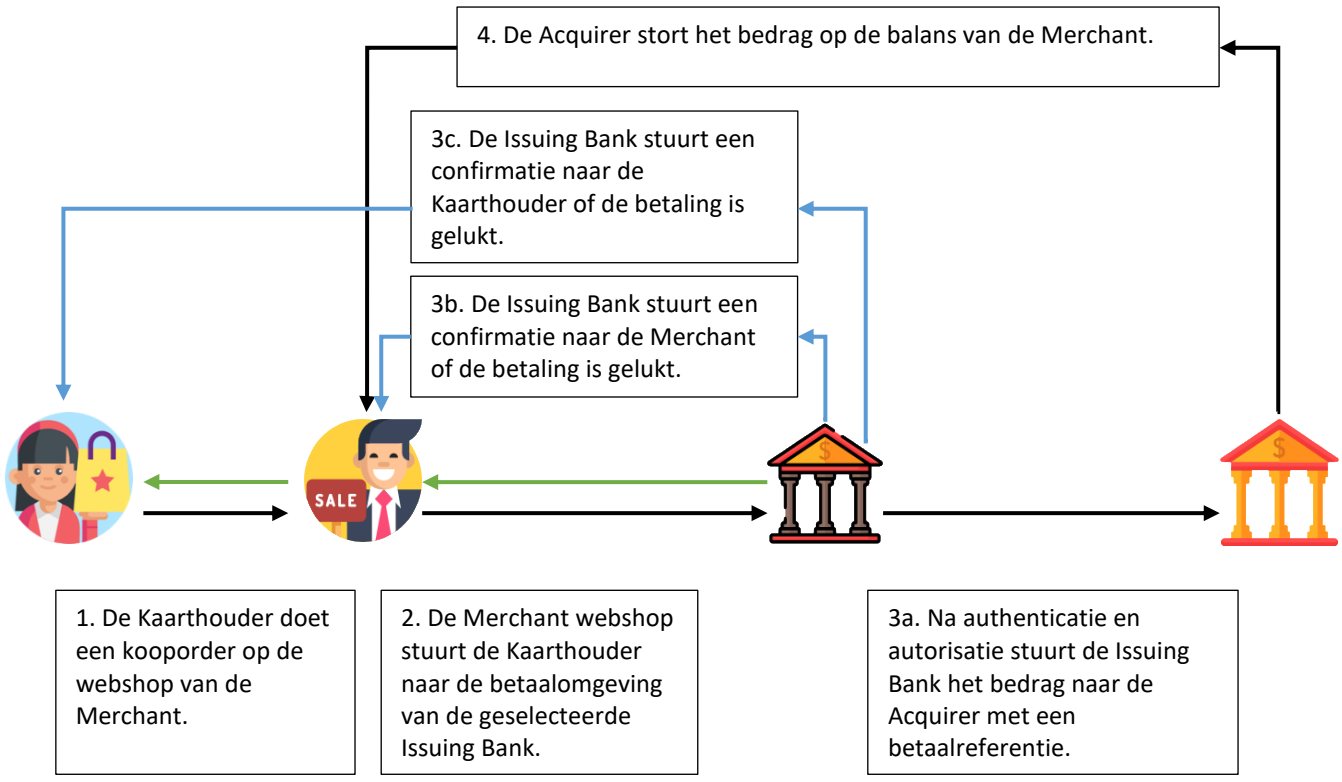
1. De Kaarthouder doet een kooporder op de webshop van de Merchant.
2. De Kaarthouder wordt van de webshop van de Merchant doorverwezen naar de online betaalomgeving van de geselecteerde bank.
3. (a) De Kaarthouder moet zichzelf authentiseren. Banken hebben voor authenticatie vaak hun eigen systeem. In het geval van de Rabobank maak je gebruik van de Rabo Scanner en in het geval van de ABN AMRO Bank maak je gebruik van een e.identifier. De Kaarthouder dient ook de betaling te autoriseren. Bij autorisatie wordt er gevraagd om een pincode en vaak ook om een uniek gegenereerde code middels een apparaat als de Rabo Scanner en de e.dentifier van de ABN AMRO Bank. Als je betaalt met de mobieletelefoonapplicatie kan het ook zijn dat je voor lage bedragen geen uniek gegenereerde code meer hoeft in te vullen. De balans wordt ook gecheckt.
   (b) De Issuing Bank stuurt een bevestiging naar de Merchant of de betaling is gelukt.
   (c) De Issuing Bank stuurt ook een bevestiging naar de Kaarthouder of de betaling is gelukt. Als de betaling is gelukt, dan wordt de Kaarthouder weer vanuit de betaalomgeving van de Issuing Bank doorverwezen naar de Merchant webshop.

[15] Deze banken zijn ABN AMRO Bank, ASN Bank, Bunq, ING Bank, Knab, Moneyou, Rabobank, RegioBank, SNS, Triodos Bank en van Lanschot Bankiers.

[16] Kijk op https://www.ideal.nl/partners/ voor een overzicht van Issuing banks, Acquirers en Payment Service Providers voor iDEAL.

4. De Issuing Bank stuurt het bedrag en de betalingsreferentie naar de Acquirer. De Acquirer verzamelt alle inkomende betalingen, verwerkt ze en stort het bedrag op de account van de Merchant.

Het hele order-, authenticatie- en autorisatieproces verloopt real-time. De settlement zelf neemt veel tijd in beslag en duurt 1 tot 3 werkdagen.[17]



Afbeelding 11: Transactieproces van iDEAL.

[17] Er worden in Nederland en Europa grote slagen gemaakt met betrekking tot het betalingsverkeer. In Nederland is Instant Payments inmiddels geleidelijk ingevoerd in het voorjaar van 2019. Hier doen momenteel zeven banken aan mee: ABN AMRO, ING, Rabobank, SNS, ASN Bank, RegioBank en Knab. Hiermee kan geld via mobiel bankieren en internetbankieren binnen enkele seconden worden bijgeschreven bij de ontvanger en kan de ontvanger het ook weer direct besteden. Naast Nederland is ook de Europese Unie bezig met het uitrollen van Instant Payments voor het internationale betalingsverkeer in de Unie. Instant Payments is echter nog niet mogelijk met iDEAL. (Betaalvereniging, 2019).

2.3.2 Creditcard (e-commerce transactie)

Zoals eerder aangegeven zijn er bij e-commercetransacties met creditcards dezelfde spelers aanwezig als bij Point-of-Saletransacties.

Allereerst doet de Kaarthouder een kooporder op de betalingspagina van de Merchant. Het is mogelijk dat de Merchant de Kaarthouder kaartgegevens als creditcardnummer, vervaldatum en CVV/CVC-code laat invullen op de betalingspagina. Echter zijn hier strikte regels aan verbonden. De Merchant moet hiervoor wel voldoen aan de reguleringen omtrent geldtransacties. Dat brengt extra kosten met zich mee.[18] Als de Merchant niet voldoet, dan mogen Kaarthouders geen creditcardgegevens invoeren op de betalingspagina van hun webshop. Indien de Merchant creditcardgegevens wil opslaan, dient deze te voldoen aan strikte regels van versleuteling door middel van tokens in datakluizen en andere beveiligingsmaatregelen. Mochten onbevoegden toegang hebben tot de datakluizen en de tokens buitmaken, dan kunnen zij uit de versleutelde tokens niet achterhalen welke creditcardgegevens daarbij horen. Als je niet gecertificeerd bent om creditcardgegevens op deze manier op te slaan, is het ook vaak mogelijk om de tokens te laten opslaan bij de Payment Service Provider die de 'datakluis tokenization dienst' aanbiedt. Het voordeel van tokenization van creditcardgegevens is dat wanneer eenzelfde klant weer een betaling wil doen op je website, de token die hoort bij de klant kan worden opgevraagd en daarmee de creditcardgegevens al vooraf automatisch wordt ingevuld op de betaalpagina. De klant hoeft dan niet meer zijn creditcardgegevens erbij te pakken. Ook is het mogelijk om de token te gebruiken om automatisch terugkerende betalingen uit te voeren bij bijvoorbeeld betalingen van abonnementen.

[18] De Merchant moet hiervoor compliant zijn met de Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is een zelfregulering van de Payment Card Industry. De verplichting is gebaseerd op overeenkomsten die betrokken partijen zoals Merchants, Payment Service Providers, Issuing Banks, enzovoorts moeten ondertekenen. Het werd ingevoerd om de fraude met creditcards te reduceren. Er bestaan verschillende niveaus van PCI DSS compliancy. Iedereen die betalingen wil accepteren moet op zijn minst voldoen aan het laagste niveau. Om certificering op hogere niveaus te voorkomen, is het mogelijk voor de Merchant om Kaarthouders naar een betaalpagina te sturen die wordt gehost door bijvoorbeeld een Payment Service Provider die wel voldoet. Wel dient de Merchant maatregelen te nemen om bijvoorbeeld te voorkomen dat criminelen klanten doorsturen naar een valse betaalpagina. Dit gebeurt geregeld aangezien de beveiliging van webshops soms te zwak is. Voor meer informatie over PCI DSS, zie: https://www.pcisecuritystandards.org/.

Ervan uitgaande dat je niet gebruikmaakt van een webshop met automatisch ingevulde creditcardgegevens, vul je in de betalingspagina zelf handmatig de creditcardgegevens in als het kaartnummer, de vervaldatum en de CVV/CVC-code die op de achterkant van de kaart staat. Vanuit de betalingspagina wordt de Kaarthouder nog doorverwezen naar een 3D-secure omgeving. 3D-secure is een betalingsprotocol dat de Kaarthouder authentiseert. Er zijn verschillende vormen waarmee je de 3D-secure code kunt opvragen. Dit kan met een kaartlezer als de Rabo Scanner, een digipas of een SMS die wordt opgestuurd vanuit de Issuing Bank naar je telefoon. Nadat de 3D-secure code juist is ingevuld, begint het proces van settlement & clearing wat ongeveer 3-5 werkdagen kan duren.

2.4 Kosten voor Merchants

In vergelijking met Bitcoin of andere blockchaintransacties, zijn traditionele transacties vrij duur. Hoewel de kosten sterk kunnen verschillen per transactie, kost een Visa- en Mastercard-transactie vaak rond de 3% en zijn er ook vaste kosten aan verbonden. Daarnaast betaalt de Merchant soms ook eenmalige en maandelijkse kosten. Andere creditcards, zoals bijvoorbeeld American Express kunnen nog duurder zijn.

Payment Service Provider	Eenmalige kosten	Kosten per maand	Kosten per transactie	Opmerking
Adyen	Geen	Geen	Visa: 1,15% + €0,1 MasterCard: 1,40% + €0,1	Minimale fee van €100 per maand
Mollie	Geen	Geen	€0,25 + 1,8% voor EU Cards €0,25 + 2,8% voor businesscards en non-EU-cards	Visa en MasterCard
MultiSafepay	€74,95	Geen	€0,15 + 2% - 3% kosten Acquirer	Kosten van een Acquirer zijn 2% - 3%.
CardGate	€75	Geen	3% + € 0,25	Minimale fee van €20/maand. Voor Mastercard en Visa jaarlijks €98 aansluitkosten
WorldPay	€135	€20	3,95%	Op basis van Business Gateway Plus pakket

Tabel 1: Transactiekosten voor Visa en Mastercard bij enkele Payment Service Providers in Nederland in 2019 (Overonlinebetalen.nl, 2019).

iDEAL-transacties zijn vaak €0,29 - €0,60. In de volgende tabel staan voor verschillende Payment Service Providers de transactiekosten voor iDEAL. Deze kunnen sterk van elkaar verschillen.

Payment Service Provider	Eenmalige kosten	Kosten per maand	Kosten per transactie	Opmerking
Mollie	Geen	Geen	€0,29	Speciaal actietarief, via OverOnlineBetalen.
ICEPAY	Geen	Geen	€0,35	Minimale fee voor 400 trxs en dat is €140
Adyen	Geen	Geen	€0,45	Minimale fee van €100 per maand
CardGate	€75	Geen	€0,58	Minimale fee van €20 per maand
WorldPay	€350	€199	€0,60	iDEAL alleen in combinatie met Corporate Gateway Account.

Tabel 2: Transactiekosten voor iDEAL bij enkele Payment Service Providers in Nederland in 2019 (Overonlinebetalen.nl, 2019).

2.5 Nadelen van het huidige betaalproces

We zien dat het betaalproces vrij omslachtig verloopt. Er zijn veel tussenpartijen betrokken zoals de Issuing Bank, het creditcardnetwerk, Acquirer en de Payment Service Provider die elk een deel van de transactiewaarde inhouden. Dit betekent dat wanneer je €100 betaalt in een winkel, de eigenaar niet daadwerkelijk €100 ontvangt op zijn rekening.

Ook is het proces van autorisatie en authenticatie omslachtig bij het uitvoeren van voornamelijk e-commercetransacties. De Kaarthouder moet naast het invoeren van zijn kaartgegevens ook een 3D-secure code invullen. Hoewel het hele proces van autorisatie en authenticatie gebeurt binnen enkele seconden, kan het proces van clearing & settlement bij creditcards drie tot vijf werkdagen duren. Bij iDEAL-betalingen duurt settlement tussen de Kaarthouder en de Merchant vaak tussen de één en drie dagen.

Daarnaast is fraude met kaartgegevens een ernstig probleem in de paymentindustrie. Volgens The Nilson Report (November, 2019), bedroeg de totale fraude met credit, debit en pre-paid cards in 2016 ongeveer $22,80 miljard USD. Dit is verder gestegen gestegen naar $23,97 miljard USD in 2017. In 2018 was de totale fraude weer verder opgelopen naar $27,85 miljard USD.

Verwacht wordt dat dit zal oplopen naar ongeveer $32,39 miljard USD in 2020. Tegelijkertijd loopt ook het totale volume van credit, debit en pre-paid cards op.[19]

Bij Bitcoin en andere cryptovaluta is het betaalproces geheel anders ingericht. En dan wel op een manier die veel cryptovaluta transactiekosten minder dan een cent laat kosten. In het geval van Bitcoin kost het in december 2019 rond de $0.30 USD om je transactie in het eerstvolgende blok te laten opnemen. Je kan er echter ook voor kiezen om je transactie zes blokken later te laten opnemen, wat ongeveer $0.22 USD kost.[20] Dat betekent ook dat settlements in het geval van Bitcoin – wat momenteel wordt gezien als een vrij verouderde en langzame cryptovaluta – ongeveer 10 minuten kan duren of langer, afhankelijk van welke transactiekosten je bereid bent te betalen. Dit is aanzienlijk sneller en voor e-commercetransacties ook een stuk goedkoper dan bijvoorbeeld PayPal, creditcards en iDEAL.

In een wereld van instant messenging en video calls is het huidige transactiesysteem, waarin we dingen van waarde als geld uitwisselen, archaïsch en langzaam. In het volgende hoofdstuk gaan we dieper in op Bitcoin als modern betaalsysteem, dat beter past bij onze huidige tijd. Bitcoin is de eerste en momenteel, op marktwaarde gebaseerd, ook de grootste blockchain.

[19] Volgens The Nilson Report (november 2019) wordt er van $100 USD aan volume ongeveer 6,86 cent aan fraude gepleegd in 2018 en neemt dit aantal na jarenlange stijgingen langzaam af in de volgende jaren.

[20] Voor een overzicht van de transactiekosten op het Bitcoin-netwerk, zie: https://bitcoinfees.info. Toen Bitcoin eind 2017 rond zijn piekwaarde was, kon een transactie echter wel $10 - $20 USD kosten. Dit kwam doordat er meer transacties per seconde werden verricht op de Bitcoin blockchain dan het netwerk aankon. Het zorgde ervoor dat Bitcoin-transacties in de wacht werden gezet. Transacties duurden destijds vaak aanzienlijk langer dan 10 minuten en als je je transactie wilde bespoedigen, moest je een extra fee betalen. Hoe het komt dat transacties met hogere fees eerder in de blockchain worden opgenomen, wordt besproken in hoofdstuk 4. Sinds Bitcoin zijn er inmiddels modernere blockchains met lagere transactiekosten. Op sommige blockchains kost een transactie minder dan een tiende van een cent.

2.6 Samenvatting, begrippen en bronnen

Samenvatting

In dit hoofdstuk hebben we gekeken naar het huidige betaalproces. Het online betaalproces bestaat grotendeels uit Point-of-Sale (PoS) transacties en e-commercetransacties. In het huidige betaalsysteem zijn bij een transactie veel verschillende partijen betrokken. Dit leidt tot een gecompliceerd betaalproces van autorisatie, authenticatie en clearing & settlement. Deze partijen zijn:

1. De Kaarthouder.
2. De Merchant.
3. De Acquirer.
4. Het creditcardnetwerk bij creditcardtransacties.
5. De Issuing Bank.
6. De Payment Service Provider.

Wanneer een Kaarthouder een betaling van €100 doet, wordt er altijd een gedeelte van het bedrag verdeeld tussen de verscheidene partijen. Daarnaast duurt het hele proces tot en met clearing & settlement bij creditcardbetalingen vaak drie tot vijf werkdagen. Bij iDEAL-betalingen gaan er ongeveer één tot drie werkdagen overheen voordat de Merchant daadwerkelijk het geld op zijn rekening gestort krijgt.

Er zijn bij geldtransacties ook strikte regels met betrekking tot hoe er om moet worden gegaan met betaalgegevens. Een Merchant moet PCI DSS compliant zijn en mag niet zomaar creditcardgegevens opslaan. Om niet op alle niveaus aan PCI DSS te voldoen, is het ook mogelijk voor een Merchant om een Payment Service Provider in te schakelen die al op hogere niveaus compliant is en de betaalpagina host voor de Merchant. Hier zijn echter wel kosten aan verbonden.

Opmerkingen die je nu kunt uitleggen

- Betalingen met reguliere betaalmethoden kennen veel tussenpartijen waardoor de kosten van de transactie vrij hoog kunnen oplopen.
- Transacties in het reguliere betaalsysteem zijn niet peer-to-peer. Hierdoor kunnen transacties makkelijker worden stopgezet, geweigerd en teruggedraaid worden.
- Clearing & settlement bij iDEAL transacties kunnen wel één tot drie werkdagen duren en bij creditcards wel drie tot vijf werkdagen.
- Er zijn veel regels betrokken bij reguliere betaalmethoden. Zo mag je bijvoorbeeld niet zomaar creditcardgegevens opslaan.

Verklarende begrippenlijst

Acquirer: Financiële instelling die transactieverzoeken stuurt vanaf de Merchant naar de Issuing Bank, de kaart van de Kaarthouder. Een Acquirer is doorgaans de bank van de Merchant.

Acquiring Processor: Financiële instelling die betaalverzoeken verwerkt voor de Merchant. Deze dienst wordt ook weleens aangeboden door een Payment Service Provider.

Assessment fee: De fee die bij een transactie wordt uitbetaald aan het creditcardnetwerk voor het bekijken en het beoordelen van de transacties.

Clearing & settlement: Het verwerkingsproces waarbij het geld van de Issuing Bank daadwerkelijk wordt uitgewisseld en verrekend met de Acquirer.

Creditcardnetwerk: Het netwerk dat creditcardtransacties verwerkt. Voorbeelden zijn Visa, Mastercard, China Union Pay en American Express.

E-commerce: Online handel. Een e-commercetransactie is een online transactie in bijvoorbeeld een webshop.

Interchange fee: De kosten die worden betaald aan de Issuing Bank.

Issuing Bank: Financiële instelling die de kaart uitgeeft aan de Kaarthouder. Vaak is deze de bank van de Kaarthouder.

Kaarthouder: Persoon die betaalt met de betaalkaart.

Merchant: De eigenaar van een winkel.

Merchant discount rate: de som van de processing fee, assessment fee en interchange fee.

Payment Service Provider: De betaaldienstverlener. Een betaaldienstverlener koppelt de Merchant met het betaalsysteem.

Point-of-Sale: Kooppunt in fysieke winkels. Een PoS-transactie is een transactie in een fysieke winkel.

Processing fee: De verwerkingskosten die door het creditcardnetwerk wordt betaald aan de Acquirer.

Bronnen

Betaalvereniging Nederland. (2019). Instant Payments in het kort. Geraadpleegd op 24 december 2019, van Betaalvereniging Nederland website: https://www.betaalvereniging.nl/betalingsverkeer/instant-payments/instant-payments-in-het-kort/

Bitcoin Transaction Fees. (2019). Geraadpleegd op 24 december 2019, van Bitcoinfees.info website: https://bitcoinfees.info

iDEAL. (2019). Partners van iDEAL. Benaderd op 24 december 2019, van iDEAL website: https://www.ideal.nl/partners/

Over Online Betalen. (2019). Vergelijk tarieven voor iDEAL en creditcard - voor ondernemers. Geraadpleegd op 24 december 2019, van Overonlinebetalen.nl website: https://overonlinebetalen.nl/vergelijk-tarieven-ideal/

Papadimitriou, O. (2009, 2 april). How Credit Card Transaction Processing Works: Steps, Fees & Participants. Benaderd op 24 december 2019, van WalletHub website: https://wallethub.com/edu/cc/credit-card-transaction/25511/

PCI Security Standards Council. (2019). Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. Benaderd van Pcisecuritystandards.org website: https://www.pcisecuritystandards.org/

The Nilson Report. (2019). *The Nilson Report 2019*. (1164).

Iconen

Kaarthouder, Merchant, Issuing Bank en Acquirer gemaakt door Freepik van www.flaticon.com

Visa-icoon gemaakt door Roundicons van www.flaticon.com

3. Bitcoin, het internet van geld

"A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers. Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it. On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it. Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.

What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014."

- Marc Andreessen (2014)

3.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat het verschil is tussen de cryptovaluta Bitcoin en de Bitcoin blockchain.
- Hoe het Proof-of-Work consensusmechanisme van Bitcoin werkt.
- Wat het Byzantine Generals Problem is en dat Bitcoin dit probleem oplost door middel van Proof-of-Work.
- Hoe consensus wordt bereikt op het Bitcoin-netwerk.
- Wat de rol is van hash cryptografie en Merkle trees in de beveiliging van de blockchain.
- Welke data er in een blok en transactie worden opgenomen.
- Hoe je een block explorer gebruikt om de data uit de blockchain te lezen.
- Hoe het monetaire beleid van Bitcoin in elkaar steekt.
- Hoe het Bitcoin-netwerk mensen aanmoedigt om deel te nemen aan het netwerk, zodat deze draaiende wordt gehouden.

Inleiding

Hoe zou ons economisch leven eruitzien als ons geld niet zou worden gecontroleerd door overheden en centrale banken? Als er niemand is die controle heeft over de inflatie van ons geld en als er geen instituut is die een limiet kan leggen op hoeveel geld we mogen overmaken naar een ander? Een dergelijke wereld van financiële vrijheid was voor velen ondenkbaar totdat Bitcoin, een peer-to-peer elektronisch geldsysteem, werd uitgevonden. Opmerkelijk is dat Satoshi Nakamoto de code compleet open source heeft gemaakt, zodat iedereen de broncode kan inzien en iedereen erop kan vertrouwen dat de totale hoeveelheid Bitcoins in omloop nooit de 21 miljoen kan overschrijden. Dit aantal zal worden bereikt in 2140.

Het eerste blok van de Bitcoin blockchain is gemijnd op 3 januari 2009.[21] Daarin opgenomen is een verwijzing naar het artikel van The Times getiteld 'Chancellor Alistair Darling on brink of second bailout for banks' dat op dezelfde dag is verschenen. Het artikel herinnert ons aan de onzekere tijden van de economische crisis, waarin overheden en centrale banken hebben getracht om het financiële systeem te redden. De toenmalige kanselier van Engeland, Alistair Darling, stond voor de moeilijke keuze om voor miljarden giftige activa van banken op te kopen en banken goedkopere staatsgegarandeerde leningen te verstrekken tegen lage rente.

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

Afbeelding 12: Het artikel waarnaar Satoshi Nakamoto verwees in het genesis blok.

[21] Je kunt het eerste blok inzien via de volgende link: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

Het doel van Bitcoin is sinds zijn ontstaan al duidelijk geweest. Het wil de bankindustrie en de industrie van geldproductie ontwrichten. Daarnaast wil het mensen controle geven over hun eigen geld, zonder dat er goedkeuring of vertrouwen nodig is in een derde partij. Dat betekent dat het immuun moet zijn voor de beslaglegging op ons geld door overheden.

Op 21 januari, 2014, publiceerde Marc Andreessen, de medeoprichter van Netscape een artikel in de New York Times over waarom Bitcoin ertoe doet.[22] Hij schrijft daarin dat de politieke idealisten hun vrijheidsidealen projecteren op Bitcoin en dat de gevestigde elite met wantrouwen, of zelfs verachting, kijkt naar het nieuwe digitale geld. In het artikel vergelijkt hij de technologische impact van Bitcoin met de PC van 1975 en het Internet van 1993. Ondanks de enorme potentie van Bitcoin bestaat er, volgens Andreessen, onder de media een groot misverstand over wat Bitcoin is. Het doel van dit hoofdstuk is om te presenteren wat Bitcoin, als zijnde een nieuwe vorm van geld voor het internet, is en welke fundamentele problemen binnen traditionele transactiesystemen het probeert op te lossen.

We maken in paragraaf 3.2 eerst een onderscheid tussen Bitcoin en het Bitcoin-netwerk. Vervolgens bespreken we in paragraaf 3.3 Bitcoin en diens ambitie om het geld van onze moderne digitale tijdperk te worden. Daarna behandelen we in paragraaf 3.4 welk fundamenteel netwerkprobleem, het zogenoemde Byzantine Generals Problem in de computerwetenschappen, Bitcoin heeft opgelost. De oplossing voor het probleem is een consensusmechanisme dat Proof-of-Work heet. Door het Proof-of-Work-concept nader te bestuderen in paragraaf 3.5, begrijp je ook op een hoger niveau wat blockchain is. In dat opzicht is dit hoofdstuk dan ook een verdieping op hoofdstuk 2. In paragraaf 3.6, lichten we het double-spendingprobleem toe. Vervolgens komt Bitcoins monetaire beleid aan bod in paragraaf 3.7 en vergelijken we in paragraaf 3.8 kort het betaalsysteem van Bitcoin met de reguliere betaalsystemen als iDEAL en creditcards die in het vorige hoofdstuk zijn behandeld. In 3.9 bespreken we op welke manier Bitcoin mensen economische stimulansen biedt om deel te nemen aan het netwerk. Daarna sluiten we in 3.10 het hoofdstuk af met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst.

[22] Netscape was in de jaren 90 nog de grootste webbrowser met een marktaandeel van 90% tot aan de eerste webbrowser oorlog met Internet Explorer. Het artikel waarin Andreessen beschrijft waarom Bitcoin belangrijk is heet 'Why Bitcoin Matters' (2014) en is hier volledig te lezen: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

3.2 Bitcoin en het Bitcoin-netwerk

Als je spreekt over Bitcoin, dan is het belangrijk om onderscheid te maken tussen de munteenheid Bitcoin en het Bitcoin-netwerk. Bitcoin is in dit geval de digitale valuta en het netwerk is de onderliggende infrastructuur, bestaande uit de nodes die alle Bitcoin-transacties helpen bijhouden middels de blockchain. Het Bitcoin-fenomeen is dus meer dan alleen het geld. Wij zullen zien dat het ook een geraffineerde en revolutionaire manier is om data op zo'n manier op te slaan dat alle betrokken partijen kunnen vertrouwen dat deze data juist zijn, zonder dat er een centrale partij aan te pas komt.

3.3 Bitcoin, de revolutionaire digitale munt

Zouden mensen je 50 jaar geleden hebben geloofd, als je toen al zei dat je in de toekomst direct met elkaar zou kunnen communiceren via elektronische tekstberichten, bestaande uit digitale nulletjes en eentjes? Toch is dit de manier voor de moderne wereld om met elkaar te communiceren sinds de opkomst van het internet. Wij gebruiken e-mail, social networking, audio- en videoberichten.

Hoewel zaken als e-mail, audio- en videoberichten in een mum van tijd van de ene partij naar de andere gestuurd kunnen worden, bleek dit toch lange tijd niet mogelijk met digitaal geld. Milton Friedman, Nobelprijswinnaar in de economische wetenschappen in 1976, zag echter al in 1999 dat het internet een grote rol zou spelen in het reduceren van de rol van de overheid in ons economische en sociale leven. Het enige wat er toen nog miste, zei Friedman, was een betrouwbaar elektronisch geldsysteem, waarmee mensen geld kunnen sturen naar elkaar, zonder dat ze elkaar noodzakelijkerwijs hoeven te kennen. Een dergelijk systeem dat zou lijken op contante transacties, en daarmee ook zou genieten van anonimiteit, zou op korte termijn worden ontwikkeld. Volgens sommigen heeft Bitcoin deze belofte ingelost.

Afbeelding 13: Milton Friedman legt uit dat het internet en een betrouwbaar elektronisch geldsysteem de rol van de overheid in ons leven aanzienlijk zullen reduceren en zullen leiden tot meer economische vrijheid.

In principe heeft Bitcoin de volgende drie belangrijke eigenschappen:

1. Het heeft schaarste geïntroduceerd in het digitale domein.
2. Het is een peer-to-peernetwerk zonder dat er vertrouwen nodig is in een derde centrale partij.
3. Het is een ordelijke manier om alle transacties te registreren en te verifiëren, zodat double-spending kan worden voorkomen.

Geld wordt namelijk waardeloos als het niet schaars is en als mensen het kunnen kopiëren om het tweemaal, driemaal, viermaal, etc. te kunnen uitgeven. In dat opzicht wordt Bitcoin regelmatig vergeleken met goud. Goud is net als Bitcoin schaars en double-spending met goud is niet mogelijk, omdat het niet kan worden gekopieerd en nogmaals uitgegeven.

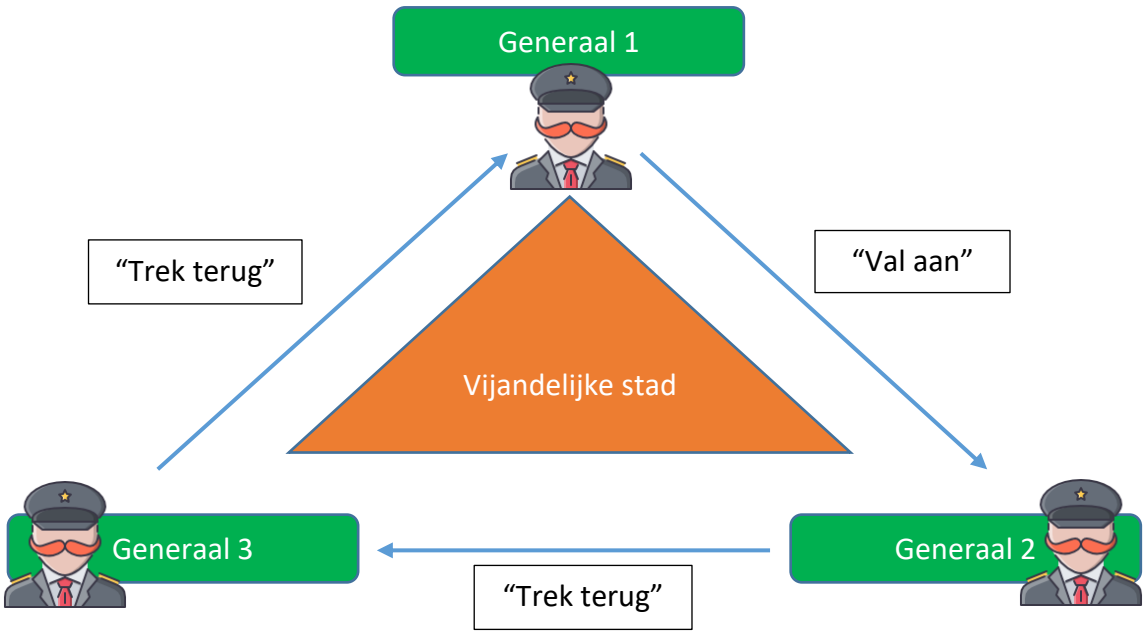
3.4 Byzantine Generals Problem

Zoals in hoofdstuk 1 is vermeld, is Bitcoin de eerste applicatie die gebruikmaakt van blockchaintechnologie. Deze technologie biedt voor het eerst een praktische oplossing voor een probleem dat onder computerwetenschappers bekendstaat als het Byzantine Generals Problem. Twee weken na de eerste openbaring van Bitcoin, stuurt Satoshi Nakamoto een mail met daarin een analogie hoe het Bitcoin-netwerk een praktische oplossing is voor het ***Byzantine Generals Problem*** (BGP).[23] Begrijpen wat het Byzantine Generals Problem is, helpt je om het Bitcoin-netwerk beter te begrijpen en te doorgronden hoe er binnen het netwerk consensus kan worden bereikt.

In het artikel, 'The Byzantine Generals Problem' (1982), hebben Lamport, Shostak en Pease dit probleem voor het eerst geschetst als een situatie waarbij het Byzantijnse leger kampeert buiten een vijandelijke stad. Het leger, bestaande uit verschillende divisies, die elk worden geleid door een afzonderlijke generaal, moeten een gezamenlijk strijdplan zien te smeden om de stad aan te vallen, maar kunnen enkel met elkaar communiceren via boodschappers. Het is mogelijk dat één of meerdere van de generaals of één van de boodschappers een verrader is, die de andere generaals in de war probeert te brengen en de loyale generaals probeert te behoeden om tot een overeenkomstig besluit te komen voor het strijdplan. Hoe kunnen deze generaals in een dergelijke situatie tot een plan komen tegen de vijandelijke stad, met de

[23] Satoshi Nakamoto schetst een situatie waarin een aantal Byzantijnse generaals elk een computer hebben en een aanval willen uitvoeren op de wifi van de koning, door het wachtwoord waarvan zij weten dat het een specifiek aantal karakters lang is, te forceren, dit wordt brute force genoemd. De e-mail is van 13 november 2008 en kan hier in zijn geheel worden gelezen: https://satoshi.nakamotoinstitute.org/emails/cryptography/11/.

zekerheid dat geen één van hen een verrader kan zijn? Of, als er verraad mogelijk is, zij in ieder geval niet de overeenstemming van een goed strijdplan kunnen dwarsbomen? Deze vertrouwenloze situatie kun je zien als een gedecentraliseerde omgeving, waarbij er geen centraal punt is om betrouwbare informatie van een gezamenlijk strijdplan te delen.



Afbeelding 14: Een systematische weergave van het Byzantine Generals Problem. De boodschapper van Generaal 1 geeft aan dat ze moeten aanvallen. Generaal 2 besluit echter om zich terug te trekken en laat zijn boodschapper de boodschap om terug te trekken doorgeven aan Generaal 3. Generaal 3 neemt de boodschap over en stuurt dezelfde boodschap die hij heeft ontvangen door naar Generaal 1. Het probleem hier is: hoe kunnen de generaals consensus bereiken in een omgeving waarin je meerdere partijen, de boodschappers en elkaar, moet vertrouwen om de juiste boodschappen aan elkaar door te geven, zodat een succesvol gecoördineerd strijdplan kan worden uitgevoerd?

Het probleem is aldus om een algoritme te vinden dat (a) in de eerste plaats kan verzekeren dat alle loyale generaals overeenstemming kunnen bereiken. De loyale generaals zullen hierbij doen wat het algoritme hen voorschrijft te doen, terwijl de verraders kunnen doen wat zij wensen. Het algoritme moet zo zijn ingericht, dat het de garantie biedt dat alle loyale generaals het volgen, ongeacht wat de verraders doen. Ook moeten deze generaals overeenstemming vinden over een redelijk strijdplan. Dat houdt in dat (b) in de tweede plaats een kleine groep verraders de loyale generaals niet kan dwingen tot het overnemen van een slecht strijdplan.

Conditie (a) kan worden verzekerd door elke generaal eenzelfde methode te laten hanteren om tot een besluit te komen en door elke loyale generaal dezelfde informatie te laten verkrijgen. Conditie (b) is lastig te bereiken, omdat je niet eenduidig kan vaststellen wat een goed of slecht

strijdplan is. Wat de één goed vindt, kan de ander als slecht zien. Wat je wel kan doen, is een regel vinden die het uiteindelijke besluit van de generaals baseert op een meerderheidsstemming tussen de generaals. Dit zorgt ervoor dat verraders alleen het besluit van de loyale generaals kunnen voorkomen als zij in een meerderheid zijn. Dit is geen perfecte methode, maar volgens Lamport et al. is dit wel de beste methode die we momenteel kennen.

Wij kunnen bovenstaand Byzantine Generals Problem vergelijken met dat van een gedecentraliseerd of gedistribueerd computernetwerk, waarbij alle deelnemers (nodes) van het netwerk elkaar niet kunnen vertrouwen, maar toch gezamenlijk tot besluiten moeten komen. Hierbij stoelt de betrouwbaarheid op het feit dat:

1. Een transactie die is gedaan, wordt opgenomen op de blockchain en gedeeld met alle deelnemers. Met andere woorden, iedereen moet toegang hebben tot dezelfde informatie.
2. Een transactie die is gedaan, wordt geauthentiseerd zodat persoon A niet de Bitcoin van persoon B kan overmaken. Bij het Byzantine Generals Problem betekent dit dat de boodschappen worden gecheckt op het feit dat zij van de juiste personen – generaals en boodschappers – vandaan komen.
3. Een transactie niet wordt vervalst. Dit betekent dat als iemand een geldige transactie doet, niemand anders de inhoud van de transactie kan wijzigen. Ofwel, wanneer een generaal een boodschap stuurt, niemand de inhoud van de boodschap kan veranderen.
4. Een transactie niet dubbel kan worden uitgevoerd. Als iemand 1 BTC heeft, kan deze persoon niet 1 BTC aan zowel persoon A als aan persoon B geven. Er is dus geen tegenstrijdige informatie mogelijk. Een generaal kan niet twee tegenstrijdige berichten sturen.

3.4.1 Byzantine Fault Tolerance (BFT)

Om de betrouwbaarheid van de data op de blockchain te waarborgen, heeft het netwerk deelnemers nodig die berichten of transacties verifiëren op hun juistheid en die andere deelnemers die corrupt en misleidend zijn, neutraliseren. De overeenkomst tussen deze nodes is wat je consensus noemt. Een systeem dat resistent is tegen het Byzantine Generals Problem kenmerkt zich door de ***Byzantine Fault Tolerance*** (BFT) eigenschap.

Er zijn meerdere manieren om Byzantine Fault Tolerant systemen in te richten. In hoofdstuk 6 bespreken we meer consensusprotocollen die dit mogelijk maken.

3.5 Proof-of-Work-consensus in het Bitcoin-netwerk

Op het Bitcoin-netwerk wordt Byzantine Fault Tolerance bereikt middels het Proof-of-Work consensusmechanisme. Het doel van Proof-of-Work is om het netwerk te beschermen tegen aanvallers, om double-spending te voorkomen en om consensus te kunnen bereiken over welke chain de ware blockchain is, wanneer er twee concurrerende chains ontstaan.

Proof-of-Work heeft de volgende eigenschappen:

1. Het maakt gebruik van ***hash cryptografie***.
2. Mijners zoeken een ***nonce*** die leidt tot een geldige hash van een blok waar Bitcoin-transacties in zijn opgeslagen.
3. Wanneer een geldige ***hash*** is gevonden, wordt het blok geverifieerd op juistheid door verschillende full nodes op het netwerk. De snelheid, ofwel ***bloktijd***, waarmee een geldige hash wordt gevonden, is gebaseerd op de ***mining difficulty***.
4. Dit nieuwe blok wordt door andere nodes op het netwerk overgenomen en toegevoegd aan hun versie van de blockchain.
5. Mocht het zijn dat er binnen ongeveer dezelfde tijd twee geldige hashes zijn gevonden onder twee verschillende mijners, dan zijn er twee concurrerende chains. In dergelijke gevallen wordt er consensus bereikt door de langste blockchain over te nemen.
6. Al met al zorgt het bovenstaande ervoor dat iedereen op het netwerk ervan uitgaat dat er één blockchain is met de juiste data. Met andere woorden, je maakt gebruik van eenzelfde grootboek, dat alle transacties heeft geregistreerd, waardoor fraude als ***double-spending*** niet mogelijk is.

Wat volgt is een nadere toelichting van de bovenstaande eigenschappen.

3.5.1 Hash cryptografie

Als we kijken naar de berichtgeving van de boodschappers binnen het Byzantine Generals Problem, zien we dat berichtgeving plaatsvindt in alledaags geschreven taal. Dit is op zich al een grote zwakte, omdat alledaags taalgebruik gemakkelijk gemanipuleerd en vervalst kan worden door de boodschappers. Daarom moet er een methode zijn binnen het consensusalgoritme om berichten te kunnen valideren, zodat we weten dat er niet met de oorspronkelijke tekst is gemanipuleerd. In het Bitcoin-consensusprotocol is dit mogelijk door gebruik te maken van (1) hash cryptografie en (2) een nonce.

De oorsprong van het woord cryptografie is te herleid uit de Griekse woorden *kryptos* en *graphein,* die respectievelijk verborgen en schrijven betekenen. Cryptografie is aldus een

methode om geschreven tekst te verhullen. Met de opkomst van nieuwe communicatiemogelijkheden, zoals de telegraaf, de radio, computer, mobiele telefoon, e-mail, instant messaging en online bankieren is er de zorg bijgekomen dat datgene wat we communiceren, kan worden afgeluisterd, waardoor onze privacy in het geding kan komen. Er is om deze reden een grote behoefte om datgene wat we communiceren te kunnen verhullen voor anderen. De methode die momenteel wijd gebruikt wordt in de digitale wereld is hash cryptografie.

Hash cryptografie is een manier om op wiskundige wijze digitale data om te zetten in een vast aantal karakters, die niet begrijpbaar en op het eerste gezicht zeer willekeurig lijken. Het wordt gebruikt om onze persoonlijke gegevens op een veilige wijze te versturen op het internet, zoals onze wachtwoorden en onze online betaaltransacties. De achterliggende gedachte om data cryptografisch versleuteld te versturen op het internet is dat wanneer het wordt onderschept door een ander persoon dan voor wie het bedoeld is, deze persoon niet kan achterhalen wat de daadwerkelijke boodschap is achter de brei van 'willekeurige karakters'.

Bitcoin maakt gebruik van een cryptografische hash technologie dat SHA-256 heet.[24] SHA staat voor Secure Hash Algorithm en 256 is het aantal bits van de hash. Het is altijd 64 karakters lang en bestaat uit hexadecimalen. Elk karakter kan dus één van de volgende 16 waarden aannemen:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Elke waarde is 4 bits groot. Als de hash een lengte heeft van 64 karakters, is de hash 64 * 4 = 256 bits lang. Om deze reden heet het algoritme SHA-256.

Hash cryptografie werkt als volgt. Je neemt data die je door het hash algoritme, SHA-256 in het geval van Bitcoin, haalt en er komt altijd een 64-karakters (of 256 bits) lange waarde uit. Er zijn online talloze SHA-256 hash calculators die je kunt gebruiken om data te hashen.[25]

[24] Naast SHA-256 zijn er nog andere cryptografische hash-functies. Andere bekende hash-functies zijn MD5 en SHA-1.

[25] In principe zou je alle digitale data kunnen hashen - zo ook de broncode van een computerapplicatie, uitgaand e-mailverkeer, of zelfs een boek. Een website waar je bijvoorbeeld SHA-256 hashes kunt genereren is https://www.xorbin.com/tools/sha256-hash-calculator.

In ons voorbeeld gaan we sonnet 18 van Shakespeare hashen met SHA-256. De sonnet is als volgt:

> Shall I compare thee to a summer's day?
> Thou art more lovely and more temperate:
> Rough winds do shake the darling buds of May,
> And summer's lease hath all too short a date:
> Sometime too hot the eye of heaven shines,
> And often is his gold complexion dimmed,
> And every fair from fair sometime declines,
> By chance, or nature's changing course untrimmed:
> But thy eternal summer shall not fade,
> Nor lose possession of that fair thou ow'st,
> Nor shall death brag thou wander'st in his shade,
> When in eternal lines to time thou grow'st,
> So long as men can breathe, or eyes can see,
> So long lives this, and this gives life to thee.

De output is de volgende hash-waarde van 64-karakters lang:

```
efcb1eec2619c42e57eb414b3f11dd93d706f4fee8093e3617ad576ded3abe76
```

Een betrouwbaar hash-algoritme moet voldoen aan de volgende voorwaarden:

1. *Het is deterministisch*. Dat betekent dat eenzelfde input altijd moet leiden tot eenzelfde output. Het hashen van sonnet 18 zal altijd leiden tot exact dezelfde output.
2. *Als je de output hebt, kun je de input niet achterhalen door middel van reverse engineering*. Dat houdt dus in dat iedereen die de hash-waarde weet van Shakespeare's sonnet 18 niet kan achterhalen dat het daadwerkelijk Shakespeare's sonnet 18 is.
3. *Het omzetten van data in een hash-waarde moet snel kunnen*.
4. *Als je de input wijzigt, dan verandert de output compleet.* Dat betekent dat wanneer we iets veranderen aan Shakespeare's sonnet 18 – bijvoorbeeld een hoofdletter veranderen in een kleine letter, punctuaties wijzigen of een spatie toevoegen of verwijderen – de output totaal anders wordt. Als we bijvoorbeeld één enkele spatie zetten aan het begin van de eerste regel, dan wordt de output als volgt:

Het is ook handig om te weten dat een hash eigenlijk niks anders is dan een getal en dat je een hexadecimale hash kan omzetten in een decimaal getal. Een rekeninstrument dat je hiervoor kunt gebruiken is https://www.rapidtables.com/convert/number/hex-to-decimal.html.

d7d12ca4131b1bc9a0d12fc405180794f5468b8802fe126aa49ea99b3e4dae45

In dat opzicht is een hash-waarde een soort vingerafdruk van data. Net zoals elke persoon een unieke biologische vingerafdruk heeft, heeft ook elke data zijn eigen unieke hash-waarde.

5. *De kans op collisies moet miniem zijn*. Francis Galton, de pionier van vingerafdrukken, schatte in dat de kans dat twee mensen exact dezelfde vingerafdrukken hebben, gelijk is aan 1 op 64 miljoen. Hoewel de kans erop zeer minimaal is, is het statistisch gezien dus toch mogelijk dat twee of meerdere mensen eenzelfde vingerafdruk hebben. Dat is ook het geval bij hashes. Statistisch gezien zijn er bij 64 hexadecimale karakters 16^{64} mogelijke ***hash-outputs***. Hoewel het aantal mogelijke outputs gigantisch is, is het niet oneindig. Daarentegen is het aantal verschillende data-input dat je kan hashen wel oneindig. Om deze reden is het mogelijk dat twee verschillende inputs leiden tot dezelfde hash-outputs. Bij een deugdelijk cryptografisch algoritme moet de kans dat twee verschillende inputs leiden tot eenzelfde output zo miniem zijn, dat het praktisch onmogelijk is.

Voorwaarden voor een betrouwbaar hash-algoritme

1. Het is deterministisch.
2. Reverse engineering van een output is niet mogelijk.
3. Omzetten van data in een hash gebeurt snel.
4. Wijziging van input escaleert in een radicale wijziging van de output.
5. Kans op collisies is vrijwel onmogelijk.

Intermezzo: Hash-cryptografie bij reguliere e-commercebetalingen

Cryptografische hash-functies als SHA-256 worden niet alleen gebruikt bij blockchains. Reguliere banktransacties maken hier ook gebruik van om de communicatie tussen de webwinkel en het online betaalplatform, de internet payment gateway, te beveiligen. Door de communicatie te versleutelen, kunnen kwaadwillenden de transactie niet inzien. We illustreren de werking hiervan door te kijken hoe European Merchant Services (EMS), een Nederlandse Payment Service Provider, webwinkels verplicht om transacties versleuteld in te sturen naar hun online payment gateway.

Voor het doen van een transactie moet er altijd een hash-waarde van de transactie worden meegestuurd naar het online betaalplatform. Deze hash-waarde wordt gegenereerd middels de waarden van de volgende vijf parameters:

1. *Storename*: dit is een unieke ID van de webwinkel, gegenereerd door EMS
2. *Txndatetime*: de dag en tijd van de transactie
3. *Chargetotal*: het totale bedrag
4. *Currency*: de valuta, uitgedrukt in valutacodes. 826 staat bijvoorbeeld voor USD
5. *Sharedsecret*: een geheime code die net als de storename dient als een unieke identifier van de webwinkel

Stel je voor dat iemand de volgende transactie doet bij een webwinkel:

1. Storename: 98765432101
2. Txndatetime: 2013:07:06-09:57:08
3. Chargetotal: 1.00
4. Currency: 978
5. Sharedsecret: TopSecret

Bovenstaande parameters worden allereerst achter elkaar gezet in een string:

987654321012013:07:06-09:57:081.00978TopSecret

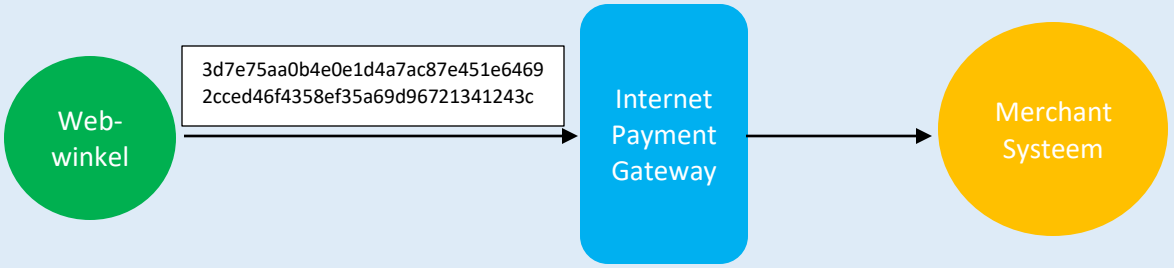
De string wordt vervolgens geconverteerd in een ASCII hexadecimale representatie:

393837363534333231303132303133 3a30373a31362d30393a35373a3038312e3030383236546f70536563726574

Bovenstaande ASCII hexadecimale representatie wordt tenslotte met SHA-256 omgezet in een hash waarde:

3d7e75aa0b4e0e1d4a7ac87e451e64692cced46f4358ef35a69d96721341243c

Hieronder vind je een grafische weergave van het transactieproces.



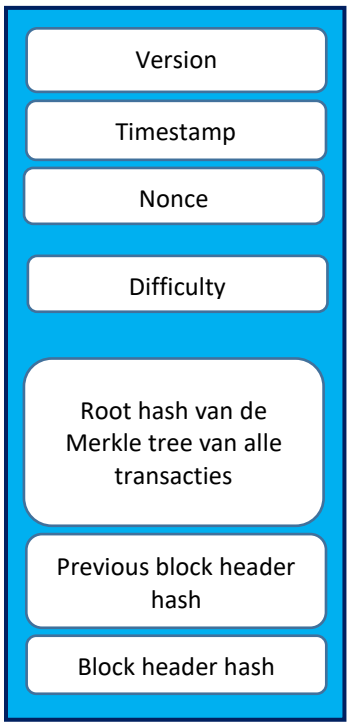
Afbeelding 15: Een transactie vanuit de webwinkel wordt versleuteld verstuurd naar de Internet Payment Gateway van EMS. Mocht een kwaadwillende de transactie onderscheppen, dan vindt hij slechts een hash-waarde van de werkelijke transactie. De Internet Payment Gateway checkt of de transactie goed is ingestuurd. Op basis daarvan stuurt deze een bericht door naar het systeem van de Merchant met een parameter of de transactie is geslaagd of niet. Vaak stuurt de Merchant dit bericht weer terug naar de webwinkel zodat de betalende klant kan zien of de transactie is geslaagd of niet.

3.5.2 Uit welke data bestaat een blok

Laten we nader kijken welke belangrijkste data in een blok worden opgeslagen. Dit zijn:

1. Version.
2. Timestamp.
3. Nonce.
4. Difficulty.
5. Root hash van de Merkle tree van alle transacties.
6. Previous block header hash.
7. Block header hash.

De punten 1 t/m 6 maken deel uit van wat je de block header noemt. Punt 7, de block header hash, is een dubbele SHA-256 hash van deze block header. Daarnaast worden uiteraard ook de transacties opgeslagen in een blok. In de volgende afbeelding vind je voor het gemak een vereenvoudigde weergave van een blok met de typen data die erin staan.



Afbeelding 16: Weergave van de verschillende gegevens die in een blok zitten.

Version

Dit is het versienummer van de Bitcoin blockchain.

Timestamp

Een timestamp is een stukje data dat certificeert wanneer het blok is gecreëerd of voor het laatst is gewijzigd. Het helpt dus bij het certificeren dat er niet is gemanipuleerd met de data binnen het blok.[26] De timestamp wordt uitgedrukt in het aantal seconden dat is verstreken sinds 1 januari 1970.[27]

Nonce

De nonce is een 32-bitveld en is de enige variabele die je kunt veranderen om een hash-waarde van het blok te verkrijgen die voldoet aan bepaalde voorwaarden, bijvoorbeeld dat het begint

[26] Als je meer wil lezen over hoe timestamps werken, dan wordt 'How to Time-Stamp a Digital Document' (1991) van Haber & Stornetta aangeraden. Het legt uit waarom timestamps belangrijk zijn en hoe ze bijdragen aan authenticatie van de data.

[27] Dit staat ook bekend als de unix timestamp. Bezoek https://www.unixtimestamp.com/ om te zien wat de huidige unix timestamp is.

met 18 opeenvolgende nullen. De mijner die als eerste de nonce weet te vinden die voldoet aan de gestelde voorwaarden mag het blok toevoegen aan de blockchain. Zo'n valide nonce wordt ook wel een ***golden nonce*** genoemd.

Omdat het veld van de nonce 32-bit is, kan de nonce een waarde hebben tussen 0 en 4.294.967.295, ofwel tussen 0 en $2^{32} - 1$. Het bereik van de nonce (0 tot 4.294.967.295) wordt ook wel de ***nonce range*** genoemd. Begrijpen wat een nonce is, is belangrijk om te weten wat een mijner eigenlijk doet. Hier komen we dadelijk op terug.

Difficulty

De difficulty is de moeilijkheidsgraad om een valide nonce te vinden. De difficulty zorgt ervoor dat er gemiddeld rond elke 10 minuten een nieuw blok wordt toegevoegd aan de blockchain door de mijner. Ook hier komen we dadelijk op terug.

Transactiedata

De transactiedata omvatten alle data die te maken hebben met transacties, zoals op welke tijd hoeveel Bitcoin is overgemaakt van de ene naar de andere wallet.

Root hash van de Merkle tree

De root hash van de ***Merkle tree*** – ook wel Merkle-boom in het Nederlands – is de hash van alle hashes van alle transacties die deel uitmaken van een blok. Dit wordt in een aparte intermezzo verder toegelicht. Voor nu is het van belang om te weten dat Merkle trees een belangrijke methode is om data op een accurate en beveiligde manier op te slaan. Het maakt het mogelijk om op snelle wijze transacties te verifiëren en om te voorkomen dat mensen valse transacties op de blockchain registreren.

Previous block hash

De previous hash is de hash-waarde van het vorige blok.

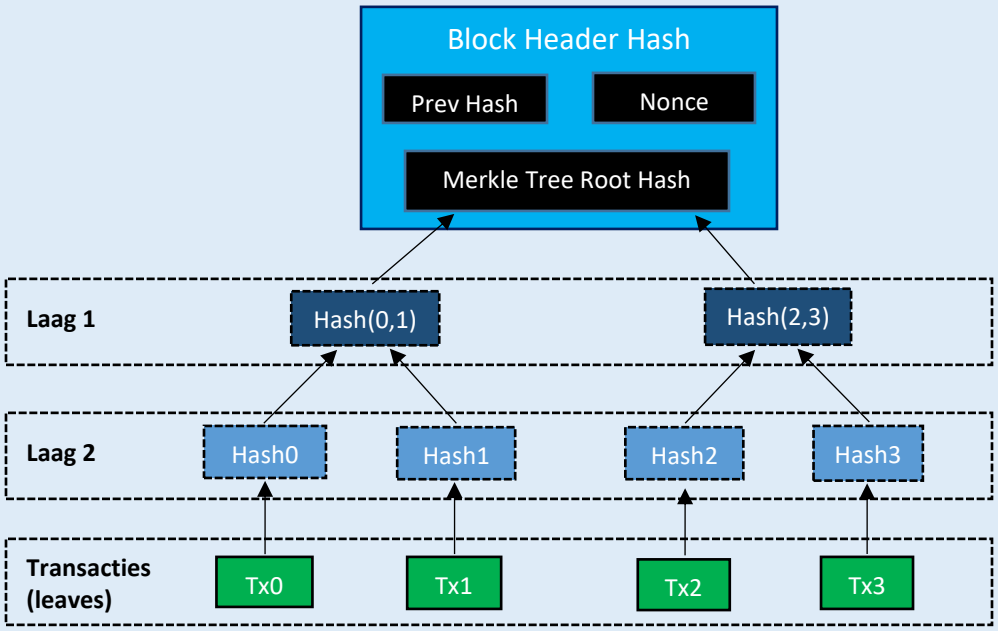
Block header hash

De block header hash is de hash-waarde van het huidige blok. De hash van een blok is het best te vergelijken met een unieke vingerafdruk van het blok. Als er wordt gesjoemeld met de data binnen het blok verandert automatisch de block header hash. Bij Bitcoin wordt de block header hash verkregen door tweemaal de block header te hashen met SHA-256.

Intermezzo: Merkle Trees, hoe ze worden gebruikt binnen de Bitcoin blockchain

Merkle trees zijn uitgevonden door de cryptograaf Ralph Merkle in 1979. Ze zijn goed bruikbaar in peer-to-peernetwerken als blockchain. Merkle trees organiseren gegevens op zo een manier dat het makkelijker wordt om bijvoorbeeld transactiegegevens te verifiëren, of om er zeker van te zijn dat de blockchain geen corrupte gegevens bevat. Daarnaast kunnen ze ook worden gebruikt om een deel van de blockchain af te stoten en zodoende schijfruimte te besparen. Hieronder volgt meer uitleg hoe dit precies te werk gaat.

Hoe werkt een Merkle tree?



Afbeelding 17: De Merkel tree van 4 transacties. Zie ook de Bitcoin white paper (2009, p. 4).

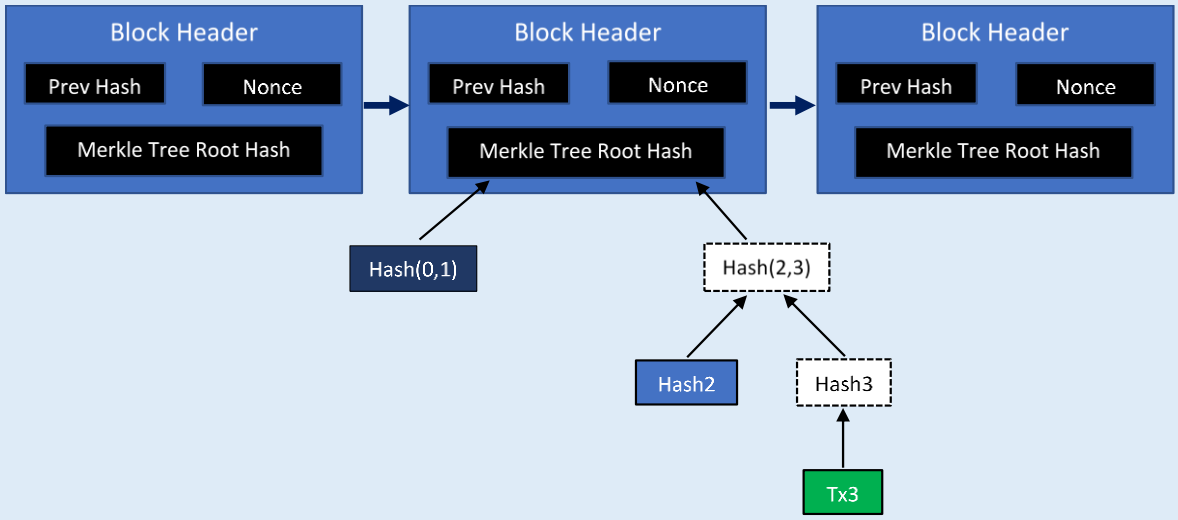
Wij hebben in dit voorbeeld een Merkle tree genomen van slechts vier transacties, hoewel een Bitcoin block wel duizenden transacties kan bevatten. De onderste laag van een Merkle tree bestaat uit de Bitcoin-transacties. Deze worden ook wel “leaves” genoemd. Elke transactie wordt gehasht. Dus Tx0 krijgt een Hash0, Tx1 krijgt Hash1, Tx2 krijgt Hash2 en Tx3 krijgt Hash3. De hashes worden in paren bij elkaar gevoegd, om vervolgens weer gehasht te worden. Hash0 en Hash1 worden dus bij elkaar geplaatst om daar een hash van te nemen, Hash(0,1). Hetzelfde wordt gedaan met het hashpaar Hash2 en Hash3, wat leidt tot Hash(2,3). Vervolgens worden de resulterende hashes, Hash(0,1) en Hash(2,3) weer samengevoegd en gehasht, zodat er nog maar één enkele hash overblijft. Deze uiteindelijke hash is de Merkle tree root hash. Deze root hash wordt opgenomen in de block header hash.

Hoe kunnen transactiegegevens worden geverifieerd met Merkle trees?

Elke hash binnen de Merkle tree is afhankelijk van de gegevensinput. Als er één transactie binnen de Merkle tree zou worden gewijzigd, dan verandert niet alleen de hash van de desbetreffende transactie, maar ook de hashes van bovenliggende lagen tot en met de root hash van de Merkle tree en de block header hash. Mocht er dus iemand zijn die corrupte transacties wil injecteren in de blockchain, dan zal dit helemaal escaleren tot een andere root hash. Voor de beveiliging van de blockchain is het belangrijk dat betrouwbare nodes opmerken dat fraudulente blokken afwijkende root hashes en block header hashes hebben en dat ze signaleren naar het netwerk dat zij invalide blokken hebben gedetecteerd.

Daarnaast kun je bij het downloaden van een blockchain ook nagaan of elke transactie die erin staat wel juist is door de root hashes, resulterend uit de transacties, te vergelijken met die van betrouwbare nodes. Mocht een root hash niet overeenkomen, dan kun je de Merkle tree aflopen tot aan de transacties om te zien met welk stukje gegeven er iets mis is.

Ook kun je, mits je een deel van de gegevens van een block weet, zelf berekenen of dat deel dat je kent klopt. Stel bijvoorbeeld dat je alleen Tx3, Hash2 en Hash(0,1) zou kennen. Dan zou je de Hash van Tx3 kunnen berekenen en deze samenvoegen met Hash2 om achter Hash(2,3) te komen. Omdat je Hash(0,1) al weet, voeg je deze samen met Hash(2,3) en bereken je de root hash. Met andere woorden, je kunt in dit voorbeeld met slechts gedeeltelijke informatie achterhalen of Tx3 een geldige transactie is.



Afbeelding 18: Een node kan ook slechts een kopie van de block headers hebben. De interieure data die zijn gelinkt aan de Merkle trees zijn niet nodig om transacties te kunnen verifiëren, zolang je de root hashes van de Merkle trees hebt en zolang je deze synchroniseert met andere betrouwbare nodes.

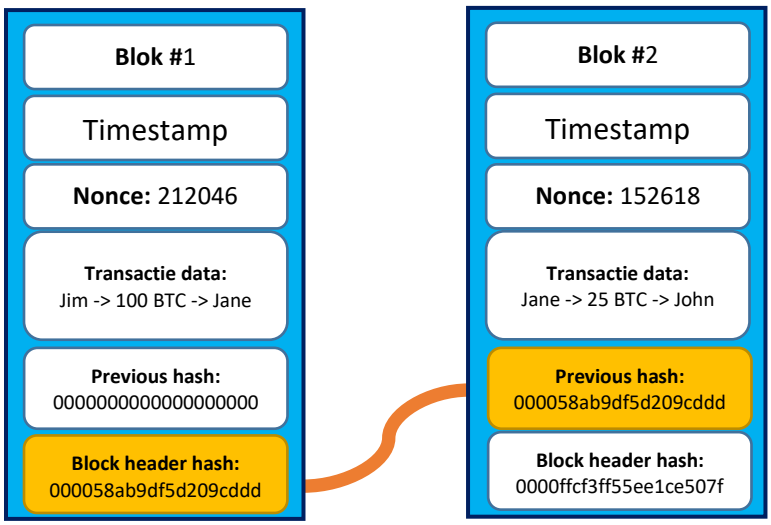
Hoe kun je Merkle trees gebruiken om de blockchain compacter te maken voor nodes?
Omdat elke verandering aan een transactie uiteindelijk leidt tot een verandering aan de Merkle root, voldoet het om slechts Merkle roots te vergelijken met de Merkle roots van betrouwbare nodes, om er zeker van te zijn dat er geen frauduleuze transacties tussen zitten. Een node hoeft hierdoor niet altijd een full node te zijn. Een full node is een node die de volledige blockchain bezit, met daarbinnen alle data. Een node zou hierdoor in principe van oudere blokken alleen de block headers kunnen opslaan en de interieure data van de Merkle root kunnen afstoten. Doordat deze methode minder data-intensief is, kan deze node zichzelf schijfruimte besparen. Een dergelijke node wordt een *pruning node* genoemd. Dit is een kostenbesparende oplossing voor mensen die geen full nodes kunnen draaien, maar wel het Bitcoin-netwerk willen ondersteunen. Het is nog wel mogelijk voor pruned nodes om de laatste Bitcoin-transacties te valideren en ze door te geven aan de andere nodes op het netwerk.

De significantie van Merkle trees
Bij het downloaden van de blockchain download je vaak de blockchain data van meerdere peers die je persoonlijk niet kent. Het risico is dat één van de peers je corrupte gegevens meegeeft. Door gebruik te maken van Merkle trees kun je er snel achterkomen of er een transactie in je blockchain zit die niet klopt en door de structuur ervan kun je sneller achterhalen bij welk blok en bij welk deel van de Merkle tree de fout ligt.

Al met al kunnen we concluderen dat Merkle trees-transacties onafhankelijk verifieerbaar zijn en de blockchain veilig maken. Ze zijn ontzettend belangrijk voor blockchains om vertrouwen te creëren in een netwerk waarin participanten elkaar niet kennen.

3.5.3 Target hash

Hieronder is een vereenvoudigd voorbeeld weergegeven van de eerste twee blokken van een blockchain. Het eerste blok noem je het ***genesis blok***. De previous hash van blok 1 staat hierbij gelijk aan 00000000000000000…, omdat er geen eerder blok is geweest. De previous hash van blok 2 is gelijk aan de hash-waarde van blok 1. Doordat een volgend blok altijd een directe verwijzing heeft naar de hash-waarde van het vorige blok is er altijd een link of keten tussen twee opeenvolgende blokken. Bij Bitcoin is de voorwaarde dat de hash alleen geldig is als het minimaal begint met een specifiek aantal nullen – momenteel is het 18 nullen. Het nummer waar een hash gelijk of kleiner aan moet zijn om als geldig te worden verklaard, noem je de ***target hash***.[28] Voor het gemak zeggen we dat onze target hash in onderstaand voorbeeld niet met 18, maar met 4 nullen begint. In dit geval is het onderstaande blok geldig, omdat het met minimaal 4 nullen start.



Afbeelding 19: Vereenvoudigde weergave van een geldig genesis block en blok #2 met daarin transactiedata.

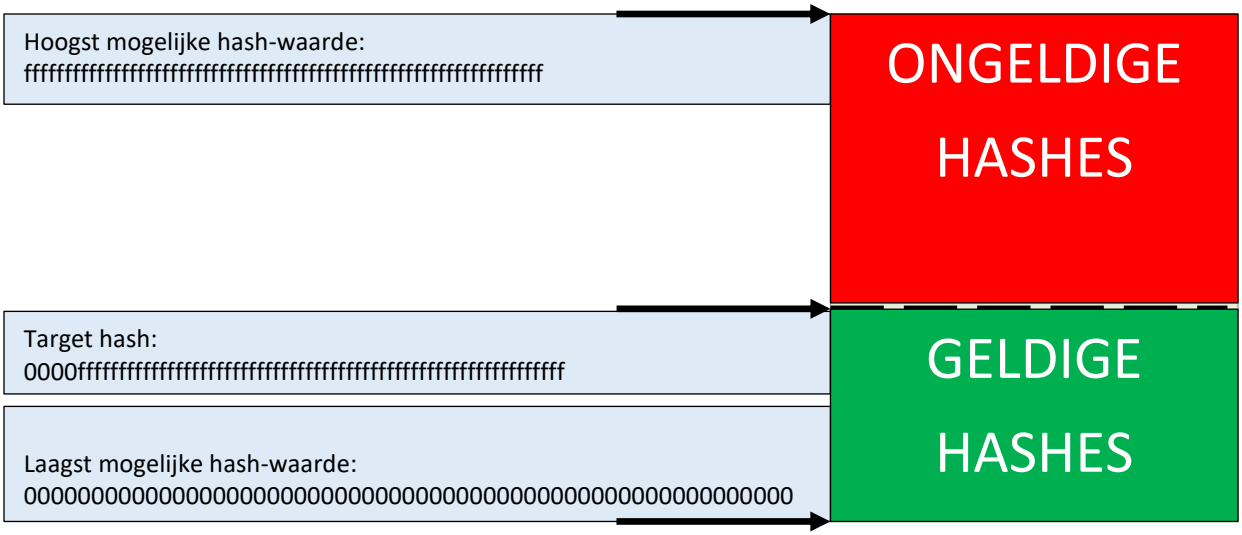
Om te verduidelijken wat een target hash is, is het handig om ons een vierhoek voor te stellen waarin alle mogelijke hash-waarden passen. In de vierhoek zijn de hash-waarden gerangschikt van hoogst mogelijke waarde (bovenin) naar laagst mogelijk waarde (onderin). Alle waarden

[28] Als je bijvoorbeeld via een Bitcoin block explorer (www.blockexplorer.com) zoekt naar blok #557315, met als timestamp Jan 6, 2019, 3:26:17 PM, dan vind je dat de hash-waarde van dit blok als volgt is:

000000000000000000188a1f2550c57cee9ded9e570f39f97dacc8bd3f1b58e4

Zoals je ziet begint de hash-waarde met 18 nullen.

groter dan de target hash zijn ongeldige hashes en alle waarden kleiner dan de target hash zijn wel geldig.



Afbeelding 20: Overzicht van ongeldige en geldige hashes. Alle waarden gelijk aan of onder de target hash zijn geldig. Alle waarden daarboven zijn ongeldig.

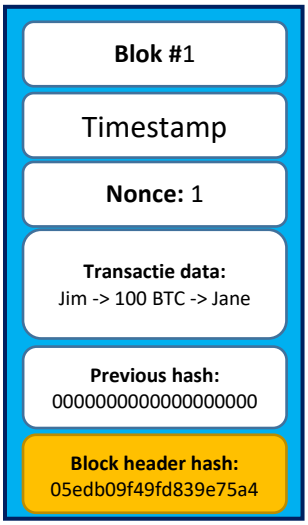
Wat is de kans dat een willekeurige block header hash een geldige hash is?
We kunnen het totaal aantal mogelijkheden van hash-waarden berekenen. Wetende dat een hash bestaat uit 64 hexadecimale getallen, zijn er in totaal 16^{64} mogelijke hashes.

Als alleen hashes die beginnen met 18 opeenvolgende nullen valide zijn, dan zijn er in totaal $16^{64-18} = 16^{46}$ valide hashes. De kans dat een willekeurige block header hash een valide hash is, is dan gelijk aan $16^{46} / 16^{64} = 16^{-18} \approx$ 0,0000000000000000002%.

Als we in ons voorbeeldblok de waarde van de nonce zouden veranderen in 1, dan verandert de hash-waarde in:

```
05edb09f49fd839e75a4adbcf1ae8197df70b9e6347f35f7ab3a9961900f3bca
```

Omdat deze hoger is dan de target hash – hij voldoet niet aan de voorwaarde van minimaal 4 startende nullen – is deze hash ongeldig en daarmee ook het blok. Het blok met een dergelijke hash zal niet worden geaccepteerd door andere nodes op het netwerk en dus ook niet worden opgenomen in de blockchain.

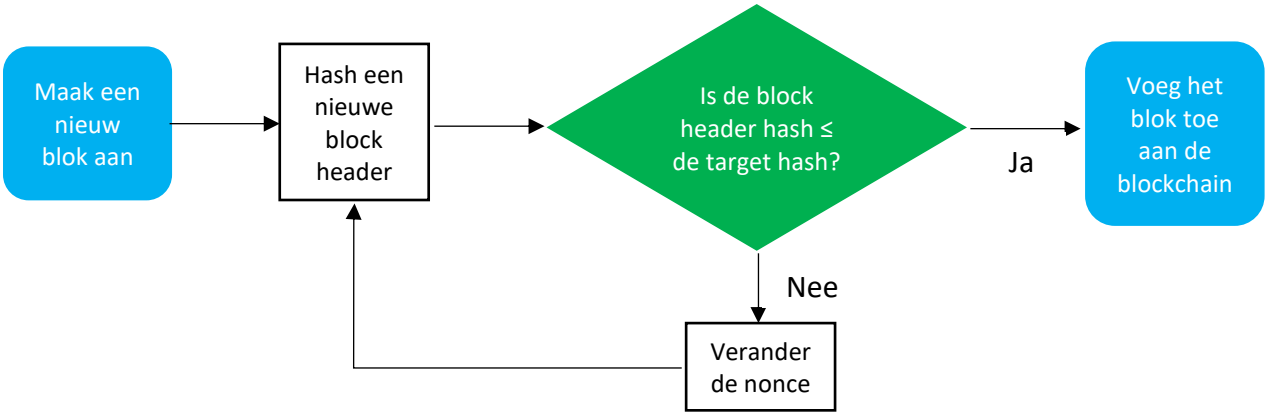


Afbeelding 21: Vereenvoudigde weergave van een ongeldig genesis blok.

3.5.4 Mijnen

Nu we weten welke data in een blok wordt opgeslagen en dat de nonce de enige parameter is die je kunt wijzigen om een geldige hash te kunnen genereren, wordt het ook duidelijker wat een mijner eigenlijk doet.

Wanneer nieuwe transacties zijn verzameld in een blok zoekt de mijner naar een nonce die, wanneer hij het samen hasht met de rest van de data in het blok, een geldige block header hash-waarde oplevert. Je kunt het vinden van de juiste nonce zien als een proces waarin er steeds een willekeurige waarde van een nonce wordt geprobeerd, totdat een waarde onder de target hash wordt bereikt.



Afbeelding 22: Een schematisch proces van wat een mijner doet.

Voor het vinden van een nonce die leidt tot een geldige hash is computerkracht vereist. Meer computerkracht leidt tot meer ***hashing power***. Wanneer een mijner de juiste nonce weet te vinden en het blok wordt opgenomen in de blockchain, wordt de mijner beloond met de transactiefees van de transacties in het blok en met een blokbeloning van momenteel 12,5 BTC. Dat betekent dat het aanbod van Bitcoin momenteel stijgt met 12,5 BTC per gevonden geldige hash.

De mijner heeft in dit geval bewijs geleverd dat hij werk of computerkracht heeft geleverd aan het netwerk om een geldige hash te vinden. De mijner heeft met andere woorden Proof-of-Work geleverd en mag om deze reden een nieuw blok produceren.

In het volgende hoofdstuk wordt een verdere verdieping van het mijningproces gegeven.

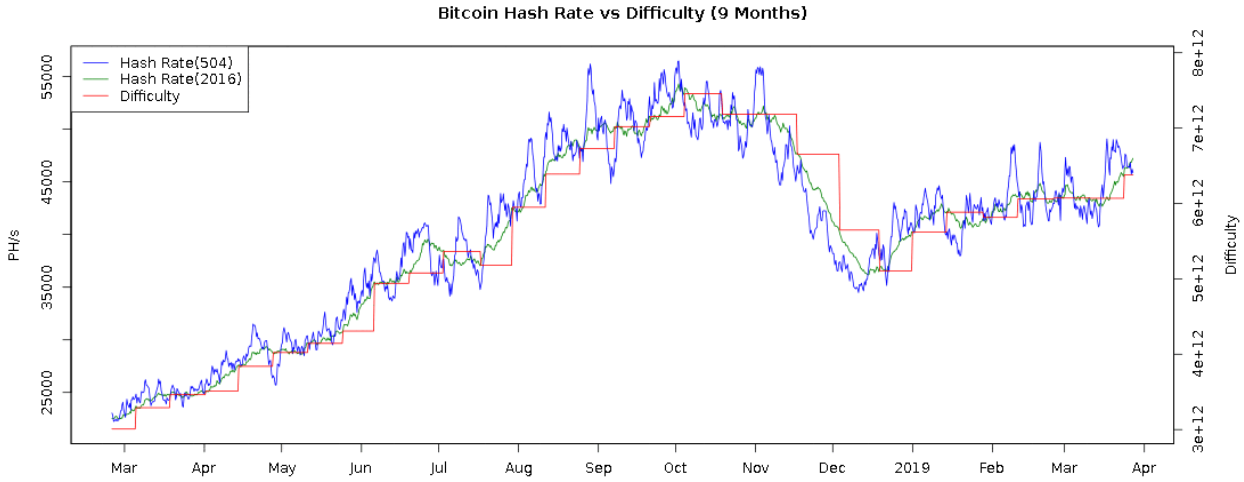
3.5.5 Mining difficulty en bloktijd

Hoe hoger de target hash is, hoe makkelijker het wordt om een hash te vinden die geldig is. Andersom geldt hetzelfde: hoe lager de target hash is, hoe moeilijker het is om een geldige hash te vinden. De rol van een target hash is aldus om de mining difficulty te bepalen. De mining difficulty is de moeilijkheidsgraad voor een mijner om een geldige hash te vinden. Bij een hogere mining difficulty, wordt de target hash verlaagd.

Het aantal hashes per seconde dat wordt berekend in het netwerk wordt ook wel de ***hash rate*** genoemd.[29] Hoe meer computerkracht er wordt gebruikt om geldige hashes te vinden, hoe groter de hash rate. Satoshi Nakamoto wil niet dat er te veel geldige hashes worden gevonden, omdat dat betekent dat er meer Bitcoin in omloop komt. Om deze reden is de mining difficulty variabel en past het zich om de 2.016 blokken (ongeveer 2 weken) aan, aan de totale hoeveelheid computerkracht die mijners beschikbaar stellen aan het netwerk. Als de mining difficulty niet variabel zou zijn en zich niet zou aanpassen aan de hash rate, zou het aanbod van Bitcoin lineair stijgen met de stijging in de hash rate. Er is namelijk een directe relatie tussen de hash rate en de snelheid waarmee er een geldige hash wordt gevonden.

De volgende afbeelding geeft goed weer wat de relatie is tussen de hash rate en de mining difficulty.

[29] De hash rate op 8 januari, 2019, staat op 42.887.764.036 GH/s, ofwel bijna 43 miljard GH/s. Eén GH/s staat voor 1 miljard hashes per seconde.



Afbeelding 23: De Bitcoin hash rate afgezet tegen de mining difficulty van maart 2018 t/m maart 2019 (Bitcoinwisdom.com, 2019).

<u>Hoe de mining difficulty wordt berekend</u>

De difficulty is gecodeerd binnen het blockchainprotocol, waardoor er geen derde partij nodig is om de difficulty te bepalen. Dit is vastgesteld middels de volgende formule:

$$\text{Difficulty} = \frac{current\ target}{max\ target}$$

De current target is het nummer waar een hash gelijk of kleiner aan moet zijn om als geldig te worden verklaard.

De max target is de difficulty-waarde van de eerste blok van de Bitcoin blockchain. In hexadecimale waarden is deze:

00000000FFFF0000000000000000000000000000000000000000000000000000

Met andere woorden, de difficulty vertelt ons hoeveel moeilijker het nu is om een hash te vinden die kleiner of gelijk is aan de current target, dan het vinden van een hash die kleiner of gelijk is aan de max target. De difficulty van blok #576.081 is 6.702.169.884.349,14.[30] Dit geeft aan dat het ongeveer 6,7 biljoen maal moeilijker is om een geldige hash te vinden bij blok #576.081 dan bij blok #1, het genesis blok.

[30] Je kunt de difficulty van blok #576081 hier vinden: https://www.blockchain.com/btc/block-height/576081.

Zoals eerder vermeld moet de difficulty zich om de 2.016 blokken aanpassen, zodat er gemiddeld om de 10 minuten een nieuwe geldige hash wordt gevonden. Dit brengt ons bij de ***bloktijd*** (block time).

De bloktijd

De bloktijd is de periode waarin er een geldige hash wordt gegenereerd en het blok kan worden toegevoegd aan de blockchain. Bij Bitcoin is de bloktijd 10 minuten. Echter, is deze tijd niet absoluut. Soms vindt een mijner in meer of minder tijd een geldige hash. Om ervoor te zorgen dat de bloktijd rond de 10 minuten blijft, past de mining difficulty zich aan. Bij een hogere hash rate, wordt de Bitcoin difficulty ook hoger, zodat er niet te veel wordt afgeweken van de 10 minuten bloktijd.

3.5.6 Bij concurrerende chains is de langste chain de ware blockchain

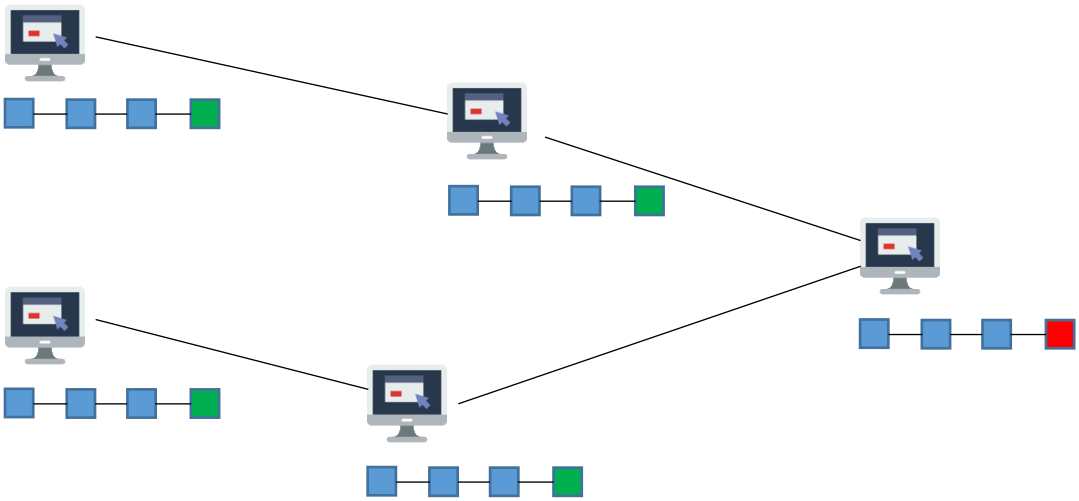
Het kan weleens gebeuren dat verschillende mijners rond dezelfde tijd een geldige hash hebben gevonden en deze rond dezelfde tijd een nieuw blok hebben toegevoegd aan hun blockchain. De ene node heeft dus te laat doorgekregen dat een andere node al een geldige hash heeft gevonden. Dit komt doordat er in een netwerk altijd wat vertraging is in informatieoverdracht tussen verschillende nodes.

Stel je voor dat mijner A een geldige hash heeft gevonden. In ons voorbeeld is de mijner ook een full node die het blok verifieert en toevoegt aan zijn blockchain. Mijner A communiceert naar andere mijners – mijners B, C en D die tevens ook full nodes zijn – in zijn directe omgeving dat hij een nieuwe geldig blok heeft aangemaakt. Mijners B, C en D verifiëren dat het nieuwe blok een geldige hash heeft, nemen deze over en voegen deze toe aan hun eigen blockchain. In de volgende afbeelding kun je zien waar full nodes nieuwe blokken op checken.

1. Check syntactic correctness
2. Reject if duplicate of block we have in any of the three categories
3. Transaction list must be non-empty
4. Block hash must satisfy claimed *nBits* proof of work
5. Block timestamp must not be more than two hours in the future
6. First transaction must be coinbase (i.e. only 1 input, with hash=0, n=-1), the rest must not be
7. For each transaction, apply "tx" checks 2-4
8. For the coinbase (first) transaction, scriptSig length must be 2-100
9. Reject if sum of transaction sig opcounts > MAX_BLOCK_SIGOPS
10. Verify Merkle hash
11. Check if prev block (matching *prev* hash) is in main branch or side branches. If not, add this to orphan blocks, then query peer we got this from for 1st missing orphan block in *prev* chain; done with block
12. Check that *nBits* value matches the difficulty rules
13. Reject if timestamp is the median time of the last 11 blocks or before
14. For certain old blocks (i.e. on initial block download) check that hash matches known values

Afbeelding 24: Regels van het Bitcoin-protocol waar full nodes zich aan moeten houden. Nieuwe transacties en blokken worden onder andere hierop gecheckt. Een volledigere lijst van protocolregels en checks kun je vinden op: https://en.bitcoin.it/wiki/protocol_rules.

Echter, heeft mijner E ook een geldige hash gevonden voordat hij informatie heeft ontvangen dat er al door mijner A een geldig blok is geverifieerd en toegevoegd. Dan produceert mijner E ook een geldig blok en voegt hij deze toe aan zijn blockchain. Binnen een netwerk waarin verschillende apparaten met elkaar communiceren vindt er altijd ***netwerklatentie*** plaats. Netwerklatentie is een vertraging in datacommunicatie over een netwerk. In het geval van blockchain, kunnen er hierdoor twee verschillende of concurrerende chains ontstaan en is het de vraag welke van de twee chains de juiste is. Dit is vergelijkbaar met twee groepen van concurrerende generaals in het Byzantine Generals Problem, waarbij de ene groep zegt dat ze moeten aanvallen en de andere groep zegt dat ze moeten terugtrekken. Een schematische weergave van de voorgaande situatie vind je in de volgende afbeelding.

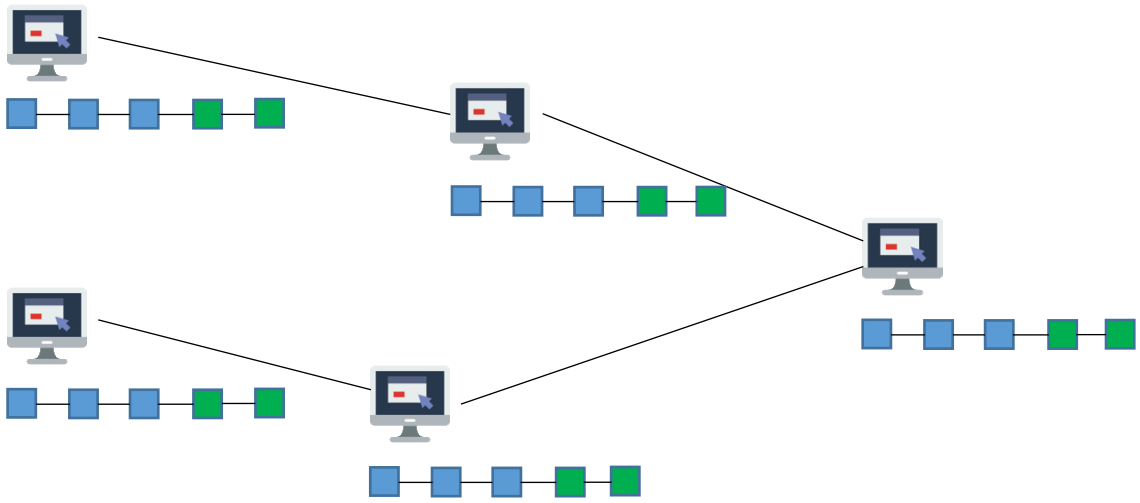


Afbeelding 25: Een netwerk van vijf mijners waarvan er vier een nieuw blok (groen) hebben toegevoegd aan hun blockchain. Hun blockchain wijkt af van de blockchain van de mijner die rond hetzelfde tijdstip een ander blok (rood) heeft toegevoegd aan zijn blockchain.

Mijner A, B, C en D hebben nu allemaal een nieuw blok (groen) toegevoegd aan hun blockchain. Mijner E heeft echter een ander nieuw blok (rood) toegevoegd aan zijn blockchain. In dit geval wordt er gekeken welke blockchain de langste is en wordt deze overgenomen door de andere deelnemers op het netwerk. Aangezien ze allemaal een gelijk aantal blokken hebben, is het nog afwachten welke blockchain de langste gaat worden.

Zoals eerder uitgelegd, is de kans waarop een mijner een geldige hash voor een nieuw blok kan vinden, gebaseerd op de hashing rate van de mijner. Stel je in ons voorbeeld voor dat de hashing rate van elk van de mijners gelijk staat aan 1 megahash per seconde (MH/s), ofwel 1 miljoen hashes per seconde. Dat betekent dat er in totaal een hash rate van 4 MH/s is voor mijners met het groene blok. Daarentegen is er in totaal maar 1 MH/s voor de mijner met het rode blok. De kans dat er het snelst een nieuwe geldige hash wordt gevonden door een mijner met een groen blok is dus viermaal groter. De blockchain met het groene blok zal om die reden na verloop van tijd langer zijn dan de blockchain met het rode blok. Het gevolg is dat de blockchain met het rode blok ongeldig wordt verklaard door het netwerk en de mijner met het rode blok de blockchain met het groene blok zal overnemen. Dit is hoe consensus op het blockchainnetwerk tot stand komt. Het blok dat niet wordt opgenomen in de ware blockchain, in dit geval het rode blok, wordt een ***orphaned blok*** (weesblok) genoemd. Orphaned blokken zijn legitieme blokken met geldige hashes en geldige transacties. Echter, zijn ze onderdeel van een blockchain die heeft verloren van een langere blockchain, waar meer computerkracht aan is besteed – ofwel een blockchain met meer Proof-of-Work. Het nadeel van orphaned blokken

is dat ze de veiligheid van blockchain omlaag brengen, omdat een gedeelte van de computerkracht die normaal gesproken wordt gespendeerd aan de ware blockchain wordt verdeeld. Als bijvoorbeeld 25% van de blokken orphaned blokken zijn, betekent het dat een aanvaller 25% minder computerkracht nodig heeft om de ware blockchain aan te vallen middels een 51%-aanval. Als er een mijner is met malafide bedoelingen, zou hij dus theoretisch gezien in staat zijn om het netwerk te overtuigen van zijn malafide blockchain, zolang hij sneller blokken aanmaakt dan de rest. Dit betekent echter wel dat hij een meerderheid in computerkracht – ofwel hash rate – moet hebben. Een dergelijke aanval heet een 51%-aanval. Uitgebreidere informatie over orphaned blokken en hoe 51%-aanvallen werken, komen later in hoofdstuk 6 aan bod.



Afbeelding 26: De blockchain van de mijner/full node met het orphaned blok, het rode blok, is ongeldig verklaard. Deze mijner/full node heeft de langste blockhain, wat de blockchain met groene blokken betreft, overgenomen.

3.6 Double-spendingprobleem

Omdat iedere full node nu weer een exacte kopie heeft van eenzelfde blockchain is er onder alle deelnemers op het netwerk een ‘gedeelde waarheid’. Zij hebben allemaal dezelfde informatie en weten precies wie hoeveel Bitcoin heeft. Daardoor is het haast onmogelijk voor een persoon om van zijn 1 BTC, 1 BTC te versturen naar Alice en 1 BTC te versturen naar Bob. Op deze manier wordt double-spending voorkomen door Proof-of-Work.

Het ***double-spendingprobleem*** heeft lang in de magen gezeten van ontwikkelaars van digitale munten. Door digitalisering kun je immers een digitale kopie van een bestand maken, bijvoorbeeld door een ‘copy/paste’ van een tekstbestand, of door eenzelfde tekstbestand naar meerdere mensen te e-mailen. Om te voorkomen dat digitale munten werden gekopieerd en

op die manier meerdere malen werden uitgegeven, was een vertrouwde derde partij nodig die bijhield wie hoeveel van de munten bezat. Deze partij kon malafide transacties tegenhouden en kwaadwillenden toegang tot het systeem ontzeggen. Er was echter nog wel het risico dat deze partij zelf corrumpeerbaar was en dat de database die werd beheerd door deze partij een honingpot was voor hackers. Met de komst van blockchain is er geen vertrouwen meer nodig in een tussenpartij die double-spending voorkomt.

3.7 Bitcoins monetair beleid

Bitcoin heeft net als traditionele valuta ook een monetair beleid. Het verschil met traditionele valuta is dat het monetaire beleid van Bitcoin niet wordt beheerd door centrale banken en overheden, maar door transparante software. Het beleid bij Bitcoin is onder te verdelen in twee principes:

1. Bitcoin-halvering.
2. Blokfrequentie.

3.7.1 Bitcoin-halvering

Bitcoin heeft een gecontroleerd aanbod. Na elke 210.000 geproduceerde blokken – dus ongeveer om de 4 jaar – wordt het aantal Bitcoin dat in omloop komt per gevonden geldige hash gehalveerd. In de eerste vier jaar kwamen er 10.500.000 Bitcoins in omloop. De volgende vier jaar was dat 5.250.000 Bitcoins. De vier jaar daarop 2.625.000 Bitcoins etc. ***Deze Bitcoin-halvering*** is voorgeprogrammeerd en leidt ertoe dat er tegen het jaar 2140 maximaal ongeveer 21 miljoen Bitcoins kunnen zijn. Na die tijd zullen mijners alleen nog maar inkomsten ontvangen uit de transactiekosten die zijn betaald in het blok dat zij hebben geproduceerd. Het achterliggende idee is dat bij grootschalige adoptie, de prijs van Bitcoin zoveel is gestegen, dat de mijnersactiviteiten voldoende inkomsten genereren uit de transactiekosten. Satoshi Nakamoto denkt zelfs dat er nodes zullen zijn die transacties gratis willen verwerken.[31]

3.7.2 Blokfrequentie

De ***blokfrequentie*** heeft ook invloed op Bitcoins monetaire beleid. De blokfrequentie is het aantal keer dat een geldige hash en daardoor ook een geldig blok wordt gegenereerd binnen een bepaalde tijd. Zoals eerder vermeld, is de frequentie ongeveer eenmaal per 10 minuten. Dit

[31] Zie de e-mail van Satoshi Nakamoto naar de Cryptography mailing list van 8 januari 2009: https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html

is wat we de bloktijd noemen. Het kan echter zijn dat een mijner een geldige hash vindt binnen meer of minder tijd.

3.7.3 Inflatie

Mijners ontvingen initieel 50 Bitcoins per gevonden blok. Dit is wat we de ***blokbeloning*** (block reward) noemen. Momenteel heeft er al tweemaal een Bitcoin-halvering plaatsgevonden, waardoor mijners nu 12,5 Bitcoins ontvangen. De derde halvering staat gepland voor mei 2020. Het vooraf geprogrammeerde aanbod aan Bitcoins staat in sterk contrast met hoe het aanbod van traditionele munteenheden als de USD en EUR wordt gereguleerd. Het aanbod van de USD en de EUR wordt bijvoorbeeld respectievelijk gereguleerd door de Amerikaanse ***Federal Reserve*** (Fed) en de ***Europese Centrale Bank*** (ECB). Dit zijn centrale instituten die als doel hebben om prijsstabiliteit te bewerkstelligen. De ECB wil de jaarlijkse geldhoeveelheid zoveel laten groeien dat de prijsinflatie iets onder de 2% is.[32] Deze geldgroei wordt ook wel geldinflatie genoemd. Omdat een groei van de geldhoeveelheid kan leiden tot prijsinflatie – het duurder worden van producten in termen van USD en EUR – is het voor de economie belangrijk dat de geldhoeveelheid niet te snel groeit. Dat zou namelijk kunnen leiden tot prijsinstabiliteit en zelfs hyperinflatie, waarbij het geld zelf te snel minder waard wordt en de producten in termen van USD en EUR dus te snel duurder worden.

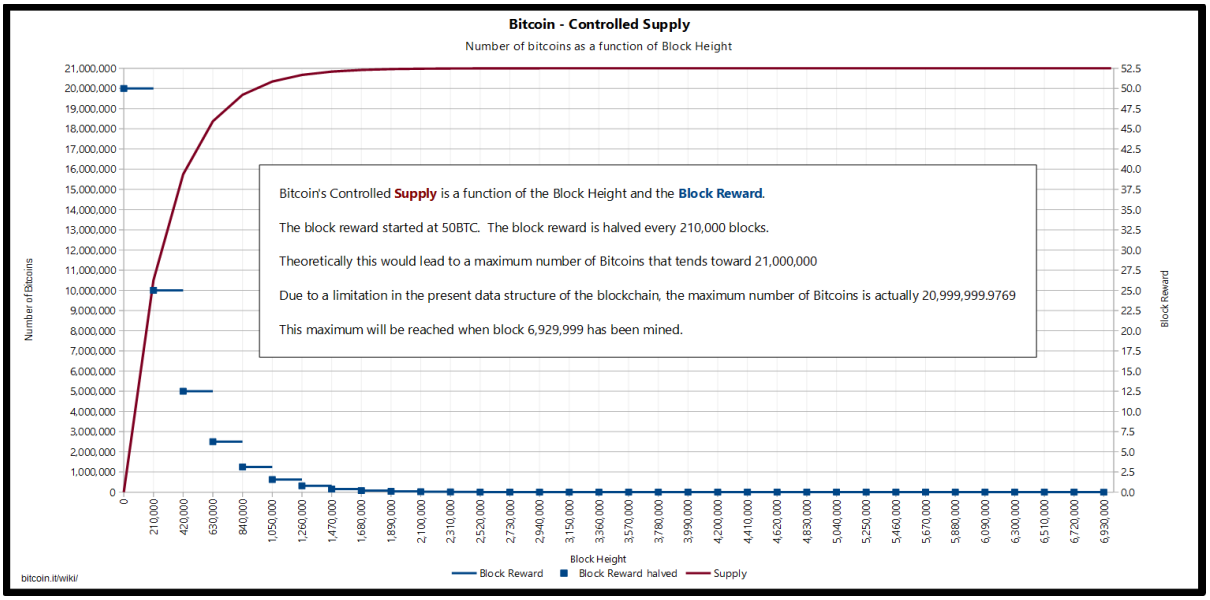
Onderstaand vind je twee figuren. Eén toont de gecontroleerde hoeveelheid Bitcoin die er in omloop wordt gebracht, terwijl de ander de geldgroei toont van de EUR. Wat opmerkelijk is aan de geldgroei van de EUR is dat deze elk moment kan worden veranderd door de ECB.[33] Eén van de grote hekelpunten aan het huidige financiële systeem volgens Satoshi Nakamoto (2009) is dat mensen in het traditionele model erop moeten vertrouwen dat centrale banken een goed monetair beleid naleven, terwijl de geschiedenis uitwijst dat dat vertrouwen regelmatig wordt geschaad. Satoshi Nakamoto zegt er het volgende over:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."

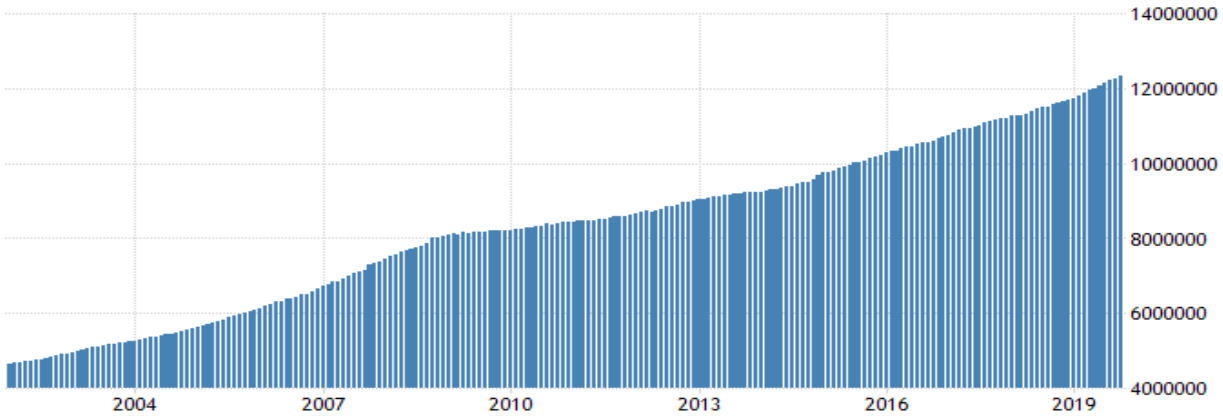
[32] De theorie dat er een beetje inflatie moet zijn om de economie stabiel te houden is gebaseerd op de assumptie dat mensen bij prijsdeflatie, het tegenovergestelde van prijsinflatie, liever geld oppotten en hun consumptie uitstellen. Met hetzelfde geld dat ze hebben, kunnen ze namelijk meer goederen en diensten kopen.

[33] Het huidige financieel systeem wordt uitgebreider besproken in hoofdstuk 13.

Omdat de geldhoeveelheid van traditionele valuta jaarlijks groeit, worden deze valuta's ook wel inflatoire valuta's genoemd. Bitcoin daarentegen is deflatoir, omdat het aantal nieuwe Bitcoins dat wordt uitgegeven met de tijd daalt. In deel II van het boek gaan we meer in op het geldsysteem en bespreken we uitvoeriger wat de nadelen zijn van het huidige systeem waarin centrale banken en overheden de monopolie op geldproductie hebben.



Afbeelding 27: Het gecontroleerde aanbod van Bitcoin is een functie van hoeveel blokken er zijn aangemaakt en de blokbeloning. De blokbeloning was initieel 50 Bitcoins, maar is sindsdien om de 210.000 blokken gehalveerd. Het aanbod van Bitcoin is daardoor asymptotisch het maximale aanbod dat 21.000.000 Bitcoins benadert, maar nooit exact zal bereiken. We zeggen ook wel dat Bitcoin deflatoir is, omdat de geldgroei steeds minder wordt. (BitcoinWiki, 2019)



Afbeelding 28: De geldhoeveelheid (M2) in het Eurogebied is sinds 1 januari 2002 t/m 1 maart 2019 bijna verdrievoudigd (TradingEconomics.com, 2019). Duidelijk is dat deze groei niet vermindert met de tijd, zoals het geval is bij Bitcoin. De EUR is om deze reden inflatoir. Belangrijk is ook om te weten dat er meerdere manieren zijn om de geldhoeveelheid te meten: de zogenaamde M1, M2 en M3.[34]

[34] Je kunt hier meer informatie vinden over de classificatie van geld in M1, M2 en M3 door de Europese Centrale Bank: https://www.ecb.europa.eu/stats/money_credit_banking/monetary_aggregates/html/index.en.html.

3.8 Wat is het verschil tussen Bitcoin en huidige betaalsystemen?

In het vorige hoofdstuk hebben we besproken hoe huidige betaalsystemen als iDEAL en creditcards werken. Het belangrijkste verschil tussen Bitcoin en deze betaalsystemen is dat er bij Bitcoin geen vertrouwen nodig is in een derde partij. Het Bitcoin-netwerk is een zelfregulerend systeem dat peer-to-peertransacties mogelijk maakt en het geld dat daarop draait, de Bitcoin, is geld dat niet kan worden gemanipuleerd of ingenomen door centrale banken en overheden. Hopelijk is het ook duidelijker geworden hoe Bitcoins Proof-of-Work-consensus minder fraudegevoelig is en er geen anti-fraudetechnieken als 3D-secure nodig zijn.

Aan de andere kant zijn Bitcoin-transacties wel onomkeerbaar en is het belangrijk dat je niet je ***privésleutel*** (private key) kwijtraakt of aan derden laat zien. De private key kun je zien als een wachtwoord waarmee je je Bitcoin wallet kunt openen en je Bitcoin kunt spenderen. Private keys komen uitgebreider aan bod in het volgende hoofdstuk over ***public key cryptografie***. Daarnaast staat Proof-of-Work in sterk contrast met het conventionele model, waarin er een vertrouwde centrale autoriteit – bijvoorbeeld een bank – nodig is om elke transactie te controleren op double-spending. Bij het Bitcoin-netwerk hebben full nodes op het netwerk een kopie van de blockchain en controleren zij elke transactie op fraude als double-spending.

3.9 Economische stimulansen om deel te nemen aan het Bitcoin-netwerk

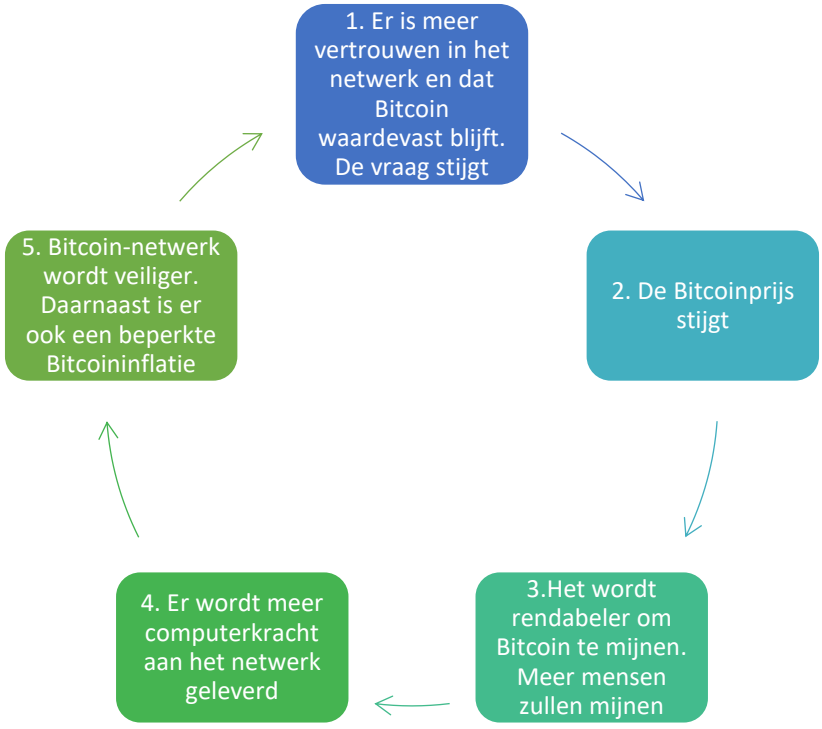
Nu de verschillende elementen van het Bitcoin-netwerk zijn toegelicht, is het makkelijker om te begrijpen hoe het komt dat Bitcoin vrij succesvol is geworden. Het geniaalste concept achter Bitcoin is wellicht het volgende: het stimuleert mensen om te participeren door middel van een positieve feedback loop van economische stimulansen.[35]

Deze feedback loop zorgt ervoor dat het Bitcoin-netwerk een organisch systeem is geworden, dat zichzelf in stand houdt zonder dat er een partij is die mensen hoeft te dwingen deel te nemen. Deze feedback loop is als volgt:

1. Er is een groter vertrouwen in het Bitcoin-netwerk, waardoor de vraag naar Bitcoin stijgt.

[35] In een post op het P2PFoundation forum van 18 februari, 2009, stelt Satoshi Nakamoto dat Bitcoin ook wel op edelmetalen, zoals bijvoorbeeld goud en zilver, lijkt. In plaats van dat er een centraal instituut is die het aanbod verandert om de waarde enigszins gelijk te houden, is het aanbod al vooraf bepaald in de Bitcoin-software en verandert de waarde van Bitcoin. Het gelimiteerde aanbod biedt potentie voor een positieve feedback loop waarbij het grotere gebruik van Bitcoin leidt tot een hogere waarde en deze hogere waarde weer meer gebruikers aantrekt om te profiteren van een stijgende prijs.

2. Hierdoor stijgt de Bitcoin-prijs.
3. Door de hogere prijs van de Bitcoin wordt het rendabeler om Bitcoin te mijnen. Hierdoor zullen meer mensen proberen om Bitcoin te mijnen.
4. Doordat er meer wordt gemijnd, gaat de totale computerkracht die wordt geleverd aan het netwerk omhoog.
5. Dit leidt ertoe dat het Bitcoin-netwerk veiliger wordt. Een 51%-aanval uitvoeren op het netwerk wordt namelijk moelijker. In hoofdstuk 7 wordt een 51%-aanval nader besproken. Daarnaast wordt de moeilijkheidsgraad om te mijnen ook verhoogd wanneer er meer totale computerkracht wordt gebruikt om te mijnen. Door de hogere moeilijkheidsgraad zal er nog steeds gemiddeld om de 10 minuten een blok worden aangemaakt waarbij er momenteel 12,5 Bitcoin extra in omloop komt. Ook blijft de inflatie van Bitcoin beperkt, omdat er om de vier jaar een Bitcoin-halvering plaatsvindt – er kan dus in totaal niet meer dan ongeveer 21 miljoen Bitcoin zijn. Betere beveiliging en beperkte inflatie leiden ertoe dat er meer vertrouwen komt in het Bitcoin-netwerk.



Afbeelding 29: Bitcoin bevindt zich in een positieve feedback loop van economische stimulansen (Ammous, 2018).

De studie van blockchainprotocollen en hoe deze zo efficiënt mogelijk ingericht dienen te worden, is het onderzoeksonderwerp van het vakgebied ***cryptoeconomics***. Cryptoeconomics komt in hoofdstuk 10 aan bod.

Intermezzo: Hoe je de Bitcoin blockchain leest met een block explorer

Een ***block explorer*** stelt je in staat om informatie in de blockchain op te zoeken. Zo kun je opzoeken of je transacties zijn aangekomen, hoeveel Bitcoin een wallet heeft, wie de mijner is van een blok, enzovoorts. In dit intermezzo behandelen we hoe je de data binnen de Bitcoin blockchain kunt lezen met de explorer van www.blockchain.com/explorer.

De startpagina met een overzicht van de belangrijkste Bitcoin-gegevens

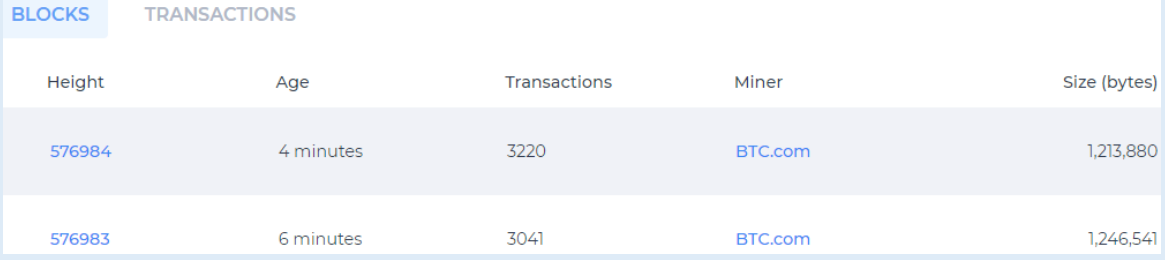
Op de startpagina zien we direct een overzicht van de volgende Bitcoin-gegevens:

1. *Prijs*: de huidige prijs van de Bitcoin.
2. *Hashrate*: de schatting van hoeveel tera hashes per seconde (th/s) het Bitcoin-netwerk uitvoert. Eén tera hash staat gelijk aan 1 biljoen hashes.
3. *Difficulty*: de moeilijkheid om een nieuwe geldige blok te produceren. Het getal geeft weer hoeveel moeilijker het nu is om een geldige blok te vinden ten opzichte van het vinden van het eerste Bitcoin-blok.
4. *Tx per day*: het aantal dagelijkse transacties die zijn bevestigd door het netwerk.
5. *Average value*: het gemiddelde transactiebedrag dat op het netwerk plaatsvindt.
6. *Average fee*: de gemiddelde kosten voor een transactie.
7. *Unconfirmed*: de hoeveelheid transacties die in de wachtrij staan om te worden bevestigd door het netwerk.
8. *Mempool*: De totale grootte in bytes van alle transacties in de wachtrij.

Afbeelding 30: De startpagina van blockchain.com/explorer. Geraadpleegd op 20 mei 2019.

Lijst van blokken

Verder onderaan zie je een lijst van blokken die zijn toegevoegd aan de blockchain.



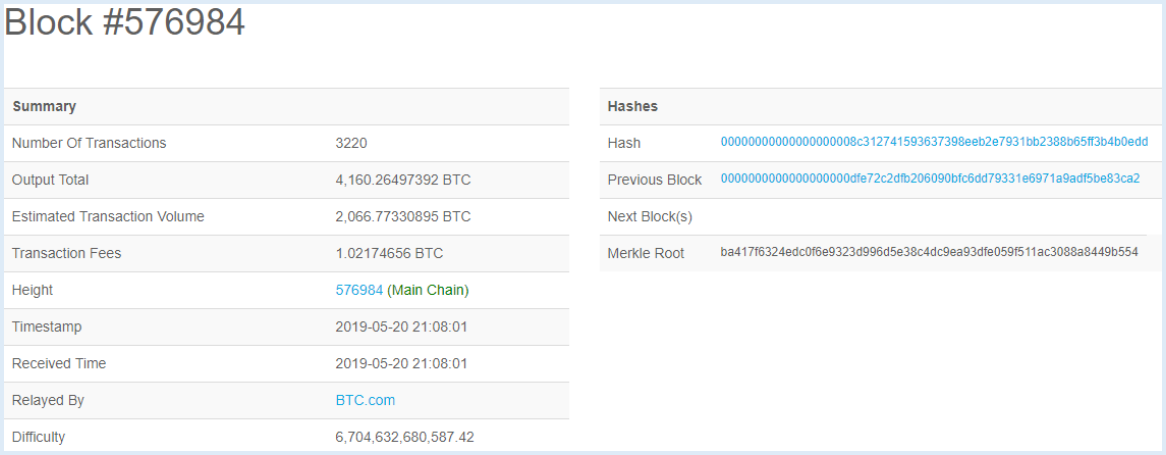
Afbeelding 31: Lijst van recente blokken die zijn toegevoegd aan de blockchain.

In de lijst is het volgende aangegeven:

1. *Height*: het bloknummer. In het vorige voorbeeld zie je dat de Bitcoin blockchain op dat moment bestaat uit 576.984 blokken.
2. *Age*: hoeveel minuten geleden het blok is aangemaakt.
3. *Transactions*: het aantal transacties die in het blok zijn opgenomen.
4. *Mijner*: de partij die het blok heeft geproduceerd.
5. *Size* (bytes): de grootte van het blok in bytes.

Data in een blok

Als we één van het blokken openen, door te klikken op diens height, zien we een samenvatting van de data in het blok en zien we welke hashes er in de block header zitten.



Block #576984

Summary	
Number Of Transactions	3220
Output Total	4,160.26497392 BTC
Estimated Transaction Volume	2,066.77330895 BTC
Transaction Fees	1.02174656 BTC
Height	576984 (Main Chain)
Timestamp	2019-05-20 21:08:01
Received Time	2019-05-20 21:08:01
Relayed By	BTC.com
Difficulty	6,704,632,680,587.42

Hashes	
Hash	00000000000000000008c312741593637398eeb2e7931bb2388b65ff3b4b0edd
Previous Block	00000000000000000000dfe72c2dfb206090bfc6dd79331e6971a9adf5be83ca2
Next Block(s)	
Merkle Root	ba417f6324edc0f6e9323d996d5e38c4dc9ea93dfe059f511ac3088a8449b554

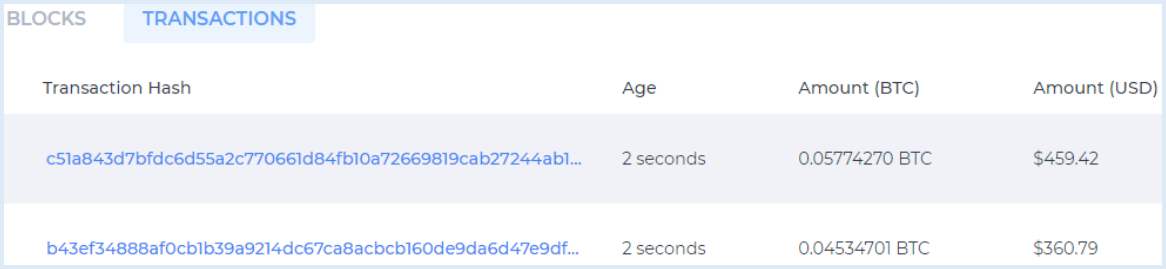
Afbeelding 32: Data van block #76.984.

De belangrijkste data die je al bekend zullen voorkomen, zijn:

1. *Timestamp*: de tijd waarop het blok is aangemaakt.
2. *Difficulty*: de moeilijkheid waaronder het blok is geproduceerd.
3. *Version*: versie van de blockchain.
4. *Nonce*: het getal waarmee de mijner een geldige blok hash heeft kunnen vinden.
5. *Previous block*: de hash van het vorige blok.
6. *Merkle root*: de root hash van de Merkle tree van alle transacties.
7. *Hash*: de hash van de block header. Deze is verkregen door de zes bovenstaande parameters te hashen.

Lijst van transacties

Naast de lijst van blokken is er ook een lijst van transacties die je kunt inzien.



Afbeelding 33: Lijst van transacties.

In de lijst is het volgende aangegeven:

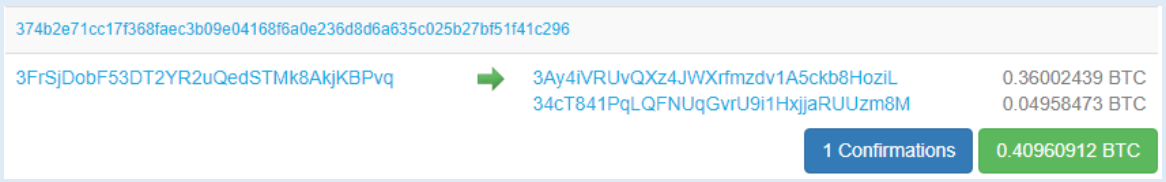
1. *Transaction hash*: de hash van de desbetreffende transactie.
2. *Age*: hoeveel seconden of minuten geleden de transactie is uitgevoerd.
3. *Amount* (BTC): het bedrag van de transactie in Bitcoin.
4. *Amount* (USD): de waarde van het bedrag in USD.

Data in een transactie

Je kunt elk van deze transacties bekijken door op de transaction hash te klikken.

Afbeelding 34: Een Bitcoin-transactie die nog niet is toegevoegd aan de blockhain.

Wat opvalt aan deze transactie is dat er staat “Unconfirmed Transaction!” Dat betekent dat er nog geen blok is toevoegd aan de blockchain waar de transactie in zit. In onderstaande afbeelding zien we een weergave van dezelfde transactie die inmiddels is bevestigd en toegevoegd aan de blockchain: “1 Confirmations”. Hoe meer bevestigingen er zijn, hoe meer blokken er zijn geplaatst bovenop het blok met deze transactie. Bij meer bevestigingen kun je zekerder zijn dat de transactie niet meer kan worden gewijzigd of verwijderd.



Afbeelding 35: Een Bitcoin-transactie die inmiddels is bevestigd en toegevoegd aan de blockchain.

We zien dat er bij de voorgaande transactie eigenlijk twee transacties hebben plaatsgevonden: één van 0,36002439 BTC en één van 0,04958473 BTC. Hier gaan we wat dieper op in.

Transaction inputs en outputs

Summary	
Size	404 (bytes)
Weight	854
Received Time	2019-05-20 21:38:03
Lock Time	Block: 576988
Included In Blocks	576989 (2019-05-20 21:54:54 + 17 minutes)
Confirmations	13

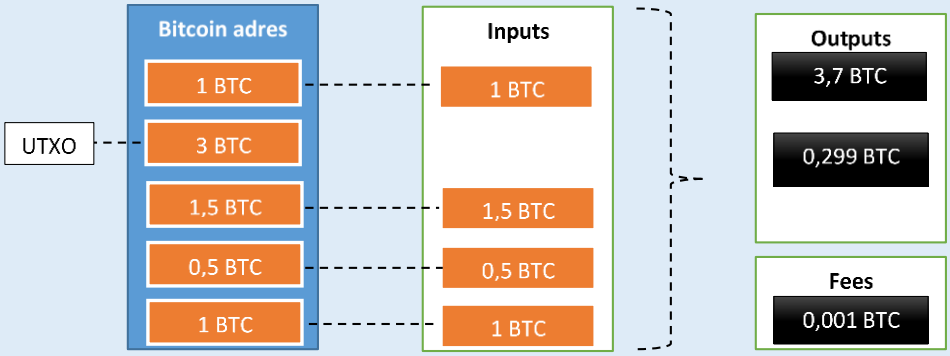
Inputs and Outputs	
Total Input	0.40982412 BTC
Total Output	0.40960912 BTC
Fees	0.000215 BTC
Fee per byte	53.218 sat/B
Fee per weight unit	25.176 sat/WU
Estimated BTC Transacted	0.04958473 BTC

Afbeelding 36: Een samenvatting van onze voorbeeldtransactie met inputs en outputs. De fees zijn het verschil tussen de totale input en totale output. Deze fees gaan naar de mijner van het blok. De received time en included in blocks geven respectievelijk aan wanneer de transactie is ontvangen door het netwerk en in welk blok deze is toegevoegd.

Stel dat je net als in het voorgaande voorbeeld 0,40982412 BTC – dat is de totale input – hebt en je wil een transactie uitvoeren van 0,36002439 BTC naar adres X. Bij een Bitcoin-transactie wordt de 0,36002439 BTC niet van de 0,40982412 BTC afgetrokken om dan te versturen naar X. Wat er gebeurt, is dat het hele bedrag dat op jouw adres staat, 0,40982412 BTC, wordt gesplitst in twee verschillende outputs. Eén output is de 0,36002439 BTC naar adres X en de andere is de rest som van 0,04958473 BTC naar jouw ***change-adres***. Het change-adres heb jij zelf in beheer en wordt gebruikt om het wisselgeld (totale input – bedrag dat je wil overmaken naar X – transactiekosten) naartoe te sturen. In moderne wallets worden change-adressen automatisch voor je aangemaakt, dus hier heb je geen omkijken naar. Vanuit een technisch perspectief is deze manier van transacties uitvoeren veiliger.

Als we beide outputs optellen, dan komen we op een som van 0,36002439 + 0,04958473 = 0,40960912 BTC. Dat is minder dan de totale input van 0,40982412 BTC. Het verschil tussen de totale input en totale output zijn de transactiekosten. Deze kosten staan in de block explorer als “fees”. In dit geval zijn de kosten 0,000215 BTC.

Unspent transaction outputs (UTXOs)



Afbeelding 37: Een overzicht van inputs, outputs en transactiekosten.

Je kunt de balans van je Bitcoin-adres zien als een batch van verschillende Bitcoin-transacties die je hebt ontvangen. In het voorgaande voorbeeld bevat het Bitcoin-adres in totaal 7 BTC. Er wordt een bedrag overgemaakt van 3,7 BTC naar een ander adres. Om dit bedrag over te maken, worden verschillende Bitcoin-transacties die je hebt ontvangen bij elkaar gevoegd om als input te dienen voor de transactie naar het andere adres. Je kunt geen ontvangen Bitcoin-transactie splitsen. Daarom worden inputs bij elkaar gevoegd, totdat de totale som daarvan groter is dan het bedrag dat je wil overmaken. In het voorbeeld nemen we inputs van 1 BTC, 1,5 BTC, 0,5 BTC en 1 BTC. Daarvan gaat 3,7 BTC naar het andere adres, een deel gaat naar de mijner van het blok in de vorm van fees en het andere deel krijg je teruggestort als soort van wisselgeld naar je change-adres. De 3 BTC die in je Bitcoin-adres zit en niet wordt gebruikt als input wordt de ***unspent transaction output*** (UTXO) genoemd. Het is namelijk een output die je hebt ontvangen en kan spenderen.

Bij een Bitcoin-transactie is het dus mogelijk om verscheidene input- en outputadressen te hebben. Zoals eerder vermeld, automatiseren vele Bitcoin wallets dit proces. Zij tonen de gebruiker één bedrag dat de som van alle UTXO's representeert. Hoewel de Bitcoin blockchain transparant is, bieden change adressen toch een hogere mate van privacy.

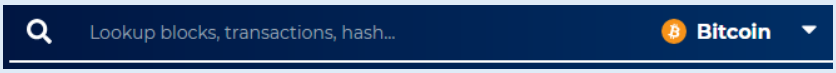
Adresgegevens

Summary	
Address	3FrSjDobF53DT2YR2uQedSTMk8AkjKBPvq
Hash 160	9b5a35eb8168c6bd354ca138d63649a3bc2d6a7e
Transactions	
No. Transactions	2
Total Received	0.40982412 BTC
Final Balance	0 BTC

Afbeelding 38: Een samenvatting van de adresgegevens.

Je kunt ook van de transactie het bijbehorende Bitcoin-adres openen. Hier vind je het aantal verzonden en ontvangen transacties van het adres en wat de balans is.

Zoekfunctie naar blokken, transacties en hashes



Afbeelding 39: De zoekfunctie van de block explorer.

Tot slot kun je ook de zoekfunctie gebruiken om dergelijke dingen als blokken, transacties en hashes op te zoeken in de block explorer.

3.10 Samenvatting, begrippen en bronnen

Samenvatting

Bitcoin is de digitale valuta en de Bitcoin blockchain is de onderliggende infrastructuur, bestaande uit de nodes die alle Bitcoin-transacties helpen bijhouden. In principe heeft Bitcoin de volgende drie belangrijke eigenschappen:

1. Het heeft schaarste geïntroduceerd in het digitale domein.
2. Het is een peer-to-peernetwerk zonder dat er vertrouwen nodig is in een derde centrale partij.
3. Het is een ordelijke manier om alle transacties te registreren en te verifiëren, zodat double-spending kan worden voorkomen.

Bitcoin is ook een oplossing voor het Byzantine Generals Problem. Dit probleem kun je vergelijken met dat van een gedecentraliseerd of gedistribueerd computernetwerk, waarbij alle deelnemers (nodes) van het netwerk elkaar niet kunnen vertrouwen, maar toch gezamenlijk tot besluiten moeten komen. De overeenkomst tussen deze nodes is wat je consensus noemt. Een systeem dat resistent is tegen het Byzantine Generals Problem noemen we Byzantine Fault Tolerant. Het consensusmechanisme dat Bitcoin het Byzantine Fault Tolerance eigenschap geeft, heet Proof-of-Work.

Proof-of-Work heeft de volgende eigenschappen:

1. Het maakt gebruik van hash cryptografie.
2. Mijners zoeken een nonce die leidt tot een geldige hash van een blok waar Bitcoin-transacties in zijn opgeslagen.
3. Wanneer een geldige hash is gevonden, wordt het blok geverifieerd op juistheid door verschillende full nodes op het netwerk. De snelheid, ofwel bloktijd, waarmee een geldige hash wordt gevonden, is gebaseerd op de mining difficulty.
4. Dit nieuwe blok wordt door andere nodes op het netwerk overgenomen en toegevoegd aan hun versie van de blockchain.
5. Mocht er binnen ongeveer dezelfde tijd twee geldige hashes zijn gevonden onder twee verschillende mijners, dan zijn er twee concurrerende chains. In dergelijke gevallen wordt er consensus bereikt door de langste blockchain over te nemen.
6. Al met al zorgt het bovenstaande ervoor dat iedereen op het netwerk ervan uitgaat dat er één blockchain is met de juiste data. Met andere woorden, je maakt gebruik van eenzelfde grootboek, dat alle transacties heeft geregistreerd, waardoor fraude als double-spending niet mogelijk is.

Het belangrijkste verschil tussen Bitcoin en reguliere betaalsystemen is dat er bij Bitcoin geen vertrouwen nodig is in een derde partij. Het Bitcoin-netwerk is een zelfregulerend systeem dat peer-to-peertransacties mogelijk maakt en het geld dat daarop draait, de Bitcoin, is geld dat niet kan worden gemanipuleerd of ingenomen door centrale banken en overheden.

Het geniaalste concept achter Bitcoin is wellicht het volgende: het stimuleert mensen om te participeren door middel van een positieve feedback loop van economische stimulansen.

Opmerkingen die je nu kunt uitleggen

- De Bitcoin blockchain is de technologie achter de Bitcoin cryptovaluta.
- Het double-spendingprobleem is met behulp van de blockchain opgelost door Satoshi Nakamoto.
- Proof-of-Work is een consensusmechanisme dat een oplossing biedt voor het Byzantine Generals Problem.
- Hash cryptografie wordt toegepast binnen de Bitcoin blockchain om een geldige hash van een nieuwe blok te vinden.
- Met de nonce kun je een geldige hash vinden.
- Hoe meer computerkracht er wordt geleverd aan het netwerk, hoe veiliger het netwerk wordt en hoe moeilijker het wordt om een geldige blok te mijnen.
- De target hash daalt wanneer er meer computerkracht wordt geleverd aan het netwerk.
- Wat Bitcoin anders maakt dan nationale valuta is dat het deflatoir is.
- Het Bitcoin-netwerk moedigt mensen aan om deel te nemen aan het beveiligen van het netwerk.

Verklarende begrippenlijst

Bitcoin-halvering: De halvering van het aantal nieuwe Bitcoins dat vrijkomt als beloning nadat er een geldige blok is aangemaakt door een mijner.

Block explorer: Een applicatie die je in staat stelt om informatie in de blockchain op te zoeken.

Blokbeloning: De beloning die een mijner ontvangt voor het produceren van een geldige blok.

Blokfrequentie: Het aantal keer dat een geldige blok wordt gegenereerd binnen een bepaalde tijd.

Bloktijd (block time): De gemiddelde tijd waarin er een geldige blok wordt geproduceerd.

Byzantine Fault Tolerance: De eigenschap om het Byzantine Generals Problem te weerstaan.

Byzantine Generals Problem: Het probleem om overeenstemming te vinden binnen een gedecentraliseerd netwerk, waarbij kwaadwillenden de overeenstemming niet kunnen kapen.

Change-adres: Het adres waarnaar het wisselgeld in Bitcoin wordt gestuurd bij een transactie.

Cryptoeconomics: De studie van blockchainprotocollen en hoe deze zo efficiënt mogelijk ingericht dienen te worden. Zie ook de definitie van cryptoeconomics in hoofdstuk 10.

Double-spending: Het dubbel kunnen uitgeven van je Bitcoin. Als je bijvoorbeeld maar 1 BTC hebt, dat je het ene BTC uitgeeft aan persoon A en aan persoon B.

Double-spendingprobleem: Het fundamentele probleem dat je je Bitcoin dubbel kan uitgeven en dat Satoshi Nakamoto heeft weten op te lossen met de blockchain.

ECB: Europese Centrale Bank.

Federal Reserve (Fed): Amerikaanse centrale bank.

Genesis blok: Het eerste blok van een blockchain.

Golden nonce: De nonce die leidt tot een geldige hash.

Hash cryptografie: Cryptografische methode waarbij gegevens worden omgezet in een hash.

Hash rate: Het aantal hashes per seconde dat in een netwerk wordt berekend.

Hash: Een cryptografische representatie van data.

Hashing power: De computerkracht om hashes te kunnen berekenen.

Hash-output: De hash die je krijgt nadat je data in een hash-functie stopt.

Merkle tree (Merkle-boom): De hash van alle hashes van alle transacties die deel uitmaken van een blok. Een Merkle tree wordt bijvoorbeeld gebruikt om gegevens veilig tussen twee computers te sturen en na te gaan of de aangekomen gegevens onbeschadigd zijn. SPV-nodes gebruiken de Merkle tree om snel te verifiëren of een transactie is opgenomen in een blok.

Mining difficulty: De moeilijkheid om te mijnen. De difficulty is afhankelijk van de totale computerkracht die op het netwerk aanwezig is.

Netwerklatentie: Vertraging in de communicatie tussen nodes binnen een netwerk.

Nonce range: Het bereik van de nonce. Deze is van 0 tot 4.294.967.295.

Nonce: Het getal dat door een mijner kan worden toegevoegd aan de data van een blok om daarmee een geldige hash te genereren.

Orphaned blok (weesblok): Een blok dat wordt gemijnd, maar niet wordt toegevoegd aan de ware blokchain. Het is mogelijk dat een mijner op geldige wijze een blok produceert, maar deze toch niet wordt geaccepteerd door andere nodes.

Private key (privésleutel): De sleutel waarmee je je transacties ondertekent en dus Bitcoins kunt versturen. Dit is vergelijkbaar met de pincode van je rekeningnummer en moet zo goed mogelijk bewaard worden.

Public key cryptografie: Cryptografische technologie die gebruik maakt van private-public sleutelparen.

Target hash: Het nummer waar een hash gelijk of kleiner aan moet zijn om als geldig te worden verklaard.

Unspent transaction output (UTXO): De Bitcoin die in je Bitcoin-adres zit, maar niet wordt gebruikt als input voor een transactie. Het is een output die je eerder hebt ontvangen en kan uitgeven.

Bronnen

Ammous, S. (2018, 3 juni). Bitcoin & Economics: What would a Bitcoin standard look like? [YouTube]. Geraadpleegd van https://youtu.be/1WBrdLQhUrg

Andreessen, M. (2014, 22 januari). Why Bitcoin Matters. Geraadpleegd op 25 december 2019, van DealBook website: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Bitcoin Wiki. (z.d.). Geraadpleegd op 25 december 2019, van Bitcoin.it website: https://en.bitcoin.it/wiki/

BitcoinWisdom.com. (2019). Bitcoin Difficulty and Hashrate Chart. Geraadpleegd op 25 december 2019, van Bitcoinwisdom.com website: https://bitcoinwisdom.com/bitcoin/difficulty

Blockchain.com. (z.d.). Blockchain Explorer. Benaderd op 25 december 2019, van Blockchain.com website: http://www.blockchain.com/explorer

European Central Bank. (2019). Monetary aggregates. Geraadpleegd op 25 december 2019, van European Central Bank website: https://www.ecb.europa.eu/stats/money_credit_banking/monetary_aggregates/html/index.en.html

Lamport, L., Shostak, R., & Pease, M. (1983). The Weak Byzantine Generals Problem. *Journal of the ACM*, *30*(3), 668–676. https://doi.org/10.1145/2402.322398

Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency. Geraadpleegd op 25 december 2019, van P2Pfoundation.ning.com website: https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

Rapidtables.com. (z.d.). Hexadecimal to Decimal converter. Geraadpleegd op 25 december 2019, van Rapidtables.com website: https://www.rapidtables.com/convert/number/hex-to-decimal.html

Trading Economics. (z.d.). Money Supply M2. Geraadpleegd op 25 december 2019, van Tradingeconomics.com website: https://tradingeconomics.com/euro-area/money-supply-m2

Xorbin.com. (z.d.). SHA-256 hash calculator. Benaderd op 25 december 2019, van Xorbin.com website: https://www.xorbin.com/tools/sha256-hash-calculator

Iconen

Generaal gemaakt door Nikita Golubev van www.flaticon.com

Computer gemaakt door Prettycons van www.flaticon.com

4. Mijning, nodes, BIPS en forks

"I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world."

- Peter Thiel (z.d.)

"If you don't believe it or don't get it, I don't have the time to try to convince you, sorry."

- Satoshi Nakamoto (2010)

4.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Hoe een transactieproces in elkaar steekt.
- Hoe mijners transacties selecteren om ze toe te voegen aan een blok.
- Wat de invloed is van de verschillende typen data in een blok op het vinden van een geldige hash.
- Wat de verschillende typen nodes zijn.
- Hoe er een verbetervoorstel kan worden ingediend voor de Bitcoin blockchain.
- Op welke manieren er een update kan plaatsvinden in de blockchain.

Inleiding

In het vorige hoofdstuk hebben we gezegd dat een mijner binnen het mijningproces nieuwe transacties verzamelen in een blok. De mijner zoekt vervolgens naar een nonce die, wanneer hij het samen hasht met de rest van de data in het blok, een geldige hash-waarde oplevert. Wanneer een mijner als eerste deze golden nonce weet te vinden, mag hij het blok in de blockchain opnemen en wordt hij beloond met de fees van de transacties in het blok en met een blokbeloning van momenteel 12,5 BTC.

In dit hoofdstuk gaan we dieper in op de rol van de mijner en het mijningproces. We bespreken in paragraaf 4.2 eerst wat een mempool is. Vervolgens wordt in paragraaf 4.3 uitgelegd hoe mijners transacties kiezen uit de mempool om die aan een blok toe te voegen. Er wordt hier

ook behandeld wat de impact is van de nonce range en de timestamp op het vinden van een golden nonce. In paragraaf 4.4, bespreken we welke typen nodes er zijn. Hier komen de verschillende varianten van full nodes en lightweight nodes aan bod. Dit wordt vervolgd door een paragraaf over hoe je een verbetervoorstel kunt indienen voor de Bitcoin blockchain. In paragraaf 4.6, behandelen we de verschillende typen forks. Vervolgens sluiten we het hoofdstuk af met een samenvatting, een lijst van verklarende woorden en een bronnenlijst in paragraaf 4.7.

4.2 Memory pool (mempool)

Voor de uitvoering van een transactie op het Bitcoin-netwerk, worden de volgende stappen ondernomen:

1. Je ondertekent met je wallet een transactie digitaal door een combinatie van je public en private key.
2. Er zijn één of meerdere unspent transaction outputs (UTXO's) gekozen om de transactie uit te voeren.[36]
3. Je zendt je transacties uit naar alle nodes op het netwerk.
4. Elke node verzamelt nieuwe transacties in een blok.
5. Elke node probeert een geldige blok hash te vinden voor zijn blok.
6. Wanneer een node deze vindt, wordt het blok uitgezonden naar alle nodes.
7. De nodes accepteren het blok alleen als alle transacties valide zijn.
8. De nodes uiten hun acceptatie van het blok door te werken aan een nieuw blok in de keten. Voor het nieuwe blok gebruiken zij de hash van het geaccepteerde blok als de previous hash.[37]

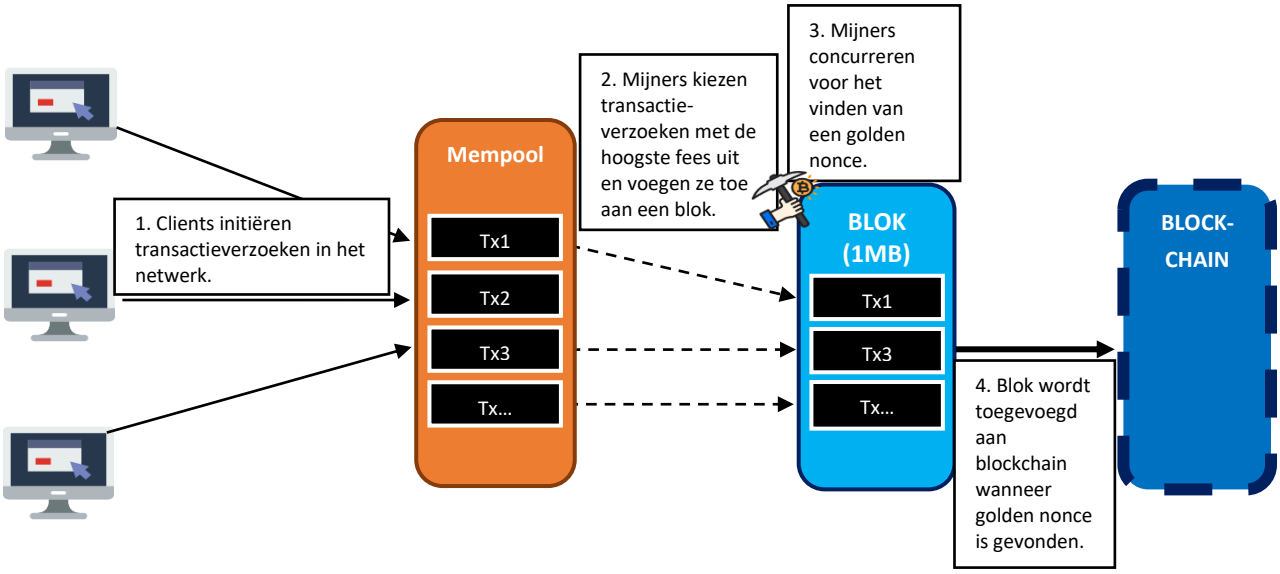
Transacties die worden uitgezonden naar het netwerk worden noch direct toegevoegd aan een blok door de mijner, noch worden ze direct opgeslagen in een blockchain. Ze komen eerst namelijk terecht in een ***memory pool*** (mempool) met andere transacties die nog moeten worden toegevoegd aan een blok door mijners en die nog door het netwerk moeten worden bevestigd.[38] Je kunt de mempool zien als een wachtruimte voor alle binnenkomende

[36] Voor meer informatie over UTXO's, zie de intermezzo 'Hoe je de Bitcoin blockchain leest met een block explorer' in hoofdstuk 3.

[37] Zie ook sectie 5 van de Bitcoin white paper (2008).

[38] Er zijn verschillende vereisten aan een transactie voordat deze wordt toegevoegd aan de mempool. Zo moet de som van de inputwaarden groter zijn dan de som van de outputwaarden. Met andere woorden, je moet meer BTC in je wallet hebben dan je wil uitgeven in de transactie. Voor een completer overzicht, zie 'An in-depth guide into how the mempool works' (Deneuville, 2016).

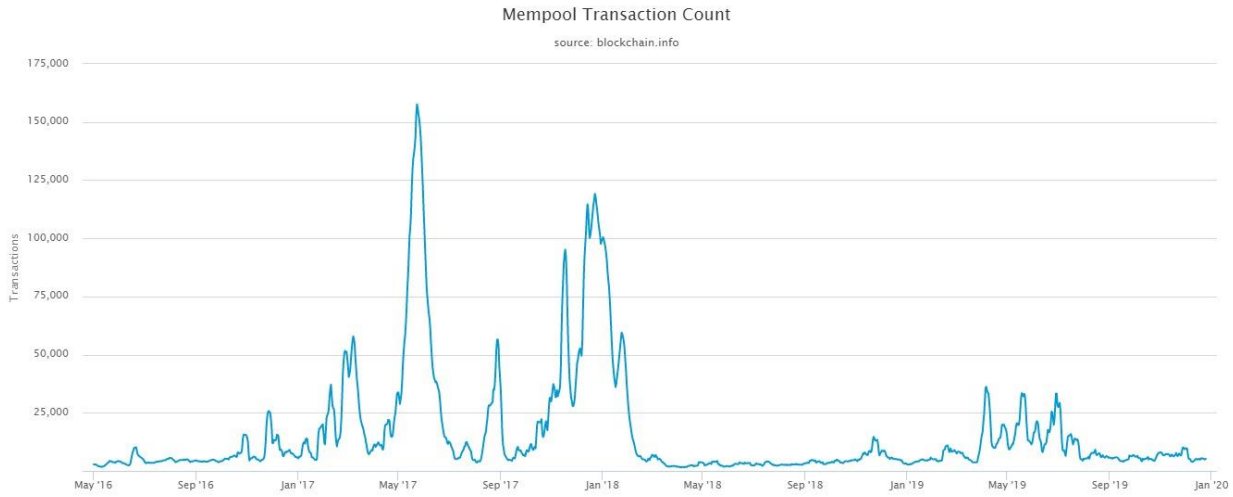
transacties die nog moeten worden bevestigd door het netwerk. Elke mijner heeft een eigen mempool en het is mogelijk dat de afzonderlijke mempools per mijner verschillen. Dat komt doordat er altijd netwerklatentie is binnen een computernetwerk: het kost altijd een beetje tijd voordat een transactie die naar het netwerk is verzonden alle mijners op het netwerk heeft bereikt. Daarnaast worden transacties in de mempool bewaard in het RAM-geheugen van de mijner.[39] Omdat elke mijner die is aangesloten op het netwerk kan kiezen welke hardware hij gebruikt voor het mijnen, kunnen mijners verschillende RAM-capaciteiten hebben voor de opslag van de onbevestigde transacties.



Afbeelding 40: Schematische weergave van hoe een transactie wordt toegevoegd aan de blockchain. De mempool is waar onbevestigde transacties binnenkomen en worden bewaard. De grootte van een blok is vastgesteld op 1MB, waardoor mijners een keuze moeten maken welke van de transacties uit de mempool zij willen toevoegen aan het blok waarvan zij de geldige blok hash proberen te vinden. Als mijners de blokgrootte overschrijden door te veel transacties toe te voegen, zal het blok niet worden geaccepteerd. Aangezien mijners naast de blokbeloning van momenteel 12,5 BTC ook de transactiekosten mogen innen, worden zij gestimuleerd om transacties uit de mempool te kiezen met de hoogste transactiekosten.

Hoeveel transacties er in een mempool zitten, varieert van tijd tot tijd. In de volgende afbeelding zie je een grafiek van hoeveel Bitcoin-transacties er in een mempool zitten over de periode vanaf 2016. Hoe meer activiteit er plaatsvindt op de blockchain, hoe meer transacties er in de mempool komen. In een ideale situatie zou je willen dat er zoveel mogelijk transacties uit de mempool komen en deze dus zoveel mogelijk leeg blijft. Echter, kan het Bitcoin-netwerk momenteel niet voldoende transacties per seconde verwerken.

[39] RAM staat voor Ramdom-access memory.



Afbeelding 41: Het aantal transacties in een mempool vanaf mei 2016 tot 25 december 2019. Omdat elke mijner een eigen mempool bijhoudt, is het mogelijk dat er onderling verschillen zijn in de transactieaantallen in de mempool. Uit de grafiek blijkt dat halverwege 2017 tot en met het begin van 2018 de mempool de meeste transacties had. Dit was de periode waarin Bitcoin qua prijs een grote stijging doormaakte naar boven de $18.000 USD en daarna weer omlaag ging. (Blockchain.com, 2019)

4.3 Hoe mijners transacties uit de mempool kiezen

Zoals we in een eerder hoofdstuk hebben geconstateerd, proberen mijners een geldige block header hash te genereren. Voor het genereren van deze hash worden de volgende data als input genomen:

1. Blockchain version.
2. Timestamp.
3. Nonce.
4. Difficulty.
5. Root hash van de Merkle tree van alle transacties in het blok.
6. Previous block header hash.

Punt 5 is afhankelijk van de transacties die door de mijner zijn gekozen om toe te voegen aan het blok waar hij aan werkt. Elke transactie die een mijner toevoegt of weglaat, resulteert in een andere root hash van de Merkle tree, wat weer verder escaleert tot een andere block header hash. Deze transacties komen uit de mempool en het is geheel aan de mijner welke transacties hij wil toevoegen.

Elke transactie komt met transactiekosten – de transactiefees. Mijners worden economisch gestimuleerd om transacties met de hoogste fees toe te voegen aan hun blok, omdat zij deze

kosten innen wanneer zij als eerste een geldige blok hash kunnen vinden en het blok mogen produceren. Doordat transacties met hogere fees eerder door mijners worden opgenomen binnen hun blok, is het verstandig om bij een Bitcoin-transactie een hogere fee op te geven als je wilt dat deze snel wordt verwerkt. In tijden waarin het netwerk overspoeld raakt met meer transacties dan het direct kan verwerken, kunnen de gemiddelde transactiekosten van Bitcoin vrij hoog oplopen.[40] Het is ook mogelijk dat transacties met te lage fees te lang in de mempool blijven hangen. Sinds de update van het netwerk naar Bitcoin Core versie 0.12 in februari 2016, is er een standaard vervaltijd van 72 uur. Als de transactie in die tijd niet is opgepakt door een mijner en niet is toegevoegd aan de blockchain, keert het automatisch weer terug naar de wallet.

4.3.1 Waarom mijners niet alle transacties uit de mempool in één blok kunnen stoppen

Op het moment van schrijven, december 2019, is de limiet van de ***blokgrootte*** (block size) gezet op 1MB. Mijners kunnen kiezen hoeveel zij van het blok willen opvullen met transacties.[41] Echter, blokken zullen worden geweigerd wanneer zij de limiet overschrijden. Naast de consequentie dat dit het netwerk langzamer maakt en de transactiekosten hoger, zijn er wel degelijk ook voordelen. De voor- en nadelen zullen uitvoeriger worden besproken in hoofdstuk 6 bij het onderwerp schaalbaarheid.

4.3.2 De kans dat een mijner een geldige hash vindt door de volledige nonce range uit te proberen

Zoals eerder vermeld is het nonce veld 32-bit. Hierdoor kan de nonce een waarde aannemen tussen 0 en 4.294.967.295.[42]

Een hash zelf bestaat uit 64 hexadecimale getallen. Dat betekent dat het aantal mogelijke hash-waarden gelijk is aan 16^{64}.

Gegeven dat de huidige mining difficulty vereist dat hashes alleen geldig zijn wanneer ze beginnen met 18 opeenvolgende nullen, kunnen we concluderen dat er $16^{64-18} = 16^{46}$ geldige hashes zijn.

[40] Zie https://bitcoinfees.info/ voor de huidige Bitcoin-transactiekosten.

[41] Zie https://bitinfocharts.com/comparison/bitcoin-size.html voor een historische grafiek van de blokgrootte.

[42] 4.294.967.295 wordt berekend door $(2^{32} - 1)$ te doen.

De kans dat een willekeurig gekozen hash een geldige hash is, is gelijk aan $16^{46}/16^{64} = 16^{-18}$. Dit is ongeveer 0,0000000000000000002%.

Een nonce kan echter maar een waarde aannemen tussen 0 en 4.294.967.295. Dit is aanzienlijk kleiner dan de kans dat een willekeurige hash een geldige hash is. Als een mijner alle waarden van een nonce probeert, is er slechts een kans van $2^{32} * 16^{-18}$ dat de mijner een geldige hash vindt. Dit is berekend door het aantal mogelijke noncewaarden (2^{32}) te vermenigvuldigen met de kans op een willekeurige valide hash (16^{-18}). De kans hierop is gelijk aan ongeveer 0,0000000001%. Deze kans is extreem laag.

Het heeft niet veel nut voor een mijner om steeds weer dezelfde nonce range af te lopen als de rest van de gegevens in het blok gelijk blijft. Er zijn naast de nonce nog twee andere typen gegevens die de staat van het blok kunnen veranderen:

1. De timestamp.
2. De lijst van transacties die een mijner heeft toegevoegd aan het blok.

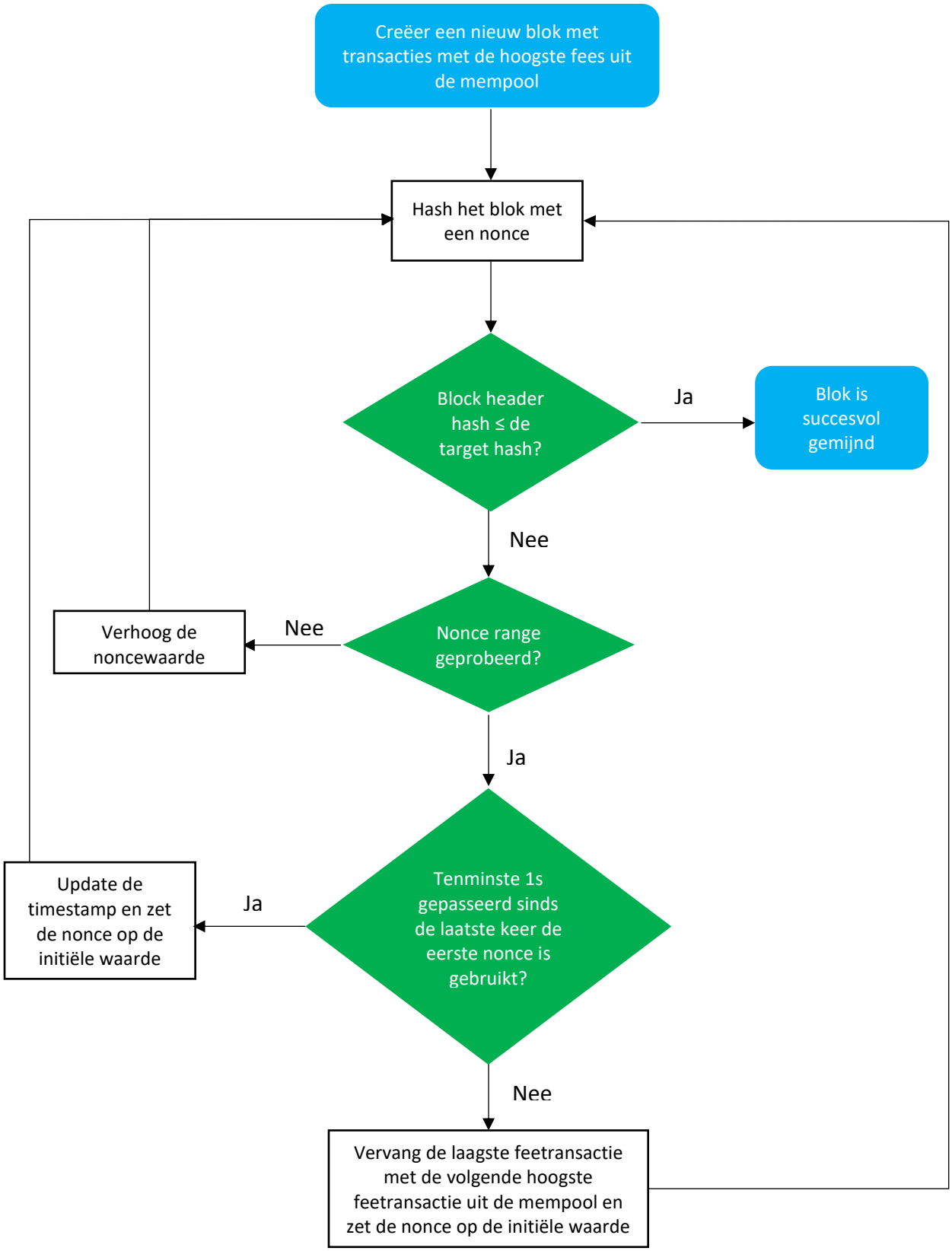
4.3.3 De invloed van de timestamp op het vinden van een geldige blok hash

De timestamp is de tijd in seconden die is verstreken sinds 1 januari 1970. Elke seconde verandert de timestamp, wat verder escaleert in een verandering van de blok hash. Dat betekent dat de mijner om de seconde weer door alle mogelijke noncewaarden tussen 0 en 4.294.967.295 heen kan gaan, wetende dat de resulterende hashes anders zullen zijn dan die zijn verkregen op de momenten van de vorige timestamps.

Dit is wat een mijner met bescheiden rekenkracht zou doen. Wat zouden mijners doen die door alle mogelijke noncewaarden heen kunnen, binnen een fractie van 1 seconde? Sommige mijners hebben hun rekenkracht gebundeld in ***mijning pools*** en kunnen gemakkelijk meer dan 4.294.967.295 hashes binnen een seconde genereren. In plaats van dat zij wachten totdat een seconde is verlopen en de timestamp is veranderd, veranderen zij de lijst van transacties die zij in het blok hebben toegevoegd. Het voordeel van mijning pools is dat ze een stabieler inkomen bieden voor de mijners, omdat mijning pools over een periode meer geldige blokken produceren en de mijners over meerdere momenten een evenredig deel van de blokbeloningen ontvangen.

4.3.4 De invloed van de lijst van transacties uit de mempool op het vinden van een blok hash

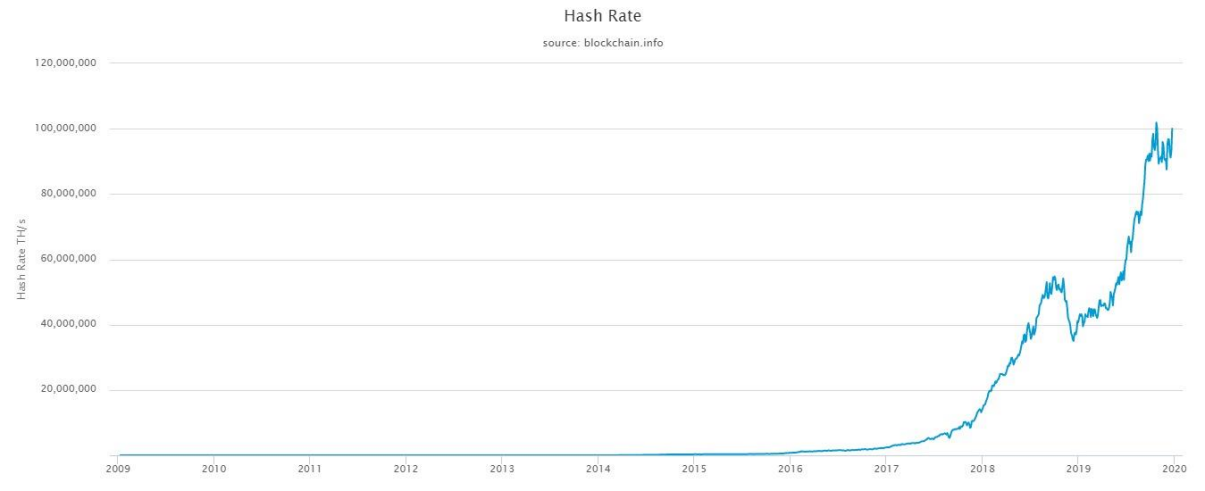
De transacties die mijners toevoegen aan hun blok komen uit de mempool. In eerste instantie zullen zij de transacties toevoegen met de hoogste transactiekosten. Echter, wanneer zij binnen een fractie van een seconde al alle nonces uit de nonce range hebben geprobeerd, zullen zij de resterende tijd van de seconde gebruiken om de transactielijst in het blok zo aan te passen dat zij weer een nieuwe nonce range kunnen uitproberen. Zij zullen hierbij de transactie met de laagste fee in het blok vervangen door een transactie met de hoogste fee die nog in de mempool aanwezig is. Vervolgens gaan zij nogmaals door de nonce range heen, hopende dat één van de nonces leidt tot een geldige blok hash. Mocht er weer geen geldige blok hash worden verkregen, dan zullen zij weer de transactie met de laagste fee in het blok vervangen door een transactie uit de mempool die de twee na hoogste fee heeft. Dit proces herhaalt zich totdat de timestamp wordt bijgewerkt met een seconde.



Afbeelding 42: Schematische weergave van de acties die een mijner onderneemt om een geldige blok hash te vinden. Zie ook: 'Mining difficulty, Hash Power, Nonce Range and the like. An Introduction to Bitcoin Mining' (Murabito, 2019).

Intermezzo: Mijning farms, mijningapparatuur en de energiebelasting van Bitcoins mijnen

Bij het mijnen van Bitcoin draait het erom hoe snel je een geldige blok hash kunt vinden. Hoe meer SHA-256 hashes per seconde je apparatuur kan berekenen, hoe groter de kans is dat je als eerste de hash kunt vinden van een Bitcoin-blok. De totale computerkracht die wordt geleverd aan het vinden van dergelijke hashes is sinds de begindagen van Bitcoin sterk toegenomen. Hieronder vind je de ontwikkeling van de hash rate in Tera Hashes / seconde. Eén Tera Hash staat gelijk aan 1 biljoen hashes.



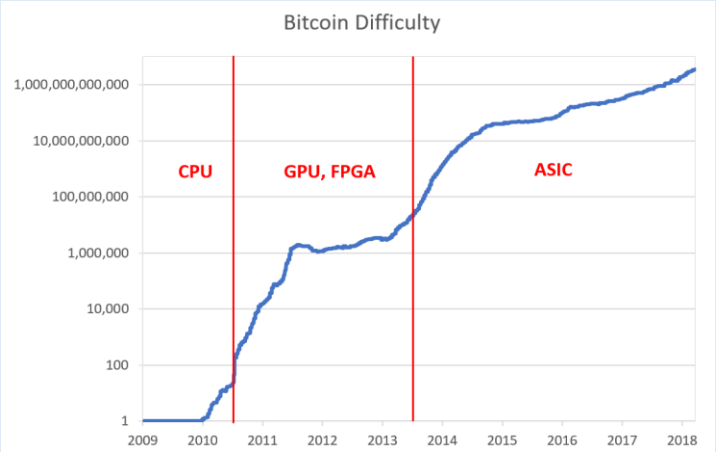
Afbeelding 43: Totale hash rate in Tera Hashes / seconde voor het Bitcoin-netwerk (Blockchain.com, 2019). 1 Tera Hash = 1 biljoen hashes.

CPU vs GPU vs ASICS

In de begindagen van Bitcoin werd het mijnen gedaan middels een ***Central Processing Unit*** (CPU) op een PC. Een CPU wordt ook vaak gezien als het brein van de computer. Deze voert berekeningen en instructies uit van je computerprogramma's. Het is geschikt om verschillende taken van een computer uit te voeren. Het is echter niet efficiënt in het uitvoeren van grote berekeningen – iets wat wel van belang is wanneer je snel hashes wil berekenen. Een efficiëntere manier om Bitcoin te mijnen is door gebruik te maken van een ***Graphics Processing Unit*** (GPU), ook wel bekend als een videokaart. GPU's konden vele malen sneller hashes berekenen dan een CPU. Met de groeiende populariteit van Bitcoin in 2017, groeide de verkoop van GPUs zo snel, dat er geen GPU's van bijvoorbeeld AMD en Nvidia meer beschikbaar waren voor gamers. Toen het mijnen met GPUs steeds competitiever werd, stapten er steeds meer mijners over op een ***Field-Programmable Gate Array*** (FPGA). De werking van GPU's is al vastgelegd door de producent en niet meer programmeerbaar. FPGA's daarentegen zijn programmeerbaar voor bepaalde doeleinden. Zo werden zij door Bitcoin-mijners geprogrammeerd om nog sneller Bitcoins te mijnen.

De beste manier om te mijnen is echter om gebruik te maken van een ***Application-Specific Integrated Circuit*** (ASIC). Dit is een microchip die speciaal is ontwikkeld om zo snel mogelijk enkel hash-algoritmes uit te voeren. Een ASIC kan wel 100.000 maal sneller hash-berekeningen maken dan een snelle CPU.

Hieronder zie je een afbeelding van de Bitcoin difficulty over de jaren heen en hoe de difficulty is gestegen bij de introductie van verbeterde mijningapparatuur.



Afbeelding 44: De Bitcoin difficulty is over de jaren heen hoger geworden met de introductie van verbeterde mijningapparatuur. Zie ook https://en.bitcoin.it/wiki/Mining_hardware_comparison voor een vergelijking van de prestaties van verscheidene mijningapparatuur.

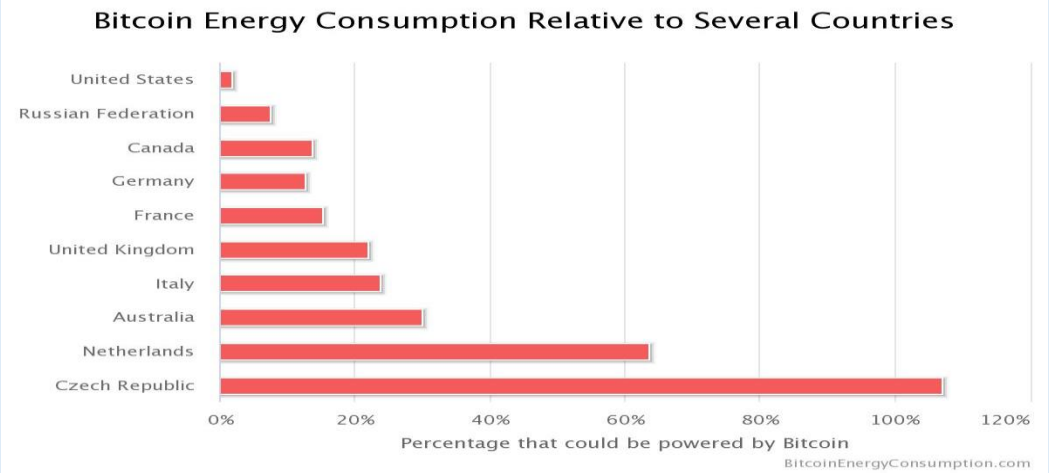
Mijning farms

De wedloop op betere mijningapparatuur die almaar sneller hashes kan berekenen, heeft de competitie dusdanig geïntensiveerd dat er ware mijning farms zijn ontstaan. Mijning farms zijn datacenters, soms wel met duizenden mijningcomputers. Aangezien vele Bitcoin mijning farms zelf gebruikmaken van ASICs, is het vrijwel onmogelijk om met een CPU, GPU of FPGA Bitcoin nog winstgevend te kunnen mijnen.

Energiebelasting van Bitcoin

Het Proof-of-Work-proces van Bitcoin kost veel computerkracht en daardoor ook veel energie. De energieconsumptie wordt regelmatig aangehaald als zeer belastend voor het milieu. Volgens 'The Carbon Footprint of Bitcoin' (Stoll, Klaaßen & Gallersdörfer, 2019) was de jaarlijkse energieconsumptie van Bitcoin, gemeten in november 2018, gelijk aan 45.8 TWh en werd er tussen de 22,0 en 22,9 $MtCO_2$ uitgestoten. De uitstoot is daarmee ongeveer gelijk aan wat Jordanië en Sri Lanka produceren.

BitcoinEnergyConsumption.com probeert het totale energievebruik van Bitcoin ook in kaart te brengen en schat dat het totale energieverbruik van Bitcoin gelijk is aan ongeveer 63,7% van het totale energieverbruik in Nederland.



Afbeelding 45: Het totale energieverbruik van Bitcoin is ongeveer gelijk aan 63,7% van het totale energieverbruik in Nederland. De data is geraadpleegd op 25 december 2019.

Het is echter ook belangrijk om ons af te vragen welke energiebronnen worden gebruikt. Als het grootste deel van de Bitcoin-consumptie gebeurt op plekken waar goedkope elektriciteit rijkelijk voorhanden is en wordt geproduceerd met energie die niet gemakkelijk kan worden opgeslagen en getransporteerd, dan is de energieconsumptie van Bitcoin niet zo beangstigend als sommigen beweren. Daarnaast is het ook belangrijk om de energieconsumptie van Bitcoin in relatie te zien met de energieconsumptie van industrieën die Bitcoin probeert te ontwrichten. Wat is de totale energieconsumptie van het financiële systeem? Hierbij moeten we rekening houden met het beheer van de fysieke gebouwen van financiële instellingen, het aantal werknemers die in de industrie werkt, de transportmiddelen die zij gebruiken om op het werk te komen, de grondstoffen die worden gebruikt om fysiek geld te maken en de verscheping ervan. Tot slot ontwikkelt de Bitcoin-technologie zich voortdurend en is het niet onmogelijk dat de technologie op den duur energiezuiniger wordt. Het is belangrijk om deze factoren mee te nemen voor een gebalanceerde discussie over het energieverbruik.

Satoshi (2010) zelf gelooft dat de Bitcoin-energieconsumptie geoorloofd is en maakt de vergelijking met goudwinning. Hij stelt dat de marginale kosten van goudwinning neigen naar de goudprijs. Alhoewel de goudwinning verspilling is, is de verspilling minder dan het nut om goud beschikbaar te hebben als een handelsmiddel:

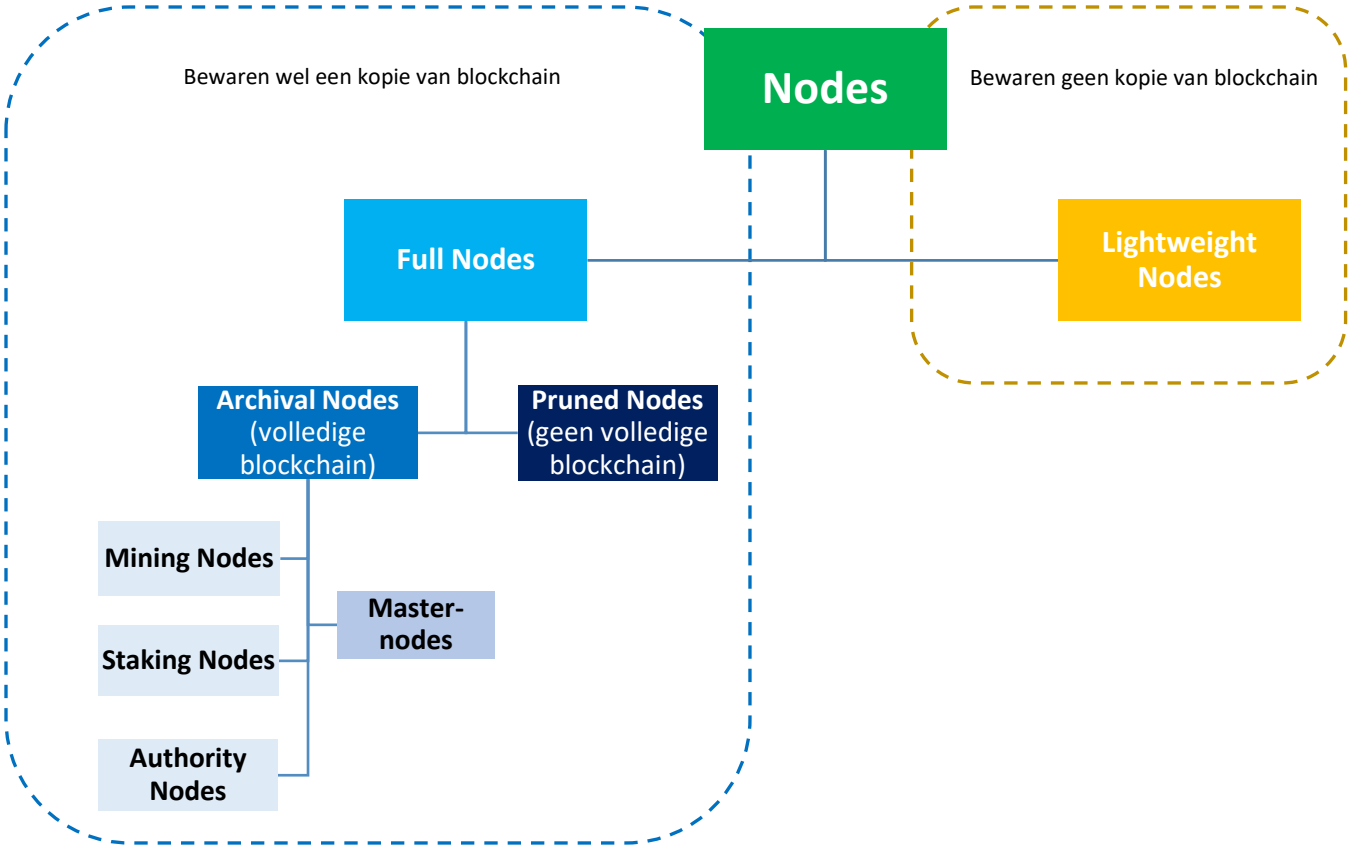
> "It's the same situation as gold, and gold mining. The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange. I think the case will be the same for Bitcoin. The utility of the exchanges made possible by Bitcoin will far exceed the cost of electricity used. Therefore, not having Bitcoin would be the net waste."

4.4 Nodes

Een node is een apparaat dat is gekoppeld en deelneemt aan het blockchainnetwerk. Dit kan een computer, een telefoon, een televisie of zelfs een printer zijn, zolang deze is verbonden aan het netwerk middels internet. Nodes kunnen verscheidene taken hebben, zoals het distribueren van data over het hele netwerk, het valideren en bevestigen van transacties en het netwerk helpen beveiligen. Tot dusver hebben we voornamelijk gekeken naar één type node, de mijner. Echter, bestaan er naast mijners nog andere nodes.

In deze sessie bespreken we de typologie van verschillende typen nodes.[43] Hierbij wordt er allereerst onderscheid gemaakt tussen full nodes en lightweight nodes. Je kunt full nodes onderverdelen in archival nodes en pruned nodes. Archival nodes kunnen worden onderverdeeld in mining nodes, authority nodes, staking nodes en masternodes.

[43] Wij maken hierbij gebruik van dezelfde typologie als www.nodes.com.



Afbeelding 46: Typologie in nodes.

4.4.1 Full nodes

Full nodes downloaden elke blok van de blockchain en verifiëren daarnaast transacties. Hun belangrijkste taak is om consensus op de blockchain te waarborgen en om ervoor te zorgen dat de blockchain beveiligd blijft. Full nodes zenden ook blokken en transacties uit naar het netwerk voor anderen om te downloaden. Daarnaast maken zij beslissingen over de toekomst van het netwerk. Dat doen zij door te stemmen op verbetervoorstellen voor het netwerk, zoals de ***Bitcoin Improvement Proposals*** (BIPs). Hoe dit te werk gaat, wordt later in het hoofdstuk besproken.

Full nodes zijn verder onder te verdelen in ***pruned full nodes*** en ***archival full nodes***.

4.4.2 Lightweight nodes

Lightweight nodes zijn alle apparaten die gekoppeld zijn aan het netwerk, maar geen kopie van de blockchain bewaren. Zij maken een koppeling met een full node om de huidige staat van het netwerk op te halen en zenden daarnaast transacties uit om te worden verwerkt. De interactie

met de blockchain gebeurt middels ***Simplified Payment Verification*** (SPV). SPV maakt het mogelijk om transacties toch te verifiëren, zonder de hele blockchain nodig te hebben.[44] Deze downloadt hiervoor alleen de block headers. Om te weten of een transactie is opgenomen in een blok, kijkt de lightweight node of zijn block header hash overeenkomt met de block header hash die full nodes hebben. Als dit klopt, dan kan de lightweight node ervan uitgaan dat de transactie daadwerkelijk in het desbetreffende blok is opgenomen.[45] Omdat lightweight nodes geen volledige blockchain bevatten en altijd afhankelijk zijn van full nodes om de laatste status van de blockchain in te zien, dragen ze niet zoveel bij aan de beveiliging van het netwerk als full nodes dat doen. Daartegenover staat wel dat ze niet veel resources verbruiken en makkelijk in gebruik te nemen zijn. Een voorbeeld van lightweight nodes zijn Bitcoin mobile wallets. Gezien het lagere opslaggeheugen van mobiele telefoons is het belangrijk voor mobile wallets om de laatste status van de blockchain op te kunnen vragen en transacties via de wallet te versturen naar het netwerk, zonder dat zij een gehele geschiedenis van de blockchain hoeven op te slaan.

4.4.3 Archival nodes

Archival nodes zijn full nodes die een volledige blockchain hebben. Wanneer mensen in een versimpelde uitleg van blockchain vermelden dat het een gedistribueerd grootboek is over een netwerk van computers, die allemaal een volledige kopie van de blockchain hebben, dan verwijzen ze hiermee eigenlijk naar archival nodes. Hun belangrijkste taken is om blokken te valideren en consensus te bereiken over de staat van de blockchain. Mijners zijn voorbeelden van archival nodes.

---

[44] De lightweight node die gebruikmaakt van SPV wordt ook wel een SPV node genoemd.

[45] Twee dagen nadat Satoshi Nakamoto zijn Bitcoin white paper had aangekondigd op de Cryptography mailing list, kreeg hij als respons van James A. Donald dat het systeem niet schaalbaar zou zijn als iedereen een full node zou moeten draaien. Als reactie schreef Satoshi Nakamoto (2008):

> "… it would be safe for users to use Simplified Payment Verification (section 8) to check for double spending, which only requires having the chain of block headers, or about 12KB per day. Only people trying to create new coins would need to run network nodes. At first, most users would run network nodes, but as the network grows beyond a certain point, it would be left more and more to specialists with server farms of specialized hardware."

Zie in het intermezzo over Merkle trees in hoofdstuk 4 hoe je met alleen block headers transacties kunt verifiëren. Zie voor verder informatie over Simplified Payment Verification ook sectie 8 van de Bitcoin white paper (2018).

4.4.4 Pruned nodes

Pruned nodes hebben een limiet aan opslag die zij beschikbaar hebben gesteld voor de blockchain. In plaats van dat zij de volledige geschiedenis van de blockchain bewaren, bewaren zij slechts een gedeelte van de blockchain. Zij kunnen zelf de mate waarin zij snoeien in hun blockchain instellen. Zo kunnen zij bijvoorbeeld een opslaglimiet instellen van 500MB. Van de nieuwe blokken die passen binnen de limiet zullen alle volledige data worden opgeslagen. Van de oudere blokken zal alleen maar een gedeelte van de data bewaard worden – bijvoorbeeld alleen de block headers. Binnen de block header wordt de root hash van de Merkle tree bewaard. Deze verwijst naar alle transacties binnen het blok. Mocht er een ongeldige transactie tussen zitten, dan zou de root hash dusdanig anders zijn dan de block header van een eerlijke node, waardoor het netwerk het blok als niet valide kan aanmerken. Op die manier kunnen pruned nodes nog steeds transacties verifiëren en betrokken zijn bij het waarborgen van consensus.[46] Ook geven zij nieuwe transacties door aan de rest van het netwerk.

Pruned nodes dragen dus nog steeds bij aan de beveiliging van het netwerk, zonder dat ze gebruik hoeven te maken van te veel opslagcapaciteiten.

4.4.5 Mining nodes

Mining nodes voegen transacties toe aan een blok en zoeken naar een geldige blok hash zodat zij het blok mogen toevoegen aan de blockchain. De eerste mijner die de geldige blok hash heeft kunnen vinden, stuurt het resultaat van zijn werk door naar het netwerk, zodat de andere full nodes kunnen verifiëren of het blok met de daarin opgenomen transacties daadwerkelijk geldig is. Voor het vinden van de juiste blok hash, verdienen mijners een blokbeloning en transactiefees.

4.4.6 Staking nodes

Staking nodes spelen een belangrijke rol binnen het consensusmechanisme dat Proof-of-Stake heet. Wij hebben ons tot nu voornamelijk gericht op Proof-of-Work, het consensusmechanisme waar Bitcoin gebruik van maakt en waarin mijners een belangrijke rol spelen in het creëren van een geldige blok. Bij Proof-of-Stake heten degenen die nieuwe blokken aanmaken geen mijners, maar ***forgers***. Om deel te mogen nemen aan het Proof-of-Stakeproces als forger, moet je een

[46] Zie sectie 7 van de Bitcoin white paper (2008) voor Satoshi Nakamoto's uitleg hoe pruned nodes schijfruimte besparen. Daarin wordt uitgelegd hoe Merkle trees werken en hoe je technisch gezien transacties uit een blok kunt afstoten uit de blockchain, zonder dat het verificatieproces van transacties in het geding komt. Zie daarnaast ook het Intermezzo over Merkle trees uit hoofdstuk 3.

bepaald aantal coins vasthouden in je wallet. De kans dat je een nieuw blok mag produceren, is dan afhankelijk van het aantal coins dat je vasthoudt. Stel dat je 1% van alle coins hebt, dan heb je bijvoorbeeld 1% kans om het volgende blok te mogen produceren. Er kunnen bij bepaalde blockchains ook andere factoren meespelen die je kans beïnvloeden, zoals de tijdsduur waarin je je coins hebt vastgehouden. Het voordeel hierbij is dat er niet geconcurreerd wordt in rekenkracht door blokproducenten. Een doorsnee computer zou in principe al voldoende moeten zijn om een blok te kunnen produceren.

Wij behandelen Proof-of-Stake in meer detail in hoofdstuk 6.

4.4.7 Authority nodes

Bij het opzetten van een consensusmechanisme dient er altijd een afweging plaats te vinden tussen decentralisatie en ***schaalbaarheid***. Een netwerk dat zeer gedecentraliseerd is en bestaat uit vele nodes, zoals de Bitcoin blockchain, kan minder transacties per seconde verwerken dan een netwerk bestaande uit weinig nodes. Een oplossing voor het schaalbaarheidsprobleem is om voorwaarden te stellen aan wie er blokken mogen creëren en valideren. Dit selecte groepje nodes worden ***authority nodes*** genoemd. Dit staat in contrast met bijvoorbeeld de Bitcoin blockchain waar iedereen een full node mag opzetten.

Het consensusmechanisme dat gebruikmaakt van authority nodes is Proof-of-Authority. De voorwaarden waar je aan moet voldoen om een authority node te mogen zijn en het aantal authority nodes binnen een netwerk kunnen per blockchain verschillen. De taken van authority nodes zijn dezelfde als die van andere full nodes. Het nadeel van het gebruik van authority nodes is dat ze gevoeliger kunnen zijn voor manipulatie, omdat je erop moet vertrouwen dat een select groepje nodes hun taken op verantwoordelijke wijze uitvoert.

In hoofdstuk 6 behandelen we onder andere Proof-of-Stake en Proof-of-Authority. Daar gaan we ook meer in op de voor- en nadelen van een netwerk dat gebruikmaakt van authority nodes.

4.4.8 Masternodes

Masternodes hebben net als andere full nodes ook een kopie van de blockchain en helpen ook transacties te verifiëren. Wat masternodes onderscheidt van andere full nodes is dat ze specialistische functies hebben binnen de blockchain. In de Dash blockchain maken zij het bijvoorbeeld mogelijk om transacties uit te voeren met meer privacy (PrivateSend) en met

grotere snelheden (InstantSend).[47] In ruil voor hun specialistische diensten krijgen zij vaak meer beloning dan andere full nodes. Daarnaast nemen de masternodes van Dash ook deel aan de governance en kunnen zij dus stemmen op proposals. Tot slot kunnen de Dash masternodes ook stemmen welke projecten worden gefinancierd. Echter, om een masternode te mogen zijn moet je wel coins als onderpand in je wallet hebben. Het verschilt per blockchain hoeveel onderpand een masternode moet inleggen. Bij Dash moet je bijvoorbeeld minimaal 1.000 Dash coins hebben.

4.4.9 Lightning nodes

Tot slot bespreken we nog ***lightning nodes***. Ze worden hier kort genoemd, omdat de implementatie daarvan binnen de Bitcoin community tot veel discussies heeft geleid. Lightning nodes vallen noch onder full nodes, noch onder lightweight nodes. Ze werden geïntroduceerd binnen het Bitcoin-netwerk om transacties buiten de blockchain om te regelen, zodat het netwerk zou worden ontlast. Het idee achter lightning nodes is dat ze transacties zouden versnellen tegen lagere kosten. Het netwerk van lightning nodes wordt het ***lightning netwerk*** genoemd. In hoofdstuk 6 vind je een verdere uitleg over hoe lightning nodes en het lightning netwerk werken.

[47] Dash, een samenvoeging van “digital cash”, is een cryptovaluta en heeft net als Bitcoin de ambitie om als digitaal geldmiddel gebruikt te worden.

Intermezzo: De functies van Dash Masternodes

Een Dash masternode is een server met een volledige kopie van de Dash blockchain. Net als andere full nodes valideert de Dash masternode ook blokken. Echter heeft de masternode daarnaast ook specialistische functies als PrivateSend, InstaSend. Daarnaast kunnen ze ook stemmen op improvement proposals van het netwerk en stemmen ze op budget proposals.

PrivateSend

Privatesend is een manier om transacties eerst te mixen voordat ze worden uitgestuurd naar hun eindbestemmingen. Door ze eerst te mixen, maak je het moeilijker om de transacties te herleiden naar de afkomst. Dit biedt meer privacy voor transacties.

InstantSend

InstantSend is een manier om transacties vrijwel direct te bevestigen door het masternode netwerk. Een Dashtransactie duurt normaal ongeveer 2,5 minuten, maar met InstantSend worden transacties bevestigd en geverifieerd binnen enkele seconden.

Blokbeloning

Bij Dash wordt de blokbeloning als volgt verdeeld: 45% van de beloning gaat naar de mijner, 45% gaat naar een masternode middels een protocol dat Proof-of-Service heet en de overige 10% wordt pas aan het eind van de maand gecreëerd. Gedurende de maand kan iedereen een budgetvoorstel indienen. Als het voorstel goedkeuring krijgt van minimaal 10% van de masternodes, dan wordt het voorstel gefinancierd met de Dash die aan het eind van de maand wordt uitgekeerd. Hiermee financiert het netwerk dus eigenlijk zijn eigen projecten.

Bij elk geproduceerde blok wordt er van een deterministische masternode lijst een masternode beloond. De masternode die is beloond, wordt dan weer achteraan op de lijst geplaatst. Dat betekent dat wanneer er meer masternodes zijn, er gemiddeld meer tijd zit tussen de beloningen die een masternode ontvangt. Daarnaast wordt de masternode van de lijst verwijderd wanneer deze het onderpand heeft uitgegeven, of wanneer deze langer dan één uur geen masternode diensten heeft geleverd. Op deze manier worden masternodes gestimuleerd om goede diensten te verlenen.

4.5 Bitcoin Improvement Proposals (BIPs)

Binnen een centraal netwerk is het makkelijk om het netwerk een update te geven. De beheerder van de centrale server beslist over de invoering van een update. Bitcoin heeft echter geen centraal bestuur. Toch is er ook binnen het Bitcoin-netwerk behoefte aan verbeteringen. Hoe wordt in een decentrale omgeving als Bitcoin toch overeenstemming bereikt met betrekking tot updates?

Omdat Bitcoin open source is, is de broncode openbaar en kan iedereen binnen het Bitcoin-netwerk een verbetervoorstel, een zogenaamde ***Bitcoin Improvement Proposal*** (BIP), indienen.[48] In de praktijk zijn het voornamelijk ontwikkelaars die deze voorstellen indienen. Een aanzienlijk deel van Bitcoin-ontwikkelaars zijn vrijwilligers, of waren ooit gestart als vrijwilligers. De ontwikkelaars die prominenter bijdragen leveren aan Bitcoin en ook meer tijd spenderen aan het project worden soms financieel gesponsord door een persoon of door ondernemingen zoals cryptohandelsbeurzen. Vervolgens is het aan de full nodes van het netwerk om te stemmen op deze verbetervoorstellen. De eerste BIP, BIP-0001 werd door Amir Taaki ingediend op 19 augustus 2011.[49] Hierin werd vastgelegd wat de voorwaarden van BIPs zouden moeten zijn.

4.5.1 Drie typen BIPs

Er zijn drie typen BIPs te onderscheiden. Deze zijn:

1. Standards Track BIP.
2. Informational BIP.
3. Process BIP.

---

[48] Je kunt een lijst van alle BIPs en diens statussen volgen via https://github.com/bitcoin/bips.

[49] De BIP-0001 kun je in de volledigheid vinden op https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki. Hierin staan de voorwaarden van een BIP omschreven.

Amir Taaki is een Brits-Iraanse hacktivist en softwareontwikkelaar die sterk is gedreven door zijn anarchistische filosofie. Hij is één van de vooraanstaandste Bitcoin-ontwikkelaars geweest en heeft onder andere 'The libbitcoin Manifesto' (2013) geschreven. Hierin wordt het revolutionaire karakter van Bitcoin omschreven en waarschuwt hij voor een verloedering van Satoshi Nakamoto's oorspronkelijke gedachtegoed voor Bitcoin:

> "Bitcoin is the future. Act like you believe it. Act to prevent corruption of the system. Act to prevent Bitcoin becoming coopted in any way. We must preserve the principles of Satoshi Nakamoto."

Standards Track BIP

Een ***Standards Track BIP*** beschrijft een wijziging die invloed heeft op vrijwel alle Bitcoin-implementaties, zoals veranderingen aan het netwerkprotocol.

Informational BIP

Een ***Informational BIP*** beschrijft een Bitcoin design issue of biedt algemene richtlijnen of informatie voor de community, maar stelt zelf geen nieuwe feature voor.

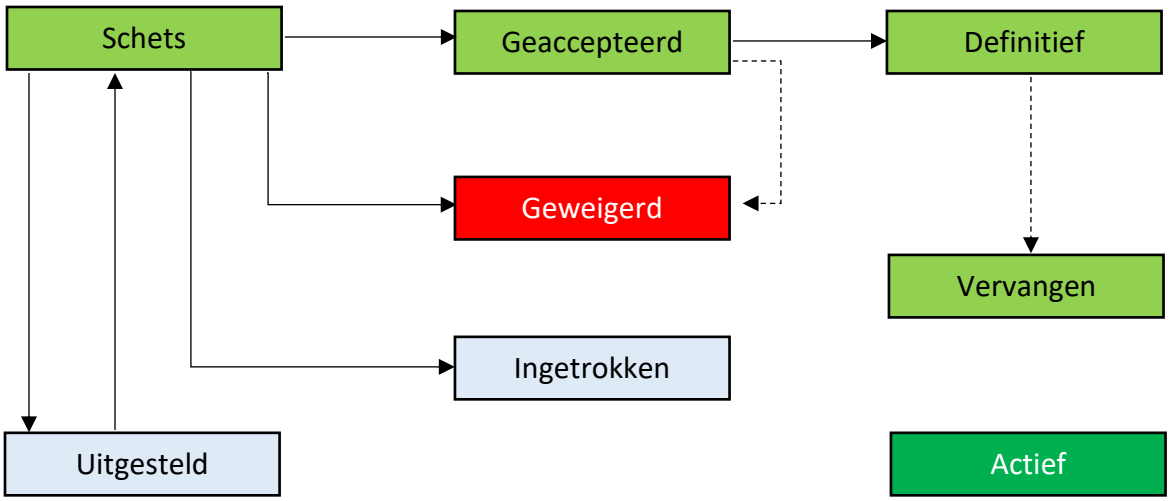
Process BIP

Een ***Process BIP*** beschrijft het proces omtrent Bitcoin, of stelt een wijziging van het proces voor. Het lijkt op een Standards Track BIP, maar wordt alleen toegepast bij zaken die geen betrekking hebben op het Bitcoin-protocol.

4.5.2 BIP Work Flow

Het BIP-proces begint met een nieuw idee voor Bitcoin. Het wordt aangeraden om eerst het idee te bespreken met de Bitcoin community in bijvoorbeeld fora, voordat het daadwerkelijk wordt ingediend, zodat de community erover kan discussiëren en er licht kan worden geworpen op de toepasbaarheid van het idee. Vervolgens dien je het idee te delen met de bitcoin-dev e-maillijst en de BIP-redacteur. De BIP-redacteur bewaakt het format van de BIP en bekijkt of de BIP aan alle gestelde voorwaarden voldoet. Bij goedkeuring zal hij de BIP voorzien van een label die aangeeft of het een Standards Track, Informational of Process BIP betreft. Daarnaast voorziet de redacteur de BIP ook van de status “Schets”.

Het is mogelijk voor de schrijver van de BIP om deze terug te trekken, bij te werken of nog uit te stellen. In onderstaande afbeelding vind je de verschillende statussen die een BIP kan hebben en de verschillende wegen die een BIP kan bewandelen.



Afbeelding 47: BIP work flow.

Het democratiseringsproces waarbij full nodes kunnen stemmen of ingediende voorstellen van de community moeten worden geaccepteerd, kunnen ook weleens leiden tot splitsingen in de blockchain. Over het algemeen wordt er onderscheid gemaakt tussen de volgende splitsingen:

1. Tijdelijke forks.
2. Soft forks.
3. Hard forks.

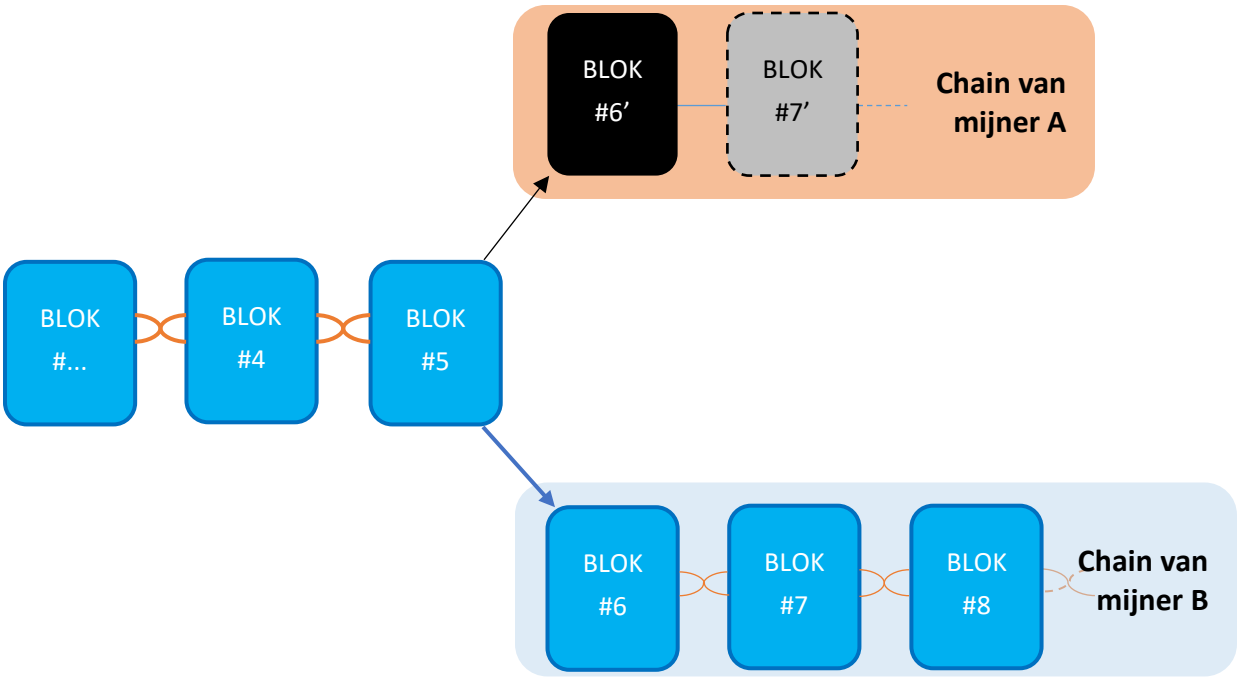
4.6 Forks

Wij hebben in het vorige hoofdstuk al kort forks besproken die tijdelijk ontstaan wanneer er rond dezelfde tijd door meer dan één mijner een geldig blok is gevonden.

4.6.1 Tijdelijke forks

Volgens het Proof-of-Work-consensusprotocol is de juiste staat van de blockchain altijd de chain met de meeste consensus, met de meeste Proof-of-Work. Dit is de chain die wordt ondersteund door de meeste computerkracht en die daardoor ook het langst is.[50] In onderstaande afbeelding hebben mijner A en mijner B rond dezelfde tijd een geldig blok aangemaakt. Als alle nodes met dezelfde blockchainversie als mijner B gezamenlijk meer computerkracht bezitten dan nodes met de blockchainversie van mijner A, zullen er sneller nieuwe blokken worden toegevoegd aan de blockchainversie van mijner B. Dit leidt ertoe dat deze blockchain langer wordt en de blokken 6’ en 7’ van mijner A orphaned blokken worden.

[50] Een overzicht van orphaned blokken bij de Bitcoin blockchain kun je hier vinden: https://www.blockchain.com/btc/orphaned-blocks.



Afbeelding 48: Mijner A en B maken rond dezelfde tijd een geldige blok aan. De chain met de meeste Proof-of-Work, ofwel de langste chain, wordt gezien als de ware blockchain. Deze ware blockchain wordt geadopteerd door de rest van het netwerk.

Aangezien orphaned blokken niet worden gezien als onderdeel van de ware blockchain, zullen de transacties die zijn goedgekeurd in de orphaned blokken ook geen deel uitmaken van de ware blockchain. Als je kijkt naar de ware blockchain, dan lijkt het alsof de transacties in de orphaned blokken nooit hebben plaatsgevonden. Het is echter wel mogelijk dat deze transacties vanuit de mempool zowel zijn opgenomen in de chain van mijner A als in die van mijner B. Hierbij maakt het voor de verzender van de transactie niet uit dat de nieuwe blokken van mijner A orphaned blokken zijn geworden, aangezien zijn transactie toch is opgenomen en goedgekeurd in de ware blockchain. Echter, kunnen er ook transacties zijn binnen een orphaned blok die niet voorkomen in het 'ware blok'. Deze transacties komen na verloop van tijd automatisch weer in de mempool terecht, waarna ze eventueel kunnen worden opgepikt in het volgende blok.

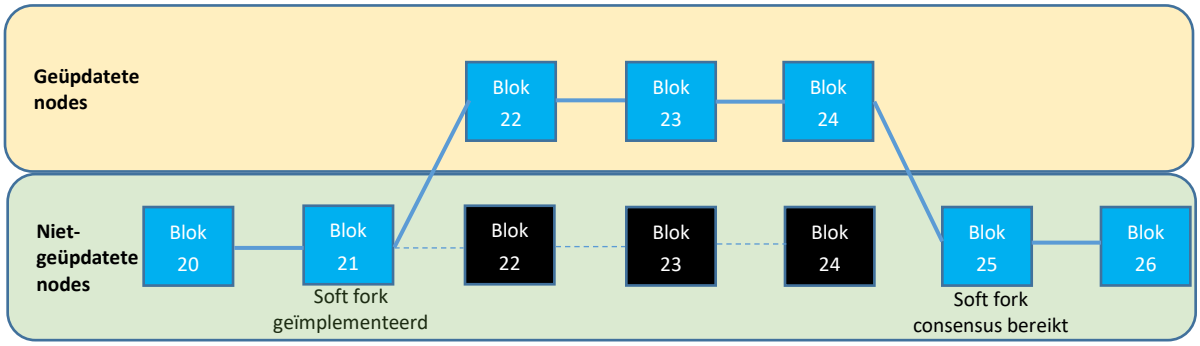
Zoals eerder vermeld, kunnen mensen improvement proposals insturen voor de Bitcoin blockchain. Omdat blockchains gedecentraliseerde netwerken zijn, moeten de deelnemers aan het netwerk samen consensus zien te bereiken over wat de regels van het netwerk zijn. Als de update een verandering aan de software betreft, kan er gekozen worden tussen een soft fork en een hard fork.

4.6.2 Soft forks

Bij een ***soft fork*** is er een verandering aan de software die backward compatibel is. Dat betekent dat nodes die geen update hebben doorgevoerd nog steeds transacties kunnen verwerken en toevoegen aan de blockchain, zolang ze zich houden aan de nieuwe protocolregels. Dat betekent ook dat alle blokken op de nieuwe blockchain de set aan regels volgen van zowel de oude als de nieuwe blockchain.

Een voorbeeld van een soft fork is een nieuwe regel om de blokgrootte te verkleinen van 1MB naar 300kb.[51] Oudere nodes zullen nog steeds in staat zijn om transacties te verwerken en blokken die 300kb of kleiner zijn te delen met andere nodes. Als deze oudere node echter een blok van 1MB heeft goedgekeurd en dan probeert te pushen naar de rest van het netwerk, zullen de geüpdatete nodes dit blok afwijzen, aangezien zij alleen blokken van 300kb of kleiner accepteren. Dit stimuleert de oudere nodes om een update te doen naar het nieuwe protocol.

Een soft fork wordt altijd geïmplementeerd bij een bepaald blok, bijvoorbeeld bij blok #20.000. In de regel staat geschreven dat er binnen een bepaald aantal blokken, bijvoorbeeld 1.000 blokken, een bepaald aantal % consensus moet zijn bereikt voor het nieuwe protocol om in te gaan. Mocht er niet voldoende consensus zijn bereikt voor een bepaald blok, dan gaat de update niet door en springt de nieuwe softwareversie automatisch weer terug naar de oude versie. In de volgende afbeelding vind je een grafische weergave van hoe dit te werk gaat. De zwarte blokken zijn blokken die de nieuwe regels overtreden. De blauwe blokken voldoen aan de nieuwe regels.



Afbeelding 49: Weergave van een soft fork. De soft fork wordt geïmplementeerd in blok 21 en de beoogde consensus is bereikt bij blok 25.

[51] Luke Dashjr (2019), één van de core developers van Bitcoin, stelt dit overigens voor zodat het makkelijker wordt om een full node te draaien. Als er meer mensen zelf een full node draaien is de blockchain ook decentraler.

4.6.3 Hard forks

Bij een ***hard fork*** is er ook een verandering in het protocol. Echter is deze verandering niet compatibel met de vorige versies, waardoor de nodes die geen update hebben doorgevoerd naar de nieuwe versie geen transacties kunnen verwerken. Zij kunnen ook geen nieuwe blokken pushen naar de blockchain.

Een voorbeeld van een hard fork is een nieuwe regel waarbij de blokgrootte wordt verhoogd van 1MB naar 2MB. Als een geüpdatete node een blok van 2MB wil pushen naar de blockchain, dan zullen de nodes die niet zijn geüpdatet deze blokken afwijzen.

Hard forks kunnen zowel gepland als omstreden zijn.

Geplande hard forks

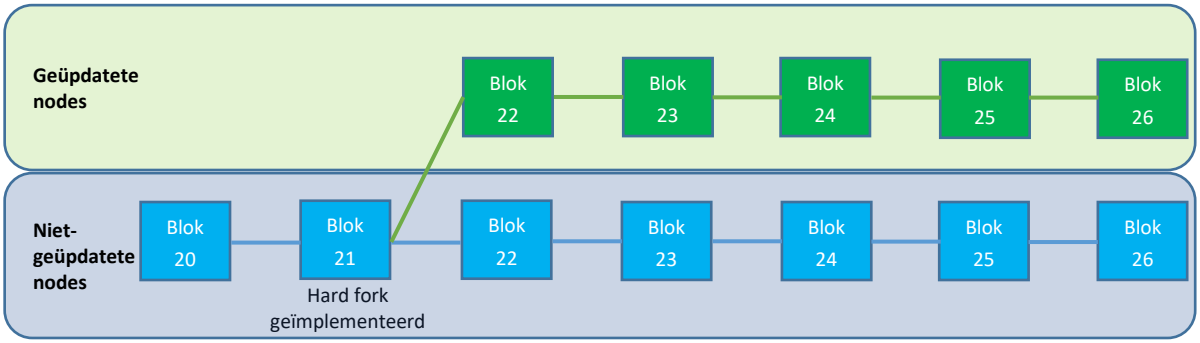
Bij een ***geplande hard fork***, hebben de nodes besloten om vrijwillig hun software te updaten en het nieuwe protocol te volgen. Degenen die de update niet hebben doorgevoerd, zullen nog steeds de oude blockchainversie draaien, waar weinig mensen gebruik van zullen maken. Omdat deze oude blockchain door een klein aantal nodes wordt gedraaid is deze niet zo gedecentraliseerd als de nieuwe blockchain en is deze door de kleine hoeveelheid computerkracht die erachter zit ook minder veilig.

Omstreden hard forks

Bij een ***omstreden hard fork*** is er zo'n grote dusdanige onenigheid binnen de community over de upgrade, dat een significant deel van de community besluit om de update door te voeren en een ander deel niet. Dit zorgt ervoor dat er twee blockchains ontstaan die niet compatibel met elkaar zijn. De munt op de ene blockchain werkt daarnaast dusdanig anders van de munt op de andere blockchain, dat ze niet heen en weer gestuurd kunnen worden van de ene naar de andere blockchain. Er ontstaan dus eigenlijk twee verschillende munten. Omdat een fork altijd gebaseerd is op de originele blockchain, bevat de nieuwe blockchain ook alle transacties van de originele blockchain. Dat betekent dat als je 10 munten had op de originele blockchain, je dan ook 10 munten krijgt op de nieuwe blockchain. Hierdoor lijkt het alsof je gratis nieuwe munten krijgt.

In de volgende afbeelding vind je een grafische weergave van een dergelijke hard fork. Bij blok 21 wordt de hard fork geïmplementeerd. De groene chain is de nieuwe gevorkte chain en de

blauwe chain is de originele. Zoals je kunt zien hebben ze een gedeelde transactiegeschiedenis tot en met blok 21.



Afbeelding 50: Weergave van een hard fork. De hard fork wordt geïmplementeerd in blok 22. De groene chain is de gevorkte blockchain en de blauwe chain is de originele blockchain. Zij hebben tot en met blok 21 een gedeelde geschiedenis. Beide blockchains zijn niet meer gelijk aan elkaar en de munten van de groene blockchain zijn wezenlijk anders geworden van de munten van de blauwe blockchain, zodat ze niet meer cross-blockchain naar elkaar kunnen worden gestuurd.

Een bekend voorbeeld van een dergelijke situatie was de omstreden hard fork van de Bitcoin blockchain wat leidde tot een nieuw type Bitcoin-munt, de Bitcoin Cash. Deze hard fork vond plaats op 1 augustus 2017. De communities van beide blockchains staan sindsdien wat op gespannen voet met elkaar. Zie het volgende intermezzo voor meer informatie over de omstreden splitsing.

Het is bij een fork altijd nog maar de vraag hoeveel van de nodes achter de nieuwe software-update staan. Bij een hard fork kan het zijn dat er haast geen nodes zijn die de ene blockchainversie ondersteunen, waardoor deze versie al gauw uitsterft. Het is ook mogelijk dat beide blockchains worden geaccepteerd, maar dat er één is die duidelijk dominanter is en aanzienlijk meer ondersteuning krijgt van de nodes. De klassieke Bitcoin is momenteel nog steeds dominanter dan haar afgeleide, de Bitcoin Cash. Naast Bitcoin Cash zijn er nog verscheidene andere hard forks geweest van Bitcoin, zoals Bitcoin Private en Bitcoin Gold.

Intermezzo: Bitcoin vs Bitcoin Cash vs Bitcoin SV

Vanaf het ontstaan is Bitcoin de cryptovaluta geweest met de grootste marktkapitalisatie. Lange tijd was het ook de meest gebruikte blockchain. Met de toenemende populariteit van blockchains nam het steeds meer tijd in beslag om een transactie bij te schrijven en liepen de tarieven op het Bitcoin-netwerk op. Dit leidde in 2017 tot een hevige discussie of Bitcoin de blokgrootte niet moest vergroten om het aantal transacties toe te laten nemen en de tarieven te verlagen. De blokgrootte was indertijd 1MB, wat het aantal transacties tot 7 per seconde limiteerde. Onder andere de bekende Bitcoin-voorvechter Roger Ver sprak zich hiervoor uit en insinueerde dat tegenstanders, zoals grotere Bitcoin-mijners, de voortgang van Bitcoin stopten, omdat deze grotere mijners liever geen lagere tarieven en minder winstgevendheid wilden. Roger Ver denkt dat als Bitcoin niet gaat opschalen naar meer transacties per seconde, Bitcoin geen alternatief elektronisch geld kan worden dat kan concurreren met nationale valuta. (Popper, 2017)

De grotere Bitcoin-mijners werden indertijd gesteund door de core developers van Bitcoin. Als alternatief voor een grotere blockgrootte stelden de core developers BIP 91 voor. Hierin werd de Segregated Witness-aanpassing (SegWit) voorgesteld, waarmee bepaalde delen van een transactie niet meer mee werden genomen in een blok, zodat er meer transacties in het blok zouden passen. De groep tegenstanders was niet akkoord met BIP 91 en splitste zich in augustus 2017 af via een hard fork. Dit resulteerde in Bitcoin Cash. Bitcoin Cash maakte gebruik van een 8MB blokgrootte en gebruikt SecurSigs in plaats van SegWit. Als hard fork heeft Bitcoin Cash net als Bitcoin tevens een maximaal aanbod van 21 miljoen tokens.

Verschillen tussen Bitcoin en Bitcoin Cash

Naast een update in de blokgrootte, liet Bitcoin Cash de mining difficulty mede afhangen van het aantal mijners. (CoinTelegraph, 2019) Van deze methode stapte Bitcoin Cash af, nadat bleek dat de moeilijkheidsgraad instabiel was en er gemiddeld sneller dan 10 minuten geldige blokken werden gevonden. In plaats hiervan kwam Bitcoin Cash aan met een algoritme dat de moeilijkheidsgraad om de 144 blokken opnieuw berekent. Dit wordt het Emergency Difficulty Adjustment (EDA) genoemd en is een toevoeging aan de gebruikte Difficulty Adjustment Algorithm (DAA). (Aggurwal & Tan, 2019, pp. 3-4)

De mining difficulty bij Bitcoin Cash is op het moment van schrijven van dit boek (10 december 2019) ongeveer 2% van de mining difficulty bij Bitcoin. Als gevolg hiervan is het laagdrempeliger om Bitcoin Cash te mijnen, waardoor je meer kleine mijners verwacht bij Bitcoin Cash. Op 10 december 2019 hebben de tien grootste mijning pools bij Bitcoin Cash dan ook net meer dan 51% van de blokken geverifieerd over de laatste weken, terwijl de tien grootste mijning pools bij Bitcoin meer dan 90% hebben geverifieerd. (Coin Dance, 2019)

Bitcoin SV en hash war

In november 2018 werd er ook van Bitcoin Cash een nieuwe blockchain gesplitst via een hard fork. Dit resulteerde in Bitcoin Satoshi Vision (Bitcoin SV). Wat er gebeurde, was dat een groep rond Bitcoin Cash, bestaande uit Roger Ver en Jihan Wu, een upgrade van het protocol voorstelde om non-cashtransacties en smart contracts mogelijk te maken. Hierdoor zou het netwerk onder andere orakels en atomic swaps kunnen gaan gebruiken. Een groep tegenstanders, bestaande uit onder andere online gokmiljardairs Calvin Ayre en Craig Wright, zagen dit als onveilig en niet in lijn met de oorspronkelijke visie van Bitcoin als digitaal geldsysteem. Zij stelden dan ook een alternatieve blockchain voor met 128MB blokgrootte. (Sfox, 2019) Bitcoin Cash heeft sinds 15 mei 2018 een blokgrootte van 32MB.

Een pikant detail bij deze splitsing is dat gezien beide systemen SHA-256 gebruiken en de grote mijners van Bitcoin Cash in meerderheid het Bitcoin SV initiatief ondersteunen, het mogelijk zou zijn dat de Bitcoin SV groep een 51%-aanval uitvoert op Bitcoin Cash, zodat alleen de Bitcoin SV chain zou overleven. Craig Wright, de aanstichter van Bitcoin SV, hintte op het starten van deze zogenaamde ***hash war***. Deze oorlog is op het moment van schrijven nog uitgebleven. (Van Wirdum, 2018)

Op moment van schrijven, op 10 december 2019, heeft Bitcoin SV meer transacties per week dan Bitcoin en Bitcoin Cash. Voor meer informatie zie https://blocktivity.info/. Hierbij is het wel belangrijk om te beseffen dat het aantal transacties op een blockchain niks zegt over de kwaliteit en de waarde van de transacties.

Intermezzo: Hoe je zelf een Bitcoin full node opzet

Een full node helpt het netwerk door alle transacties en blokken te valideren. Daarnaast helpen ze ook de blokken uit te zenden naar andere full nodes, zodat het hele netwerk beschikt over dezelfde staat van de blockchain. Het opzetten van een Bitcoin full node is even simpel als het downloaden, installeren en opstarten van een applicatie.

Minimale vereisten

Om een full node te draaien, dien je aan een aantal vereisten te voldoen. Je kunt het draaien op een recente versie van je Windows-, Mac OS- en Linux-besturingssystemen. Daarnaast heb je ook vrije schijfruimte nodig van meer dan 200GB en 2GB aan RAM-geheugen.

Bitcoin full node opzetten

1. Ga naar de downloadpagina van Bitcoin Core: https://bitcoin.org/en/download. Bitcoin Core is de meestgebruikte Bitcoin client.
2. Download de software voor het besturingssysteem dat je gebruikt.
3. Open het bestand en doorloop de setup wizard.

4. Je kunt ervoor kiezen om een Bitcoin Core Graphical User Interface (GUI) te installeren, een Bitcoin Core daemon (Bitcoind) of een combinatie van de twee. De Bitcoin GUI is de meest gebruikersvriendelijke optie voor als je geen ontwikkelaar bent.
5. Doorloop verder alle stappen.
6. Wanneer je alle stappen hebt doorlopen, gaat de client de blockchain synchroniseren. Gezien de grootte van de Bitcoin blockchain kan dit langer dan een week duren.
7. Als je blockchain is gesynchroniseerd, heb je een werkende full node. Gefeliciteerd, je draagt hiermee bij aan de Bitcoin community. Je full node is tevens je wallet. Je kunt vanuit hier Bitcoins versturen en ontvangen.

4.7 Samenvatting, begrippen en bronnen

Samenvatting

Transacties die worden uitgezonden naar het netwerk komen eerst terecht in een memory pool (mempool) met andere transacties die nog moeten worden toegevoegd aan een blok door mijners. Hoe meer activiteit er plaatsvindt op de blockchain, hoe meer transacties er in de mempool komen. Mijners worden economisch gestimuleerd om transacties met de hoogste fees toe te voegen aan hun blok, omdat zij deze kosten innen wanneer zij als eerste een geldige blok hash kunnen vinden en het blok mogen produceren.

Het heeft niet veel nut voor een mijner om steeds weer dezelfde nonce range af te lopen als de rest van de gegevens in het blok gelijk blijft. Daarom kijkt de mijner die al alle nonces hebben uitgeprobeerd binnen een bepaalde timestamp of hij een transactie uit zijn blok kan vervangen door een andere transactie uit de mempool.

Een node is een apparaat dat is gekoppeld en deelneemt aan het blockchainnetwerk. Wij maken hierbij onderscheid tussen full nodes en lightweight nodes. Full nodes zijn weer te verdelen in archival nodes en pruned nodes. Archival nodes bestaan weer uit mining nodes, staking nodes, authority nodes en masternodes.

Binnen een centraal netwerk is het makkelijk om een update door te voeren, omdat een centrale partij hierover beslist. Binnen een decentraal netwerk moet er echter eerst consensus worden bereikt over de update. Omdat Bitcoin open source is, is de broncode openbaar en kan iedereen binnen het Bitcoin-netwerk een verbetervoorstel, een zogenaamde Bitcoin Improvement Proposal (BIP), indienen. Er zijn drie typen BIPs te onderscheiden. Deze zijn:

1. Standards Track BIP.
2. Informational BIP.
3. Process BIP.

Het democratiseringsproces waarbij full nodes kunnen stemmen of ingediende voorstellen van de community moeten worden geaccepteerd, kunnen ook weleens leiden tot splitsingen in de blockchain. Over het algemeen wordt er onderscheid gemaakt tussen de volgende typen splitsingen:

1. Tijdelijke forks.
2. Soft forks.
3. Hard forks.

Bij een soft fork is er een verandering aan de software die backward compatibel is. Dat betekent dat nodes die geen update hebben doorgevoerd nog steeds transacties kunnen verwerken en toevoegen aan de blockchain, zolang ze zich houden aan de nieuwe protocolregels. Dat betekent ook dat alle blokken op de nieuwe blockchain de set aan regels volgen van zowel de oude als de nieuwe blockchain.

Bij een hard fork is er ook een verandering in het protocol. Echter is deze verandering niet compatibel met de vorige versies, waardoor de nodes die geen update hebben doorgevoerd naar de nieuwe versie geen transacties kunnen verwerken. Zij kunnen ook geen nieuwe blokken pushen naar de blockchain.

Opmerkingen die je nu kunt uitleggen

- Mijners die alle nonces kunnen uitproberen binnen een seconde zullen transacties in het blok waar ze aan werken vervangen door transacties uit de mempool.
- De kans dat een willekeurig gekozen hash een geldige hash is, is gelijk aan 0,00000000000000000002%.
- De kans dat je binnen een bepaalde timestamp een geldige hash vindt door het hele nonce-bereik te proberen, is ongeveer 0,0000000001%.
- Lightweight nodes maken gebruik van Simplified Payment Verification (SPV). SPV maakt gebruik van Merkle trees.
- Forgers zijn een soort van mijners, maar dan op een Proof-of-Stake blockchain.
- Om een BIP (verbetervoorstel) voor Bitcoin in te dienen, moet je een heel proces doorlopen.
- Bitcoin Cash is het resultaat van een hard fork op de Bitcoin blockchain.
- Het is mogelijk dat de blockchain tijdelijk splitst.
- Het nadeel van een fork is dat de computerkracht van de initiële chain wordt verdeeld over de de initiële chain en de nieuwe chain die ontstaat uit de fork.

Verklarende begrippenlijst

Application-Specific Integrated Circuit (ASIC): Microchip die speciaal is ontwikkeld om zo snel mogelijk alleen hash-algoritmes uit te voeren.

Archival full nodes: Full nodes die een volledige blockchain bewaren, transacties helpen verifiëren en transacties en blokken uitzenden naar de rest van het netwerk.

Authority nodes: Een groepje nodes dat is geselecteerd om blokken te mogen aanmaken. Proof-of-Authority blockchains maken gebruik van authority nodes. Deze blockchains zijn permissioned en worden gebruikt in een private blockchainomgeving.

BIP: Zie Bitcoin Improvement Protocol.

Bitcoin Improvement Proposal (BIP): Een verbetervoorstel voor Bitcoin.

Blokgrootte (block size): De grootte van een blok.

Central Processing Unit (CPU): Een processor in een computer die berekeningen uitvoert. In de begindagen van Bitcoin werden CPU's gebruikt om te mijnen.

Field-Programmable Gateway Array (FPGA): Geïntegreerde schakeling van programmeerbare logische componenten.

Forger: Een node op een Proof-of-Stake blockchain die nieuwe blokken produceert. Forgers doen dat door hun coins te staken. Blokproducenten op een Proof-of-Work blockchain zijn mining nodes. Mijners produceren nieuwe coins door computerkracht te leveren.

Full nodes: Nodes die elke nieuwe blok van de blockchain valideren en transacties verifiëren. Zij zorgen ervoor dat consensus op de blockchain wordt gewaarborgd en zenden blokken en transacties uit naar het netwerk voor anderen om te downloaden.

Geplande hard fork: Bij een geplande hard fork, hebben de nodes besloten om vrijwillig hun software te updaten en het nieuwe protocol te volgen.

Graphics Processing Unit (GPU): Een grafische processor die gebruikt wordt voor videotaken. GPU's bevinden zich meestal op videokaarten.

Hard fork: Een permanente splitsing van de blockchain. Er zijn twee typen hard forks: een geplande hard fork en een omstreden hard fork. Bij een geplande hard fork, hebben de nodes besloten om vrijwillig hun software te updaten en het nieuwe protocol te volgen. Bij een omstreden hard fork is er zo'n grote dusdanige onenigheid binnen de community over de upgrade, dat een significant deel van de community besluit om de update door te voeren en een ander deel niet.

Hash war: Oorlog om hash rate tussen bijvoorbeeld twee blockchains.

Informational BIP: Een verbetervoorstel dat een Bitcoin design issue beschrijft of algemene richtlijnen of informatie voor de community biedt, maar zelf geen nieuwe feature voorstelt.

Lightning netwerk: Een off-chain schalingsoplossing. Het netwerk wordt onderhouden door lightning nodes.

Lightning nodes: Nodes die het lightning netwerk onderhouden.

Lightweight nodes: Alle apparaten die gekoppeld zijn aan het netwerk, maar geen kopie van de blockchain bewaren. Zij maken een koppeling met een full node om de huidige staat van het netwerk op te halen en zenden daarnaast transacties uit om te worden verwerkt.

Masternodes: Hebben net als andere full nodes ook een kopie van de blockchain en helpen ook transacties te verifiëren. Wat masternodes onderscheidt van andere full nodes is dat ze specialistische functies hebben binnen de blockchain. Bij Dash zijn dat PrivateSend en InstantSend.

Memory pool (mempool): Een wachtruimte voor alle binnenkomende transacties die nog moeten worden bevestigd door het netwerk. Mijners kiezen transacties uit de memory pool om ze toe te voegen aan het blok waar ze aan werken. Elke mijner heeft een eigen memory pool. Het is dus mogelijk dat de afzonderlijke memory pools per mijner verschillen.

Mempool: Zie memory pool.

Mijning pool: Een groep mijners die computerkracht bundelt om een geldige blok te vinden.

Mining nodes: Full nodes die transacties toevoegen aan een blok en zoeken naar een geldige blok hash om het blok te mogen toevoegen aan de blockchain. Voor het vinden van een geldige blok, ontvangen zij een blokbeloning.

Omstreden hard fork: Bij deze hard fork is er een dusdanige onenigheid binnen de community over de upgrade, dat een significant deel van de community besluit om de update door te voeren en een ander deel niet. Het gevolg is een permanente splitsing van de blockchain.

Process BIP: Een verbetervoorstel dat het proces omtrent Bitcoin beschrijft, of een wijziging van het proces voorstelt. Het lijkt op een Standards Track BIP, maar wordt alleen toegepast bij zaken die geen betrekking hebben op het Bitcoin-protocol.

Pruned full nodes: Full nodes die slechts een deel van de blockchain op de computer bewaren om schijfruimte te besparen. Hierbij kunnen ze nog wel transacties helpen verifiëren en transacties en blokken uitzenden naar de rest van het netwerk.

Schaalbaarheid: De verwerkingscapaciteit van een blockchain. Hierbij wordt voornamelijk gekeken naar het aantal transacties per seconde dat een blockchain kan verwerken.

Simplified Payment Verification (SPV): Een manier om transacties te verifiëren, zonder de hele blockchain nodig te hebben. Hierbij wordt gebruik gemaakt van Merkle trees.

Soft fork: Een tijdelijke splitsing van de blockchain. Met andere woorden, er is een verandering aan de software die backward compatibel is. Dat betekent dat nodes die geen update hebben doorgevoerd nog steeds transacties kunnen verwerken en toevoegen aan de blockchain, zolang ze zich houden aan de nieuwe protocolregels. Dat betekent ook dat alle blokken op de nieuwe blockchain de set aan regels volgen van zowel de oude als de nieuwe blockchain.

Staking nodes: Nodes op een Proof-of-Stake blockchain die hun coins staken.

Standards Track BIP: Een verbetervoorstel dat een wijziging die invloed heeft op vrijwel alle Bitcoin-implementaties beschrijft, zoals veranderingen aan het netwerkprotocol.

Bronnen

Aggarwal, V., & Tan, Y. (2019). A Structural Analysis of Bitcoin Cash's Emergency Difficulty Adjustment Algorithm. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3383739

Ammous, S. (2018, 3 juni). Bitcoin & Economics: What would a Bitcoin standard look like? [YouTube]. Geraadpleegd van https://youtu.be/1WBrdLQhUrg

Blocktivity. (z.d.). Block'tivity. Geraadpleegd op 26 december 2019, van Blocktivity.info website: https://blocktivity.info/

Blockchain.com. (z.d.). Hash Rate. Geraadpleegd op 26 december 2019, van Blockchain.com website: https://www.blockchain.com/charts/hash-rate

Blockchain.com. (z.d.). Mempool Transaction Count. Geraadpleegd op 26 december 2019, van Blockchain.com website: https://www.blockchain.com/charts/mempool-count

Bitcoin Core. (z.d.). Download - Bitcoin. Geraadpleegd op 3 december 2019, van Bitcoin.org website: https://bitcoin.org/en/download

Bitcoin Github. (2016, 1 januari). Bitcoin/bips. Geraadpleegd op 26 december 2019, van GitHub website: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki

Bitcoin Wiki. (z.d.) Mining hardware comparison. Geraadpleegd op 26 december 2019, van Bitcoin.it website: https://en.bitcoin.it/wiki/Mining_hardware_comparison

Bitcoinfees.info. (z.d.). Bitcoin Transaction Fees. Geraadpleegd op 26 december 2019, van Bitcoinfees.info website: https://bitcoinfees.info/

Coin Telegraph. (z.d.). Difference Between Bitcoin and Bitcoin Cash. Geraadpleegd op 26 december 2019, van Cointelegraph website: https://cointelegraph.com/bitcoin-cash-for-beginners/btc-bch-differences

Luke Dashjr. (2019, 21 mei). Briefly, Why Block Sizes shouldn't be too big. [Youtube]. Geraadpleegd van https://youtu.be/CqNEQS80-h4

Murabito, E. (2019, z.d.). Mining difficulty, Hash Power, Nonce Range and the like. An Introduction to Bitcoin Mining. Geraadpleegd op 6 juni 2019 van https://medium.com/bitcoin-cryptocurrencies-and-blockchain-technology/hash-power-nonce-range-and-mining-difficulty-c4c4e58775f3

Nakamoto, S. (2008). Bitcoin P2P e-cash paper. Geraadpleegd op 26 december 2019, van Nakamotoinstitute.org website: https://satoshi.nakamotoinstitute.org/emails/cryptography/2/

Nakamoto, S. (2010). Re: Bitcoin minting is thermodynamically perverse. [Online forum comment]. Bericht geplaatst op https://satoshi.nakamotoinstitute.org/posts/bitcointalk/327/

Nodes.com. (z.d.). Blockchain Nodes: How They Work (All Types Explained) Geraadpleegd op 15 december 2019, van Nodes.com website: https://nodes.com/

Popper, N. (2017, 25 juli). Some Bitcoin Backers Are Defecting to Create a Rival Currency. *The New York Times*. Geraadpleegd van https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html

SFOX. (2019, 3 juni). Bitcoin Cash vs. Bitcoin SV: Six Months after the Hash War. Geraadpleegd op 26 december 2019, van Medium website: https://blog.sfox.com/bitcoin-cash-vs-bitcoin-sv-six-months-after-the-hash-war-e6d92a03b891

Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The Carbon Footprint of Bitcoin. *Joule*, *3*(7), 1647–1661. https://doi.org/10.1016/j.joule.2019.05.012

Taaki, A. (2013). *The libbitcoin Manifesto*. Geraadpleegd van https://libbitcoin.dyne.org/libbitcoin-manifesto.pdf

van Wirdum, A. (2018, 14 november). When the Fork Forks: What You Need to Know as Bitcoin Cash Goes to War. Geraadpleegd op 26 december 2019, van Bitcoin Magazine website: https://bitcoinmagazine.com/articles/when-fork-forks-what-you-need-know-bitcoin-cash-goes-war

Iconen

Computer gemaakt door Prettycons van www.flaticon.com

Mijner gemaakt door Srip van www.flaticon.com

5. Cryptografie: symmetrische, asymmetrische en Zero-Knowledge Proofs

"We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature."

- Whitfield Diffie en Martin Hellman (1976)

"When privacy is outlawed, only outlaws will have privacy."

- Philip Zimmermann (1991)

5.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat symmetrische cryptografie is en wat de grootste zwakheden hiervan zijn.
- Wat asymmetrische (public key) cryptografie is en hoe dit wordt toegepast om Bitcoin-transacties te ondertekenen.
- Wat de beveiligingsdoelen zijn van public key cryptografie.
- Waar een Bitcoin wallet uit bestaat.
- Hoe public key cryptografie wordt toegepast, in bijvoorbeeld Public Key Infrastructuur, om vertrouwen te creëren binnen een netwerk van partijen die elkaar niet eerder hebben ontmoet.
- Wat Zero-Knowledge Proofs (ZKP) zijn en hoe deze kunnen worden toegepast om privacy te waarborgen op de blockchain.
- Dat cryptografie van wezenlijk belang is om onze privacy te kunnen waarborgen in de digitale wereld, maar dat dit tegelijkertijd vaak op gespannen voet staat met de wens van de overheid om toezicht te houden op haar burgers.
- Hoe je je eigen e-mails eventueel kunt versleutelen om je privacy te waarborgen.

Inleiding

In dit hoofdstuk komen de drie meest gangbare cryptografische ontwikkelingen aan bod.

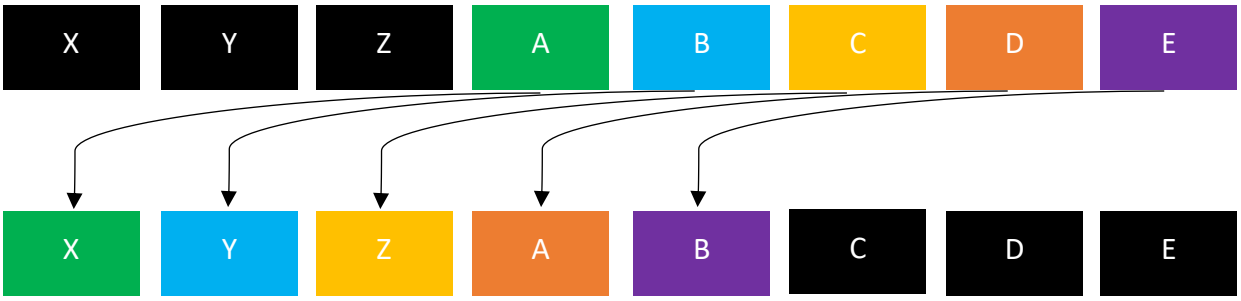
Eerst behandelen we in paragraaf 5.2 symmetrische cryptografie en vervolgens in 5.3 asymmetrische of public key cryptografie. In paragraaf 5.4 komt aan bod hoe public key cryptografie wordt toegepast bij de Bitcoin blockchain in het ondertekenen van Bitcoin-transacties. Daarna bespreken we Zero-Knowledge Proofs (ZKP) in paragraaf 5.5, als zijnde een nieuwe vorm van cryptografie, waarbij het mogelijk is voor een partij om te bewijzen dat deze beschikt over een specifieke waarheid of kennis, zonder dat deze waarheid of kennis onthuld hoeft te worden. Deze vorm van cryptografie is uitermate geschikt om privacy te bewaken. Denk hierbij bijvoorbeeld aan het kunnen verifiëren wat je leeftijd of postcode, zonder deze daadwerkelijk te hoeven onthullen aan een verifieerder. In paragraaf 5.6 geven we de algemene geschiedenis weer van public key cryptografie en hoe de eerste en tweede crypto-oorlogen zijn ontstaan. Tot slot sluiten we af in paragraaf 5.7 met een samenvatting van het hoofdstuk en een lijst van belangrijke begrippen en bronnen.

5.2 Symmetrische cryptografie

Het gebruik van cryptografie is al meer dan 4.000 jaar oud. In het oude Egypte werd er bijvoorbeeld gebruikgemaakt van hiërogliefen voor de decoratie van tombes van overleden koningen. Deze hiërogliefen vertelden het levensverhaal van de desbetreffende koning. Ze waren echter niet bedoeld om geheimen te bewaken, maar om extra gewichtigheid te geven aan de teksten.

5.2.1 Klassiek voorbeeld: Caesarrotatie

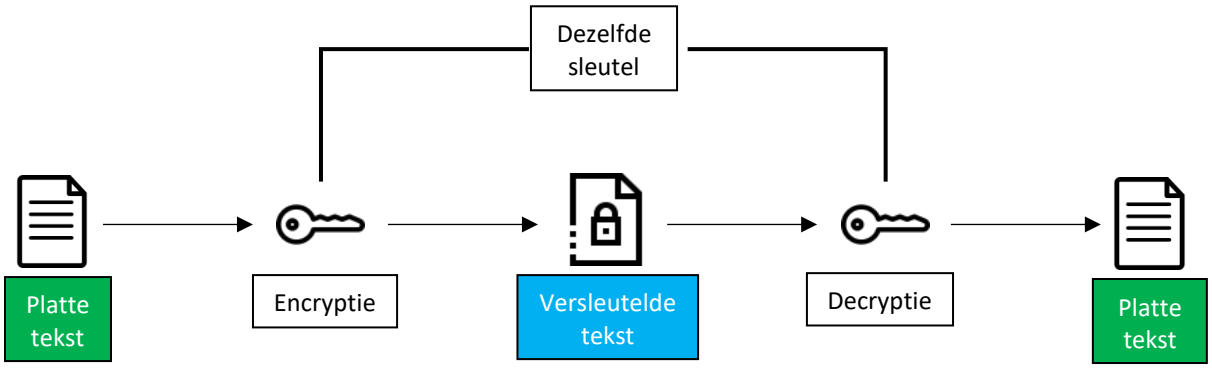
Een ander klassiek voorbeeld is de Caesarrotatie. Deze werd in de eerste eeuw voor Christus gebruikt door Julius Caesar om berichten van militair belang te delen met zijn veldheren. Het principe van de Caesarrotatie was simpel. De ontvanger van het bericht moest elke letter vervangen met een letter die een vast aantal posities verderop in het alfabet stond. Julius Caesar maakte zelf gebruik van een rotatie naar rechts van drie. A werd dan in de encryptietekst bijvoorbeeld een D, E een H, X een A, etc. Een dergelijke rotatietechniek werd ook toegepast door de Romeinse keizer Augustus. Hij maakte echter gebruik van een rotatie van één naar links, waarbij hij dus A schreef voor B, B voor C, etc.



Afbeelding 51: Caesarrotatie met een rotatie van drie naar links. Hierbij wordt A dus bijvoorbeeld X in de encryptietekst en B wordt Y.

Een Caesarrotatie is in vergelijking tot moderne encryptiemethoden vrij gemakkelijk te breken. Om erachter te komen of er sprake is van een Caesarrotatie zou je bijvoorbeeld een frequentieanalyse van letters kunnen maken. Zo zie je of de letters in de encryptietekst eenzelfde frequentiepatroon hebben als een typisch Nederlandse of Engelstalige tekst. Verder heeft elk letter in een Caesarrotatie slechts 25 mogelijkheden. Je kunt een tabel maken waarbij je alle 25 rotatiemogelijkheden opschrijft. Een computer kan dat binnen een mum van tijd uitwerken.[52]

5.2.2 Nadelen van symmetrische cryptografie



Afbeelding 52: Symmetrische encryptie. De verzender van het bericht heeft dezelfde sleutel als de ontvanger van het bericht. De sleutel wordt gebruikt voor zowel encryptie als decryptie.

Cryptografen maakten tot aan de jaren 70 van de 20e eeuw alleen gebruik van ***symmetrische cryptografie***. Bij symmetrische cryptografie kun je met eenzelfde sleutel, de ***secret key*** (geheime sleutel), zowel een bericht ***encrypten*** (versleutelen) als een bericht ***decrypten***

[52] Zie de volgende webapplicatie, waarmee je op eenvoudige wijze je eigen tekst kunt encrypten met de Caesarrotatie: https://www.xarg.org/tools/caesar-cipher/.

(ontsleutelen). Voor de ontvanger is het noodzakelijk om dezelfde secret key te hebben als hij het bericht van de verzender wil kunnen decrypten en lezen.

Nadelen van een dergelijk systeem zijn, ten eerste, dat de secret key op de één of andere manier – liefst over een beveiligd kanaal – moet worden gedeeld tussen de verzender en ontvanger, voordat berichten veilig kunnen worden uitgewisseld. Een tweede nadeel is dat de secret key zich op twee plekken bevindt. Het derde nadeel is dat jij, als verzender van een bericht, de ontvanger van het bericht moet vertrouwen dat deze de secret key niet steelt of kopieert. Het is vergelijkbaar met het delen van je huissleutel, waarbij je erop vertrouwt dat de ander je sleutel niet steelt of kopieert. Om deze reden zou het verstandig zijn om voor iedereen met wie je communiceert een aparte secret key te gebruiken. Deze drie aspecten verhogen de kans aanzienlijk dat de secret key in handen komt van ongewenste personen. Daarnaast is er een schaalbaarheidsprobleem. Een dergelijk systeem zou betekenen dat gebruikers die communiceren met vele partijen allemaal een database moeten bijhouden met een veelvoud aan secret keys. Om een dergelijk systeem gebruiksvriendelijk te laten werken, is er een infrastructuur van gespecialiseerde distributiecentra nodig die elke keer secret keys genereren, voordat twee mensen een privégesprek willen initiëren. Het vierde grote nadeel van symmetrische cryptografie is dat zo'n infrastructuur beduidend gecentraliseerd is, een Single Point of Failure bevat en de distributiecentra over veel gegevens beschikken die hackers aan zullen trekken.

Nadelen van symmetrische cryptografie

1. De secret key moet worden gedeeld tussen de verzender en ontvanger, voordat berichten veilig kunnen worden uitgewisseld, liefst over een beveiligd kanaal.
2. De secret key bevindt zich op twee plekken.
3. De verzender van het bericht moet de ontvanger vertrouwen dat hij de secret key niet steelt of kopieert.
4. Het is niet schaalbaar voor bijvoorbeeld grootschalige e-commerce.

De Caesarrotatie wordt ook geschaard onder symmetrische cryptografie, omdat je het bericht zowel kunt versleutelen als ontsleutelen met een enkele secret key – bijvoorbeeld rotatie van één naar links. Een moderner voorbeeld van symmetrische encryptie is de ***Data Encryption Standard*** (DES) die op de markt kwam in 1975. De DES is ontwikkeld door IBM en is voornamelijk bedoeld om elektronische communicatie tussen bedrijven als banken en andere grote financiële organisaties te beschermen. Tot de komst van DES was cryptografie voornamelijk een bezigheid van overheden om staatscommunicatie te beschermen. In eerste

instantie werd de DES goed ontvangen door cryptografen, totdat het encryptiesysteem nader werd onderzocht en mensen erachter kwamen dat de Amerikaanse inlichtingendienst, de ***National Security Agency*** (NSA), zelf invloed had gehad op de ontwikkeling ervan en dat de encryptiesleutel slechts 56 bits lang was (Levy, p. 53, 2001).[53] Dat betekent dat er 2^{56} aantal mogelijke sleutelcombinaties zijn.[54]

Whitfield Diffie en Martin Hellman, twee Stanford University professoren die een jaar later public key cryptografie uitvonden, dachten dat de sleutel niet lang genoeg was en geloofden dat geavanceerde computers in staat zouden zijn om al de verschillende sleutelcombinaties te proberen, totdat de juiste is gevonden. Een aanval door alle verschillende sleutelcombinaties uit te proberen, wordt ook wel een ***brute-force search*** genoemd. Als de juiste sleutel eenmaal is gevonden, kun je deze gebruiken om berichten die zijn encrypted te decrypten en te lezen. Het proces of de studie om een sleutel of bericht te kraken, heet ***cryptanalyse***.[55]

5.3 Asymmetrische cryptografie (public key cryptografie)

Kort na de publicatie van DES, werd ***asymmetrische encryptie*** – ook wel ***public key cryptografie*** genoemd – uitgevonden door Whitfield Diffie en Martin Hellman.[56] Dit was een grote revolutie

[53] Het algoritme voor de DES werd ontwikkeld door IBM en met navolging van de Amerikaanse inlichtingendienst, de NSA, aangepast. IBM maakte oorspronkelijk gebruik van 64-bit sleutelgroottes, maar heeft deze na consultatie met de NSA verlaagd naar sleutelgroottes van 56-bit om de encryptie te verzwakken. (Corrigan-Gibbs, 2014) Veel cryptologen waren sceptisch over de DES. Martin Hellman, één van de twee uitvinders van public key cryptografie uitte zijn ongenoegen als volgt in een brief (1976) aan de toenmalige minister van Economische Zaken, Elliot Richardson:

> "I am writing to you because I am very worried that the National Security Agency has surreptitiously influenced the National Bureau of Standards in a way which seriously limited the value of a proposed standard, and which may pose a threat to individual privacy. I refer to the proposed Data Encryption Standard, intended for protecting confidential or private data used by non-military federal agencies. It will also undoubtedly become a de facto standard in the commercial world. … I am convinced that NSA in its role of helping NBS design and evaluate possible standards has ensured that the proposed standard is breakable by NSA."

[54] Eén bit kan een 0 of een 1 zijn. Als een sleutel bestaat uit 56 bits, dan zijn er 2^{56} mogelijkheden.

[55] Zie ook *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (Electronic Frontier Foundation, 1998) om meer te lezen over hoe DES kan worden gekraakt en hoe de Amerikaanse overheid het volk heeft voorgelogen over de veiligheid van DES-encryptie.

[56] Diffie en Hellman kregen voor hun bijdrage aan moderne cryptografie de ACM A.M. Turing prijs (2015) uitgekeerd. De prijs is de hoogste onderscheiding binnen de computerwetenschappen.

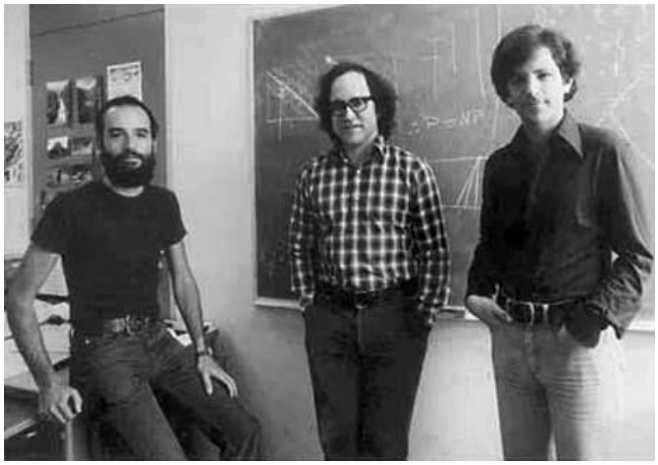
in cryptografie, omdat er tot dan het paradigma heerste dat er altijd een gedeelde secret key moest zijn voor de beveiliging van de communicatie tussen een verzender en ontvanger. De vraag die Diffie en Hellman proberen op te lossen, is kort gezegd hoe je een beveiligde communicatie kunt bewerkstelligen over een onbeveiligd kanaal, wanneer de twee communicerende mensen nooit eerder contact met elkaar hebben gehad.[57] De public key cryptografie staat aan de basis van vele moderne encryptietechnieken als PGP, SSL en Internet Protocol Security (IPsec).[58] Daarnaast gaf de ontdekking ook momentum aan cryptografisch onderzoek buiten de kringen van geheime inlichtingendiensten.

Public key cryptografie werd geïntroduceerd door Diffie en Hellman in het artikel 'New Directions in Cryptography' (1976). Geïnspireerd door het werk van Diffie en Hellman, hebben drie jonge professoren aan de Massachussets Institute of Technology (MIT) genaamd Ron

[57] Een UC Berkeley student, Ralph Merkle, hield zich in die tijd ook bezig met de vraag. Zijn oplossing betrof het creëren van ruis over de communicatielijn. Het concept werkt als volgt:
Bob en Alice willen communiceren. Bob is de verzender en Alice is de ontvanger van een geheim berichtje. Eve is een afluisteraar die toegang heeft tot alles wat door het communicatiekanaal tussen Bob en Alice wordt verzonden. Om ruis te creëren, maakt Bob voor de communicatie puzzels. Elke puzzel is een berichtje, dat is versleuteld met een kleine sleutel, die in relatief korte tijd kan worden gekraakt middels een brute-force aanval. Bob creëert wel miljoenen van zulke puzzels en stuurt ze allemaal naar Alice. Alice kiest één puzzel, voert een brute-force aanval uit en decrypt deze met haar computer. De oplossing is een lange reeks van nummers. Naast deze lange reeks zitten ook een identifier (bijv.: "Ik ben Puzzel No. 3") en een lange digitale sleutel. Alice stuurt een bericht terug naar Bob die precies weet welke puzzel welk nummer is, en dat hij moet kijken naar de sleutel van "Puzzel No. 3". Op dit punt beschikken zij beiden over een gedeelde secret key. Eve die als afluisteraar de miljoenen puzzels kan onderscheppen, kan ook horen dat het "Puzzel No. 3" is. Echter, weet ze niet welke van de miljoenen puzzels het betreft en zou het te veel tijd kosten om, op zoek naar deze puzzel, alle puzzels te kraken. Op deze manier zouden dus twee mensen die op voorhand nog geen secret key hebben gedeeld toch op veilige wijze een secret key kunnen delen over een onbeveiligd communicatiekanaal. (Levy, 2001, pp. 205-205)
Merkle is onder andere bekend als uitvinder van Merkle trees, een concept dat is toegepast in Bitcoin en uitvoerig is besproken in de Bitcoin White Paper. Je kunt in een intermezzo van hoofdstuk 3 lezen hoe Merkle trees werken.
[58] PGP staat voor Pretty Good Privacy, één van de meest gebruikte encryptieprogramma's voor onder andere e-mailbestanden en geklassificeerde documenten. Het werd onder andere gebruikt door Edward Snowden en de journalist Glenn Greenwald bij de overhandiging van topgeheime documenten van de NSA in 2013.
SSL, Secure Sockets Layer, was ontwikkeld door Netscape om privédocumenten te versturen via het internet. Het creëert een beveiligde verbinding tussen een server en een client. De meeste webbrowsers ondersteunen SSL. URL's die een SSL-connectie vereisen, beginnen met Hypertext Transfer Protocol Secure, HTTPS. De gebruiker kan een HTTPS-connectie herkennen aan het gesloten sloticoontje voor de Uniform Resource Locator, URL.
IPsec is een beveiligingsstandaard voor het internetprotocol (IP).

Rivest, Adi Shamir en Leonard Adleman het welbekende RSA public key cryptografiesysteem ontwikkeld in 1977.

Afbeelding 53: Van links naar rechts: Ralph Merkle, Martin Hellman en Whitfield Diffie. (Foto: Chuck Painter/Stanford News Service)



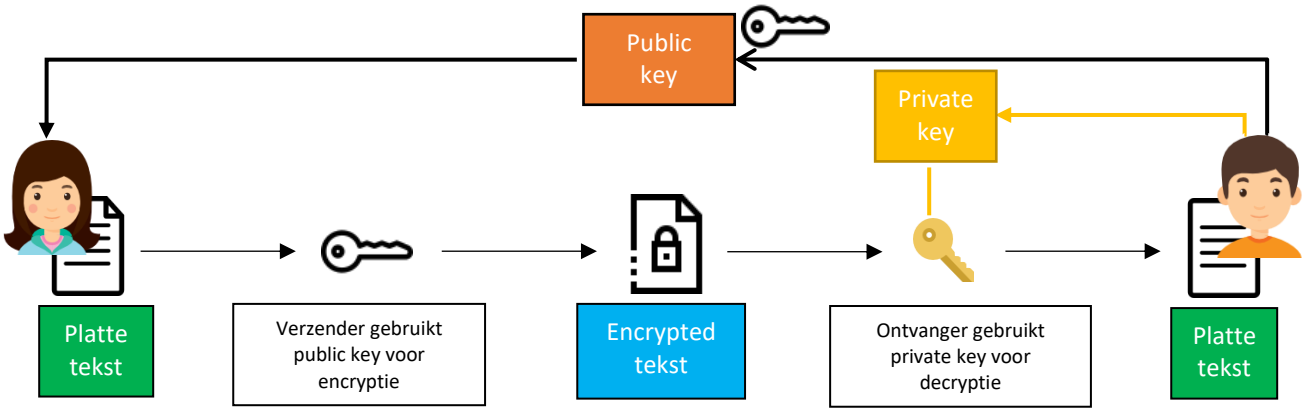
Afbeelding 54: Van links naar rechts: Adi Shamir, Ron Rivest en Len Adleman. (Foto: Dan Wright's RSA Algoritme cursus op imps.mcmaster.ca)

Terwijl er bij symmetrische encryptie gebruik wordt gemaakt van één sleutel, wordt er bij public key cryptografie gebruikgemaakt van twee verschillende sleutels die wiskundig met elkaar corresponderen. Eén sleutel kun je publiekelijk beschikbaar stellen en de ander moet je privé bewaren. Je gebruikt een ***private key*** (privésleutel) die je nooit deelt met een ander om de data die je ontvangt te decrypten. Daarnaast gebruik je een corresponderende ***public key*** (publieke sleutel) die publiekelijk bekend mag zijn om de data te versleutelen. Wat de public key cryptografie zo elegant maakt, is dat de encryptiefunctie een ***tweerichtingsfunctie*** is: je kunt met de public key het bericht encrypten en met de private key decrypen. Daarnaast kun je vanuit de public key niet achterhalen wat de private key is.[59] Hierdoor kun je deze public key vrij delen met partijen met wie je versleutelde data wil uitwisselen. Deze partijen gebruiken jouw public key dan om de data te versleutelen, alvorens ze de data sturen naar jou, zodat jij

[59] De wiskundige functie waarbij je een bericht als input kunt stoppen en als resultante een output krijgt die je niet meer kan omzetten naar het originele bericht, wordt een eenrichtingsfunctie genoemd. Dit is het geval bij hashing. Bij goede cryptografische functies kan het soms, met huidige computers, miljoenen jaren of meer duren om het bericht te kraken.

het kunt ontsleutelen met je private key. Je kunt het enigszins vergelijken met de bank die een sleutel heeft voor een kluis die je binnen de bank bewaart. Deze sleutel is privé en wordt met niemand gedeeld. Daarnaast geeft de bank jou een publieke sleutel. Wanneer je de kluis wil openen om bij je kostbaarheden te komen, moet je zowel de private key van de bank als jouw sleutel tegelijkertijd gebruiken.

In termen van Alice en Bob, onze fictieve figuren die geheime berichten naar elkaar willen sturen, werkt public key cryptografie als volgt. Alice wil veilig kunnen communiceren met Bob. Hiervoor heeft zij de public key van Bob nodig. Bob heeft een uniek sleutelpaar: een private key en een public key. Hij stuurt haar zijn public key op. Dit kan over een onbeveiligd communicatiekanaal. Alice gebruikt de public key van Bob om haar bericht te encrypten dat alleen degene met de bijbehorende private key het bericht kan decrypten. Het doet er niet toe of Eve, de afluisteraar in het onbeveiligde communicatiekanaal, de public key heeft onderschept, omdat zij niet over de private key van Bob kan beschikken voor de decryptie van het bericht. Zie in de volgende schematische weergave hoe dit te werk gaat.



Afbeelding 55: Asymmetrische (public key) cryptografie voor versleutelde berichten. De ontvanger, Bob, beschikt over een corresponderende private key en een public key. Hij verstuurt zijn public key naar de verzender over een onbeveiligd communicatiekanaal. De verzender, Alice, gebruikt de public key om haar bericht te encrypten en stuurt het versleutelde bericht naar Bob. Bob gebruikt vervolgens zijn private key om het versleutelde bericht te decrypten.

5.3.1 Digitale handtekeningen

Public key cryptografie gaat echter verder dan alleen het kunnen versleutelen van berichten en het veilig versturen hiervan. Het kan ook worden gebruikt om de verzender van een elektronisch bericht te authentiseren. Als Alice haar bericht niet zou versleutelen met de public key van iemand anders, maar met haar eigen private key, dan kan het versleutelde bericht worden ontsleuteld met de public key van Alice. Mocht je dus een bericht ontvangen van een

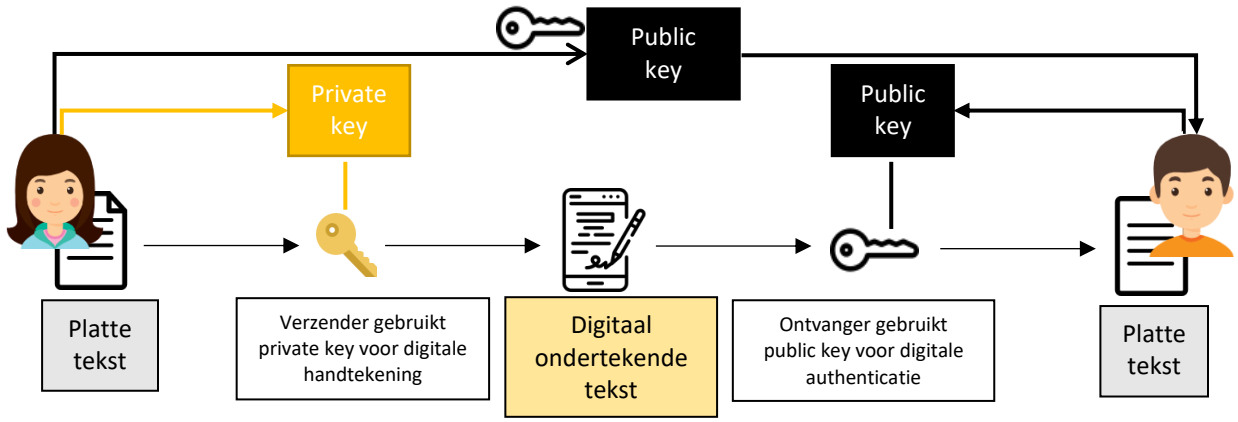
persoon, John Locke, en willen weten of dit bericht daadwerkelijk van John Locke afkomt, dan kun je zijn public key opzoeken en gebruiken om zijn bericht te decrypten. Als de resultante hiervan platte tekst is, dan weet je dat het bericht van John Locke afkomt – ervan uitgaande dat John Locke de enige persoon is op de wereld met de enige private key die een dergelijk bericht kan produceren. Met andere woorden: het toepassen van een private key op een bericht is equivalent aan het zetten van een ***digitale handtekening*** (digital signature).

Digitale handtekeningen bieden de volgende drie belangrijke beveiligingsaspecten:

1. Het biedt bewijs wie het bericht of document heeft ondertekend als de digitale handtekening wordt gelinkt aan een identificeerbare identiteit.
2. Het biedt data-integriteit, omdat het aan kan tonen dat het bericht of document niet meer is gewijzigd sinds het ondertekenen.
3. Het legt onweerlegbaar vast dat de ondertekenaar het bericht of document heeft ondertekend. Hij kan niet ontkennen dat hij het heeft gedaan.

Er zijn twee belangrijke verschillen tussen deze digitale handtekening en de handtekening die je met pen en papier zet. De digitale handtekening kan ten eerste niet worden vervalst, tenzij de vervalser beschikt over de private key. Als er, ten tweede, een digitale handtekening wordt geplaatst met een private key, dan wordt het bericht versleuteld. Mocht iemand het bericht onderscheppen en de originele platte tekst willen wijzigen, dan is dit mogelijk als hij deze eerst decrypt met de corresponderende public key. Om het daarna te versturen met een juiste digitale handtekening, zal hij echter wel ook toegang moeten krijgen tot de private key. De private key is echter, als het goed is, alleen in handen van degene die het origineel heeft ondertekend. Omdat een digitaal ondertekend bericht alleen kan worden geproduceerd door degene die de private key heeft, kunnen we er redelijkerwijs vanuit gaan dat het ondertekende bericht daadwerkelijk van de private-keyeigenaar komt. Daardoor is het met de komst van public key cryptografie voor het eerst mogelijk om officiële digitale geldtransacties of documenten als contracten en ontvangstbewijzen te ondertekenen over een computernetwerk. Zonder public key cryptografie zou de huidige e-commerce, een globale markt van ongeveer €2.500 miljard in 2018, onmogelijk zijn geweest.[60]

[60] Zie 'Global ecommerce sales grow 18% in 2018' (Young, 2019).



Afbeelding 56: Asymmetrische (public key) cryptografie voor digitale handtekening. De verzender, Alice, beschikt over een corresponderende private key en public key. Zij gebruikt haar private key om haar bericht te voorzien van een digitale handtekening. Daarnaast heeft Alice haar public key beschikbaar gemaakt voor iedereen die wil authentiseren dat haar berichten daadwerkelijk van haar afkomen. De ontvanger, Bob, gebruikt de public key van Alice om haar bericht te decrypten. Als het resultaat een platte tekst is, dan weet hij dat de tekst alleen kan zijn ondertekend door de persoon die de corresponderende private key bezit – in dit geval is dat Alice.

5.3.2 Beveiligingsdoelen van public key cryptografie

Public key cryptografie heeft kort gezegd de volgende beveiligingsdoelen.

Beveiligingsdoelen van public key cryptografie

1. *Vertrouwelijkheid*: de data is niet beschikbaar voor ongeautoriseerde personen of processen.
2. *Integriteit*: de data is niet gewijzigd.
3. *Entiteitauthenticatie*: het proces waarbij een verifieerder wordt verzekerd van de ware identiteit van een entiteit op het internet. Een entiteit kan een website, een organisatie, een gebruiker of zelfs een fysiek apparaat zijn, die is verbonden met het internet.
4. *Data-authenticiteit*: het proces waarbij de integriteit van de data is gewaarborgd en waarbij de bron van de data kan worden vastgesteld. Banken moeten bijvoorbeeld de authenticiteit van elektronische financiële transacties kunnen achterhalen.
5. *Onweerlegbaarheid*: het voorkomt dat een entiteit ontkent dat deze een bepaalde actie heeft uitgevoerd. In veel landen zijn elektronische contracten net zo bindend als papieren contracten. Het moet zo zijn dat partijen die betrokken zijn bij een elektronisch contract niet in staat zijn om het contract later te ontkennen.

Public key cryptografie kan aan al deze beveiligingseisen voldoen. (Buchmann et al., 2013, pp. 2-5) Hiervoor is er een ***Public Key Infrastructuur*** (PKI) opgesteld. Meer uitleg hierover is te vinden in het volgende intermezzo.

Naast eerder genoemde beveiligingsdoelen kun je nog denken aan andere doelen, zoals anonimiteit en ondwangmatigheid. Het is bijvoorbeeld noodzakelijk dat mensen bij verkiezingen kunnen stemmen op de partij van hun voorkeur, zonder dat hun identiteit bekend is. Daarnaast moet het zo zijn dat mensen niet kunnen worden gedwongen om een bepaalde stem uit te voeren.

Verschil tussen hashing en encryptie (versleuteling)

Hashing is een eenrichtingsfunctie. Dit betekent dat het hashen van data leidt tot een hash-output. Vanuit de output is het niet meer mogelijk om de originele data te achterhalen. Dat maakt hashing uitermate geschikt voor het creëren van een unieke vingerafdruk van de data.

Public key cryptografie is daarentegen een tweerichtingsfunctie. Je kunt met de public key het bericht encrypten en met de private key decrypten. Daarnaast kun je vanuit de public key niet achterhalen wat de private key is. Dat maakt public key cryptografie uitermate geschikt voor het delen van geheime berichten over een onbeveiligd kanaal.

Intermezzo: Public Key Infrastructuur (PKI)

Wij zijn er in het voorgaande van uitgegaan dat de persoon met wie Alice veilig wil communiceren, Bob, daadwerkelijk Bob is. Hoe weten we zeker dat er niet iemand anders is die zich voordoet als Bob en zijn eigen public key deelt met Alice, waarna Alice haar geheime communicatie deelt met hem? Voor de beveiliging van onze huidige internetcommunicatie is er een infrastructuur van public keys opgezet die dergelijke aanvallen tegengaat. Deze infrastructuur wordt ook wel de Public Key Infrastructuur (PKI) genoemd. Dit is een set aan standaarden, procedures en software voor het authentiseren van gebruikers middels public key cryptografie en digitale certificaten. Zonder PKI zou het onmogelijk zijn om veilige gebruik te maken van zaken als e-commerce en eHealth.

Hoe werkt PKI?

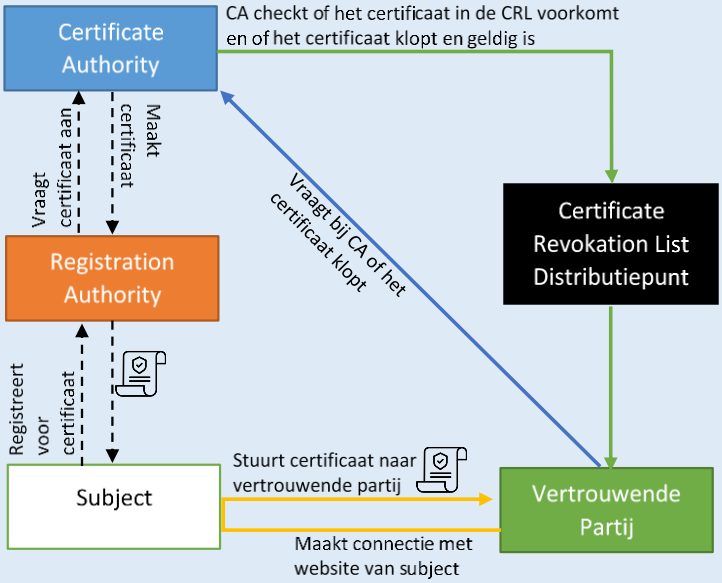
Een belangrijke taak van PKI is dat het authenticiteitsbewijzen van public keys biedt. Digitale certificaten zijn geassocieerd met personen of bedrijven en zijn te vergelijken met een identiteitskaart waarmee personen, websites of bedrijven zichzelf kunnen identificeren. De beveiligde connecties tussen twee communicerende partijen, bijvoorbeeld de bezoeker van een website in de website zelf, is mogelijk nadat de identiteiten van beide partijen zijn geverifieerd op basis van de certificaten. Hierbij spelen digitale certificaten een grote rol. Een voorbeeld van een dergelijk certificaat is het SSL-certificaat. Een certificaat moet voldoen aan een bepaalde standaard – de X.509-standaard – en bevat minimaal de volgende gegevens:

1. De naam van het subject, bijvoorbeeld de persoon of organisatie.
2. De public key die is gekoppeld aan de entiteit.
3. Het cryptografisch algoritme waarmee de public key wordt gebruikt.
4. Het serienummer van het certificaat.
5. De geldigheidsperiode van het certificaat.
6. De naam van de uitgever van het certificaat die het certificaat heeft ondertekend.
7. Restricties die van toepassing zijn op het gebruik van de public key in het certificaat.

Binnen PKI zijn er ***certificate authorities*** (CA) die gespecialiseerd zijn in het uitgeven, opslaan en ondertekenen van deze digitale certificaten. In het certificaat zit een public key die correspondeert met de gebruikers. Er zijn wereldwijd meer dan 1.200 verschillende CA's. Een gebruiker vraagt een certificaat aan bij een ***registration authority*** (RA), vaak met een bewijs dat ze zijn wie ze zijn. Nadat de RA de gebruiker heeft geverifieerd, geeft de CA het certificaat uit waarmee het subject zich kan identificeren. Het subject kan een persoon,

bedrijf of object zijn, die verbonden is met het internet. Alle certificaten die worden aangevraagd, ontvangen en ingenomen door de CA en RA worden bewaard in een versleutelde database met certificaten. Certificaten die zijn ingetrokken – bijvoorbeeld omdat ze zijn verlopen of anderzijds niet meer te vertrouwen zijn – worden bijgehouden in een ***certificate revocation list*** (CRL).

De CA ageert als een vertrouwde derde partij voor de eigenaar van het certificaat, het subject en voor de vertrouwende partij die wil communiceren met het subject. Als een vertrouwende partij, degene die gebruik wil maken van de website van het subject, connectie maakt met het subject ontvangt hij het certificaat van het subject. Om er zeker van te zijn dat het subject is wie hij zegt dat hij is, vraagt de vertrouwende partij nog bij de CA of het certificaat overeenkomt met wat de CA heeft geregistreerd. Als dit klopt, wordt er een beveiligde verbinding gelegd tussen het subject en de vertrouwende partij. Onderstaand vind je een versimpelde weergave van de belangrijkste aspecten van PKI.



Afbeelding 57: Grafische weergave van het PKI-proces.

Het nadeel van PKI is dat het gecompliceerd is en er vertrouwen moet zijn dat de CA's hun rol goed vervullen. CA's kunnen een certificaat ondertekenen voor iedere persoon of elke computer. Ook zijn CA's wereldwijd verspreid en onderhevig aan nationale wetgevingen. Wat gebeurt er als een CA is gehackt of als een overheid een CA onder druk zet om een public key van een subject, bijvoorbeeld Google, te geven? Hiermee zou de overheid zich kunnen voordoen als Google. Zie hoofdstuk 12 over hoe blockchain PKI veiliger kan maken.

5.4 Hoe wordt public key cryptografie gebruikt bij Bitcoin?

Wij hebben eerder al gesproken hoe er gebruik wordt gemaakt van hash-cryptografie bij het vinden van (a) een geldige hash en daarmee het recht voor de mijner om een volgend blok te mogen aanmaken en (b) het aan elkaar vastketenen van datablokken waarbij de previous hash verwijst naar de hash-waarde van het vorige blok. Als iemand de blockchain wil manipuleren door valse data in een datablok te zetten, dan merkt het netwerk dat de hash van het betreffende datablok is veranderd. Naast de eerder genoemde cryptografische techniek maakt de Bitcoin blockchain ook gebruik van public key cryptografie bij bijvoorbeeld het aanmaken van een Bitcoin-adres en het ondertekenen van een transactie.

Bij het aanmaken van een Bitcoin-adres worden er twee corresponderende keys gegenereerd.[61] Deze keys zijn de public key en de private key van het desbetreffende Bitcoin-adres. Vanuit de public key wordt het Bitcoin-adres verkregen.[62] Je kunt jezelf identificeren met het Bitcoin-adres en dat vrij delen met anderen, zodat zij Bitcoin naar jou kunnen overmaken. Als houder van de private key kun je jezelf identificeren als de eigenaar van het Bitcoin-adres, en kun je je transacties digitaal ondertekenen. Het proces verloopt als volgt:

1. De private key wordt gebruikt om de data van jouw transactie te ondertekenen. Hieruit volgt een hash.
2. De hash is een digitale handtekening. Goed om hierbij te weten is dat niemand je private key kan achterhalen als ze je digitale handtekening weten.
3. Iedereen kan met jouw digitale handtekening, de transactiedata en jouw public key verifiëren dat de digitale handtekening en de public key corresponderen met eenzelfde private key. Daarmee kunnen ze dus achterhalen dat je de transactie hebt ondertekend met een legitieme private key.

Het is belangrijk om te weten dat je zonder digitale handtekening geen transacties kunt uitvoeren. Aangezien de digitale handtekening alleen mogelijk is met een private key, dien je zorgvuldig om te gaan met je private key. Het is verder ook niet mogelijk om vanuit je public key de private key te achterhalen.

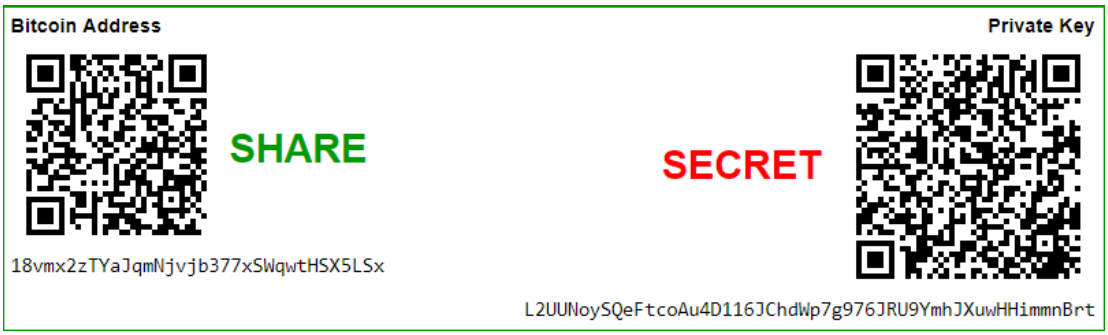
---

[61] Bij Bitcoin wordt het private en public sleutelpaar verkregen door middel van ***Elliptic Curve Digital Signature Algorithm*** (ECDSA).

[62] Als je meer wil weten over hoe je een Bitcoin-adres kunt genereren vanuit de public key, zie: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses#How_to_create_Bitcoin_Address.

Je kunt het Bitcoin-adres het best vergelijken met een rekeningnummer en de private key met de pincode waarmee je toegang krijgt tot je rekeningnummer en waarmee je ook transacties kunt uitvoeren. Als je je private key kwijt raakt, dan verlies je dus de toegang tot je Bitcoins.

In de volgende afbeelding zie je een Bitcoin wallet, bestaande uit een Bitcoin-adres en een private key. De Bitcoin wallet uit de afbeelding wordt een paper wallet genoemd, omdat de wallet bedoeld is om uitgeprint en bewaard te worden in een offline omgeving. Je wallets offline bewaren is veiliger, omdat deze niet gestolen kan worden door online hackers en niet verloren gaat als je computer crasht of stukgaat.



Afbeelding 58: Bitcoin paper wallet, aangemaakt op www.bitaddress.org. Het Bitcoin-adres is vergelijkbaar met een rekeningnummer. Als iemand Bitcoin naar je wil overmaken, dan moet deze persoon de Bitcoin overmaken naar dit adres. Met de private key kun je je Bitcoin-adres openen, heb je toegang tot de Bitcoins die daarop staan en kun je je Bitcoins middels een digitale handtekening versturen; digitaal ondertekenen. Om deze reden is het belangrijk dat je je private key met niemand deelt.

5.4.1 Multisignature

Het Bitcoin-netwerk ondersteunt ook ***multisignature***. Zoals het woord al doet vermoeden, zijn er bij multisignatures meer dan één digitale handtekening van één key nodig om een Bitcoin-transactie uit te voeren. Zo kun je bijvoorbeeld zeggen dat een transactie door ten minste 2 van de 3 private keys moet worden ondertekend en deze private keys verdelen over verschillende mensen. Dit noemen we een 2-of-3 transactie.[63] Hiermee kan de verantwoordelijkheid van het bezit over Bitcoins worden verspreid over meerdere partijen. Dit is bijvoorbeeld handig wanneer een bedrijf om veiligheidsredenen niet wil dat maar één werknemer toegang heeft tot de Bitcoin wallet van het bedrijf. Een transactie heeft dan toestemming nodig van meerdere werknemers. Veel Bitcoin wallets hebben al multisignature geïmplementeerd.

[63] ***M-of-N transacties*** vereisen dat de transacties worden ondertekend door M aantal keys. 4-of-5 transacties betekent bijvoorbeeld dat er in totaal 5 keys zijn en dat minimaal 4 van de 5 keys de transactie moeten hebben ondertekend. ***M-of-N multisignature wallets*** zijn wallets die M-of-N transacties mogelijk maken.

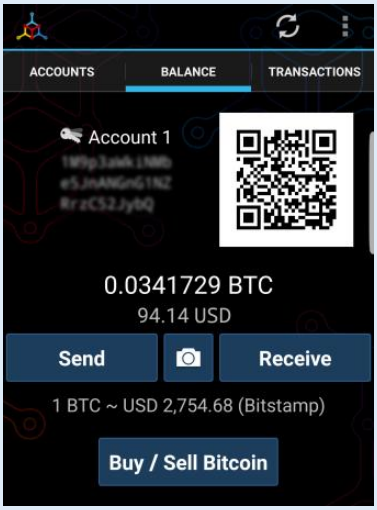
Intermezzo: Bitcoin wallets

Een wallet is een digitaal bestand die een private key bevat met de corresponderende public key. Het is ook mogelijk dat de wallet meerdere private keys en public keys bevat. Eigenlijk bevatten wallets niet echt Bitcoins. De Bitcoins bestaan namelijk op de blockchain.

Naast paper wallets bestaan er nog andere typen wallets zoals hardware wallets, desktop wallets, mobile wallets en web wallets. Een hardware wallet is een type wallet waarbij de private keys in een beveiligd stukje hardware worden opgeslagen. Omdat de private keys de hardware nooit verlaten, is dit een veilige manier om je Bitcoin mee op te slaan.
Voorbeelden zijn Trezor en Ledger.

Afbeelding 59: Een Trezor wallet die gekoppeld is aan een laptop. Zie https://trezor.io voor meer informatie.

Een desktop wallet is een wallet die je gebruikt vanaf je computer of laptop.
Een mobile wallet biedt een user interface op de mobiele telefoon en is over het algemeen het gebruikersvriendelijkst. Een voorbeeld hiervan is de Bitcoin wallet Mycelium.



Afbeelding 60: Een screenshot van de Mycelium mobile wallet.

Een web wallet wordt over het algemeen beheerd door een derde partij. Deze beheert de private keys voor jou en biedt een online omgeving, waarin je toegang krijgt tot je wallet. Je moet de partij wel vertrouwen dat die veilig omgaat met jouw private keys, je Bitcoins niet stelen en ze goed beveiligen.

5.5 Zero-Knowledge Proofs

Een nieuwere vorm van encryptie is ***Zero-Knowledge Proofs*** (ZKP). Deze werd het eerst geïntroduceerd door Shafi Goldwasser, Silvio Micali en Charles Rackoff, onderzoekers aan de Massachussetts Institute of Technology (MIT), in hun artikel, 'The Knowledge Of Interactive Proof Systems' (1989). Het is in essentie een methode waarbij een partij (de ***bewijzer***) kan bewijzen aan een andere partij (de ***verifieerder***) dat hij de waarheid van iets, bijvoorbeeld een bepaalde waarde, kan verifiëren zonder te onthullen dat hij kennis heeft van deze waarheid.

Kort gezegd voldoen Zero-Knowledge Proofs aan de volgende drie eigenschappen:

1. *Compleetheid*: als het statement waar is, dan zal de eerlijke verifieerder overtuigd zijn van dit feit door de eerlijke bewijzer.
2. *Betrouwbaarheid*: als het statement onwaar is, dan is de kans waarop een misleidende bewijzer de eerlijke verifieerder overtuigt dat deze waar is, minimaal.
3. *Zero-Knowledge*: als het statement waar is, dan leert de verifieerder niets anders dan dat het statement waar is.

Om het concept van Zero-Knowledge Proofs beter te bevatten, is het handig om de circulaire gang analogie te nemen van Jean-Jacques Quisquater et al.[64] Deze analogie gaat als volgt.

[64] De analogie van Quisquater et al. is beschreven in het fictieve verhaal,'How to Explain Zero-Knowledge Protocols to Your Children' (1998). Een andere bekende analogie die ook regelmatig wordt gebruikt om Zero-Knowledge Proofs uit te leggen, is 'Andrew Yao's millionaires' problem' (1982), de problematische situatie waarbij twee miljonairs van elkaar willen weten wie er rijker is, zonder te onthullen hoe rijk zij zelf zijn.
Weer een andere analogie is de analogie waarbij twee werknemers, Alice en Bob, exact dezelfde hoeveelheid werk verrichten met dezelfde kwaliteit. Echter, verdenken zij hun werkgever ervan dat hij hen niet dezelfde salarissen uitbetaalt. Nu willen zij van elkaar weten of deze verdenking klopt, zonder tegen elkaar te vertellen hoeveel zij exact verdienen.

Afbeelding 61: Structuur van de grot waarbij de magische deur is gesloten.

Afbeelding 62: Structuur van de grot waarbij de magische deur is geopend.

Peggy (de bewijzer) weet een geheim woord waarmee zij een magische deur in een grot kan openen. De grot heeft de vorm van een ring, waarbij de ingang splitst in een gang links en een gang rechts. Beide gangen lopen dood tegen een magische deur die, als deze er niet zou zijn, beide gangen met elkaar zou verbinden.

Victor (de verifieerder) wil weten of Peggy het geheime woord weet, waarmee zij de magische deur kan openen. Peggy, daarentegen, wil het geheime woord niet delen met Victor, maar wil wel kunnen aantonen dat zij het echt weet. Dit wordt opgelost door het volgende te doen. Victor wacht eerst buiten de grot, terwijl Peggy de grot ingaat. Victor mag niet zien of Peggy de linker- of de rechtergang neemt. Nadat Peggy één van beide gangen heeft genomen, komt Victor binnen en roept hij uit via welke kant – de linker- of rechtergang – hij wil dat Peggy uit de grot komt. Als Peggy het geheime woord echt weet, dan zal zij als het nodig is de geheime deur openen om altijd uit de grot te komen langs de kant die Victor wil. Als Peggy het geheime woord niet weet, dan heeft zij altijd 50% kans om via de juiste gang de grot uit te komen. Als we deze situatie meerdere keren zouden herhalen, bijvoorbeeld 20 keer, dan wordt de kans dat Peggy op basis van puur geluk steeds de juiste gang neemt $0{,}5^{20}$. Dat is bijna 1 op de miljoen. Om die reden kunnen we zeggen dat Peggy (vrijwel) absoluut zeker het geheime woord van de magische deur weet, zonder dat zij dit geheim hoeft te delen met Victor. Omdat er altijd een kleine kans is dat Peggy zonder het geheime woord te weten toch 20 of meerdere malen achter elkaar via de juiste gang de grot verlaat, zijn Zero-Knowledge Proofs probabilistische bewijzen en geen deterministische bewijzen. Goede Zero-Knowledge Proofs gebruiken technieken die de kans dat een bewijzer op basis van puur geluk de verifieerder kan overtuigen, verkleint tot een verwaarloosbaar percentage.

Waarom zijn Zero-Knowledge Proofs zo relevant voor blockchain? Zero-Knowledge Proofs zijn ideaal om informatie uit te wisselen tussen verschillende partijen, zonder dat ze de data zelf uitwisselen. Met andere woorden: Zero-Knowledge Proofs maken het mogelijk voor gebruikers van blockchainapplicaties om hun privacy te waarborgen. Bij blockchain worden alle transacties

namelijk gevalideerd door nodes die deelnemen aan het blockchainnetwerk. Dit betekent dat deze nodes de blockchaintransacties kunnen inzien en er dus ook geen privacy mogelijk is.

Met Zero-Knowledge Proofs kunnen we bijvoorbeeld authenticaties uitvoeren, waarbij geen wachtwoorden hoeven te worden uitgewisseld en dus ook geen wachtwoorden kunnen worden gestolen. Zo is er geen kwaadwillende die jouw communicatie kan stelen, of kan inzien welke bestanden je met een ander deelt.

5.5.1 Interactieve vs non-interactieve Zero-Knowledge Proofs

Het is belangrijk om te weten dat Zero-Knowledge Proofs zowel interactief als non-interactief kunnen zijn. Bij interactieve Zero-Knowledge Proofs wordt de bewijslast getoond tussen twee partijen, bijvoorbeeld Peggy en Victor. Als de bewijslast ook dient te worden getoond aan anderen, moet er nogmaals gedemonstreerd worden door de bewijzer dat deze beschikt over een bepaalde kennis of waarheid. Het zou idealer zijn als elke node zelf de bewijslast kan verifiëren nadat de bewijzer deze eenmaal heeft getoond. Bij non-interactieve Zero-Knowledge Proofs is dit mogelijk.[65]

5.5.2 ING en Zero-Knowledge Range Proofs

De ING heeft bijvoorbeeld een variant erop ontwikkeld, Zero-Knowledge Range Proofs (ZKRP), waarmee iemand iets zou kunnen bewijzen wat binnen een gespecificeerd bereik valt.[66] Voorbeelden hiervan zijn:

1. Valideren dat iemands leeftijd tussen 18 en 65 jaar oud is, zonder de leeftijd te onthullen.
2. Valideren dat iemand in Europa woont, zonder de exacte locatie te onthullen.
3. Valideren dat iemand een salaris heeft dat binnen een bepaald bereik valt om een hypotheek af te kunnen sluiten, zonder het precieze salaris te onthullen.

Er zijn meerdere varianten en toepassingen van Zero-Knowledge Proofs mogelijk. Eén belangrijke toepassing die we nog willen onderstrepen, is het valideren van ***Know Your Customer*** (KYC) gegevens, zoals bijvoorbeeld het woonadres, zonder deze werkelijk te

[65] ***Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*** (ZK-SNARKs) is een variant van non-interactieve Zero-Knowledge proofs. Deze techniek wordt onder andere gebruikt door anonieme cryptovaluta als Zcash. Zie hiervoor een uitgebreidere uitleg over ZK-SNARKs: https://z.cash/technology/zksnarks.

[66] ING heeft de code van Zero Knowledge Rang Proofs openbaar gemaakt op Github: https://github.com/ing-bank/zkproofs.

onthullen. KYC is een proces om nieuwe en bestaande klanten te verifiëren en wordt soms door overheden verplicht gesteld. Je kunt meer lezen over KYC en de kosten ervan in het intermezzo in hoofdstuk 12.

5.6 De overheid tegen publieke encryptie

Hoewel Diffie, Hellman, Rivest, Shamir en Adleman rond dezelfde tijd public key cryptografie hadden ontwikkeld, gaat het opmerkelijke verhaal dat deze vorm van encryptie al tegen 1970 conceptueel was uitgewerkt door James Ellis – een wiskundige bij de Government Communications Headquarters (GCHQ), de Britse inlichtingendienst. Ellis noemde het concept “non-secret encryption”. Echter, wist er niemand binnen de GCHQ hoe ze het idee praktisch konden implementeren. Deze situatie bleef tot 1973 toen Clifford Cocks, een jonge wiskundige die destijds net in dienst kwam bij de GCHQ, een algoritme bedacht waarmee Ellis’ idee van public key cryptografie toepasbaar werd. Het algoritme van Cocks was gebaseerd op het factoriseren van priemgetallen en leek op het RSA-algoritme van Rivest, Shamir en Adleman. Kort daarna had een andere wiskundige bij de GCHQ, genaamd Malcolm Williamson, geprobeerd om Cocks’ algoritme te kraken. Hoewel dit niet was gelukt, ontdekte hij in zijn kraakpoging wel een eigen algoritme, dat leek op die van Diffie en Hellman. Deze nieuwe vormen van encryptie werden echter lange tijd nog niet toegepast door de GCHQ, omdat ze niet volledig vertrouwden dat het systeem onkraakbaar was. Hierdoor verschoof destijds vrijwel alle innovatie binnen moderne cryptografie naar de academische wereld en de private sector. Daarnaast viel het werk van Ellis, Cocks en Williamson onder staatsgeheim. Cocks, Ellis en Williamson kregen daardoor niet de waardering voor hun bijdragen aan public key cryptografie, totdat deze informatie werd gedeclassificeerd en Cocks in 1997 publiekelijk vertelde over hun uitvindingen.

De publieke toegang tot public key encryptietechnieken werd al vroeg door de overheid tegengewerkt. Tot aan de uitvinding van public key cryptografie door Diffie en Hellman, was cryptografie voornamelijk het domein van geheime inlichtingendiensten. Diffie en Hellman waren er destijds van overtuigd dat het komende computertijdperk toepassingen nodig had die de informatie van computergebruikers konden beveiligen – ook als dat zou betekenen dat zelfs de overheid niet bij de persoonlijke communicatie van computergebruikers kon. De NSA dacht er anders over en vreesde voor de opkomst van onkraakbare communicatiesystemen. Al sinds 1975 verzocht de NSA het National Science Foundation, een Amerikaans overheidsinstituut dat wetenschappelijke onderzoeken financiert en onder andere ook het onderzoek van Diffie en Hellman heeft gesteund, om de financiering van onderzoeken naar cryptografie stop te zetten.

In 1977 kregen de onderzoekers als Diffie, Hellman, Merkle, Rivest, Shamir en Adleman te horen dat hun publicaties over cryptografie in strijd waren met de ***International Traffic in Arms Regulations*** (ITAR) wetgeving. De wet reguleert de import en export van defensieartikelen en services. Gevechtsvoertuigen, raketten en geweren zijn oorlogsinstrumenten en mochten niet worden geëxporteerd, zonder specifieke toestemming van de overheid. Omdat cryptografie onder oorlogsinstrumenten viel, werd het verboden om presentaties en publicaties over cryptografie te exporteren. Hiervoor was namelijk een exportlicentie nodig. Deze wetgeving wierp veel vragen op. Konden ze echt de gevangenis ingaan als ze het werk zouden delen met mensen van buiten de Verenigde Staten? Shamir, één van de uitvinders van RSA-encryptie, is van Israëlische afkomst. Zouden zijn collega's de gevangenis in moeten als zij hem zijn eigen publicatie zouden opsturen?[67] Ondanks de bedreigingen van de NSA besloten de cryptografen toch hun werk te distribueren naar het buitenland. Hiermee werd public key cryptografie globaal. Dit leidde ook meteen de ***eerste crypto-oorlog*** in.

5.6.1 De eerste crypto-oorlog

In de jaren 80 probeerden bedrijven cryptografie te commercialiseren. Rivest, Shamir en Adleman hadden succesvol RSA gepatenteerd gekregen en produceerden een product genaamd Mailsafe, waarmee gebruikers beveiligd elektronische berichten konden sturen naar elkaar. Belangstellenden in RSA-technologie waren onder andere AT&T, IBM, Xerox, Lotus Development Corp en Microsoft. Andere bedrijven maakten gebruik van de Diffie-Hellman-patenten. Tegen het begin van de jaren 90 waren de exportcontroles op encryptie nog steeds van kracht en moesten bedrijven die encryptie wilden implementeren in hun producten twee versies maken: één met een sterke public key encryptie voor verkoop binnen de Verenigde Staten en een tweede met een zwakkere encryptie, die werd gedoogd door de Amerikaanse overheid voor buitenlandse klanten. Deze situatie werd niet meer houdbaar toen Phil Zimmerman zijn PGP-cryptosysteem, wat volgens de overheid onder de categorie van zeer sterke cryptografie viel, in 1991 open source maakte en gratis beschikbaar stelde voor iedereen die het wilde downloaden. Het programma kwam uiteraard ook beschikbaar in het buitenland via het Internet. Wat PGP bijzonder maakte, was dat het zo'n licht programma was, dat gedraaid kon worden op een pc.

[67] Zie ook Henry Corrigan-Gibbs' 'Keeping Secrets' (2014) over de strijd tussen de NSA en wetenschappers die onderzoek doen naar cryptografie.

Daarnaast kwam AT&T in 1992 met het plan om een telefoon, de TSD-3600-D, op de markt te brengen, die gesprekken kon encrypten middels zelf ontwikkelde algoritmes. Als reactie heeft de NSA geprobeerd om zelf een chip te ontwikkelen voor de private sector. De chip zou bekend worden als de ***Clipper chip*** en zou voorzien worden van een ***key escrow***systeem. De encryptie van de Clipper chip zou, zoals de overheid had beloofd, sterk genoeg zijn om de privacy van gebruikers te waarborgen. Het key escrowsysteem zelf splitst de private keys van gebruikers in twee delen die apart van elkaar bewaard worden in overheidsfaciliteiten. In het geval dat de overheid de communicatie van mensen wil aftappen, kan de overheid dat nog steeds doen met de private keys. Het argument dat destijds werd gebruikt, is dat onkraakbare encryptietoepassingen een gevaar zijn voor de nationale veiligheid als ze in handen zouden komen van terroristen en andere louche personen. Daardoor was het, volgens de NSA, noodzakelijk dat er toch een ingang kon worden gevonden tot de encryptie. Bedrijven mochten van de overheid hun communicatieapparaten ongestoord aanbieden in het buitenland, zolang deze apparaten voorzien waren van de Clipper chip.[68]

Het eerste apparaat dat gebruik mocht maken van de chip was AT&T's TSD-3600-E als AT&T hun plannen voor de TSD-3600-D-versie zou afblazen.[69] Mensen als Diffie, Helmann, Rivest, Shamir, Adleman, Zimmerman en andere privacy voorstanders vonden dit onacceptabel en zagen de ontwikkeling van de Clipper chip als een gevaar voor Amerikaanse burgers.[70] Vanaf 1991 kregen ***cryptoanarchisten*** en ***cypherpunks***, mensen die cryptografie gebruiken voor hun politiek activisme en technologieën hebben ontwikkeld waar Bitcoin gebruik van maakt, steeds meer aanhang.[71] Om het nog erger te maken voor de Amerikaanse overheid werd de Clipper chip gekraakt in 1994.[72] Het Amerikaanse publiek keerde zich steeds meer en meer tegen de

[68] Dit zou overigens de NSA ook de mogelijkheid bieden om buitenlandse gebruikers af te luisteren.

[69] De Amerikaanse overheid had een deal gesloten met AT&T dat zij de afnemers zouden zijn van de eerste producties.

[70] Zie ook het artikel 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' (1997), waarin een groep leidende cryptografen zich uitspreekt tegen de zwakheden van het key escrowsysteem in onder andere de Clipper chip.

[71] In hoofdstuk 14 van deel II wordt de filosofische achtergrond van cryptoanarchisten en cypherpunks verder besproken. Zij hebben een grote invloed gehad op de ontwikkeling van blockchain. Hun scepticisme tegenover de overheid en hun ideologie is nog steeds merkbaar in de blockchain community. Bezorgd om onze privacy hadden zij producten ontwikkeld als ontraceerbare e-mail en ontraceerbare betalingen. Zij hadden de fundamenten voor blockchain en Bitcoin al gelegd, voordat deze werden geïntroduceerd door Satoshi Nakamoto.

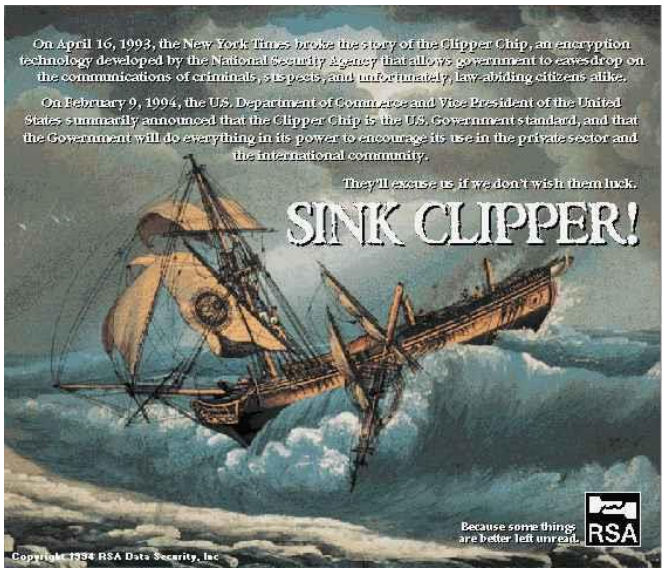
[72] Zie ook John Markoff's artikel, 'Flaw discovered in federal plan for wiretapping' (1994), dat verscheen in The New York Times.

chip. De chip werd niet omarmd door consumenten en bedrijven, waarna de productie ervan in 1996 werd gestopt. In hetzelfde jaar werd commerciële encryptie van de munitielijst gehaald van ITAR en werd het Ministerie van Economische Zaken verantwoordelijk over de regelgeving omtrent encryptie. Het ministerie besloot de regels met betrekking tot de export van encryptie en open source encryptiesoftware te versoepelen in 2000. Dit was een grote overwinning voor cryptoactivisten en werd gezien als het einde van de eerste crypto-oorlog.

5.6.2 De tweede crypto-oorlog

Met de opkomst van blockchain, de onthullingen van Edward Snowden en Wikileaks en andere ontwikkelingen zoals de FBI die in 2016 wilde dat Apple de beveiliging van de iPhone verzwakte, zijn encryptie en privacy weer terug in het publieke debat. Deze ontwikkelingen hebben een tweede crypto-oorlog veroorzaakt. Ook nu staan weer enthousiastelingen van encryptie en privacy tegenover overheidslieden die meer toezicht willen op de bevolking.

Afbeelding 63: AT&T's TSD-3600-E, uitgerust met de Clipper chip. (Foto: Cryptomuseum)



Afbeelding 64: Grafische campagne van RSA Security, de onderneming die werd opgericht door Rivest, Shamir en Adleman, tegen de Clipper chip. (Foto: RSA Data Security, Inc)

De geschiedenis van cryptografie heeft aangetoond dat er spanning bestaat tussen degenen die de privacy van burgers onverzetbaar willen waarborgen en degenen die toezicht willen kunnen houden op burgers. De spanning is ook nu sterk merkbaar in de blockchainwereld. De argumenten die in de jaren 70, 80 en 90 door overheidslieden werden gebruikt tegen encryptie zien we tegenwoordig ook terug in publieke discussies over Bitcoin. Bitcoin zou volgens sommigen alleen worden gebruikt door criminelen, net zoals sommigen beweerden dat encryptie alleen zou worden gebruikt door criminelen. Bitcoin zou volgens hen vooral gebruikt worden voor de handel in drugs, net zoals mensen beweerden dat de

drugsmaffia encryptie zou gebruiken om illegale drugdeals te sluiten. Bitcoin zou daarnaast een gevaar zijn voor de nationale veiligheid, net zoals encryptie dat ook zou zijn in de jaren 70, 80 en 90.[73] Het is niet zo verwonderlijk waarom de overheid zich zorgen maakt om cryptografie. Sterke encryptie is immers een ideale methode die kan worden gebruikt om de overheid buitenspel te zetten in het afluisteren van haar burgers.

[73] Steven Mnuchin (2019), de minister van Financiën in het kabinet van Donald Trump, noemt Bitcoin en andere cryptovaluta een issue van nationale veiligheid. Daarnaast gaan er binnen de EU onder politici stemmen op om encryptie te verzwakken of om backdoors te creëren (Stupp, 2016). De voormalige premier van het Verenigd Koninkrijk, Theresa May, heeft bijvoorbeeld in haar tijd als premier haar wens uitgesproken om backdoors te implementeren in communicatiesystemen (World Economic Forum, 2018).

Intermezzo: Je e-mailberichten beveiligen met Pretty Good Privacy (PGP)

Er zijn momenteel verscheidene applicaties waarmee een gebruiker zijn e-mail of bestanden kan encrypten. De ene applicatie is gebruiksvriendelijker dan de andere.

Hier bespreken we hoe je op gemakkelijke wijze je e-mailberichten kunt encrypten middels ***PGP***. PGP is momenteel één van de meest gebruikte encryptieprogramma's en werd overigens ook gebruikt door Edward Snowden om zijn topgeheime documenten van de Amerikaanse inlichtingendienst, de National Security Agency, te delen met The Guardian.

Afbeelding 65: Logo van Mailvelope. Zie https://www.mailvelope.com/en/ voor meer informatie over Mailvelope.

Voor het eenvoudig encrypten van je e-mailberichten op basis van de PGP-standaard kun je gebruikmaken van de Chrome of Firefox browserextensie, Mailvelope. Mailvelope biedt end-to-endencryptie, wat inhoudt dat zelfs de server waarover het bericht wordt verstuurd geen inzicht heeft in de data. Je berichten kunnen daardoor verstuurd worden over een potentieel onbeveiligd kanaal als e-mail. Instant messagingdiensten als Signal bieden ook end-to-endencryptie. Door Mailvelope te installeren binnen je browser, kun je je e-mails direct vanuit je webmail encrypten en decrypten.

Mailvelope werkt in de basis als volgt. Om middels encryptie te communiceren, dien je je e-mail te encrypten op een manier zodat alleen de ontvanger hier toegang tot krijgt. Voor de encryptie van de e-mail gebruik je de public key van de ontvanger. Dat betekent dat de ontvanger ook een private-public sleutelpaar moet hebben aangemaakt. Dit kan ook in andere PGP-programma's dan Mailvelope. Deze ontvanger heeft daarnaast ook een private key die correspondeert met de public key, waarmee je de e-mail hebt versleuteld. Met deze private key kan de ontvanger de e-mail die is versleutelen met zijn public key decrypten en de inhoud ervan lezen.

5.7 Samenvatting, begrippen en bronnen

Samenvatting

Het gebruik van cryptografie is al meer dan 4.000 jaar oud. Een klassiek voorbeeld is de Caesarrotatie. Deze werd in de eerste eeuw voor Christus gebruikt door Julius Caesar om berichten van militair belang te delen met zijn veldheren. De ontvanger van het bericht moest elke letter vervangen met een letter die een vast aantal posities verderop in het alfabet stond.

De Caesarrotatie is een voorbeeld van symmetrische cryptografie. Een ander voorbeeld is de Data Encryption Standaard (DES) uit 1975 van IBM. Bij symmetrische cryptografie kun je met eenzelfde sleutel, de secret key (geheime sleutel), zowel een bericht encrypten (versleutelen) als een bericht decrypten (ontsleutelen). Voor de ontvanger is het noodzakelijk om dezelfde secret key te hebben als hij het bericht van de verzender wil kunnen decrypten en lezen. Dit brengt een aantal nadelen met zich mee.

Kort na de publicatie van DES, werd asymmetrische encryptie – ook wel public key cryptografie genoemd – uitgevonden door Whitfield Diffie en Martin Hellman. Terwijl er bij symmetrische encryptie gebruik wordt gemaakt van één sleutel, wordt er bij public key cryptografie gebruikgemaakt van twee verschillende sleutels die wiskundig met elkaar corresponderen. Eén sleutel kun je publiekelijk beschikbaar stellen en de ander moet je privé bewaren. Je gebruikt een private key (privésleutel) die je nooit deelt met een ander om de data die je ontvangt te decrypten. Daarnaast gebruik je een corresponderende public key (publieke sleutel) die publiekelijk bekend mag zijn om de data te versleutelen. Wat de public key cryptografie zo elegant maakt, is dat de encryptiefunctie een ***tweerichtingsfunctie*** is: je kunt met de public key het bericht encrypten en met de private key decrypen. Daarnaast kun je vanuit de public key niet achterhalen wat de private key is.

Public key cryptografie gaat echter verder dan alleen het kunnen versleutelen van berichten en het veilig versturen hiervan. Het kan ook worden gebruikt om de verzender van een elektronisch bericht te authentiseren. Het toepassen van een private key op een bericht is equivalent aan het zetten van een digitale handtekening (digital signature).

Bij het aanmaken van een Bitcoin-adres worden er twee corresponderende keys gegenereerd: de public key en de private key van het desbetreffende Bitcoin-adres. Vanuit de public key wordt het Bitcoin-adres verkregen. Het is belangrijk om te weten dat je zonder digitale

handtekening geen transacties kunt uitvoeren. Aangezien de digitale handtekening alleen mogelijk is met een private key, dien je zorgvuldig om te gaan met je private key.
Het Bitcoin-netwerk ondersteunt ook multisignature. Bij multisignatures zijn er meer dan één digitale handtekening van één key nodig om een Bitcoin-transactie uit te voeren.

Een nieuwere vorm van encryptie is Zero-Knowledge Proofs (ZKP). Het is in essentie een methode waarbij een partij (de bewijzer) kan bewijzen aan een andere partij (de verifieerder) dat hij de waarheid van iets, bijvoorbeeld een bepaalde waarde, kan verifiëren zonder te onthullen dat hij kennis heeft van deze waarheid.

In 1977 kregen cryptografen als Diffie, Hellman, Merkle, Rivest, Shamir en Adleman te horen dat hun publicaties over cryptografie in strijd waren met de International Traffic in Arms Regulations (ITAR) wetgeving. Ondanks de bedreigingen van de National Security Agency (NSA) besloten de cryptografen toch hun werk te exporteren naar het buitenland. Hiermee werd public key cryptografie globaal. Dit leidde ook meteen de eerste crypto-oorlog in. De geschiedenis van cryptografie heeft aangetoond dat er spanning bestaat tussen degenen die de privacy van burgers onverzetbaar willen waarborgen en degenen die toezicht willen kunnen houden op burgers. De spanning is ook nu merkbaar in de blockchainwereld. De argumenten die in de jaren 70, 80 en 90 door overheidslieden werden gebruikt tegen encryptie zien we tegenwoordig ook terug in publieke discussies over Bitcoin en encryptie.

Opmerkingen die je nu kunt uitleggen

- Symmetrische cryptografie kent een aantal zwakheden die worden opgelost door asymmetrische (public key) cryptografie.
- Als je een geheim berichtje wil versturen naar persoon A, dan moet je de public key van persoon A gebruiken om het berichtje te encrypten.
- Voor de decryptie van een bericht, gebruik je de private key.
- Een Bitcoin-adres is niet hetzelfde als een Bitcoin public key.
- Met Zero-Knowledge Proofs kun je aantonen dat je tussen de 18 en 65 jaar oud bent zonder je exacte leeftijd te onthullen.
- Cryptografen en voorstanders van privacy staan op gespannen voet met overheidslieden die toezicht willen houden op de communicatie van burgers, bijvoorbeeld om criminelen op te kunnen sporen.
- Veel argumenten die worden gebruikt in discussies omtrent encryptie en privacy zien we ook terug in de discussies in de jaren 70, 80 en 90.

Verklarende begrippenlijst

Asymmetrische encryptie (public key cryptografie): Een cryptografische methode waarbij er gebruik wordt gemaakt van een private-public sleutelpaar.

Bewijzer: De partij die een statement probeert te bewijzen.

Brute-force aanval: Een aanval die wordt bewerkstelligd door alle verschillende sleutelcombinaties uit te proberen.

Brute-force search: Het zoeken naar de correcte sleutelcombinatie door alle verschillende combinaties uit te proberen.

Certificate Authority (CA): Instelling die gespecialiseerd is in het uitgeven, opslaan en ondertekenen van digitale certificaten.

Certification revocation list (CRL): Lijst van ingetrokken certificaten.

Clipper chip: Chip met een backdoor die is ontwikkeld door de Amerikaanse overheid.

Cryptanalyse: Het proces of de studie om een sleutel of bericht te kraken.

Cryptoanarchisten: Zie cryptoanarchisten in hoofdstuk 14.

Cypherpunks: Zie cypherpunks in hoofdstuk 14.

Data Encryption Standard (DES): Een data-encryptiestandaard die is ontwikkeld door IBM na consult van de NSA. De standaard kwam op in 1975 en maakte gebruik van symmetrische cryptografie.

Decrypten (onsleutelen): Ontsleutelen van data.

Eenrichtingsfunctie: Een wiskundige functie waarbij je vanuit het één het ander niet kunt achterhalen. Zo kun je bijvoorbeeld van een public key niet de private key achterhalen. Ook kun je van een hash niet de data achterhalen die hebben geleid tot de hash.

Eerste crypto-oorlog: De strijd die werd gevoerd door mensen die voorstanders zijn van cryptografie en privacy en hiermee vechten tegen de Amerikaanse overheid. De Amerikaanse overheid wilde namelijk exportcontroles op cryptografie en dat mensen gebruikmaken van zwakke encryptie die gekraakt kan worden door de overheid.

Elliptic Curve Digital Signature Algorithm (ECDSA): Een cryptografische methode om een private-public sleutelpaar te verkrijgen.

Encrypten (versleutelen): Versleutelen van data.

International Traffic in Arms Regulations (ITAR): Amerikaanse wet die de import en export van defensieartikelen en diensten reguleert. Cryptografie viel tot in de jaren 90 onder ITAR, waardoor cryptografen hun presentaties en publicaties over cryptografie niet mochten exporteren.

ITAR: Zie International Traffic in Arms Regulations.

Key escrow: Een systeem dat de private keys van gebruikers in twee delen splitst die apart van elkaar bewaard worden in overheidsfaciliteiten. In het geval dat de overheid de communicatie van mensen wil aftappen, kan de overheid dat nog steeds doen met de private keys.

Know Your Customer (KYC): Een proces om nieuwe en bestaande klanten te verifiëren.

KYC: Zie Know Your Customer.

M-of-N transactie: Transactie die vereist dat een M aantal private keys van een totaal van N private keys de transactie ondertekenen. Bij 2-of-3 transacties, moeten er 2 van de 3 private keys de transacties ondertekenen.

M-of-N wallet: Een wallet die M-of-N transacties aanbieden.

Multisignature (multisig): Methode waarbij meerdere private keys benodigd zijn om een transactie digitaal te ondertekenen. Hiermee kun je de verantwoordelijkheid over wallets decentraliseren. Daarnaast voorkom je hiermee ook een Single Point of Failure.

National Security Agency (NSA): De Amerikaanse inlichtingendienst.

Ontsleutelen: Zie decrypten.

Pretty Good Privacy (PGP): Een encryptieprogramma dat is ontwikkeld door Philip Zimmerman. Het programma is licht genoeg dat het kan worden gedraaid op een consumentencomputer.

Private key (privésleutel): Eén van de twee verschillende sleutels die bij asymmetrische cryptografie bij elkaar horen. De private key is bedoeld om een versleuteld bericht te decrypten.

Public key (publieke sleutel): Eén van de twee verschillende sleutels die bij asymmetrische cryptografie bij elkaar horen. De public key is bedoeld om uitgewisseld te worden met degene met wie je wil communiceren. Deze persoon gebruikt je public key om zijn bericht te encrypten.

Public key cryptografie: Zie asymmetrische encryptie.

Public key Infrastructuur: De infrastructuur van public keys voor het authentiseren van gebruikers en digitale certificaten.

Registration Authority (RA): Instelling die een gebruiker verifieert zodat de CA een certificaat uit mag geven aan de gebruiker.

Secret key (geheime sleutel): Een sleutel, zoals de private key, die je met niemand mag delen. Bij symmetrische cryptografie kun je met de secret key een bericht encrypten en decrypten.

Signature: Digitale handtekening.

Symmetrische encryptie: Een encryptiemethode waarbij de secret key zowel data encrypt als decrypt.

Verifieerder: De partij die de waarheid van een statement verifieert.

Versleutelen: Zie encrypten.

Wallet: Digitale portemonnee.

Zero-Knowledge Proof (ZKP): Een cryptografische methode waarbij een partij kan bewijzen aan een andere partij dat hij een waarde x weet zonder enige andere informatie te verlenen dan het feit dat hij de waarde x weet.

Zero-Knowledge Succinct Non-interactive Argument of Knowledge (ZK-SNARKs): Een variant van non-interactieve Zero-Knowledge proofs. Deze techniek wordt onder andere gebruikt door Zcash.

Zero-Knowledge: De verifieerder van een statement leert niets anders dan dat het statement waar is.

ZK-SNARKs: Zie Zero-Knowledge Succinct Non-Interactive Argument of Knowledge.

Bronnen

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Schneier, B. (2010). The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. *Academic Commons*. https://doi.org/10.7916/D8GM8F2W

Bambrough, B. (2019, 27 juli). The U.S. Treasury Secretary Made A Dire Warning Over The Future Of Bitcoin. *Forbes*. Geraadpleegd op 26 december 2019, van https://www.forbes.com/sites/billybambrough/2019/07/27/the-u-s-treasury-secretary-made-a-dire-warning-over-the-future-of-bitcoin/

Bitcoin Wiki. (z.d.). Technical background of version 1 Bitcoin addresses. Geraadpleegd op 26 december 2019, van Bitcoin.it website: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses#How_to_create_Bitcoin_Address

Buchmann, J. A., Wiesmaier, A., & Karatsiolis, E. (2016). *Introduction to Public Key Infrastructures*. Berlin Springer Berlin Springer.

Corrigan-Gibbs, H. (2014, November 7). Keeping Secrets. Geraadpleegd op 26 december 2019, van Stanfordmag.org website: https://stanfordmag.org/contents/keeping-secrets

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/tit.1976.1055638

Electronic Frontier Foundation. (1998). *Cracking DES: secrets of encryption research, wiretap politics & chip design*. Sebastopol, Calif.: O'reilly.

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, *18*(1), 186–208. https://doi.org/10.1137/0218012

ING Bank. (2019, 23 juli). Zero Knowledge Proofs. Geraadpleegd op 26 december 2019, van GitHub website: https://github.com/ing-bank/zkrp

Levy, S. (2001). *Crypto : how the code rebels beat the government, saving privacy in the digital age*. New York: Viking.

Mailvelope. (z.d.). Communicating safely with Mailvelope. Geraadpleegd op 26 december 2019, van Mailvelope.com website: https://www.mailvelope.com/en/

Markoff, J. (1994, 2 juni). Flaw discovered in federal plan for wiretapping. *The New York Times*. Geraadpleegd op 26 december 2019, van https://www.nytimes.com/1994/06/02/us/flaw-discovered-in-federal-plan-for-wiretapping.html

May, T. (2018, 25 januari). Theresa May's Davos address in full. Geraadpleegd op 26 december 2019, van World Economic Forum website: https://www.weforum.org/agenda/2018/01/theresa-may-davos-address/

Quisquater, J.-J., Quisquater, M., Quisquater, M., Quisquater, M., Guillou, L., Guillou, M. A., … Guillou, S. (1998). How to Explain Zero-Knowledge Protocols to Your Children. *Advances in Cryptology — CRYPTO' 89 Proceedings*, 628–631. https://doi.org/10.1007/0-387-34805-0_60

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Stupp, C. (2016, 30 maart). EU cybersecurity agency slams calls for encryption backdoors. Geraadpleegd op 26 december 2019, van www.euractiv.com website: https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors/

Trezor.io. (z.d.). Trezor Hardware Wallet. Geraadpleegd op 26 december 2019, van Trezor.io website: https://trezor.io

Yao, A.C. (1982). Protocols for secure computations. *IEEE Foundations of Computer Science. 23rd Annual Symposium*,160–164.

Young, J. (2019). Global ecommerce sales grow 18% in 2018. Geraadpleegd op 26 juli 2019 van Digital Commerce 360 website: https://www.digitalcommerce360.com/article/global-ecommerce-sales/

Zcash. (2018). What are zk-SNARKs? Geraadpleegd op 26 december 2019, van Zcash website: https://z.cash/technology/zksnarks

Zimmermann, P. (1991). Why I wrote PGP. Geraadpleegd op 26 december 2019, van Philzimmermann.com website: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Iconen

Alice, Bob, privésleutel, publieke sleutel en platte tekst gemaakt door Freepik van www.flaticon.com

Certificaat gemaakt door Kranshastry van www.flaticon.com

Digitale handtekening gemaakt door Wanicon van www.flaticon.com

Versleutelde tekst gemaakt door Pixelmeetup van www.flaticon.com

6. Proof-of-Stake en blockchain performance

"Over the past few years there has been considerable research into 'proof of stake' (PoS) based blockchain consensus algorithms. In a PoS system, a blockchain appends and agrees on new blocks where anyone who holds coins inside of the system can participate, and the influence an agent has is proportional to the number of coins (or 'stake') it holds. This is a vastly more efficient alternative to proof of work (PoW) 'mining' and enables blockchains to operate without mining's high hardware and electricity costs."

- Vitalik Buterin & Virgil Griffith (2019)

6.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Dat er alternatieve consensusprotocollen zijn zoals Proof-of-Stake.
- Wat Proof-of-Stake is.
- Verschillende varianten van Proof-of-Stake zoals Delegated Proof-of-Stake, Leased Proof-of-Stake, Proof-of-Stake Velocity en Proof-of-Authority.
- Wat de voornaamste verschillen zijn tussen Proof-of-Work en Proof-of-Stake.
- Dat het consensusprotocol van een blockchain grote impact heeft op de schaalbaarheid van een blockchain.
- Dat er momenteel verschillende initiatieven lopen om de schaalbaarheid van blockchains te vergroten.
- Dat het mogelijk is om een passief inkomen te genereren door je cryptomunten te staken op een Proof-of-Stake blockchain.

Inleiding

In dit hoofdstuk komen verscheidene essentiële elementen van blockchain aan bod. Hierbij kijken we naar alternatieven voor Proof-of-Work en wat de impact van consensusprotocollen is op de schaalbaarheid van een blockchain.

Vanaf paragraaf 6.2, wordt er gekeken naar consensusprotocollen die een alternatief zijn op het Proof-of-Work-protocol van bijvoorbeeld Bitcoin. De belangrijkste van deze alternatieven is

Proof-of-Stake (paragraaf 6.3) en diens afgeleiden: Delegated Proof-of-Stake (6.4), Leased Proof-of-Stake (6.5) en Proof-of-Stake Velocity (6.6). Daarnaast bespreken we een consensusmechanisme dat lijkt op Delegated Proof-of-Stake, maar veelvuldig wordt gebruikt binnen private blockchains: Proof-of-Authority (6.7). Deze consensusprotocollen zijn duurzamere mechanismen om consensus te bereiken dan Proof-of-Work, omdat het mogen produceren van een blok niet afhankelijk is van de hoeveelheid computerkracht die je levert aan het netwerk. Vervolgens bespreken we in paragraaf 6.8 wat de voordelen zijn van klassiek Proof-of-Stake ten opzichte van Proof-of-Work. In paragraaf 6.9 behandelen we de schaalbaarheid van blockchains en trekken we een relatie tussen de schaalbaarheid en consensusmechanismen. Tot slot sluiten we af met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst van het hoofdstuk in 6.10.

6.2 Alternatieve consensus-protocollen

In hoofdstuk 4 hebben we besproken dat het essentieel is om vertrouwen te creëren onder de verschillende deelnemers binnen een gedistribueerd netwerk. Er moet vertrouwen zijn dat de deelnemers niet corrupt zijn en dat de data die onderling verdeeld worden niet gecorrumpeerd zijn. Om dit vertrouwen te waarborgen, moeten de deelnemende nodes berichten of transacties verifiëren op hun juistheid en moeten zij andere deelnemers die corrupt en misleidend zijn, kunnen neutraliseren: de oplossing voor het hiervoor besproken Byzantine Generals Problem. De essentie van het probleem is hoe er consensus kan worden bereikt over het gedistribueerde netwerk van nodes, waarbij sommige potentieel corrupt zijn. Hoe kan er op veilige wijze consensus worden bereikt tussen de verschillende nodes, ervan uitgaande dat het netwerk tussen de nodes onbetrouwbaar is?

Tot nog toe hebben we één oplossing besproken voor het Byzantine Generals Problem: het Proof-of-Work-consensusprotocol, zoals deze bijvoorbeeld bij Bitcoin is ingericht. Volgens dit protocol mag een datablok alleen worden toegevoegd aan de blockchain wanneer er een geldige hash van het blok is gevonden. Het vinden van een geldige hash wordt gedaan door mijners met behulp van computerkracht. Hoe meer computerkracht een mijner levert aan het netwerk, hoe sneller hij een geldige hash kan vinden en dus ook hoe groter de kans is dat hij het volgende blok mag produceren en toevoegen aan de blockchain. Bij het vinden van een geldige hash heeft de mijner zogezegd ‘bewezen dat hij werk heeft verricht’ (Proof-of-Work). Volgens de beloningsstructuur van Proof-of-Work-protocollen ontvangen mijners die het eerst de geldige hash kunnen vinden een beloning van momenteel 12,5 Bitcoin binnen het Bitcoin-netwerk. Dit heeft als consequentie dat er onder Bitcoin-mijners een hevige competitie is

ontstaan in computerkracht. Daardoor is het elektriciteitsverbruik van het Bitcoin-netwerk ook zo gigantisch.

Proof-of-Work is echter het eerste consensusmechanisme dat is toegepast in blockchain. Naast Proof-of-Work zijn er sindsdien verscheidene consensusprotocollen ontwikkeld die het Byzantine Generals Problem op een efficiëntere manier trachten op te lossen. Het voornaamste alternatieve protocol dat ook het energieverbruik drastisch weet te reduceren, is Proof-of-Stake. Dit protocol is inmiddels geïmplementeerd binnen verscheidene blockchainprojecten.

6.3 Proof-of-Stake (PoS)

Proof-of-Stake werd voor het eerst geïmplementeerd bij PeerCoin en Nxt in respectievelijk 2012 en 2013. Momenteel is Ethereum, de één na grootste blockchain op basis van marktkapitalisatie, in een overgangsfase van Proof-of-Work naar een Proof-of-Stake-protocol genaamd Casper.

Terwijl mijners bij Proof-of-Work nieuwe blokken mogen produceren wanneer zij een geldige hash kunnen vinden, wordt een blokproducent bij Proof-of-Stake gekozen op basis van (a) een willekeurig selectieproces en (b) een '***stake'*** als bijvoorbeeld het aantal coins dat hij bezit. Dat betekent dat er bij Proof-of-Stake geen dure mijningapparatuur benodigd is. Het enige wat nodig is, is een standaardcomputer, een internetverbinding en het hebben van een coin. De blokproducent bij Proof-of-Stake heet dan ook geen mijner, maar wordt een ***forger*** genoemd. Omdat de forger bij het produceren van een nieuw blok ook een beloning ontvangt, kun je Proof-of-Stake ook als een methode zien waarbij je een passief inkomen verdient op je coins. Hoe meer stake je hebt, hoe hoger de kans bestaat dat jij het volgende blok mag produceren. Naast het produceren van blokken valideren ze ook transacties, waardoor ze het netwerk helpen beveiligen.

Er zijn binnen Proof-of-Stake verschillende varianten die hun eigen unieke eigenschappen hebben. Hoewel er meerdere varianten zijn, zullen we de volgende vier verder toelichten:

1. Delegated Proof-of-Stake (dPoS).
2. Leased Proof-of-Stake (lPoS).
3. Proof-of-Stake Velocity (PoSV).
4. Proof-of-Authority (PoA).

Hierbij willen we wel een kanttekening maken dat het dubieus is of Proof-of-Authority onder Proof-of-Stake valt. Het wordt soms gezien als een vorm van Delegated Proof-of-Stake.

6.4 Delegated Proof-of-Stake (DPoS)

Delegated Proof-of-Stake is ontwikkeld door Dan Larimer, de oprichter van BitShares, Steemit en EOS – blockchainprojecten die allemaal gebruikmaken van dit consensusmechanisme. Andere bekende projecten die delegated Proof-of-Stake hebben geïmplementeerd, zijn Lisk en Cardano.

Bij delegated Proof-of-Stake kun je niet zomaar je coins staken om nieuwe blokken te mogen produceren. Een delegated Proof-of-Stake-systeem kun je het best vergelijken met een voortdurende representatieve democratie waarbij iedereen die een coin heeft kan stemmen op ***witnesses*** en ***delegates***. De witnesses en delegates moeten zich hiervoor wel verkiesbaar hebben gesteld en een bepaald aantal stemmen hebben binnengehaald om hun functie als witness en delegate te mogen uitvoeren.

6.4.1 Witnesses

De rol van witnesses is om transacties te valideren en nieuwe blokken te mogen produceren. Voor het verlenen van deze service krijgen zij een beloning per geproduceerd blok.

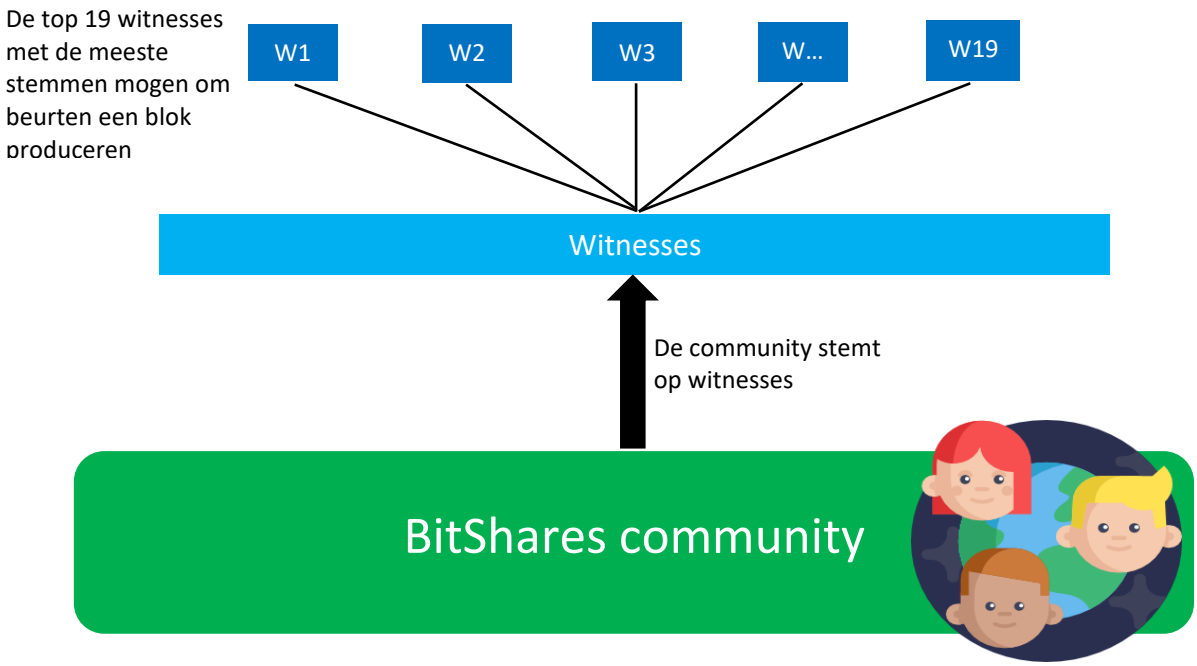
Als we BitShares, een exchange gebouwd op blockchaintechnologie (Decentralized Exchange), als voorbeeld nemen, dan zien we dat de top 19 witnesses om beurten een nieuwe blok mogen produceren. Omdat er van tevoren al is vastgesteld wie de volgende blokproducent wordt, is er geen willekeurig selectieproces meer nodig om een producent te vinden en hoeft er ook niet, net zoals bij Proof-of-Work, geconcurreerd te worden wie de volgende producent mag worden. Daarnaast hoeven de transacties in vergelijking tot het Proof-of-Work-mechanisme van Bitcoin maar door een gelimiteerd aantal van 19 witness nodes te worden goedgekeurd. Deze eigenschappen zorgen ervoor dat er op snelle, efficiënte en energiezuinige manier nieuwe blokken kunnen worden toegevoegd aan de blockchain. Dit komt de ***schaalbaarheid*** van de blockchain ten goede. Transacties worden gemiddeld goedgekeurd binnen ongeveer 1,5 seconde en om de 3 seconden wordt er een nieuwe blok aangemaakt. Het aantal transacties dat per seconde kan worden verricht op BitShares is daardoor ook 3300+ transacties per

seconde.[74] Dit is aanzienlijk meer dan bij het Bitcoin-netwerk dat maar ongeveer 7 transacties per seconde kan verwerken.

Zoals eerder vermeld, zijn er bij delegated Proof-of-Stake voortdurend verkiezingen. Bij delegated Proof-of-Stake is het belangrijk dat de witnesses, net zoals bij een representatieve democratie, zichzelf kenbaar maken bij de community en campagnes voeren om stemmen te krijgen. Er wordt ook van hen verwacht dat zij zo goed mogelijk hun taken uitvoeren en hun nodes zo weinig mogelijk uitvallen. Mochten witnesses hun taken niet goed uitvoeren, dan is er altijd een mogelijkheid voor de community om op iemand anders te stemmen die zij meer vertrouwen. Hiermee dreigen slecht functionerende witnesses hun inkomen als blokproducent te verliezen.

Je kunt bij BitShares op elk moment van de dag een stem uitbrengen. Om de dag worden alle stemmen bij elkaar opgeteld en op basis daarvan worden de top 19 witnesses, die om beurten een blok mogen produceren, bepaald. Het gewicht van de stemmen is gebaseerd op de hoeveelheid coins, bijvoorbeeld BitShares coins (BTS), die een persoon bezit. Dat betekent dat een stem van iemand met 1,000 BTS proportioneel zwaarder meeweegt dan een stem van iemand met 1 BTS.

[74] Sommige documenten hebben de transactiesnelheid van BitShares overschat door te stellen dat het systeem 100.000 transacties per seconde kan verwerken.



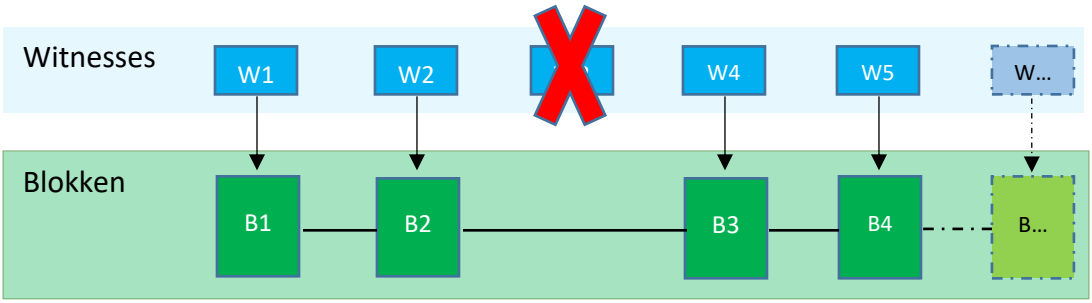
Afbeelding 66: Delegated Proof-of-Stake bij BitShares.

Bij het op blockchain gebaseerde socialmediaplatform Steemit, zijn er 20 actieve witnesses. Naast deze actieve witnesses zijn er ook reserve witnesses. Nadat de 20e witness een blok heeft geproduceerd, vindt er een loting plaats onder de reserve witnesses om als 21e witness een blok te mogen produceren. Zo loont het bij Steemit ook om een witness te zijn, zonder dat je in de top 20 komt.

Echter, kan het weleens gebeuren dat een witness (a) terwijl hij aan de beurt is om een blok te produceren uitvalt of (b) na het produceren van een blok te laat signaleert naar de andere witnesses dat hij het blok heeft aangemaakt.

Een witness valt tijdelijk uit en kan geen blok produceren

Wanneer een witness tijdelijk uitvalt en geen blok kan produceren, wordt de witness automatisch overgeslagen en is de volgende witness aan de beurt. De blockchain mist hierdoor één blok, maar de transacties die in het missende blok zouden zitten, zijn dan wel opgenomen in het blok erop.

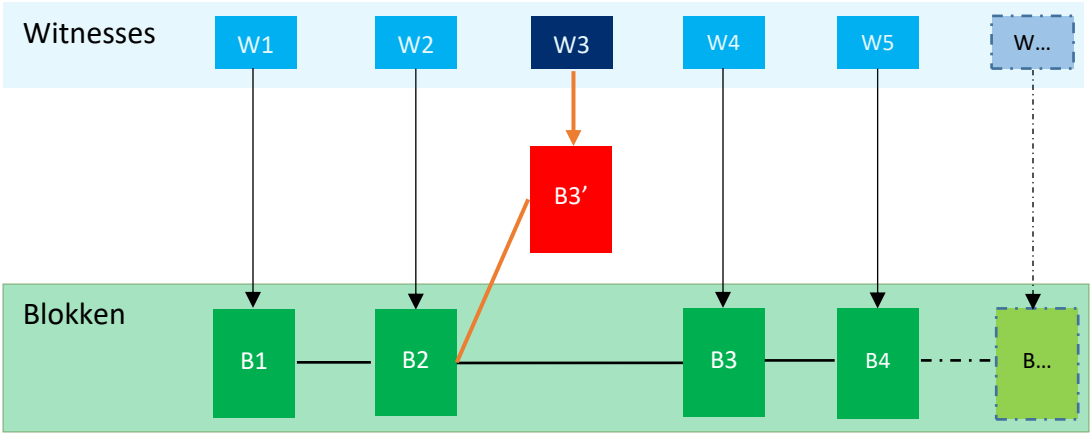


Afbeelding 67: Wanneer een witness (W3) uitvalt en geen blok kan produceren, wordt zijn beurt overgeslagen.

Een witness signaleert te laat naar de andere witnesses dat hij een blok heeft aangemaakt

Het kan weleens voorkomen dat een witness te laat signaleert naar de andere witnesses dat hij een blok heeft aangemaakt. In zulke gevallen kan de volgende witness zelf al een nieuw blok hebben geproduceerd, waardoor er een tijdelijke splitsing is in de blockchain. Hoe wordt er dan bepaald wat de ware blockchain is?

De ware blockchain is net zoals bij Proof-of-Work altijd de langste blockchain. Dit is namelijk de blockchain met de meeste consensus. Hieronder vind je een grafische weergave van de situatie.



Afbeelding 68: Wanneer een witness (W3) te laat naar andere witnesses signaleert dat hij een blok heeft aangemaakt, kan het zijn dat een andere witness (W4) de blokproductie op zich heeft genomen. In dit voorbeeld heeft W4 een blok 3 (B3) geproduceerd en gekoppeld aan blok 2 (B2). In dit geval ontstaan er twee chains: de groene en de rode blockchains. De ware blockchain is altijd de langste chain – bij dit voorbeeld is dat de groene blockchain. W3 zal hierdoor zijn lokale blockchain moeten synchroniseren met het netwerk om het weer gelijk te krijgen met de langste blockchain.

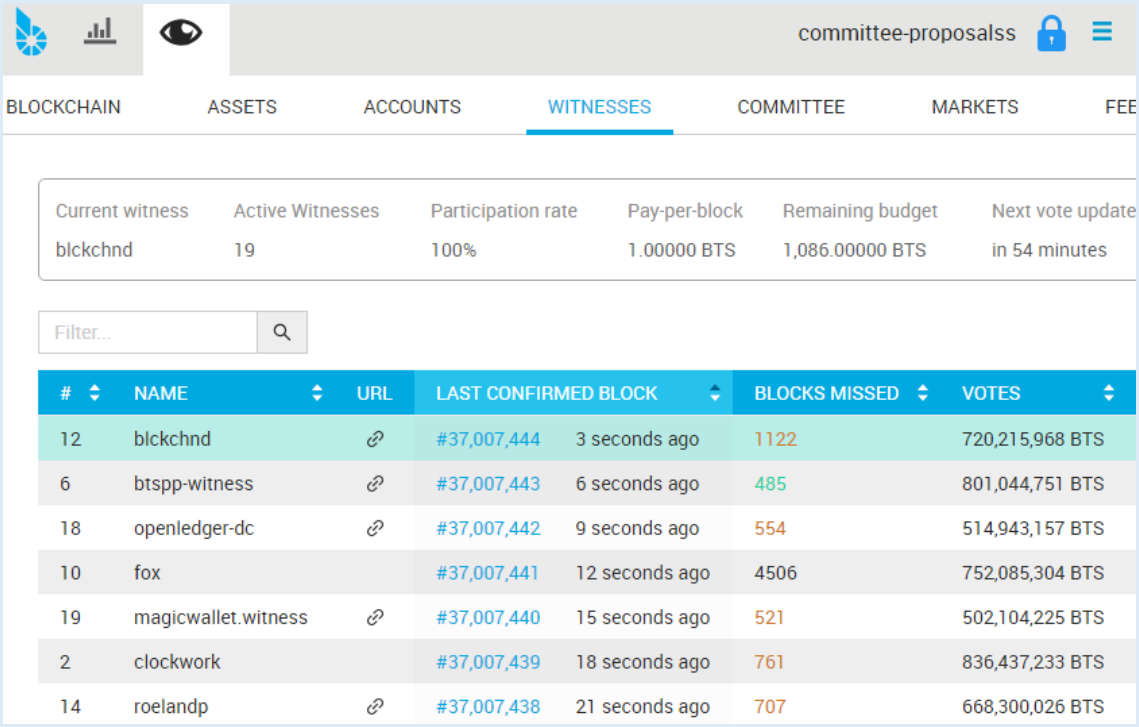
De community van delegated Proof-of-Stake-systemen stemt naast witnesses ook op delegates.

6.4.2 Delegates

Delegates (gedelegeerden) spelen geen rol in het verifiëren van transacties en het valideren en produceren van blokken. De rol van delegates is om de governance structuur van het blockchainprotocol te overzien. Zij kunnen bijvoorbeeld een voorstel indienen om de grootte van de blokken of om de beloning voor witnesses te wijzigen. Als een delegate een voorstel heeft ingediend, kan de community voor of tegen stemmen.

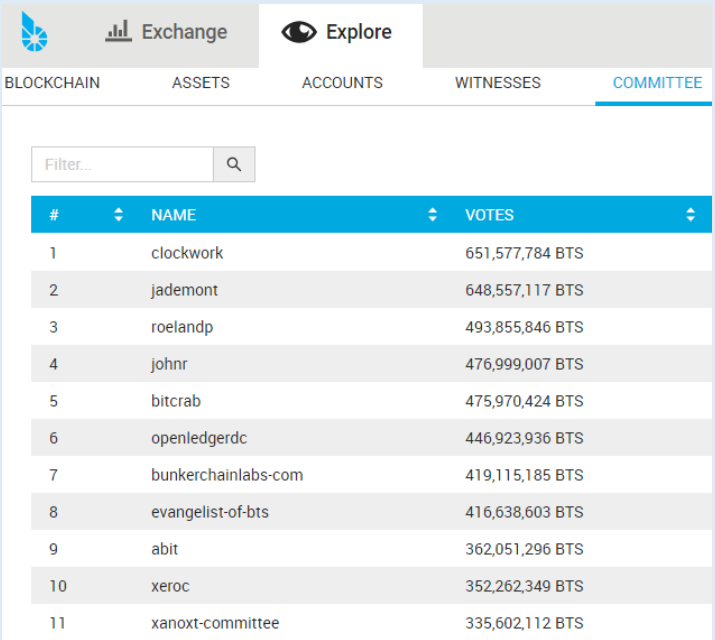
Intermezzo: De BitShares block explorer

BitShares heeft een transparante block explorer waar je alle witnesses, delegates en transacties kunt terugvinden. Deze explorer kun je vinden via https://wallet.bitshares.org.



#	NAME	URL	LAST CONFIRMED BLOCK		BLOCKS MISSED	VOTES
12	blckchnd		#37,007,444	3 seconds ago	1122	720,215,968 BTS
6	btspp-witness		#37,007,443	6 seconds ago	485	801,044,751 BTS
18	openledger-dc		#37,007,442	9 seconds ago	554	514,943,157 BTS
10	fox		#37,007,441	12 seconds ago	4506	752,085,304 BTS
19	magicwallet.witness		#37,007,440	15 seconds ago	521	502,104,225 BTS
2	clockwork		#37,007,439	18 seconds ago	761	836,437,233 BTS
14	roelandp		#37,007,438	21 seconds ago	707	668,300,026 BTS

Afbeelding 69: Je ziet dat er om de 3 seconden een blok wordt goedgekeurd en hoeveel stemmen, uitgedrukt in BTS, elke witness heeft ontvangen van de community.

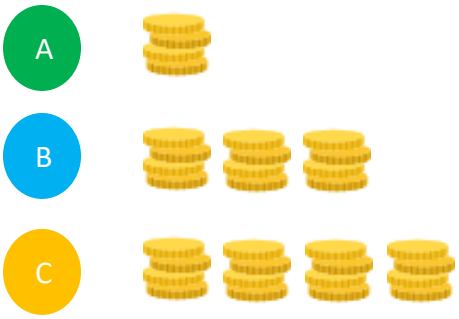


#	NAME	VOTES
1	clockwork	651,577,784 BTS
2	jademont	648,557,117 BTS
3	roelandp	493,855,846 BTS
4	johnr	476,999,007 BTS
5	bitcrab	475,970,424 BTS
6	openledgerdc	446,923,936 BTS
7	bunkerchainlabs-com	419,115,185 BTS
8	evangelist-of-bts	416,638,603 BTS
9	abit	362,051,296 BTS
10	xeroc	352,262,349 BTS
11	xanoxt-committee	335,602,112 BTS

Afbeelding 70: Een verkorte lijst van BitShares delegates in mei 2019. Het is ook inzichtelijk hoeveel stemmen elke delegate heeft ontvangen.

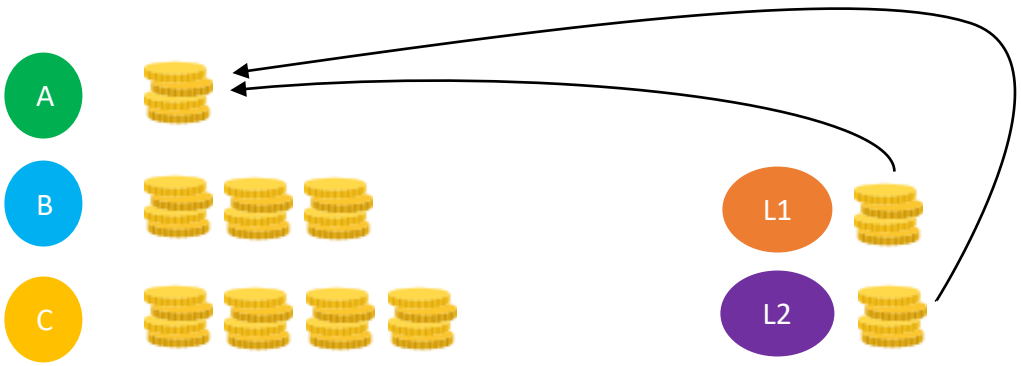
6.5 Leased Proof-of-Stake (LPoS)

Bij het klassieke Proof-of-Stake-model is er voor iedereen die hun coins ‘staket’ een kans om een blok te mogen produceren. De kans hierop is gebaseerd op de hoeveelheid coins die de persoon als belang houdt. Houders van een kleine hoeveelheid coins hebben dus een kleinere kans. Dit kan ervoor zorgen dat mensen met weinig coins niet genoeg gestimuleerd worden om deel te nemen. Als de vele kleine houders niet willen deelnemen aan het stakingproces, dan kan de blockchain wellicht te gecentraliseerd worden. Er is dan slechts een kleine groep deelnemers die in het bezit van veel coins is, die het netwerk helpen onderhouden.



Afbeelding 71: Dit is een voorbeeld van klassieke Proof-of-Stake, waarbij er drie staking nodes zijn: A, B en C. Staking node A heeft 1 stack aan coins, staking node B heeft 3 stacks en staking node C heeft 4 stacks. In totaal zijn er dus 8 stacks. Als dit alle stake is binnen het netwerk, dan heeft staking node A 1/8 kans om een volgende blok te mogen produceren. Staking node B heeft 3/8 kans en staking node C heeft 4/8 kans.

Met ***leased Proof-of-Stake*** zou je deze issue kunnen oplossen door iedereen de mogelijkheid te geven om hun coins te leasen aan staking nodes. Wanneer deze staking nodes meer coins als lease hebben gekregen, is de kans dat de staking nodes een blok mogen produceren groter. De staking nodes zullen de beloning dan proportioneel verdelen tussen henzelf en iedereen die coins heeft geleased aan hen. Het vooruitzicht om hiermee zelfs als kleinhouder ook regelmatig beloond te worden, stimuleert mensen met kleine hoeveelheden coins om te leasen en daarmee ook deel te nemen aan het stakingproces. Daarnaast hoef je als leaser niet dag en nacht een staking node te draaien en is technische kennis van servers ook niet vereist. Hierbij is het wel belangrijk dat je bij het leasen van je coins geen controle over je coins verliest. De staking node kan je coins niet uitgeven of zelf innemen. Je kunt zelf op elk moment besluiten of je de lease stop wil zetten. Tijdens de lease kun je je coins echter niet verhandelen.



Afbeelding 72: Dit is een voorbeeld van leased Proof-of-Stake. Hierbij zijn er drie staking nodes: A, B en C. Daarnaast zijn er twee nodes, L1 en L2 die hun coins leasen aan staking node A. Staking node A heeft hierdoor niet 1, maar 3 stacks aan coins. De kans dat staking node A een volgende blok mag produceren is daardoor niet meer 1/8, maar 3/10. Wanneer staking node A een blok mag produceren, dan zal hij zijn beloning proportioneel verdelen tussen hemzelf en de nodes L1 en L2.

Het grootste blockchainproject dat gebruikmaakt van leased Proof-of-Stake is Waves. Waves is een platformblockchain waar je blockchainapplicaties op kunt bouwen en je eigen cryptotokens op kunt maken, die je op hun eigen ***gedecentraliseerde exchange*** (DEX) kunt verhandelen. Een gedecentraliseerde exchange is een handelsbeurs die is gebouwd op een blockchain. In het geval van de Waves DEX is de exchange gebouwd op de Waves blockchain.

6.6 Proof-of-Stake Velocity (PoSV)

De naam, ***Proof-of-Stake Velocity***, komt van de term 'velocity of money'.[75] Het Proof-of-Stake Velocityprotocol is een variant van Proof-of-Stake. Het doel is om te voorkomen dat mensen alleen hun coins oppotten in het stakingproces. Wat Proof-of-Stake Velocity onderscheidt van klassieke Proof-of-Stake is dat gebruikers worden beloond voor (a) het aantal coins dat zij houden en (b) hoe actief zij hun coins gebruiken. De community wordt dus gestimuleerd om niet alleen de coins te bewaren, maar ze ook daadwerkelijk te gebruiken voor transacties. Een project dat gebruikmaakt van dit protocol is Reddcoin, een cryptovaluta voor het doen van microtransacties en het geven van tips op socialmedianetwerken.

6.7 Proof-of-Authority (PoA)

Het concept van ***Proof-of-Authority*** werd geïntroduceerd door Ethereum mede-oprichter, Gavin Wood. Wij behandelen Proof-of-Authority in dit hoofdstuk, omdat het consensusmechanisme veel lijkt op dat van Delegated Proof-of-Stake.

[75] De velocity of money geeft aan hoe snel geld van persoon wisselt.

Delegated Proof-of-Stake-systemen worden vaak geïmplementeerd in open blockchains, waar iedereen zichzelf op pseudoanonieme wijze verkiesbaar kan stellen om een witness te worden. In dat opzicht zou je kunnen zeggen dat witness-aspiranten worden 'goedgekeurd' door de community om hun rol als witness op zich te nemen, door middel van een stemming. Bij Proof-of-Authority worden de blokproducenten (authority nodes) echter geauthentiseerd en goedgekeurd op basis van hun identiteit en reputatie. Door de reputatie te linken aan identiteit, worden authority nodes extra gestimuleerd om goed gedrag te vertonen en geen malafide transacties op te nemen in de blockchain. Mochten zij dat wel doen, dan brengt dat reputatieschade met zich mee.

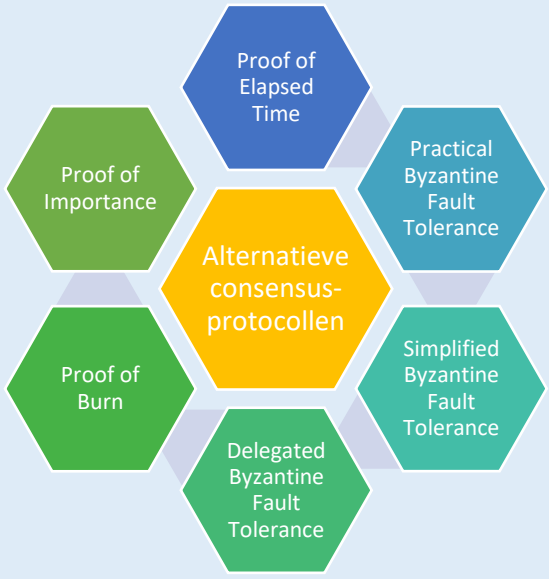
Twee implementaties van Proof-of-Authority zijn Parity en Geth. Dat zijn twee welbekende applicaties voor ***permissioned*** settings van Ethereum. (De Angelis et al., 2018) Permissioned en permissionless worden besproken in hoofdstuk 9. Voor nu is het belangrijk om te weten dat permissioned betekent dat er goedkeuring moet plaatsvinden om een blokproducent of validator te zijn. Dit maakt Proof-of-Authority ook geschikt binnen de context van een gesloten blockchain, waar behoefte is om er zeker van te zijn dat alleen gekwalificeerde partijen transacties goedkeuren.

Omdat er bij Proof-of-Authority al bekend is wie valideren en wie nieuwe blokken mogen aanmaken, is er geen concurrentie nodig op computerkracht. Dit komt de blockchainperformance ten goede. Het nadeel van Proof-of-Authority is dat het niet zo gedecentraliseerd is en daardoor gevoelig is voor censuur. Een ander mogelijk nadeel van Proof-of-Authority is dat als de validators bekend zijn, de validators kunnen worden gecorrumpeerd om malafide activiteiten op de blockchain uit te voeren. Daarnaast kunnen validators ook een blacklist maken van mensen die geen gebruik mogen maken van de blockchain. Dat laatste kan overigens ook worden gezien als een voordeel van Proof-of-Authority.

Bedrijven die liever controle willen houden op wie er data mogen schrijven naar en lezen van hun blockchain, maken liever geen gebruik van open publiekelijke blockchains, waarbij onbekenden validators kunnen zijn. Proof-of-Authority kan voor hun een uitkomst bieden. Als de authority nodes de gebruikers toch al kennen en als er toch geen gebruik wordt gemaakt van mijnen, is het ook mogelijk geen transactiekosten in te stellen.

Intermezzo: Alternatieve consensusprotocollen

Er bestaan naast eerdergenoemde consensusprotocollen diverse alternatieven. Hieronder vind je een overzicht van enkele andere protocollen. Wij bespreken er drie.



Afbeelding 73: Verscheidene alternatieve consensusprotocollen die noch Proof-of-Stake, noch Proof-of-Work zijn.

Proof-of-Elapsed Time (PoET)

PoET wordt vooral gebruikt bij permissioned blockchains. Om te bepalen wie een blok mag produceren, wordt er een willekeurige wachttijd vastgesteld voor elke node. De node wiens wachttijd voorbij is, mag het volgende blok produceren. Het systeem vereist dat wachttijden eerlijkd worden gegenereerd en dat niemand meerdere nodes kan draaien.

Practical Byzantine Fault Tolerance (pBFT)

Bij pBFT worden nodes sequentieel geordend. Eén node is een leader node en de rest zijn back-up nodes. Wanneer iemand een transactie stuurt naar de leader node, zendt de leader deze uit naar andere nodes ter verificatie. Na elke ronde dat een blok is toegevoegd door de leader wordt er geroteerd, zodat een back-up node een leader wordt. Bij uitval van een leader, wordt een back-up node ook een leader. Het systeem vereist dat 2/3 van de nodes niet malafide is. Hyperledger Fabric, Tendermint en Zilliqa maken gebruik van pBFT.

Proof of Importance (PoI)

PoI lijkt op PoS, alleen wordt er ook gekeken naar de activiteiten, het aantal transacties en de waarde van de transacties die een node doet om te bepalen wie het volgende blok mag produceren. Een project dat gebruikmaakt van PoI is New Economy Movement (NEM).

6.8 De voordelen van klassiek Proof-of-Stake ten opzichte van Proof-of-Work

Er zijn bepaalde voordelen aan Proof-of-Stake ten opzichte van Proof-of-Work. Wat Proof-of-Stake voordeliger maakt zijn:

1. Energie-efficiëntie.
2. Door het gemak om te staken kunnen meer mensen de blockchain onderhouden.
3. Het uitvoeren van een 51%-aanval is minder aantrekkelijk.

6.8.1 Energie-efficiëntie

Zoals eerder vermeld is Proof-of-Stake energie-efficiënter dan Proof-of-Work, omdat er geen mining nodes nodig zijn die met elkaar concurreren op basis van computerkracht om geldige hashes te vinden en blokken te mogen produceren. Met Proof-of-Stake kan iedereen met een redelijke computer hun coins staken en op die manier transacties helpen valideren en meedingen om een blok te mogen produceren.

6.8.2 Door het gemak om te staken kunnen meer mensen de blockchain onderhouden

Proof-of-Work kan specialistische kennis en hardware vereisen als je een kans wil hebben om een blok te produceren. Staken vereist daarentegen vaak geen serverkennis. Het staken van je coins wordt in sommige blockchainprojecten zo makkelijk gemaakt dat je het binnen een minuut op kunt zetten. Daarnaast kun je soms al staken met slechts één coin. Omdat de instapbarrière laag is, kunnen meer mensen staken waardoor de blockchain beter beveiligd is.

6.8.3 Het uitvoeren van een 51%-aanval is minder aantrekkelijk

Voor het uitvoeren van een 51%-aanval bij Proof-of-Stake, moet de aanvaller een meerderheid – 51% – van de coins bezitten. Tijdens het accumulatieproces van grote hoeveelheden van deze coins, zeker wanneer het op een open markt gebeurt, zal de prijs van de coins waarschijnlijk stijgen. Daardoor wordt een 51%-aanval bij Proof-of-Stake financieel onaantrekkelijk. Hoewel een dergelijke aanval mogelijk is, dient dit financiële aspect als een sterke afweer. Mocht de aanvaller in staat zijn om een 51%-aanval uit te voeren, dan kan de community alsnog besluiten om een hard fork uit te voeren en de stake van de aanvaller uit de blockchain verwijderen.

Bij Proof-of-Work moet de aanvaller een meerderheid van de totale computerkracht bezitten. Dat betekent dat de aanvaller moet investeren in hardware. Mocht de aanval mislukken, kan de aanvaller zijn hardware richten op het aanvallen van een ander Proof-of-Work-project. Er zijn zodoende minder negatieve consequenties voor de aanvaller als hij een 51%-aanval uitvoert op Proof-of-Work. De 51%-aanval komt in het volgende hoofdstuk uitgebreider aan bod.

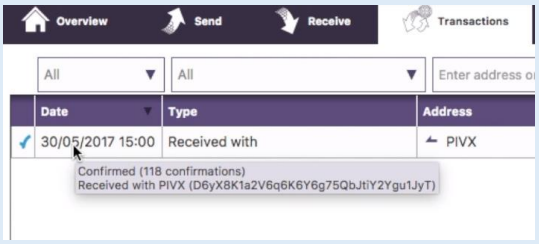
Intermezzo: Zelf coins staken en een passief inkomen verdienen (PIVX)

Als je een manier zoekt om passief inkomen te krijgen op je cryptovaluta, dan kan het lonen om je Proof-of-Stake coins te staken. Het staken van dergelijke coins is in veel gevallen ongecompliceerd.

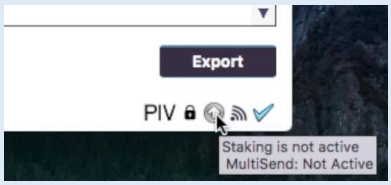
Wij nemen hier het staken van de cryptovaluta PIVX als voorbeeld. PIVX staat voor Private Instant Verified Transaction en is een anonieme cryptovaluta die gebruikmaakt van Zero-Knowledge Proofs. Je kunt bij PIVX twee typen coins staken: de publiekelijk openbare PIV coins en de anonieme zPIV coins. Als je zPIV staket, dan word je beloond met zPIV. Dit is ideaal wanneer je anoniem je coins wil staken. Je kunt ook je PIV omzetten in zPIV en andersom.

Om te staken, dien je eerst de PIVX desktop wallet te downloaden via www.pivx.org en te installeren.

1. Als je voor het eerst de wallet opent, dan synchroniseert deze met de blockchain. Laat de wallet volledig synchroniseren.
2. Je dient minimaal één PIV in je wallet te hebben. Mocht je wallet leeg zijn, zorg dan dat je minimaal één PIV overmaakt naar deze wallet.
3. Als je minimaal één PIV hebt, klik je op “Transactions”. Wees er zeker van dat je wallet minimaal 101 confirmations heeft.



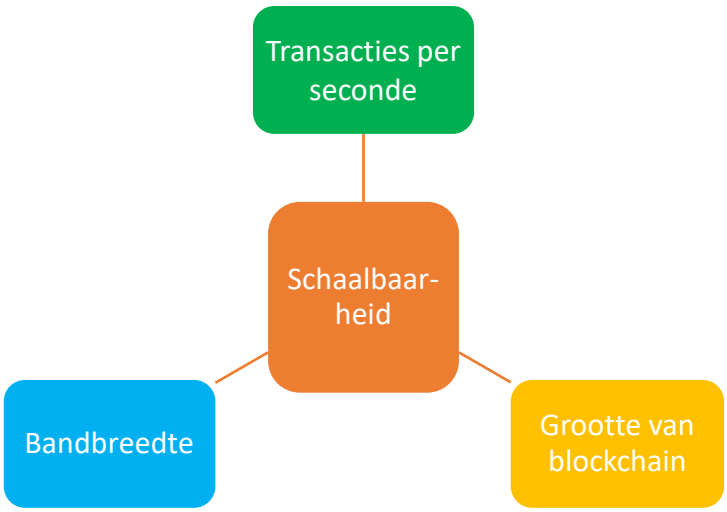
4. Als je rechtsonder met je muis boven het “pijltje omhoog” staat, zie je als het goed is “staking is not active”.



5. Om te staken, ga je naar “settings” en klik je vervolgens op “unlock wallet”.
6. Vul je “wallet passphrase” in, vink “for anonymization and staking only” aan en klik op “OK”.
7. Gefeliciteerd! Het “pijltje omhoog” wordt groen en staking is geactiveerd.

6.9 Schaalbaarheid

Wat niet in het rijtje staat onder voordelen van Proof-of-Stake ten opzichte van Proof-of-Work is de schaalbaarheid. Met de schaalbaarheid wordt voornamelijk het aantal transacties dat het blockchainnetwerk kan verwerken, bedoeld. Onder schaalbaarheid vallen echter ook bandbreedte en de grootte van de blockchain.



Met ***bandbreedte*** wordt bedoeld hoeveel data er tegelijkertijd over een bepaalde verbinding kunnen worden vervoerd. Hoe groter de bandbreedte, hoe sneller je de data kunt ontvangen en versturen. De blockchain heeft daarnaast een bepaalde grootte. De Bitcoin blockchain is op 8 januari 2020 bijvoorbeeld ongeveer 240GB groot. Hoe meer blokken er worden toegevoegd hoe groter de blockchain wordt. Als Bitcoin een gangbare betaalmiddel wordt, kan het weleens zo zijn dat de blockchain zo groot wordt dat het niet meer mogelijk wordt voor reguliere gebruikers om de Bitcoin blockchain op hun computer te bewaren. Zo kunnen ze ook niet meer de blockchain helpen onderhouden door blokken te helpen valideren. Als hiervoor gespecialiseerde dataopslagsystemen moeten worden ontwikkeld, kan de blockchain gecentraliseerder worden.[76] In de discussie die volgt richten we ons voornamelijk op het aantal transacties per seconde die een blockchain kan verwerken.

[76] Een manier om dit op te lossen is pruning. Dit is besproken in de intermezzo over Merkle trees in hoofdstuk 3 en in paragraaf 4.4.4 over pruned nodes. Een andere manier is door de blockchain op te splitsen in partities en nodes verantwoordelijk te stellen over een partitie in plaats van over de hele blockchain. Het opdelen van een blockchain in partities wordt behandeld wanneer we sharding bespreken in paragraaf 6.9.4.

Er bestaan onder de verschillende Proof-of-Stake-projecten en -varianten grote verschillen die van sterke invloed zijn op de schaalbaarheid. Hierdoor is het lastig om eenduidig te concluderen of Proof-of-Stake altijd schaalbaarder is dan Proof-of-Work of niet.

Blockchain en cryptovaluta worden steeds populairder en als de technologie wijdverbreid geadopteerd wil worden, is het belangrijk dat het een hoge verwerkingssnelheid heeft. In de volgende tabel zie je een lijst van verscheidene blockchains en hoeveel transacties die elk kunnen verwerken. Wat opvalt, is dat Bitcoin slechts 7 transacties per seconde aankan. Ethereum, een blockchainplatform waarop smart contracts en blockchainapplicaties kunnen worden gebouwd, kan zo'n 20 transacties per seconde aan.[77] Bitcoin Cash is een afgeleide van Bitcoin, maar heeft grotere blokgroottes, waardoor er per blok meer transacties in kunnen. Deze verwerkt gemiddeld 116 transacties per seconde (Coinanalysis, 2019). Volgens de officiële communicatie kan BitShares 100.000 transacties per seconde aan. Hoewel dit overschat is en in werkelijkheid dichterbij de 3.300 transacties per seconde ligt, is dit toch aanzienlijk meer dan wat Bitcoin aankan. De reden waarom BitShares zoveel sneller is, is dat het gebruikmaakt van delegated Proof-of-Stake, waarbij er van tevoren al is bepaald welke witness de volgende blokproducent wordt en waarbij er door slechts een select groepje witnesses transacties worden gevalideerd.

Visa verwerkt ongeveer 150 miljoen transacties per dag, wat neerkomt op ongeveer 1.700 transacties per seconde. Het bedrijf heeft echter capaciteit om meer dan 65.000 transacties per seconde te kunnen verwerken (Visa, 2019).[78] Dat is aanzienlijk meer dan vele blockchains. Toch is het niet onoverkomelijk voor blockchains om meer transacties te kunnen doen dan Visa. De nieuwste generatie blockchains als bijvoorbeeld EOS, wat ook gebruikmaakt van delegated Proof-of-Stake, beweert al meer dan 50.000 transacties per seconde aan te kunnen. Daarnaast heeft het EOS-team vertrouwen dat het met weinig aanpassingen zelfs meer dan een miljoen transacties per seconde zal kunnen verwerken.[79]
Over het algemeen kunnen we stellen dat de schaalbaarheid van een blockchain afhankelijk is van:

1. De bloktijd (block time).
2. De blokgrootte (block size).

[77] Ethereum heeft in december 2019 een hard fork gedaan, genaamd Istanbul, om onder andere de schaalbaarheid aan te pakken en de prijzen van Zero-Knowledge Proofs omlaag te brengen.

[78] Dit betreft de capaciteit van Visa in augustus 2017.

[79] Zie: *The Truth Machine: The Blockhain and the Future of Everything* (Vigna & Casey, p. 89).

3. Het distributie- of decentralisatieniveau van de blockchain.
4. De manier waarop blokken worden geproduceerd, transacties worden verstuurd naar de blockchain en transacties worden geverifieerd.

Binnen de blockchain community zijn er verschillende ideeën over wat de juiste oplossing is om schaalbaarheid te bereiken. Verscheidene projecten verschillen dan ook in de vier bovenstaande kenmerken die van invloed zijn op de schaalbaarheid.

6.9.1 De bloktijd

De bloktijd is de gemiddelde tijd waarin een blok wordt geproduceerd. Bij Bitcoin is de bloktijd 10 minuten. Als je transactie niet wordt opgenomen in het huidige blok, dan zul je 10 minuten moeten wachten om opgenomen te worden in het volgende blok. Een snellere bloktijd kan worden bereikt binnen Proof-of-Work door de moeilijkheidsgraad voor mijners om geldige hashes te vinden en blokken te mogen produceren te verlagen.

Het verlagen van de bloktijd zou in principe leiden tot een snellere verwerking van transacties. Het betekent echter ook dat er een grotere kans is dat er meerdere mijners rond dezelfde tijd een blok produceren waardoor er splitsingen, forks, kunnen ontstaan van de blockchain met orphaned blokken. Daarnaast heeft het netwerk altijd tijd nodig om te signaleren dat iemand al een blok heeft aangemaakt. De netwerklatentie moet dus beperkt blijven binnen een blockchain met een lagere bloktijd. Anders leidt dit ook tot meer orphaned blokken. Als er meer orphaned blokken ontstaan, heeft het netwerk meer tijd nodig om consensus te bereiken over welke blockchain de ware is. Dit is gaat weer ten koste van de schaalbaarheid. Daarnaast wordt er computerkracht besteed aan de blockchain met orphaned blokken, terwijl deze beter besteed kan worden aan de ware blockchain. Minder computerkracht voor de ware blockchain betekent dat de beveiliging hiervan ook minder is.

6.9.2 De blokgrootte

Naast de bloktijd, speelt de blokgrootte ook een belangrijke rol in de schaalbaarheid. De discussie over het vergroten van de blokgrootte heeft geleid tot controversie en onenigheid binnen de Bitcoin community. Een groep ontwikkelaars wilde in 2017 de blokgrootte van Bitcoin verhogen van 1MB naar 2MB, zodat er meer transacties per blok konden worden verwerkt. Dit zou ertoe leiden dat er tweemaal zoveel transacties per 10 minuten verwerkt konden worden.

Tegenstanders van een grotere blokgrootte, zoals Luke Dashjr, zijn van mening dat het leidt tot een grotere netwerklatentie, omdat het meer tijd kost de grotere data te verspreiden over het netwerk en de grotere hoeveelheid transacties tijdig te valideren (Luke Dashjr, 2019). Dit zou volgens hen leiden tot meer orphaned blokken. Daarnaast zou het ook duurder en lastiger worden om een node te draaien. Dit komt doordat grotere blokken ervoor zorgen dat de blockchain significant meer schijfruimte nodig zal hebben en doordat er van de nodes meer bandbreedte wordt vereist. De hogere kosten om een node te kunnen draaien zou ertoe kunnen leiden dat minder mensen een eigen node draaien, waardoor het netwerk van nodes gecentraliseerd wordt onder een selecter groepje mensen. Ook denken sommige tegenstanders dat er voldoende alternatieven zijn om de blockchain veilig op te schalen, zonder grotere blokken te implementeren.

Zoals eerder besproken in hoofdstuk 4, heeft de onenigheid omtrent de blokgrootte in 2017 geleid tot een splitsing van de Bitcoin blockchain. Deze splitsing is tot stand gekomen door middel van een hard fork. Zogezegd kan onenigheid over updates en over de richting waarop een blockchain zich moet ontwikkelen ertoe leiden dat een blockchain splitst in twee afzonderlijke chains, zoals het geval was bij Bitcoin en Bitcoin Cash.

6.9.3 Het distributie- of decentralisatieniveau van de blockchain

Het distributie- en ***decentralisatieniveau*** van de blockchain kan ook een grote rol spelen in de schaalbaarheid. Er is namelijk een sterke correlatie tussen de centralisatie en de verwerkingssnelheid van de blockchain. Zoals eerder vermeld, kan BitShares aanzienlijk meer transacties per seconde verwerken dan Bitcoin, doordat het gebruikmaakt van delegated Proof-of-Stake. Het idee hierachter is dat een blockchain met een selecte groep van 19 witnesses, van wie al op voorhand is bepaald wie het volgende blok mag produceren en transacties mogen valideren, aanzienlijk schaalbaarder is.

Sommige tegenstanders, zoals Vitalik Butterin, vinden dit systeem niet gedecentraliseerd genoeg (Mitra, 2019).[80] Ook denken zij dat dit model leidt tot stemmersapathie – een situatie

[80] Vitalik Buterin heeft bij de Blockchain Connect Conference (2019) het volgende gezegd:

> "When a blockchain project claims 'We can do 3,500 TPS because we have a different algorithm,' what we raelly mean is 'We are a centralized pile of trash because we only have 7 nodes running the entire thing.'"

waarin de community niet de tijd en moeite neemt om te stemmen op witnesses en delegates. Eenmaal gestemd, zullen apathische stemmers hun stem laten staan en niet meer heroverwegen, of ze zullen gewoonweg niet stemmen. Tot slot is het ook mogelijk dat witnesses allianties vormen en besluiten om op elkaar te stemmen, zodat zij allen onder de groep actieve witnesses vallen die blokken mogen produceren.

6.9.4 De manier waarop blokken worden geproduceerd en transacties worden geverifieerd

Tot slot kun je de schaalbaarheid vergroten door de manier waarop blokken worden geproduceerd en transacties worden geverifieerd aan te passen. Ook kun je de transactiedata aanpassen, zodat deze bijvoorbeeld kleiner worden. Het Waves Next Generation (Waves-NG) protocol is een voorbeeld waarbij meer transacties per seconde mogelijk worden gemaakt, door de manier waarop blokken worden geproduceerd te wijzigen.[81] Daarnaast is het ook mogelijk om eerst transacties buiten het blockchainnetwerk te laten plaatsen, voordat de netto verrekening ervan naar het netwerk wordt gestuurd en wordt geverifieerd door mijners.[82] Dit is wat het Bitcoin lightning netwerk doet. Verder zijn er nog andere manieren zoals sharding en plasma. Wij lichten deze drie schalingsoplossingen verder toe.

Lightning netwerk

We bespreken het lightning netwerk, omdat deze al is geïmplementeerd en tot veel discussies heeft geleid binnen de Bitcoin community. Het lightning netwerk wordt mogelijk gemaakt door een specifiek type nodes, de lightning nodes. Lightning nodes vallen noch onder full nodes, noch onder lightweight nodes.

Het ***lightning netwerk*** werd geïntroduceerd binnen het Bitcoin-netwerk om transacties buiten de blockchain om te regelen, zodat het netwerk werd ontlast. Transacties buiten de blockchain om worden ook wel ***off-chain***transacties genoemd. Ze lossen de volgende drie problemen op:

1. Bitcoin kan maar ongeveer 7 transacties per seconde verwerken, waardoor vele transacties in de mempool blijven hangen. Door het lightning netwerk kunnen meer transacties per seconde worden verwerkt, zonder dat het netwerk zwaarder wordt belast.

[81] Het Waves-NG-protocol is gebaseerd op het voorstel van Eyal et al. om Bitcoin te schalen met een nieuw protocol, genaamd Bitcoin Next Generation. Dit voorstel werd echter niet geïmplementeerd voor Bitcoin. De white paper van Bitcoin-NG kun je hier vinden: https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf.

[82] Dit is een voorbeeld van een off-chainoplossing.

2. Het netwerk van Bitcoin kan door de vele transacties verstopt raken. Dit leidt tot hogere transactiekosten, omdat mijners liever transacties met hogere fees toevoegen aan hun blok. Zij ontvangen bij het vinden van een geldige blok namelijk de fees. Gebruikers die hun transacties zo snel mogelijk verwerkt willen zien worden, geven daarom hogere fees mee. Het Bitcoin-netwerk is daardoor niet geschikt voor microbetalingen.
3. Ervan uitgaande dat een transactie in het volgende blok wordt opgenomen, duurt de transactiebevestiging gemiddeld 10 minuten. Dit kan een belemmering zijn voor winkeliers die graag willen zien dat een aankoop in hun winkel direct wordt goedgekeurd. Er is namelijk altijd een kleine kans dat de transactie toch niet wordt goedgekeurd en meegenomen in een blok. Sommige winkeliers zijn niet bereid om dat risico te lopen.

Het doel van de lightning nodes is om transacties off-chain plaats te laten vinden tegen lagere kosten, zodat het schaalbaarheidsprobleem wordt opgelost. Deze off-chaintransacties worden later geschreven naar de blockchain. Het netwerk van lightning nodes wordt het lightning netwerk genoemd. Het Lightning netwerk is ontworpen door Joseph Poon en Thaddeus Dryja in 2015. Het is een extra netwerk op het Bitcoin-netwerk en wordt om deze reden ook wel een ***layer 2-oplossing*** genoemd. Layer 2-oplossingen veranderen de regels van de onderliggende blockchain niet.

Om een transactie te bewerkstelligen op het lightning netwerk, stuurt persoon A een transactie naar het lightning netwerk, met een wallet die lightning ondersteunt. Vervolgens leg je een verbinding met een lightning node die de transactie ontvangt. We noemen hem persoon B. De verbinding tussen persoon A en persoon B wordt een betaalkanaal genoemd. Persoon A en persoon B kunnen off-chaintransacties versturen naar elkaar en alleen de netto verrekening sturen naar de blockchain. De verbinding tussen persoon A en persoon B hoeft niet altijd een directe verbinding te zijn. Er kunnen lightning nodes tussen zitten. Het grote nadeel van het lightning netwerk is dat de ontvangende partij wel online moet zijn. [83]

Sharding

In huidige blockchainpotocollen, verifiëren en verwerken alle nodes die een kopie van de blockchain hebben alle transacties. Dit komt de beveiliging van de blockchain ten goede, maar limiteert ook de schaalbaarheid van de blockchain. De vraag die ***sharding*** probeert op te lossen is of het mogelijk is dat er binnen een blockchain een kleine subset van nodes transacties

[83] Voor meer informatie over het lightning netwerk, zie: 'The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments' (Poon & Dryja, 2016).

verifieert, zonder dat de veiligheid in het geding komt. Verder is het een vereiste dat de nodes die onder de subset vallen geen supercomputers hoeven te zijn, zodat niet alleen mensen met hoogstaande hardware kunnen deelnemen aan het beveiligen van het netwerk. Door elke subset van nodes te laten focussen op het verwerken van andere transacties, kunnen verschillende subsets van nodes parallel transacties verwerken en hiermee de blockchain schaalbaarder maken.

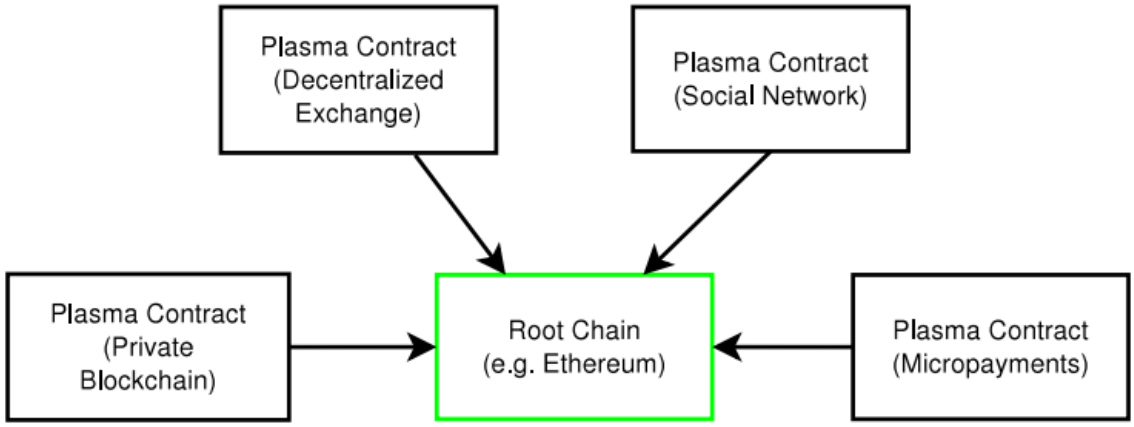
Bij sharding wordt de blockchain opgesplitst in partities, ook wel "shards" genoemd. Elke shard krijgt dan een eigen transactiegeschiedenis, zodat de nodes die een shard onderhouden alleen de transacties hoeven te verwerken die relevant zijn voor de shard. Het is wel van belang dat er voldoende nodes binnen de subset transacties verifiëren, zodat het systeem veilig is.[84]

Plasma

Plasma is een andere schalingsoplossing waar momenteel aan gewerkt wordt. Net als het Lightningnetwerk, is het een layer 2-oplossing. Het concept is ontworpen door Vitalik Buterin en Joseph Poon in augustus 2017 en is bedoeld om Ethereum op te schalen naar meer dan miljoenen transacties per seconde. Het is een framework om off-chain ***side chains*** te creëren die allen communiceren met de ***hoofdchain***, ook wel ***root chain*** genoemd, van Ethereum. Deze side chains worden ook wel ***child chains*** of ***plasmachains*** genoemd. Elke child chain kun je zien als een nieuwe blockchain die regelmatig hun staat naar de hoofdchain stuurt. Hierdoor kunnen bijvoorbeeld 1.000 transacties die normaal gesproken op de hoofdchain plaatsvinden, plaatsvinden op de side chains en alleen de resulterende staat van de side chains laten opnemen op de hoofdchain.

De bedoeling is dat iedereen een eigen side chain kan creëren voor verschillende use cases. Zo kan er bijvoorbeeld een side chain zijn voor een gedecentraliseerde exchange, een private blockchain, een sociaal netwerk. Plasma is dus een netwerk van blockchains die allemaal gelinkt zijn aan de hoofdchain.

[84] Voor meer informatie over sharding, zie de Ethereum Github pagina over sharding: https://github.com/ethereum/wiki/wiki/Sharding-FAQ.



Afbeelding 74: Een netwerk van side chains die gelinkt zijn aan de hoofd chain. Hoewel het is concept ontwikkeld was voor Ethereum, kan Plasma ook geïmplementeerd worden voor andere blockchains. (Poon & Buterin, 2017)

6.9.5 Blockchainactiviteit

De website www.blocktivity.info houdt bij hoeveel activiteit er is op verscheidene blockchains. Hierbij wordt er gekeken naar het aantal operaties dat erop plaatsvindt en niet naar het aantal transacties. Een operatie kan een transactie zijn van bijvoorbeeld een coin, maar kan ook andere acties zijn, zoals bijvoorbeeld stemmen op de blockchain, een commentaar plaatsen op de blockchain en het creëren van een account op de blockchain.

In onderstaande afbeelding vind je een screenshot van 10 blockchains met de meeste activiteiten volgens Blocktivity.[85] Wat opmerkelijk is, is dat Bitcoin, verreweg de bekendste blockchain, slechts op de vijfde plek staat met bijna een miljoen operaties in de afgelopen dag. AVI staat voor ***Activity Valuation Index*** en is de ratio tussen de blockchainactiviteit en de marktkapitalisatie van de blockchain.

$$Activity\ Valuation\ Index = \frac{Blockchainactiviteit}{Marktkapitalisatie}$$

[85] Er zijn tegenwoordig talloze blockchains. Niet alle blockchains zijn opgenomen in de analyse. Daarnaast is het de vraag in hoeverre je blockchains met elkaar kunt vergelijken door alleen het aantal operaties bij elkaar op te tellen, omdat niet alle operaties even belangrijk zijn. Zie Blocktivity's artikel, getiteld 'Operation Vs Transaction, the Blocktivity big debate' (2018), voor een verdere discussie hierover.

Wat voor ons belangrijk is, is de CUI, de ***Capacity Utilization Index*.** De CUI is de ratio tussen de dagelijkse blockchainactiviteit en de totale blockchaincapaciteit.

$$Capacity\ Utilization\ Index = \frac{Dagelijkse\ blockchainactiviteit}{Blockchainactiviteit}$$

#	Name	Activity	Average (7d)	Record	Market Cap	AVI	CUI
1	EOS	50,346,877 Op	46,788,744 Op	74,568,958 Op	$ 2.4 B	6,276	
2	TLOS	7,393,330 Op	7,035,055 Op	32,217,207 Op	$ 0.014 B	159,198	
3	XLM	1,288,980 Op	1,221,975 Op	1,362,118 Op	$ 0.903 B	423	
4	TRX	1,030,726 Op	813,070 Op	5,306,869 Op	$ 0.909 B	336	
5	KIN	1,018,726 Op	947,060 Op	5,258,216 Op	$ 0.004 B	76,910	
6	STEEM	996,699 Op	996,491 Op	2,522,380 Op	$ 0.047 B	6,323	
7	IOST	965,547 Op	1,106,990 Op	1,343,244 Op	$ 0.062 B	4,626	
8	NANO	663,230 Op	226,787 Op	1,007,236 Op	$ 0.088 B	2,228	
9	ETH	624,754 Op	607,056 Op	1,372,918 Op	$ 14 B	13	
10	BSV	525,228 Op	505,638 Op	900,436 Op	$ 1.6 B	100	
11	BTS	518,177 Op	344,376 Op	6,112,075 Op	$ 0.043 B	3,534	
12	TFD	516,242 Op	732,884 Op	1,246,665 Op	$ 0.004 B	37,857	
13	BTC	447,849 Op	468,731 Op	1,178,080 Op	$ 133 B	1.0	

Afbeelding 75: Top 13 blockchains met de meeste activiteiten op www.blocktivity.com. Geraadpleegd op 24 december, 2019. EOS heeft de afgelopen 7 dagen gemiddeld 50 miljoen operaties per dag gehad. Bitcoin daarentegen had gemiddeld bijna 450 duizend transacties.

Bitcoin heeft op 24 december ongeveer 50% van haar blockchaincapaciteit gebruikt en er zijn bijna 18.000 transacties in de wachtrij die nog niet zijn opgenomen in de blockchain. Ethereum heeft ongeveer 50% van haar capaciteiten gebruikt. Als Bitcoin en Ethereum wijdverbreid geadopteerd willen worden, dan moeten zij hun capaciteiten aanzienlijk vergroten. EOS daarentegen zit rond de 11% van haar capaciteiten, Tron (TRX) zit rond de 1% en BTS zit op 0,1%.

6.10 Samenvatting, begrippen en bronnen

Samenvatting

Tot nog toe hebben we één oplossing besproken voor het Byzantine Generals Problem: het Proof-of-Work-consensusprotocol, zoals deze bijvoorbeeld bij Bitcoin is ingericht. Volgens dit protocol mag een datablok alleen worden toegevoegd aan de blockchain wanneer er een geldige hash van het blok is gevonden. Bij Proof-of-Stake is het mogen produceren van een blok afhankelijk van (a) een willekeurig selectieproces en (b) een 'stake' als bijvoorbeeld het aantal coins dat je bezit. Dat betekent dat er bij Proof-of-Stake geen dure mijningapparatuur benodigd is. De blokproducent bij Proof-of-Stake heet dan ook geen mijner, maar wordt een forger genoemd.

Er zijn binnen Proof-of-Stake veel verschillende varianten. Wij hebben de volgende vier besproken:

1. Delegated Proof-of-Stake (dPoS).
2. Leased Proof-of-Stake (lPoS).
3. Proof-of-Stake Velocity (PoSV).
4. Proof-of-Authority (PoA).

Hierbij moet wel gezegd worden dat het dubieus is of Proof-of-Authority onder Proof-of-Stake valt. Het wordt soms gezien als een vorm van Delegated Proof-of-Stake.

Bij Delegated Proof-of-Stake kun je niet zomaar je coins staken om nieuwe blokken te mogen produceren. Een Delegated Proof-of-Stake-systeem kun je het best vergelijken met een voortdurende representatieve democratie waarbij iedereen die een coin heeft kan stemmen op witnesses en delegates (gedelegeerden). De rol van witnesses is om transacties te valideren en nieuwe blokken te mogen produceren. Voor het verlenen van deze service krijgen zij een beloning per geproduceerd blok. Delegates spelen geen rol in het verifiëren van transacties en het valideren en produceren van blokken. De rol van delegates is om de governance structuur van het blockchainprotocol te overzien.

Met leased Proof-of-Stake kan iedereen zijn coins leasen aan staking nodes. Wanneer deze staking nodes meer coins als lease hebben gekregen, is de kans dat de staking nodes een blok mogen produceren groter. De staking nodes zullen de beloning dan proportioneel verdelen tussen henzelf en iedereen die coins heeft geleased aan hen.

Wat Proof-of-Stake Velocity onderscheidt van klassieke Proof-of-Stake is dat gebruikers worden beloond voor (a) het aantal coins dat zij houden en (b) hoe actief zij hun coins gebruiken. De community wordt dus gestimuleerd om niet alleen de coins te bewaren, maar ze ook daadwerkelijk te gebruiken voor transacties.

Bij Proof-of-Authority worden de blokproducenten (authority nodes) geauthentiseerd en goedgekeurd op basis van hun identiteit en reputatie. Door de reputatie te linken aan identiteit, worden authority nodes extra gestimuleerd om goed gedrag te vertonen en geen malafide transacties op te nemen in de blockchain. Mochten zij dat wel doen, dan brengt dat reputatieschade met zich mee.

Er zijn bepaalde voordelen aan Proof-of-Stake ten opzichte van Proof-of-Work. Wat Proof-of-Stake voordeliger maakt zijn:

1. Energie-efficiëntie.
2. Door het gemak om te staken kan de blockchain beter gedistribueerd worden.
3. Het uitvoeren van een 51%-aanval is minder aantrekkelijk.

De schaalbaarheid van een blockchain is mede gelinkt aan het consensusmechanisme dat wordt gebruikt. Omdat er veel verschillende varianten van Proof-of-Stake zijn, trekken we geen eenduidige conclusie dat Proof-of-Stake blockchains altijd schaalbaarder zijn dan Proof-of-Work blockchains. Over het algemeen kunnen we wel stellen dat de schaalbaarheid van een blockchain afhankelijk is van:

1. De bloktijd (block time).
2. De blokgrootte (block size).
3. Het distributie- of decentralisatieniveau van de blockchain.
4. De manier waarop blokken worden geproduceerd, transacties worden verstuurd naar de blockchain en transacties worden geverifieerd.

Enkele schalingsoplossingen die zijn geïmplementeerd of die momenteel nog worden onderzocht zijn het lightning netwerk, sharding en plasma.

Tot slot is het belangrijk om te beseffen dat de marktkapitalisatie van een blockchain niet altijd betekent dat de blockchain ook daadwerkelijk meer mutaties verwerkt.

Opmerkingen die je nu kunt uitleggen

- Proof-of-Stake is energiezuiniger dan Proof-of-Work, omdat er geen concurrentie is op computerkracht bij de blokproductie.
- Delegated Proof-of-Stake kan meer transacties per seconde verwerken dan blockchains die gedecentraliseerder zijn.
- Bij Leased Proof-of-Stake worden mensen extra gestimuleerd om deel te nemen aan het staking proces.
- Het is mogelijk om een variant te maken van Proof-of-Stake waarbij de kans om een nieuwe blok te mogen aanmaken niet volledig afhankelijk is van het aantal munten dat je staket.
- Proof-of-Authority lijkt op Delegated Proof-of-Stake, maar wordt meer gebruikt in gesloten, permissioned blockchains.
- Je kunt de schaalbaarheid vergroten door transacties off-chain te laten plaatsvinden.

Verklarende begrippenlijst

Activity Valuation Index: De ratio tussen de blockchainactiviteit en de marktkapitalisatie van de blockchain.

Bandbreedte: De hoeveelheid data die er tegelijkertijd over een bepaalde verbinding kan worden vervoerd. Hoe groter de bandbreedte, hoe sneller je de data kunt ontvangen en versturen.

Capacity Utilization Index: De ratio tussen de dagelijkse blockchainactiviteit en de totale blockchaincapaciteit.

Child chain: Zie side chain.

Decentralisatieniveau: Hoe gedecentraliseerd een blockchain is. Een blockchain met meer nodes die een kopie van de blockchain onderhouden is gedecentraliseerder dan een blockchain met een kleiner groep aan nodes.

Delegate (gedelegeerde): Een delegate wordt gekozen om de governance structuur van een Delegated Proof-of-Stake blockchainprotocol te overzien. Zij kunnen bijvoorbeeld een voorstel indienen om de grootte van de blokken of om de beloning voor witnesses te wijzigen. Als een delegate een voorstel heeft ingediend, kan de community voor of tegen stemmen.

Delegated Proof-of-Stake (DPoS): Een consensusmechanisme waarbij een select groepje witnesses blokken produceert. Deze witnesses worden democratisch gekozen door de community.

DPoS: Zie Delegated Proof-of-Stake.

Forger: Iemand die bij een Proof-of-Stake blockchain zijn coins staket om een blok te produceren. Bij Proof-of-Work is het de mijner die computerkracht levert om blokken te mogen produceren.

Gedecentraliseerde exchange (DEX): Een handelsbeurs die is gebouwd op een blockchain. Door gebruik te maken van blockchaintechnologie, worden veel beveiligingsissues opgelost.

Leased Proof-of-Stake (LPoS): Met Leased Proof-of-Stake kun je je coins leasen aan staking nodes. Wanneer deze staking nodes meer coins als lease hebben gekregen, is de kans dat de staking nodes een blok mogen produceren groter. De staking nodes zullen de beloning dan proportioneel verdelen tussen henzelf en iedereen die coins heeft geleased aan hen.

Lightning netwerk: Een schalingsoplossing door transacties off-chain te laten plaatsvinden voordat de verrekening van de transacties wordt gestuurd naar de blockchain. Hiermee wordt het blockchainnetwerk ontlast.

LPoS: Zie Leased Proof-of-Stake.

Off-chain: Buiten de blockchain om.

Permissioned: Een permissioned blockchain is een blockchain waarbij je eerst toestemming moet krijgen om als validator van blokken en blokproducent op te kunnen treden.

Plasma: Een schalingsoplossing waarbij er side chains (child chains of plasmachains) worden gemaakt die gekoppeld worden aan de hoofdchain (root chain). Je kunt side chains zien als nieuwe blockchains die regelmatig hun staat naar de hoofdchain sturen. Plasma is dus een netwerk van blockchains die gelinkt zijn aan de hoofdchain.

Plasmachain: Zie side chain.

PoA: Zie Proof-of-Authority.

POS: Zie Proof-of-Stake.

PoSV: Zie Proof-of-Stake Velocity.

Proof-of-Authority (PoA): Blokproducenten bij Proof-of-Authority (authority nodes) worden eerst geauthentiseerd en goedgekeurd op basis van hun identiteit en reputatie. Door de reputatie te linken aan identiteit, worden authority nodes extra gestimuleerd om goed gedrag te vertonen en geen malafide transacties op te nemen in de blockchain. Dit consensusmechanisme wordt voornamelijk in gesloten en permissioned blockchains gebruikt.

Proof-of-Stake: Een consensusmechanisme waarbij een blokproducernt wordt gekozen op basis van een willekeurig selectieproces en de stake die ze bezitten.

Proof-of-Stake Velocity (PoSV): Is een variant van Proof-of-Stake dat probeert te voorkomen dat mensen hun coins oppottten. Gebruikers worden beloond voor het aantal coins dat zij houden en hoe actief zij hun coins gebruiken.

Schaalbaarheid: De verwerkingscapaciteit van een blockchain. Hierbij wordt voornamelijk gekeken naar het aantal transacties per seconde dat een blockchain kan verwerken.

Sharding: Een schalingsoplossing waarbij de blockchain wordt opgesplitst in partities, ook wel "shards" genoemd. Elke shard krijgt dan een eigen transactiegeschiedenis, zodat de nodes die een shard onderhouden alleen de transacties hoeven te verwerken die relevant zijn voor de shard. Het is wel van belang dat er voldoende nodes binnen de subset transacties verifiëren, zodat het systeem veilig is.

Side chain: Een chain die is gelinkt aan de root chain. Zie plasma.

Stake: Een aandeel dat een person bezit in een blockchain, uitgedrukt in het aantal coins dat hij bezit.

Staking: Het vasthouden van coins in een cryptowallet voor het ondersteunen van het blockchainnetwerk. De kans dat je een blok mag produceren bij Proof-of-Stake is afhankelijk van het aantal coins dat je staket.

Witness: Een witness wordt gekozen om transacties te valideren en nieuwe blokken te mogen produceren. Voor het verlenen van deze service krijgen zij een beloning per geproduceerd blok.

Bronnen

de Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain - ePrints Soton. *Soton.Ac.Uk*. https://doi.org/https://eprints.soton.ac.uk/415083/1/bc_consensus_alg.pdf

BitShares. (z.d.). BitShares. Geraadpleegd op 27 december 2019, van Bitshares.org website: https://wallet.bitshares.org

Blocktivity. (2018, 29 november). Operation Vs Transaction, the Blocktivity big debate. Geraadpleegd op 27 december 2019, van Busy website: https://busy.org/@blocktivity/operation-vs-transaction-the-blocktivity-big-debate

Blocktivity. (z.d.). Block'tivity. Geraadpleegd op 27 december 2019, van Blocktivity.info website: https://www.blocktivity.info/

Casey, M., & Vigna, P. (2019). *The truth machine : the blockchain and the future of everything*. New York, Ny: Picador ; St. Martin's Press.

Ethereum. (z.d.). , github.com/ethereum/wiki/wiki/Sharding-FAQ. Accessed 29 Dec. 2019.

Evan. (2019, 22 maart). How many transactions per second can Bitcoin Cash handle? Geraadpleegd op 27 december 2019, van Coinanalysis website: https://coinanalysis.io/how-many-transactions-per-second-bitcoin-cash/

Eyal, I., Robbert Van Renesse, Efe, A., Emin, G., Sirer, G., Gencer, A. E., … van Renesse, R. (2015). Bitcoin-NG: A Scalable Blockchain Protocol. Geraadpleegd van arXiv.org website: https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf

Luke Dashjr. (19 mei 2019). Luke Dashjr 'Briefly, Why Block Sizes Shouldn't Be Too Big [YouTube]. Geraadpleegd van https://youtu.be/CqNEQS80-h4

Mitra, R. (2019, 8 februari). Vitalik Buterin calls EOS, TRON, and NEO "centralized piece of trash." Geraadpleegd op 27 december 2019, van FXStreet website: https://www.fxstreet.com/cryptocurrencies/news/vitalik-buterin-calls-eos-tron-and-neo-centralized-piece-of-trash-201902080151

Payments. Geraadpleegd van https://lightning.network/lightning-network-paper.pdf

PIVX. (2019). PIVX. Geraadpleegd op 27 december 2019, van PIVX website: http://www.pivx.org/

Poon, J., & Buterin, V. (2017). *Plasma: Scalable Autonomous Smart Contracts*. Geraadpleegd van https://plasma.io/plasma.pdf

Poon, J. & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant

Visa. (2019). Visa Fact Sheet. Geraadpleegd op 27 december 2019, an VISA website: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

Iconen

Community en munten gemaakt door Freepik van www.flaticon.com

7. 51%-aanvallen en decentralisatie

"As revolutionary as it sounds, Blockchain truly is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved. Above anything else, the most critical area where Blockchain helps is to guarantee the validity of a transaction by recording it not only on a main register but a connected distributed system of registers, al of which are connected through a secure validation mechanism."

- Ian Khan (z.d.)

7.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat het fundamentele verschil is in het beveiligingsmodel van open blockchains en traditionele netwerken.
- Wat het blockchaintrilemma is.
- Wat een 51%-aanval is en hoe een Proof-of-Work blockchain kan worden aangevallen middels een dergelijke aanval.
- Hoe een 51%-aanval kan plaatsvinden op een Proof-of-Stake blockchain.
- Dat er verschillende niveaus van decentralisatie zijn bij de volgende aspecten van een blockchain: architectureel, politiek en logisch.
- Wat de belangrijkste redenen zijn voor decentralisatie.

Inleiding

Zoals besproken in hoofdstuk 3 is blockchain een oplossing voor het Byzantine Generals Problem. De oplossing zit hem in het bereiken van consensus.

In dit hoofdstuk bespreken we eerst in paragraaf 7.2 het fundamentele verschil in het beveiligingsmodel van Proof-of-Work en Proof-of-Stake en zetten deze af tegen het beveiligingsmodel van traditionele systemen, dat gebruikmaakt van toegangscontroles. Daarna behandelen we in 7.3 het blockchaintrilemma. Het trilemma geeft weer dat er trade-offs zijn in schaalbaarheid, beveiliging en decentralisatie. In paragraaf 7.4 komen 51%-aanvallen aan bod

bij Proof-of-Work en Proof-of-Stake blockchains. We behandelen hier hoe personen met malafide bedoelingen een aanval kunnen uitvoeren op de blockchain door een meerderheid van de consensus te kapen. Vervolgens geven we een verdieping op het begrip decentralisatie in paragraaf 7.5. Hierin komt naar voren dat er op verschillende niveaus decentralisatie mogelijk is. Het doel van de paragraaf is om je meer bewust te maken van de verschillende aspecten van decentralisatie binnen blockchains en organisaties. Tot slot sluiten we af met paragraaf 7.6 waarin een samenvatting, een lijst van belangrijke begrippen en de bronnenlijst van het hoofdstuk staan.

7.2 Beveiligingsmodel: toegangscontroles of open

Het beveiligingsmodel van Proof-of-Work en Proof-of-Stake is fundamenteel anders dan dat van traditionele systemen. Traditionele systemen hebben ***toegangscontroles*** voor gebruikers, zodat malafide gebruikers de toegang kan worden ontzegd. Om toegang te krijgen tot bijvoorbeeld een omgeving dien je geauthentiseerd te worden. Het fundamentele verschil hier met blockchainsystemen die we tot dusver hebben besproken is dat deze traditionele netwerken vertrouwen moeten hebben dat degenen die toegang hebben tot het systeem niet malafide zijn. Zo moet je bijvoorbeeld de beheerder van de database, of zelfs de gebruikers die informatie schrijven naar de database, vertrouwen. Het resultaat van dergelijke systemen is dat het vaak gesloten en kleine netwerken zijn.

Blockchainsystemen als bijvoorbeeld Bitcoin en Ethereum zijn daarentegen open. Er is geen authenticatie nodig van gebruikers en iedereen mag data proberen te schrijven naar de blockchain. Het vertrouwensmodel is hierbij dus niet gebaseerd op toegangscontroles, maar op het feit of de mijners een lastig hashingprobleem weten op te lossen of niet en of er consensus bestaat over de staat van de blockchain. Er is geen centrale autoriteit of vertrouwde derde partij in het consensus netwerk. Malafide gebruikers kunnen zich ook niet voordoen als een vertrouwde derde partij, omdat die er niet zijn. Er is ook niemand die master keys kan stelen om het netwerk plat te leggen, want deze master keys bestaan niet. Hierdoor kunnen deze netwerken open zijn voor iedereen.[86]

Andreas Antonopoulos noemt dergelijke systemen open, grenzeloos, neutraal, resistent tegen censuur en publiekelijk. Ze zijn open, omdat iedereen toegang heeft tot de blockchain. Daarnaast is het open voor ontwikkelaars die een bijdrage willen leveren aan de

[86] Zie 'Bitcoin securitymodel: Trust by computation' (Antonopolous, 2014).

blockchainsoftware. Ze zijn grenzeloos, omdat ze toegankelijk zijn voor iedereen op de wereld. Hierdoor is het ook zo lastig voor nationale overheden en centrale banken om ze te reguleren. Ze zijn neutraal, omdat macht niet kan worden gecentraliseerd. Iedereen die deelneemt aan het ecosysteem houdt zich aan het consensusprotocol. Niemand heeft extra privileges die niet zijn opgenomen in het protocol. Ze zijn resistent tegen censuur, omdat de staat van de blockchain niet zomaar kan worden gewijzigd, zonder dat er consensus bestaat. Ze zijn publiekelijk, omdat de blockchain is gedistribueerd over elke computer die een full node draait.[87]

Open blockchains

Open blockchains bevatten volgens Andreas Antonopoulos de volgende vijf eigenschappen:

1. Open source.
2. Grenzeloos.
3. Neutraal.
4. Resistent tegen censuur.
5. Publiekelijk.

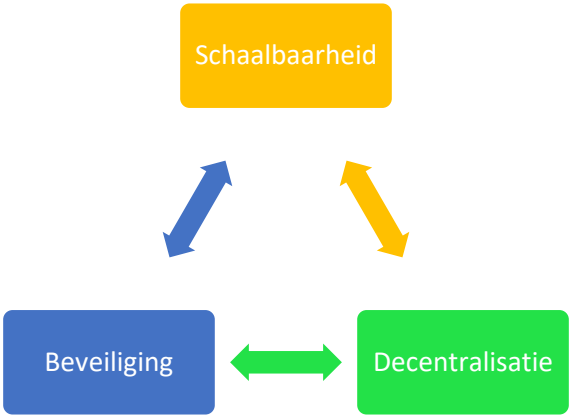
In hoofdstuk 9 komen publieke, private en consortiumblockchains aan bod. Daarnaast wordt in dat hoofdstuk ook het verschil tussen open en gesloten blockchains nader uitgelegd.

7.3 Het blockchaintrilemma

In de blockchainwereld wordt er regelmatig gesproken van het ***blockchaintrilemma*** om aan te geven dat er trade-offs zijn in de volgende drie eigenschappen van een blockchain:

1. Schaalbaarheid.
2. Beveiliging.
3. Decentralisatie.

[87] Zie ook de lezing van Andreas Antonopoulos over Open Blockchains vs Bullshit (Antonopoulos, 2017).



Afbeelding 76: Het blockchaintrilemma.

Een zeer gedecentraliseerde blockchain is beter beveiligd, maar dat gaat ten koste van de schaalbaarheid. De Bitcoin blockchain is daar een voorbeeld van. Als het zeer schaalbaar én gecentraliseerd is, is het minder goed beveiligd. Private blockchains zijn hier een voorbeeld van. Blockchainprojecten dienen om deze reden een goede afweging te maken tussen deze drie eigenschappen. (The European Union Blockchain Observatory and Forum, 2019, pp. 10-11)

7.4 51%-aanval

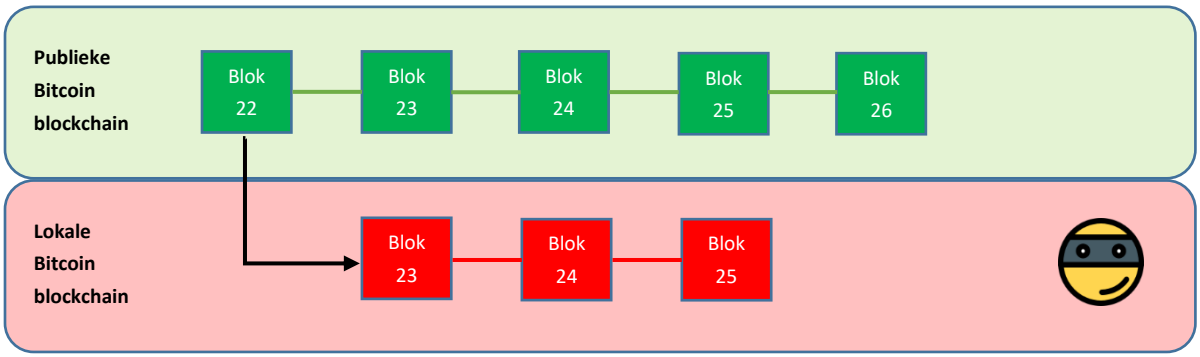
Omdat het vertrouwensmodel van blockchains gedecentraliseerd is en berust op consensus, is het mogelijk om blockchains aan te vallen door consensus te kapen met een ***51%-aanval***.
Wij behandelen hoe een 51%-aanval kan plaatsvinden bij zowel Proof-of-Work als bij pure Proof-of-Stake. Omdat verschillende blockchains ook verschillende consensusprotocollen hebben, kunnen de manieren waarop 51%-aanvallen worden uitgevoerd onderling verschillen.

7.4.1 Proof-of-Work

Zoals eerder is uitgelegd, is de ware blockchain altijd de langste blockchain. Om een succesvolle 51%-aanval uit te kunnen voeren dien je daarom de langste blockchain te creëren. Om dit te bewerkstelligen, dient de aanvaller een meerderheid te bemachtigen van de totale rekenkracht op het netwerk.

Waarom zou iemand een 51%-aanval willen uitvoeren? Een belangrijke reden om dit te doen is om Bitcoins te kunnen double-spenden. Een dergelijke aanval verloopt in de volgende vijf stappen. Hierbij gaan we ervan uit dat een malafide mijner al de beschikking heeft over een meerderheid van de hashing power en daardoor sneller blok hashes kan genereren dan de rest van het netwerk bij elkaar.

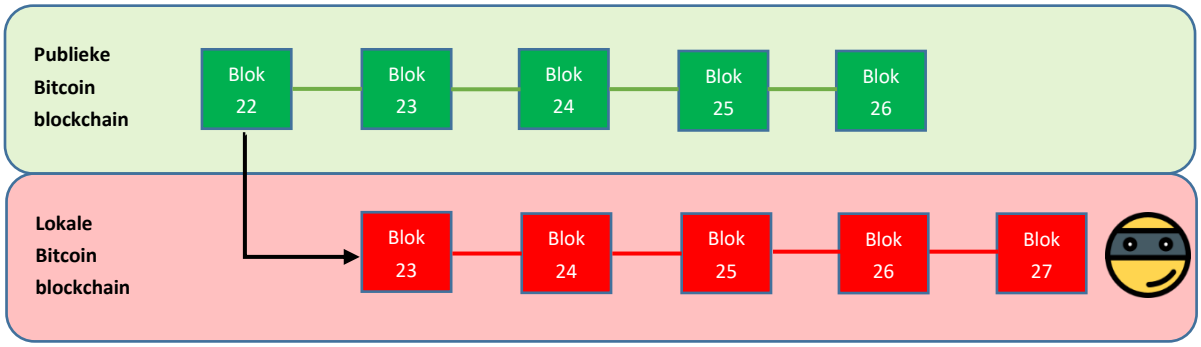
1. Eerlijke mijners voegen blokken toe aan de publieke Bitcoin blockchain en zenden deze uit over het netwerk. Ondertussen voegt de malafide mijner blokken toe aan de Bitcoin blockchain die hij lokaal houdt op zijn eigen computer. Echter, zendt hij de blokken die hij toevoegt niet uit naar het netwerk voor validatie.



Afbeelding 77: Stap 1 van een 51%-aanval op Proof-of-Work.

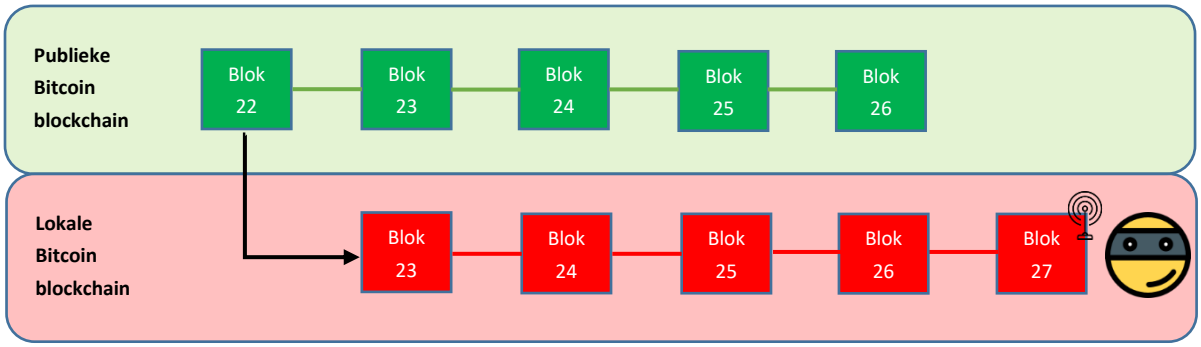
2. De malafide mijner spendeert zijn Bitcoin op de publieke blockchain in blok 25 – bijvoorbeeld voor de aankoop van een Lamborghini. De transactie wordt goedgekeurd door het netwerk en opgenomen in blok 26. De verkoper heeft niet door dat hij te maken heeft met een malafide mijner en geeft hem een Lamborghini mee. Ondertussen voegt de mijner deze transactie niet toe aan zijn lokale Bitcoin blockchain.

3. Eerlijke mijners blijven blokken toevoegen aan de publieke blockchain. Er worden echter niet meer zo snel nieuwe blokken toegevoegd, omdat de malafide mijner zijn computerkracht heeft onttrokken aan de publieke chain. Hij richt zijn computerkracht op het produceren van nieuwe blokken op zijn eigen lokale blockchain. Aangezien hij meer hashing power heeft dan alle eerlijke mijners op de publieke blockchain samen, kan hij sneller blokken aanmaken. Hij haalt de publieke blockchain in en heeft nu een langere blockchain.



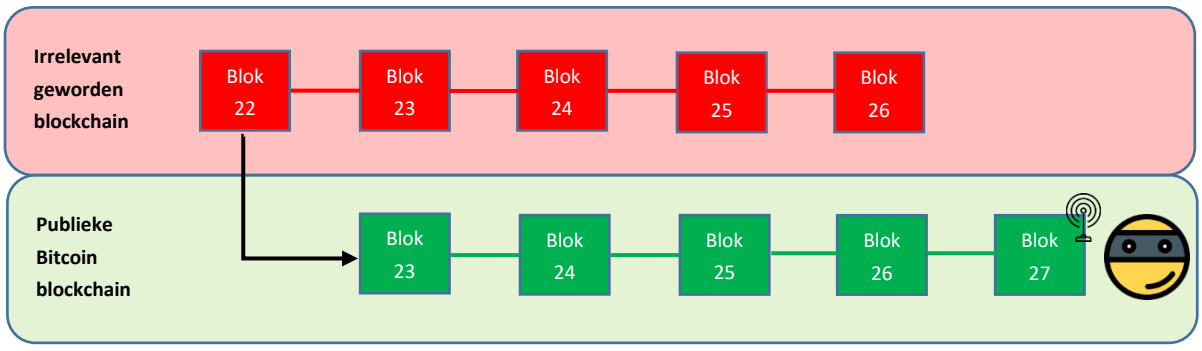
Afbeelding 78: Stappen 2 en 3 van een 51%-aanval op Proof-of-Work.

4. Eerlijke mijners volgen altijd het protocol en het protocol mandateert dat zij de langste versie van de blockchain moeten volgen. De malafide mijner zendt zijn langere versie van de blockchain uit naar de rest van het publieke netwerk. Dit zorgt ervoor dat de eerlijke mijners automatisch overgaan op de blockchainversie van de malafide mijner. Alle Bitcoin-balansen en vorige transacties zullen in overeenstemming met de malafide blockchain worden geüpdatet.



Afbeelding 79: Stap 4 van een 51%-aanval op Proof-of-Work.

5. De oude publieke blockchain wordt verlaten, omdat deze korter is. Alle data binnen deze gehele blockchain is nu irrelevant geworden. Omdat de Bitcoins die hij op de publieke blockchain heeft uitgegeven aan een Lamborghini nooit zijn gespendeerd op zijn lokale blockchain, krijgt de malafide mijner weer de beschikking over deze Bitcoins en kan hij ze nogmaals spenderen. Met andere woorden, de malafide mijner kan zijn Bitcoins double-spenden.



Afbeelding 80: Stap 5 van een 51%-aanval op Proof-of-Work.

Hoewel het uitermate lastig is voor een enkele malafide mijner om een meerderheid van de hashing power te bemachtigen, is dit toch aanzienlijk makkelijker voor mijningpoolbeheerders als zij besluiten samen te zweren.

7.4.2 Proof-of-Stake

Een 51%-aanval op een Proof-of-Stake blockchain werkt anders. Om een 51%-aanval op een Proof-of-Stake blockchain uit te voeren, dien je een meerderheid van de stake te hebben. Dat betekent dus dat je een meerderheid van de staking coin moet zien te bemachtigen. Deze coins kun je of kopen of verdienen met stakingbeloningen. Het verdienen van stakingbeloningen vereist dat je op de eerste plaats al tokens hebt.

Als je meer dan 50% van het beschikbare aanbod opkoopt, zal er een tekort komen aan liquiditeit op de markt met een flinke prijsstijging van de coin tot gevolg. Dit maakt het coördineren van de aanval, mogelijk gemaakt door de aankoop van de coins, financieel onaantrekkelijk. Daarnaast moedigt het gemak waarmee je coins kunt staken mensen aan om te staken. Hierdoor wordt de Proof-of-Stake blockchain meer gedecentraliseerd, wat het moeilijker maakt voor een partij om een meerderheid van de coins te verkrijgen.

Als er toch een 51%-aanval plaatsvindt op een blockchain, dan is er altijd nog de mogelijkheid om middels een hard fork de malafide transacties ongedaan te maken, of om een herstart te doen met een nieuwe ongeschonden chain. Liever gebeurt dit met volledige consensus van het netwerk. In het geval van Proof-of-Stake heeft de malafide mijner die de aanval heeft gecoördineerd veel financiële middelen verloren voor coins die uiteindelijk waardeloos zijn geworden. In het geval van Proof-of-Work heeft de malafide mijner dure mijningapparatuur aangeschaft. Na een mislukte 51%-aanval kan hij dezelfde apparatuur inzetten voor een aanval op een andere Proof-of-Work blockchain. Als een aanvaller van een Proof-of-Stake blockchain een andere Proof-of-Stake blockchain wil aanvallen, moet hij opnieuw een meerderheid van de coins van die andere chain bemachtigen. Dit maakt een 51%-aanval op een Proof-of-Stake chain over het algemeen minder aantrekkelijk.

Intermezzo: Overige aanvallen

Naast 51%-aanvallen zijn er nog andere talloze aanvallen die kunnen worden uitgevoerd op een blockchainproject. Net als bij traditionele internettoepassingen blijft blockchaintechnologie gevoelig voor diverse soorten aanvallen. Hierna volgen enkele voorbeelden:

1. Alle software bevat fouten, ook bij blockchaintechnologie. Deze fouten kunnen benut worden door kwaadwillenden. Dit risico kan beperkt worden door goede testmethoden vooraf en snel herstel van fouten zodra deze bekend worden.
2. Er zullen altijd mensen zijn met extra bevoegdheden, bijvoorbeeld de ontwikkelaars van software. Doorgaans vertrouwen we de ontwikkelaars, maar het is mogelijk dat kwaadwillenden zich toegang verschaffen tot de computers van de ontwikkelaars en daar stiekem wijzigingen aanbrengen in de software die later in gebruik wordt genomen. Hiertegen moeten goede maatregelen worden genomen, wat lastiger is als daar minder aandacht voor is vanwege een vrijere cultuur dan bijvoorbeeld bij banken.
3. Ook bij blockchaintoepassingen kunnen aanvallen op de infrastructuur worden uitgevoerd, bijvoorbeeld om de beschikbaarheid te verstoren.

Waar bij financiële instellingen veel geld en aandacht is voor het testen van de beveiliging, is bij publieke blockchaintoepassingen de aandacht soms meer op functionele werking en is er minder kennis en budget voor bovengenoemde aspecten.

Het is belangrijk om te beseffen dat blockchain niet de oplossing is voor alles en lang niet alle zwakheden opheft die op gecentraliseerde netwerken voorkomen. Ook blockchaintoepassingen hebben zwakheden die kunnen worden misbruikt. Verder zal blockchaintechnologie weer nieuwe uitdagingen met zich meebrengen en nieuwe manieren meebrengen om het netwerk aan te vallen. De 51%-aanval is één zo'n manier.

In het volgende tabel worden verscheidene aanvallen getoond die mogelijk zijn op een blockchainproject. Deze aanvallen zijn in de tabel onderverdeeld in vijf verschillende categorieën en kunnen verschillende oorzaken hebben (Mosakheil, 2018). Smart contracts worden in het volgende hoofdstuk behandeld.

Categorie Beveiligingsbedreigingen	Aanvalsvectoren	Oorzaken
Double-Spending bedreigingen	Race Attack	Transactie verificatiemechanisme
	Finney Attack	Transactie verificatiemechanisme
	Vector76 Attack	Transactie verificatiemechanisme
	Alternative History Attack	Transactie verificatiemechanisme
	Nothing-at-Stake Attack	Consensusmechanisme
	51% Attack	Consensusmechanisme
Mijning/Pool bedreigingen	Selfish Mining/Block-discard Attack	Consensusmechanisme
	Block-Withholding Attack	Consensusmechanisme
	Fork-After-Withhold Attack	Consensusmechanisme
	Bribery Attack	Consensusmechanisme
	Pool Hopping Attack	Consensusmechanisme
Wallet bedreigingen	Vulnerable signature	ECDSA zwakte, zwakke willekeurigheid
	Collision & Pre-Image Attack	Zwaktes in ECDSA, SHA256 en RIPEMD
	Flawed key generation	Zwaktes in ECDSA
	Bugs & Malware	Zwaktes in ECDSA
Netwerk bedreigingen	DDoS Attack	Externe resources
	Transaction Malleability Attack	Blockchainprotocol
	Timejacking Attack	Blockchainprotocol
	Partition Routing Attack	Internet routing
	Delay Routing Attack	Internet routing
	Sybil Attack	Gestructureerde P2P netwerklimitatie
	Eclipse Attack	Blockchainprotocol
	Balance Attack	Consensusmechanisme
	Punitive and Feather forking Attack	Consensusmechanisme
Smart Contracts bedreigingen	Vulnerabilities in contracts source code	Applicatiedesign
	Vulnerabilities in EVM Bytecode	EVM design
	Vulnerabilities in Blockchain	Programmadesign
	Eclipse Attack on Smart contract blockchain	EVM design

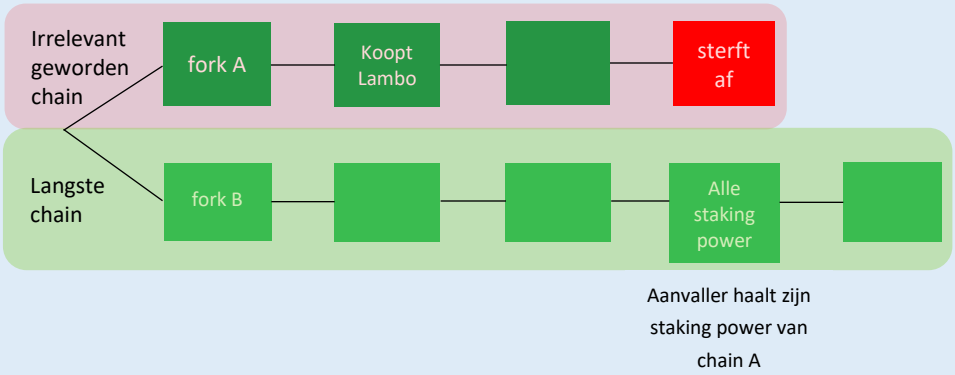
Wij zullen enkele van deze aanvallen toelichten.

Nothing-at-stake-aanval

De ***nothing-at-stake-aanval*** is een aanval die bij Proof-of-Stake voorkomt. Er kunnen bij Proof-of-Stake ook splitsingen (forks) in de blockchain voorkomen. Dit kan bijvoorbeeld gebeuren door soft forks of hard forks, maar ook wanneer er orphaned blokken ontstaan doordat er rond dezelfde tijd twee geldige blokken worden geproduceerd. Hierdoor zijn er (tijdelijk) twee chains. Bij Proof-of-Work heeft de mijner een gelimiteerde hoeveelheid computerkracht beschikbaar en zal hij deze proberen te richten op de chain waarvan hij verwacht dat die de langste chain gaat worden. De computerkracht die hij levert aan een chain die niet de langste chain wordt, is namelijk verloren elektriciteitkosten.

Bij Proof-of-Stake kan een forger zonder kosten op beide chains tegelijkertijd proberen een volgend blok aan te maken. Het aantal stake dat hij heeft is namelijk op beide chains hetzelfde. Door blokken proberen aan te maken op beide chains maakt het de forger niet uit welke van de chains de langste chain wordt, omdat hij zijn beloning toch wel krijgt als hij de blokproducent wordt van één van de chains. Forgers ontmoedigen dus geen forks in de blockchain, waardoor het makkelijker wordt om te double-spenden. Een aanvaller die wil double-spenden zou de volgende stappen kunnen ondernemen, nadat er een fork heeft plaatsgevonden:

1. De aanvaller probeert blokken voort te bouwen op beide chains (fork A en fork B).
2. De aanvaller gebruikt een deel van zijn coins op fork A om een Lamborghini te kopen.
3. Nadat de aanvaller zijn Lamborghini heeft ontvangen, richt de aanvaller zijn stake niet meer op fork A waardoor fork B een grotere stake heeft en er daar sneller een nieuw blok wordt aangemaakt.
4. Fork B wordt een langere chain.
5. Fork A sterft af, terwijl de aanvaller nog steeds de volledige beschikking heeft over zijn coins op fork B. Hiermee kan hij weer andere producten kopen.



Vulnerable signature

De creatie van public-private keys wordt bij Bitcoin en vele andere blockchains gedaan met Elliptic Curve Digital Signature Algorithm (ECDSA). Hierbij is het belangrijk dat de kans dat een ECDSA dezelfde keys genereert minimaal is. Als er een zwakte is het gebruikte ECDSA die, dan is het mogelijk dat iemand anders eenzelfde private key heeft aangemaakt als jij.

DDoS-aanval

Decentralisatie van de blockchain maakt het moeilijker voor een aanvaller om een succesvolle DDoS-aanval uit te voeren dan bij een conventioneel client-server model. Bij een DDoS-aanval wordt het netwerk overspoeld met verzoeken waardoor de servers de verzoeken niet meer kunnen verwerken en uitgeschakeld worden. Kleinere of private blockchains met weinig nodes hebben een grotere kans op DDoS-aanvallen.

Sybil-aanval

Bij een Sybil-aanval op een blockchain, creëert iemand meerdere nodes op het blockchainnetwerk. Deze nodes kunnen het netwerk dan verstoren door bijvoorbeeld te weigeren om blokken die ze hebben ontvangen door te sturen naar de eerlijke nodes. Hierdoor kunnen nodes en gebruikers worden geblokkeerd op het netwerk.

Core developers corrumperen

Andere manieren om een blockchain aan te vallen is door gewoonweg core developers te corrumperen. Een aanvaller zou de developers kunnen aansporen om malafide code schrijven. Zeker wanneer er niet voldoende toezicht is op de geschreven code, is dit een goede aanvalsmogelijkheid.

Het is ook mogelijk dat er op applicatieniveau foutieve code is geschreven. Wanneer een smart contract bijvoorbeeld fondsen vasthoudt, maar de smart contract niet goed is gescheven, kan het zomaar zijn dat iemand de fondsen uit het smart contract kan halen. Denk hiervoor bijvoorbeeld aan de Genesis DAO hack van Ethereum.

Toegang tot servers

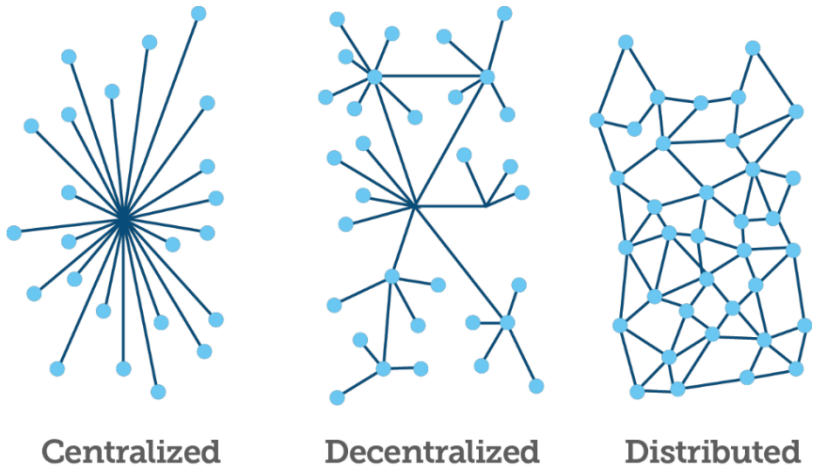
Als laatste willen we nog vermelden dat het ook mogelijk is om de keys te stelen van een serverbeheerder. Zeker bij kleine blockchainprojecten met weinig nodes is dit een groot probleem. Als een blockchain bestaat uit 5 nodes en je weet toegang te krijgen tot 3 van de 5 nodes, dan zou je het netwerk kunnen overnemen.

7.5 Decentralisatie

Zoals eerder genoemd is decentralisatie belangrijk om aanvallen te kunnen weren. Echter, is er geen eenduidige definitie van wat decentralisatie betekent. Als we spreken over ***decentralisatie***, dan wordt er dikwijls in termen van macht over de resources van een netwerk, of in termen van de manier waarop informatie zich over het netwerk beweegt, gesproken. Decentralisatie helpt namelijk voorkomen dat één of een klein groepje partijen een meerderheid van de hashing power of staking coins in handen krijgt. Het voorkomt hiermee dat slechts één of een klein groepje partijen blokken valideert, waardoor de macht over het netwerk niet gecentraliseerd wordt in één of enkele punten.

De World Wide Web Foundation omschrijft decentralisatie als het proces waarbij er geen permissie van een centrale autoriteit nodig is om iets op het web te mogen plaatsen. Er is geen centrale controlerende node en daardoor ook geen Single Point of Failure. Volgens de Web Foundation is dit ook inherent gerelateerd aan de individuele vrijheid tegen willekeurige censuur en surveillance.[88]

Een veelvoorkomende afbeelding met betrekking tot decentralisatie en diens alternatieven is de volgende van Paul Baran.



Afbeelding 81: Gecentraliseerde, gedecentraliseerde en gedistribueerde netwerkarchitectuur (Baran, 1964).

[88] Zie 'History of the Web' op Webfoundation.com (z.d.).

De afbeelding maakt onderscheid in (a) een gecentraliseerd, (b) een gedecentraliseerd en (c) een gedistribueerd netwerk. Een gecentraliseerde netwerkarchitectuur heeft een centrale database die tevens de Single Point of Failure is. Daarentegen is het onderhoud van het netwerk wel relatief gemakkelijk. De beheerder van de centrale database hoeft niet te overleggen met de anderen die aangesloten zijn op het netwerk hoe, wanneer en welke update er moet worden doorgevoerd. Ook is het netwerk minder complex om te ontwikkelen.
Een gedecentraliseerd netwerk heeft een gelimiteerd aantal punten die mogen falen. Het onderhoud daarvan is wat minder gemakkelijk dan bij een gecentraliseerd netwerk en de ontwikkeling van een dergelijk netwerk is gematigd complex.

Tot slot kan een gedistribueerd netwerk oneindig veel faalpunten hebben, zonder dat het netwerk ineenstort. Echter, is het onderhoud hiervan wel aanzienlijk moeilijker en is de ontwikkeling van een dergelijk netwerk zeer gecompliceerd. Er dient namelijk meer coördinatie plaats te vinden met betrekking tot het onderhoud en de ontwikkeling van de software.[89] In onderstaande tabel zijn de drie architecturen tegen elkaar afgezet.

Eigenschappen	Gecentraliseerd	Gedecentraliseerd	Gedistribueerd
Faalpunten	Single point	Gelimiteerd aantal	Oneindig
Onderhoud	Makkelijk	Gematigd	Moeilijk
Ontwikkelingsgemak	Minder complex	Gematigd complex	Zeer gecompliceerd

Tabel 3: De eigenschappen van een gecentraliseerd, gedecentraliseerd en gedistribueerd netwerkarchitectuur.

7.5.1 Drie typen van decentralisatie

Volgens Vitalik Buterin, één van de oprichters van Ethereum, is de indeling van Baran niet erg behulpzaam als we decentralisatie op een dieper niveau willen begrijpen. Decentralisatie is volgens Buterin meer dan alleen architectureel.[90] Hij maakt onderscheid tussen de volgende drie verschillende typen van decentralisatie:

1. ***Architecturele decentralisatie***: uit hoeveel fysieke computers bestaat het netwerk? Hoeveel van deze computers kunnen er op elk moment uitvallen, zonder dat het netwerk instort?

[89] De tabel komt deels overeen met het onderscheid dat Truong et al. maken tussen gecentraliseerde, gedecentraliseerde en gedistribueerde netwerken in 'A Survey on Trust Computation In the Internet of Things' (2016).

[90] Zie 'The Meaning of Decentralization' (Buterin, 2017).

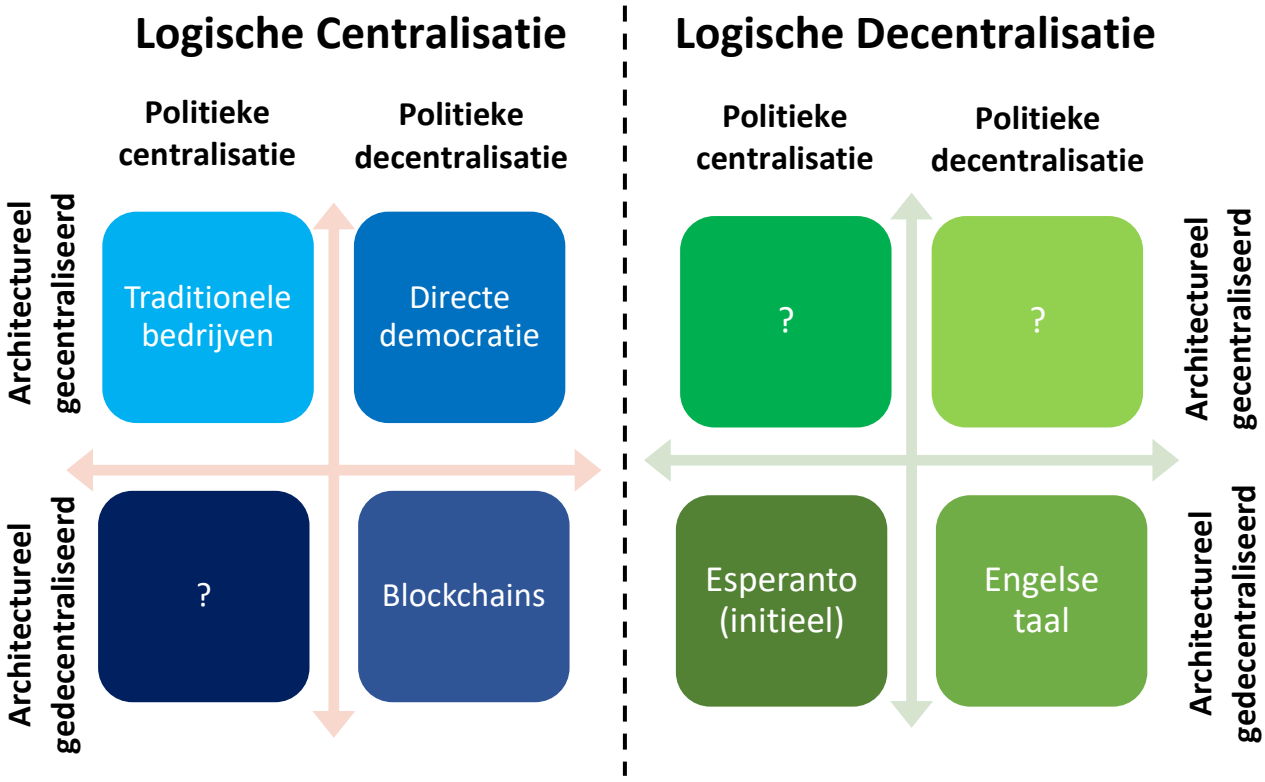
2. ***Politieke decentralisatie***: hoeveel individuen of organisaties beheren de computers waar het systeem uit bestaat?
3. ***Logische decentralisatie***: zien de interface en datastructuren die het systeem presenteert en onderhoudt eruit als een geïntegreerd geheel of als een vormloze zwerm? Met andere woorden, als je het systeem in tweeën deelt, zullen beide helften volledig kunnen opereren als onafhankelijke delen?

Blockchains kunnen een combinatie van gedecentraliseerde dimensies bevatten. Buterin heeft de verschillende combinaties van dimensies opgedeeld in een diagram en geprobeerd om daar huidige organisaties in te passen. De plaatsingen van de organisaties zijn dubieus, maar ze helpen ons wel om decentralisatie vanuit meerdere perspectieven te bekijken:

1. Traditionele bedrijven zijn politiek gecentraliseerd, omdat ze één CEO hebben. Daarnaast zijn ze architectureel gecentraliseerd, omdat ze één hoofdkantoor hebben vanwaar andere kantoren worden bestuurd. Tot slot zijn ze logisch gecentraliseerd, omdat je het bedrijf niet echt in de helft kan delen.
2. Directe democratieën zijn politiek gedecentraliseerd, omdat de stemmen zijn verdeeld over een groot aantal stemgerechtigden. Daarnaast zijn ze architectureel gecentraliseerd als het stemproces gebeurt via een gecentraliseerd forum.[91] Tot slot zijn ze logisch gecentraliseerd, omdat de stemming leidt tot een algemeen overeengekomen resultaat en tot eenduidige besluiten. Je kunt ook beargumenteren dat er één parlement is die de wetgeving maakt. Het ziet er daardoor uit als een geïntegreerd geheel.
3. Blockchains zijn politiek gedecentraliseerd, omdat er niemand is die alle macht heeft over een blockchain. Daarnaast zijn ze architectureel gedecentraliseerd, omdat er geen Single Point of Failure is. Tot slot zijn ze logisch gecentraliseerd, omdat er één algemeen overeengekomen staat van de blockchain is en het systeem zich gedraagt als één computer.
4. De Engelse taal is politiek gedecentraliseerd. Daarnaast is het architectureel gedecentraliseerd, omdat er geen centrale infrastructuur nodig is om taal in te richten. Grammaticaregels worden ook niet gecreëerd en beheerd door een enkele persoon. Tot slot is het logisch gedecentraliseerd. Je kunt een Engelssprekende bevolking namelijk opsplitsen in tweeën en de Engelse taal zal niet veranderen – hooguit langzaam evolueren in iets andere dialecten, maar de taal blijft fundamenteel Engels.

[91] Je zou kunnen beargumenteren dat het architectureel gedecentraliseerd is wanneer de community is overeengekomen om altijd naar een ander forum over te gaan, op het moment dat de eigenaars van het huidige forum valse intenties hebben.

5. Esperanto is initieel politiek gecentraliseerd, omdat Zamenhof de enige was die de regels van de taal beheerde. Daarnaast is het architectureel gedecentraliseerd, omdat er geen centrale infrastructuur is die de taal verder inrichtte toen deze eenmaal werd losgelaten. Tot slot is het logisch gedecentraliseerd, omdat je Esperantosprekende mensen kan opsplitsen zonder dat de taal instort en onherkenbaar wordt.



Afbeelding 82: Drie dimensies van decentralisatie, volgens Vitalik Buterin (2017).

7.5.2 Drie argumenten voor decentralisatie

Over het algemeen zijn dit de drie argumenten voor decentralisatie:

1. Gedecentraliseerde systemen zijn resistent tegen het falen van één of meerdere delen van het netwerk.
2. Gedecentraliseerde systemen hebben geen gevoelige centrale punten die kunnen worden gemanipuleerd of aangevallen, zonder aanzienlijke kosten om de aanval te coördineren.
3. Gedecentraliseerde systemen zijn resistent tegen collusie van deelnemers die op een manier ageren dat het hen ten koste van anderen bevoordeelt. (Buterin, 2017)

In hoeverre zijn blockchains resistent tegen falen, manipulatie, aanvallen en collusie? Het klopt dat de kans dat een veelvoud van nodes tegelijkertijd uitvallen zeer gering is. Echter, is het wel mogelijk dat een veelvoud van de nodes op dezelfde softwareversie draaien. Het gevaar hier is

dat de software een bug bevat, of dat het developmentteam corrupt is. Daarnaast kan er een concentratie zijn van mijners in bepaalde landen. Het risico hierbij is dat de overheid van deze landen kan besluiten om alle mijning farms in beslag te nemen of te sluiten. Ook is het mogelijk dat de meerderheid van de mijningapparatuur wordt gebouwd door één of een select groepje bedrijven. Deze bedrijven kunnen worden omgekocht of gedwongen om zwakheden in de apparatuur te plaatsen. Tot slot is het ook mogelijk dat een exchange een groot deel van de coins bevatten. Bij een Proof-of-Stake blockchain zou de beheerder van de exchange een 51%-aanval kunnen uitvoeren.

Om bovenstaande redenen is het belangrijk dat er verschillende, concurrerende software-implementaties zijn en dat de participatie in de softwareontwikkeling gedecentraliseerd wordt. Mensen moeten vrij zijn om deel te kunnen nemen in discussies en moeten protocollen kunnen bekritiseren.[92] Ook is het belangrijk dat onderzoekers en ontwikkelaars een verscheidenheid aan achtergronden hebben en niet van één of enkele bedrijven zijn. Mijningalgoritmes dienen dusdanig ontworpen te zijn dat er een minimaal risico is op centralisatie. Ook dient er te worden nagedacht over de voordelen van Proof-of-Stake ten opzichte van Proof-of-Work en vice versa. Wellicht kunnen hybride versies worden ontworpen, waarbij de sterke punten van beide consensusmechanismen worden overgenomen. Tot slot dient het systeem zo te zijn ingericht dat de kosten om een aanval te coördineren groter zijn dan de baten. Deze ***aanval/defensie asymmetrie*** ontmoedigt potentiële aanvallers om een aanval te coördineren.

Hoewel er in de blockchainwereld doorgaans wordt gesproken over het verwijderen van vertrouwde tussenpartijen, is er toch altijd wel vertrouwen nodig in bepaalde mensen of groepen. Mensen die zelf Bitcoin gebruiken, maar de broncode niet kunnen lezen, hebben bijvoorbeeld vertrouwen dat ontwikkelaars hun taken goed uitvoeren.

[92] Er zijn voorbeelden waarbij discussies worden gecensureerd om bepaalde meningen te onderdrukkken. Eén voorbeeld speelt zich af op Reddit en betreft het verwijderen van comments die zich positief uitspreken over het vergroten van de Bitcoin-blokgrootte. Zie ‘A (brief and incomplete) history of censorship in /r/Bitcoin’ van John Blocke (2016).

Intermezzo: Antifragiliteit

Een andere manier om te kijken naar de stressbestendigheid van blockchains is vanuit het perspectief van antifragiliteit. De term, ***antifragiel***, werd geïntroduceerd door Nassim Nicholas Taleb in zijn boek *Antifragile: Things That Gain From Disorder* (2012). Hierin zet hij antifragiliteit af tegen ***fragiliteit*** en ***robuustheid***. Een fragiel systeem zal breken als er te veel weerstand op komt. Een robuust systeem daarentegen is in staat om de weerstand te weerstaan. Een antifragiel systeem, echter, zal breken door de weerstand en zich vervolgens weer herstellen in een staat die sterker is dan voordat het brak. Antifragiele systemen zijn sterk adaptief en profiteren van de weerstand. Neem bijvoorbeeld een porseleinen kopje. Als we het kopje laten vallen, zal het breken – het is fragiel. Als we het zouden verharden totdat het niet meer breekt bij iedere val, is het kopje robuust geworden. Echter, wat als we het niet zouden verharden, maar de structuur van het kopje zo zouden veranderen dat het kopje telkens zou groeien wanneer het zou vallen? Dat is antifragiliteit.

De iteratieve en gedecentraliseerde natuur van open blockchains maakt ze antifragiel. Na iedere crisis of iedere aanval op de blockchain wordt de code herschreven om issues op te lossen, zodat de volgende versie bestendiger is tegen nieuwe aanvallen. Het internet was in zijn beginperiode ook zeer kwetsbaar voor aanvallen, maar werd gaandeweg steeds stabieler en resistenter. Net als het internet zullen aanvallen op blockchainnetwerken deze netwerken versterken, mits de ontwikkelaars leren van de zwakheden. Zo ziet het hedendaagse Bitcoinnetwerk er anders uit dan in de beginperiode. Het is door de jaren heen stabieler en resistenter geworden tegen aanvallen.

7.6 Samenvatting, begrippen en bronnen

Samenvatting

Het beveiligingsmodel van Proof-of-Work en Proof-of-Stake is fundamenteel anders dan dat van traditionele systemen. Traditionele systemen hebben toegangscontroles voor gebruikers, zodat malafide gebruikers de toegang kan worden ontzegd. Het fundamentele verschil hier met blockchainsystemen die we tot dusver hebben besproken is dat deze traditionele netwerken vertrouwen moeten hebben dat degenen die toegang hebben tot het systeem niet malafide zijn. Blockchainsystemen als bijvoorbeeld Bitcoin en Ethereum zijn daarentegen open. Er is geen authenticatie nodig van gebruikers en iedereen mag data proberen te schrijven naar de blockchain. Andreas Antonopoulos noemt dergelijke systemen open, grenzeloos, neutraal, resistent tegen censuur en publiekelijk.

In de blockchainwereld wordt er regelmatig gesproken van het blockchaintrilemma om aan te geven dat er trade-offs zijn in schaalbaarheid, beveiliging en decentralisatie.

Omdat het vertrouwensmodel van blockchains gedecentraliseerd is en berust op consensus, is het mogelijk om blockchains aan te vallen door consensus te kapen met een 51%-aanval. Bij een Proof-of-Work blockchain dient de aanvaller een meerderheid te bemachtigen van de totale rekenkracht op het netwerk. Bij een Proof-of-Stake blockchain dient de aanvaller een meerderheid van alle stake te bemachtigen.

Decentralisatie is belangrijk om aanvallen te kunnen weren. Over het algemeen zijn dit de drie argumenten voor decentralisatie:

1. Gedecentraliseerde systemen zijn resistent tegen het falen van één of meerdere delen van het netwerk.
2. Gedecentraliseerde systemen hebben geen gevoelige centrale punten die kunnen worden gemanipuleerd of aangevallen, zonder aanzienlijke kosten om de aanval te coördineren.
3. Gedecentraliseerde systemen zijn resistent tegen collusie van deelnemers die op een manier ageren dat het hen ten koste van anderen bevoordeelt. Echter, is er geen eenduidige definitie van wat decentralisatie betekent.

Vitalik Buterin maakt het onderscheid in architecturele, politieke en logische decentralisatie.

Opmerkingen die je nu kunt uitleggen

- Traditionele databasesystemen hebben toegangscontroles nodig om malafide gebruikers toegang te ontzeggen.
- Open blockchains zijn zo ingericht dat iedereen data mogen schrijven naar en lezen van de blockchain. De beveiliging wordt hier gewaarborgd door consensusmechanismen.
- Als je een blockchain inricht, moet je rekening houden met het blockchaintrilemma. Het is lastig om een schaalbare, goed beveiligde en sterk gedecentraliseerde blockchain op te zetten.
- Bij een 51%-aanval moet je proberen om de langste chain te creëren waarna je deze uitzendt naar de rest van het netwerk.
- Het gebruik van de woorden gedecentraliseerd en gedistribueerd kan verwarrend zijn.
- Blockchains zijn politiek en architectureel gedecentraliseerd, maar logisch gecentraliseerd.
- Een blockchain moet zo zijn ingericht dat de kosten om een aanval op de blockchain te coördineren groter zijn dan de baten.

Verklarende begrippenlijst

51%-aanval: Eén van de mogelijke aanvallen op een blockchain. Bij een Proof-of-Work blockchain dient de aanvaller een meerderheid te bemachtigen van de totale rekenkracht op het netwerk. Bij een Proof-of-Stake blockchain dient de aanvaller een meerderheid van alle stake te bemachtigen.

Aanval/defensie asymmetrie: De kosten om een aanval te coördineren zijn groter dan de baten.

Antifragiel: Een antifragiel systeem breekt door de weerstand om zich vervolgens weer te herstellen in een staat die sterker is dan voordat het brak. De Bitcoin blockchain wordt ook weleens een antifragiel systeem genoemd, omdat ontwikkelaars de blockchain continu updaten en sterker maken na een aanval.

Architecturele decentralisatie: Uit hoeveel fysieke computers bestaat het netwerk? Hoeveel van deze computers kunnen er op elk moment uitvallen, zonder dat het netwerk instort?

Blockchaintrilemma: Bij het inrichten van een blockchain zijn er trade-offs met betrekking tot de volgende drie eigenschappen van een blockchain: schaalbaarheid, beveiliging en decentralisatie.

Decentralisatie: De World Wide Web Foundation omschrijft decentralisatie als het proces waarbij er geen permissie van een centrale autoriteit nodig is om iets op het web te mogen plaatsen. Er is geen centrale controlerende node en daardoor ook geen Single Point of Failure. Volgens de WebFoundation is dit ook inherent gerelateerd aan de individuele vrijheid tegen willekeurige censuur en surveillance. Volgens Vitalik Buterin zijn er drie niveaus van decentralisatie: architectureel, politiek en logisch.

Fragiel: Een fragiel systeem breekt wanneer er te veel weerstand op komt.

Gedistribueerd: Zie decentralisatie.

Logische decentralisatie: Zien de interface en datastructuren die het systeem presenteert en onderhoudt eruit als een geïntegreerd geheel of als een vormloze zwerm? Met andere woorden, als je het systeem in tweeën deelt, zullen beide helften volledig kunnen opereren als onafhankelijke delen?

Open blockchain: Volgens Andreas Antonopoulos is een open blockchain open source, grenzeloos, neutraal, resistent tegen censuur en publiekelijk.

Politieke decentralisatie: Hoeveel individuen of organisaties beheren de computers waar het systeem uit bestaat?

Robuust: Een robuust systeem is in staat om weerstand te weerstaan.

Toegangscontroles: Controles op de toegang tot bijvoorbeeld een database.

Bronnen

Antonopoulos, A. (2007). Open Blockchains vs Bullshit: Thoughts on the Future of Money [YouTube]. Geraadpleegd van https://youtu.be/SMEOKDVXlUo

Antonopoulos, A. (2014). Bitcoin security model: trust by computation. Geraadpleegd op 27 december 2019, van Oreilly.com website: http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html

Baran, P. (1964). On Distributed Communications Networks. *IEEE Transactions on Communications*, *12*(1), 1–9. https://doi.org/10.1109/tcom.1964.1088883

Blocke, J. (2016, 14 november). A (brief and incomplete) history of censorship in /r/Bitcoin. Geraadpleegd op 27 december 2019, van https://medium.com/@johnblocke/a-brief-and-incomplete-history-of-censorship-in-r-bitcoin-c85a290fe43

Buterin, V. (2017, 6 februari). The Meaning of Decentralization. Geraadpleegd van https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Lee, G.M., Jayasinghe, U., Um, T. & Truong, N. B. (2016). A Survey on Trust Computation in the Internet of Things. Geraadpleegd op 27 december 2019, van Academia.edu website: https://www.academia.edu/24590240/A_Survey_on_Trust_Computation_in_the_Internet_of_Things

Mosakheil, J.H. (2018). Security Threats Classification in Blockchains. *Culminating Projects in Information Assurance*. 48.

Taleb. N.N. (2012). *Antifragile : things that gain from disorder*. New York: Random House.

The European Union Blockchain Observatory and Forum. (2019). Blockchain for Government and Public Services. Geraadpleegd van https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf

World Wide Web Foundation. (z.d.). History of the Web. Geraadpleegd op 24 december 2019, van World Wide Web Foundation website: https://webfoundation.org/about/vision/history-of-the-web/

Iconen

Broadcast gemaakt door Freepik van www.flaticon.com

Malafide mijner door FreepikMalafide mijner gemaakt door Freepik van www.flaticon.com

8. Blockchain 2.0 en Smart Contracts

"Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, Blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly."

- Vitalik Buterin (2015)

"We want a whole sequence of companies: digital title, digital media assets, digital stocks and bonds, digital crowdfunding, digital insurance. If you have online trust like the Blockchain provides, you can reinvent field after field after field."

- Marc Andreessen (2014)

8.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat blockchain 1.0 is en waarom er een behoefte is aan blockchain 2.0.
- Dat Ethereum een voorbeeld is van blockchain 2.0.
- Hoe Ethereum werkt.
- Wat smart contracts zijn en wat het verschil is tussen deterministische en non-deterministische smart contracts.
- Wat orakels zijn en wat het orakelprobleem is.
- Wat gedecentraliseerde applicaties (dApps) zijn.
- Wat gedecentraliseerde autonome organisaties (DAO's) zijn.

Inleiding

In de voorgaande hoofdstukken is voornamelijk de Bitcoin blockchain aan bod gekomen, met als eerste applicatie de Bitcoin-cryptovaluta.

In dit hoofdstuk beginnen we in paragraaf 8.2 met een beschrijving van welke typen applicaties er nog meer mogelijk zijn op de Bitcoin blockchain, door middel van bijvoorbeeld colored coins.

Daaropvolgend verschuiven we in paragraaf 8.3 onze aandacht naar een nieuwere generatie blockchains die specifiek bedoeld zijn om autonome computerapplicaties op te ontwikkelen. Dergelijke blockchains worden ook weleens vergeleken met een besturingssysteem als iOS, Android of Windows, waarop nieuwe gedecentraliseerde applicaties (dApps) kunnen worden gebouwd. Hierin geven we een introductie op de bekendste van deze typen blockchains, Ethereum. Ethereum is in december 2019 nog steeds het één na grootste blockchainproject qua marktkapitalisatie. In paragraaf 8.4 beschrijven we hoe Ethereum-transacties werken. In paragraaf 8.5 komen smart contracts aan bod die zeer relevant zijn voor Ethereum. Ze maken namelijk een nieuwe generatie dApps mogelijk. Paragraaf 8.6 gaat specifiek over wat dApps zijn. Vervolgens bespreken we in 8.7 één variant van dApps, de gedecentraliseerde autonome organisatie (DAO). Tot slot sluiten we het hoofdstuk af in paragraaf 8.8 met een samenvatting, een lijst van belangrijke woorden en een lijst van bronnen die in het hoofdstuk aan bod zijn gekomen.

8.2 Colored coins op de Bitcoin blockchain

De eerste generatie applicaties concentreerde zich voornamelijk op digitaal geld. De generatie blockchains waar deze applicaties op werden gebouwd, wordt ook wel ***blockchain 1.0*** genoemd.

Hoewel Bitcoin een geldmiddel is en voornamelijk wordt gebruikt als cryptovaluta waarbij diensten en goederen kunnen worden verhandeld, is het ook mogelijk om de scriptingtaal van Bitcoin te gebruiken voor de opslag van kleine hoeveelheden metadata in de transacties. Hierdoor zou je bijvoorbeeld in een Bitcoin-transactie een script mee kunnen geven dat er 1.000 eenheden van een nieuwe activa zijn uitgegeven en dat ze zijn toegekend aan een bepaald Bitcoin-adres. Deze eenheden kunnen worden gezien als nieuwe coins en ze kunnen bepaalde eigenschappen toegekend krijgen, waardoor ze verscheidene dingen kunnen representeren, zoals bijvoorbeeld aandelen, obligaties, eigendomsrechten op onroerend goed, coupons en alternatieve cryptovaluta. Deze coins kunnen waarden bevatten die onafhankelijk zijn van de onderliggende nominale waarde van de Bitcoin – vaak is dit de kleinste Bitcoin-eenheid, een satoshi – waarin het script is toegekend.[93] Dergelijke coins worden ***colored coins*** genoemd.

[93] Een satoshi is 1/100.000.000e Bitcoin en is de kleinste eenheid in Bitcoin. Het originele idee achter colored coins was om satoshi's te kleuren met bepaalde eigenschappen. Het protocol is verder geëvolueerd waardoor het niet

Een bank zou bijvoorbeeld colored coins kunnen uitgeven die worden gedekt door geldreserves. Mensen kunnen dan geld storten en opnemen in colored coins, deze verhandelen en gebruiken om goederen en diensten te kopen. De Bitcoin blockchain staat het hierbij dus toe om niet alleen transacties te doen in Bitcoin, maar ook in andere valuta. Het is hierbij wel belangrijk dat deze coins kunnen worden gevolgd over de blockchain heen, zodat er kan worden nagegaan wie op welk moment over welke van deze coins beschikt. Een belangrijk bijkomend voordeel van colored coins is dat ze gebruikmaken van de Bitcoin blockchain. Er is geen nieuwe infrastructuur nodig om ze op te ontwikkelen. Daarnaast geniet het ook direct van het decentrale karakter en de beveiliging van de Bitcoin blockchain. De transacties van colored coins worden door mijners gezien als ordinaire Bitcoin-transacties, maar moeten wel voldoen aan additionele voorwaarden om als geldig te worden verklaard door nodes die zich bewust zijn van de kleur van de coins.[94] (Rosenfeld, 2012, pp. 2-5)

De mogelijkheid om de Bitcoin blockchaintechnologie te gebruiken voor andere toepassingen dan valuta, zou volgens sommigen leiden tot een generatie van nieuwe toepassingen op de Bitcoin blockchain. Dit werd ook wel ***Bitcoin 2.0*** genoemd. Hoewel het mogelijk is om nieuwe typen activa en extra condities en voorwaarden vast te leggen in de colored coins, is de Bitcoin blockchain hier echter niet optimaal geschikt voor. Vitalik Buterin heeft om deze reden het idee gehad om een nieuwe blockchain, Ethereum, te ontwikkelen, waarop het creëren van nieuwe coins met hieraan hangend bepaalde condities en voorwaarden en zelfs ***gedecentraliseerde applicaties*** (dApps) op te draaien. Blockchains met dergelijke mogelijkheden worden ook wel 2e generatie blockchains genoemd: ***blockchain 2.0***.[95]

meer nodig is om satoshi's te gebruiken als drager van de eigenschappen. Zie https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Faq#coloring-satoshis voor meer informatie.

[94] Zie Meni Rosenfelds 'Overview of Colored Coins' (2012) voor meer uitleg over de voor- en nadelen van colored coins en hoe de kleur van de coins kan worden gevolgd in de blockchain.

[95] Er wordt ook weleens gesproken over ***blockchain 3.0***. Dit zijn blockchains die een cluster van issues waar blockchain 2.0 nog mee kampt, hebben opgelost. Voorbeelden van zulke issues zijn schaalbaarheid, interoperabiliteit, privacy, duurzaamheid en governance (Ackermann & Meier, p. 1). EOS en Cardano zijn voorbeelden van blockchains die zichzelf scharen onder 3.0.

8.3 Ethereum

Ethereum werd voor het eerst geïntroduceerd door Vitalik Buterin in 'Ethereum White Paper: a next generation Smart Contract & decentralized Application Platform' (2013). Hierin legt Buterin uit dat Bitcoin kan worden omschreven als een "first-to-file-systeem" waarin de order van de transacties cruciaal is. Technisch gezien kan de Bitcoin blockchain worden gezien als een simpel staatstransitiesysteem waarbij (a) de 'staat' bestaat uit de eigendomsstatus van alle bestaande Bitcoins en (b) de 'staatstransitiefunctie' die de staat en de transactie neemt om een nieuwe staat te produceren. (Buterin, 2013, pp. 1-5) Het is geschikt om een transactie vast te leggen van persoon A naar persoon B, maar niet geschikt om complexere staatstransities vast te leggen, die onderworpen zijn aan bepaalde condities en voorwaarden. Zo kan de Bitcoin blockchain uitstekend vastleggen of een UTXO[96] is uitgegeven of niet, maar is het lastig om contracten uit te voeren die een transactie door meerdere staten kan vastleggen. Zo is het bij Bitcoin haast niet mogelijk om een stuk logica mee te geven die zegt dat Bob zijn geld naar Alice kan sturen, maar dat Alice deze alleen kan opeisen nadat zij een tegenprestatie heeft geleverd. (Buterin, 2013, p. 12)

Het doel van Ethereum is om ontwikkelaars de mogelijkheid te bieden om applicaties te ontwikkelen met arbitraire condities en voorwaarden. Deze applicaties zijn, omdat ze draaien op het Ethereum blockchain, ook gebaseerd op een gedecentraliseerd consensusmechanisme en genieten daarmee van de voordelen die een blockhain biedt. Dergelijke applicaties zijn mogelijk doordat de Ethereum blockchain een ingebouwde ***Turing-compleet*** programmeertaal bevat die allerlei typen computaties ondersteunt en ontwikkelaars toestaat om ***smart contracts*** en gedecentraliseerde applicaties op te ontwikkelen, met arbitraire regels omtrent eigendomschap en staatstransitiefuncties. (Buterin, 2013, pp. 12-13) Met een Turing-compleet programmeertaal kan elke berekening of gegevensbewerking worden geprogrammeerd. De programmeertaal die hiervoor specifiek voor Ethereum is ontwikkeld, heet ***Solidity***.

8.4 Ethereum-transacties en gas

Er zijn verschillende redenen waarom gebruikers transacties sturen naar het Ethereum-netwerk. Deze transacties kunnen bestaan uit (a) het overmaken van Ether naar andere gebruikers of smart contracts, (b) het creëren van nieuwe smart contracts of (c) het oproepen van functies van een smart contract. De transacties worden geregistreerd op de Ethereum blockchain.

[96] Unspent Transaction Output. Zie de intermezzo in hoofdstuk 3 voor meer uitleg over wat een UTXO is.

De onderliggende cryptovaluta van de Ethereum blockchain is Ether (ETH). Het doen van een transactie op het Ethereum-netwerk vereist ***gas***. Gas wordt uitgedrukt in de cryptovaluta Ether. Gas is nodig om de Ethereum blokchain te laten draaien, net zoals een auto gas nodig heeft om te kunnen rijden. Gas op het Ethereum-netwerk is dus in principe hetzelfde als transactiekosten die je ook betaalt om een transactie te mogen uitvoeren. Deze wordt berekend aan de hand van standaardkosten per eenheid computerkracht x het aantal eenheden. Bij elke transactie die je uitvoert, kun je een specifieke hoeveelheid gas, oftewel transactiekosten, opgeven. De gebruiker dient een geschikte hoeveelheid gas te betalen bij de transactie. Als er te weinig gas wordt betaald, kan het zijn dat mijners de transactie niet opnemen in het blok en deze transactie dus niet wordt uitgevoerd. De mijner krijgt naast de blokbeloning van 2 Ether ook al het gas, transactiekosten, in het blok. Mijners zijn daardoor eerder geneigd om transacties met meer gas op te nemen in het blok. De crypto-economische reden dat gas is geïntroduceerd op het Ethereum-netwerk is dat het belangrijke transacties voorrang geeft. Een blok heeft slechts ruimte voor een beperkt aantal transacties en daarom is het belangrijk dat er op goede wijze wordt omgegaan met deze schaarste. Het gassysteem zorgt ervoor dat er geen energie wordt verspild aan spam of transacties met weinig waarde.

8.5 Smart Contracts

Blockchaintechnologie wordt toegepast om smart contracts mogelijk te maken. Een smart contract is een vorm van decentrale automatisering en kan worden gedefinieerd als een contract met bepaalde condities en voorwaarden die zijn vastgelegd in code. Het contract is zelfuitvoerend, omdat het zelf de juiste corresponderende acties uitvoert wanneer er aan de condities en voorwaarden wordt voldaan. Het contract moet hiervoor wel voldoende informatie bevatten van elke partij die betrokken is bij het contract, zodat het het vermogen ontneemt van partijen om het contract te verbreken. Smart contracts definiëren de consequenties van wanneer iemand zich niet houdt aan het contract en voeren deze consequenties automatisch uit. In dat opzicht bevatten smart contracts nultolerantie. Daarnaast kan een smart contract ook automatisch dispuutresoluties starten en experts met betrekking tot de issue inroepen om tot een besluit te komen over de gedane schade en de gepaste compensatie. Het toch nog kunnen inschakelen van derde partijen is handig, omdat sommige legale overeenkomsten te complex zijn om ze in een smart contract te plaatsen. (Young, 2018, pp. 7-8) Smart contracts geven aldus vooraf zekerheid wat de consequenties zijn en voorkomen daarmee discussie achteraf. Zodoende kun je je indenken dat smart contracts ook als transparant alternatief voor huidige contracten kunnen dienen.

Een smart contract zou bijvoorbeeld een arbeidsovereenkomst kunnen zijn, waarbij Alice €500 wil betalen aan Bob voor het ontwikkelen van een website. Het contract zou als volgt kunnen werken:

1. Alice zet €500 in het contract en het fonds wordt opgesloten.
2. Wanneer Bob de website heeft ontwikkeld, stuurt Bob een berichtje naar het contract om het fonds vrij te geven ten gunste van hem.
3. Het fonds wordt daadwerkelijk vrijgegeven wanneer Alice instemt.
4. Als Bob besluit om de website niet af te ronden, kan Bob zijn werk afzeggen door een bericht te sturen naar het contract, waarna het fonds automatisch wordt teruggestuurd naar Alice.
5. Als Bob beweert dat hij de website heeft afgerond, maar Alice niet akkoord is, dan zou er na een wachtperiode van 7 dagen een rechter kunnen worden ingeschakeld om een oordeel uit te spreken in het voordeel van Alice of Bob. (Buterin, 2014)

Voordelen van smart contracts

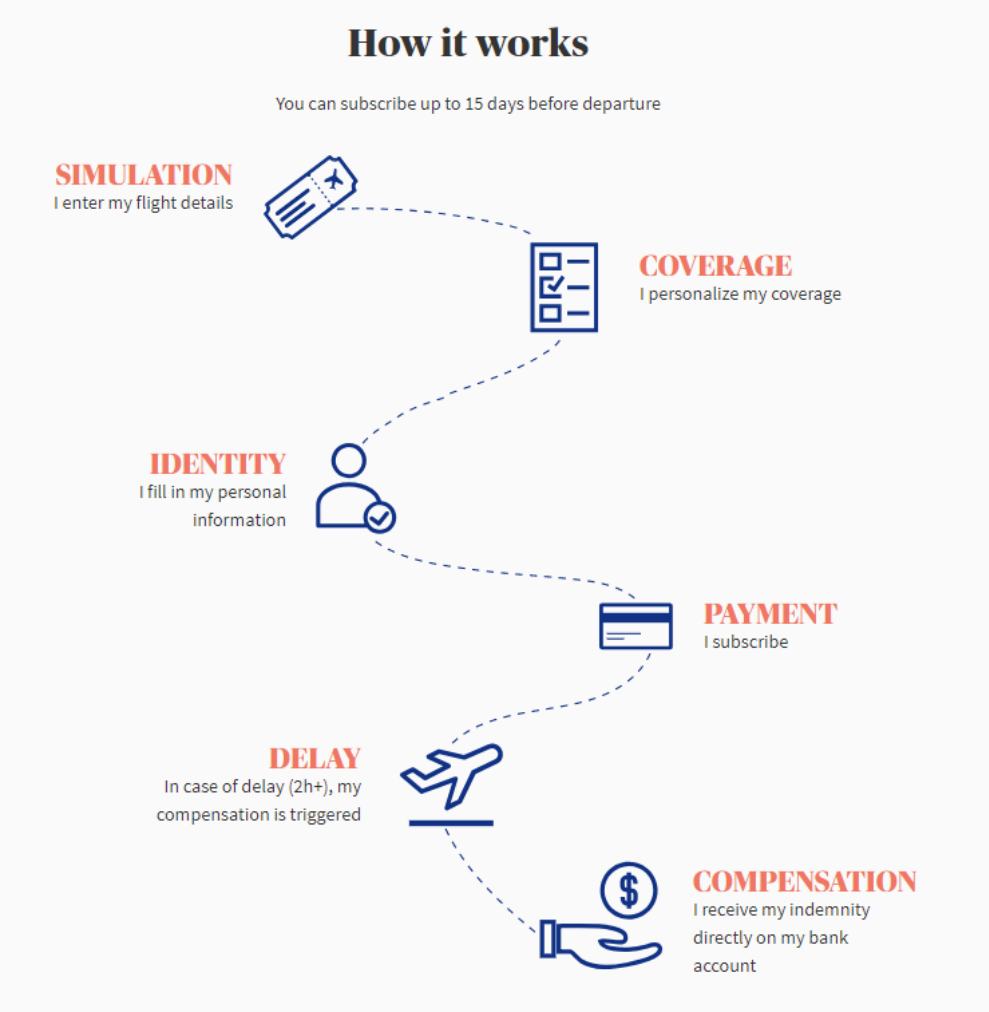
Smart contracts bieden veel voordelen. Chaintrade (2017) heeft er een elftal opgesomd.

1. *Nauwkeurigheid*: alle condities en voorwaarden dienen in detail te worden geregistreerd in een smart contract. Als er bepaalde voorwaarden worden weggelaten, kan dit leiden tot ongewenst gedrag van het smart contract.
2. *Transparantie*: alle condities en voorwaarden zijn volledig zichtbaar en toegankelijk voor alle betrokken partijen. Als het contract eenmaal definitief is vastgesteld, kun je het niet meer betwisten. Dit leidt tot totale transparantie voor alle betrokken partijen.
3. *Duidelijke communicatie*: de behoefte aan nauwgezet gedefinieerde smart contracts zorgt ervoor dat de communicatie in het contract dusdanig duidelijk is vastgelegd, dat er geen ruimte is voor miscommunicatie en misinterpretatie.
4. *Snelheid*: smart contracts kunnen traditionele bedrijfsprocessen automatiseren en aanzienlijk versnellen. Er hoeven geen aanvragen worden ingediend ter goedkeuring en er hoeven geen documenten te worden verwerkt of goedgekeurd door personen.
5. *Veiligheid*: smart contracts draaien op blockchainplatformen en maken gebruik van data-encryptie.
6. *Efficiëntie*: door de nauwkeurigheid en snelheid, voeren smart contracts bedrijfsprocessen efficiënter uit of elimineren ze deze zelfs volledig.
7. *Papiervrij*: er is geen papierwerk nodig voor de uitvoering van smart contracts. In dat opzicht is het beter voor het milieu.
8. *Opslag en back-up*: smart contracts en diens details worden permanent bewaard op de blockchain. Daardoor kunnen ze niet worden kwijtgeraakt en zijn ze makkelijk terug te vinden.
9. *Kostenbesparing*: smart contracts kunnen veel kosten besparen, doordat er minder behoefte is aan tussenpartijen als advocaten, getuigen en banken om de contracten te interpreteren en af te dwingen.
10. *Vertrouwen*: betrokken partijen kunnen erop vertrouwen dat smart contracts – indien ze goed zijn ingericht – eerlijk worden uitgevoerd, zonder mogelijkheid van datamanipulatie en vooroordelen.
11. *Gegarandeerde uitkomsten*: door gebruik te maken van zelfuitvoerende contracten, binden partijen zich aan de regels van het smart contract en zullen er minder rechtsgeschillen zijn.

Er wordt tegenwoordig steeds meer gebruikgemaakt van smart contracts. Je kunt smart contracts zo programmeren dat ze alle condities en voorwaarden die je wil opnemen bevatten. AXA-verzekeringen maakt bijvoorbeeld gebruik van smart contracts voor hun verzekeringen tegen vluchtvertragingen en annuleringen.[97] Deze werken als volgt:

1. Een klant gaat naar https://fizzy.axa en voert zijn vluchtdetails in.
2. Hij selecteert een verzekering tegen vluchtvertragingen en annuleringen en personaliseert deze naar eigen wensen.
3. Hij voert zijn persoonlijke gegevens in en rondt de aankoop af.
4. De aankoop wordt geregistreerd in een smart contract op het Ethereum-netwerk.
5. Het smart contract is verbonden aan databases van het globale luchtverkeer.
6. Het contract kijkt binnen deze databases of de vlucht van de klant vertraging heeft opgelopen.
7. Als de vlucht meer dan twee uur vertraging heeft opgelopen of is geannuleerd, zet het smart contract automatisch een proces in gang om de klant te vergoeden.
8. De klant ontvangt automatisch zijn vergoeding.

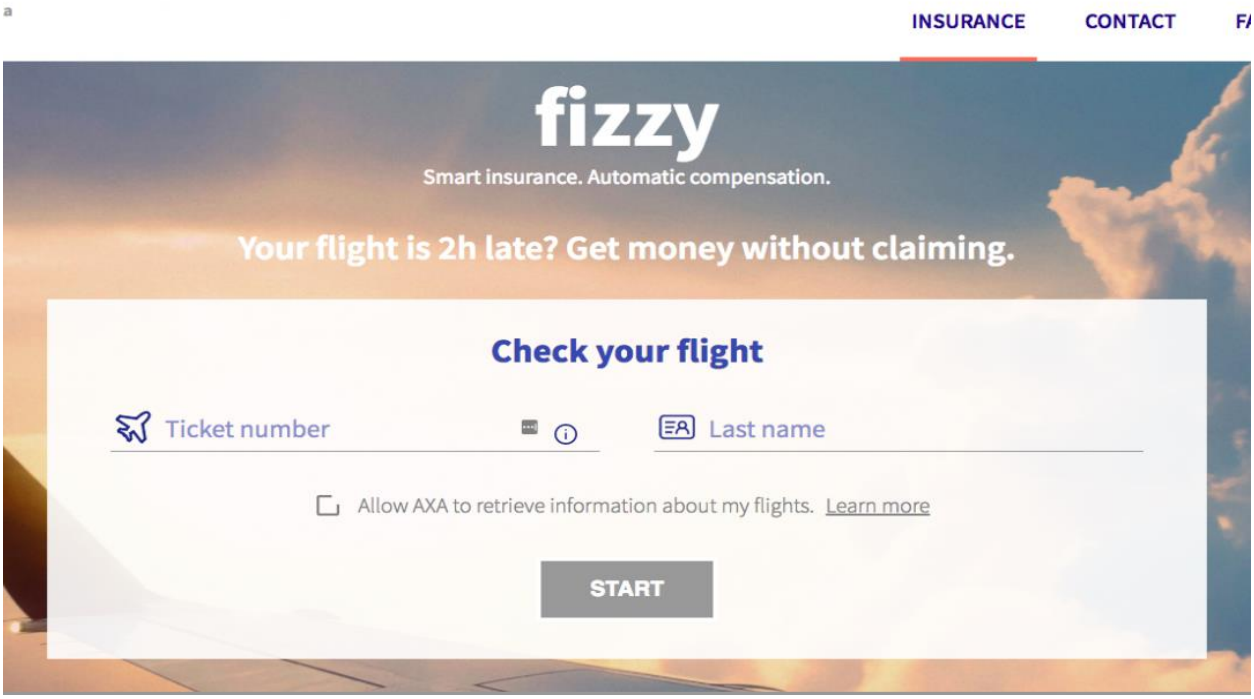
[97] Het Fizzy smart contract kun je vinden met de Ethereum block explorer, etherscan.io. Het contract is hier in te zien: https://etherscan.io/address/0xe083515d1541f2a9fd0ca03f189f5d321c73b872. Het aanmaken van het contract wordt geregistreerd alszijnde een transactie op het Ethereum-netwerk. Klik op de tab “Contract” om de inhoud van het contract te lezen.



Afbeelding 83: Hoe de Fizzy smart contract van AXA-verzekeringen werkt (Fizzy, z.d.).

Binnen het hele proces is er geen persoon nodig geweest die een vergoedingsaanvraag moet beoordelen en goedkeuren. Het smart contract bepaalt zelf of de klant moet worden vergoed of niet. Daarnaast heeft de persoon die de verzekering heeft gekocht geen aanvraag hoeven in te dienen. Het gehele proces is aldus geautomatiseerd.[98]

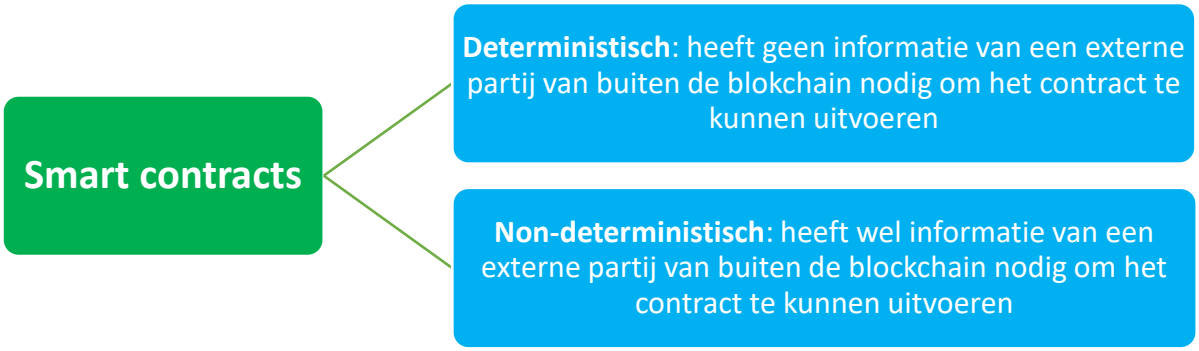
[98] Voor een uitgebreidere uitleg over hoe de Fizzy-verzekeringen van AXA werken, zie 'Fizzy by AXA: Ethereum Smart Contract in details' (Clement, 2019).



Afbeelding 84: Fizzy, AXA-verzekeringen tegen vluchtvertragingen en annuleringen op smart contracts (Fizzy, z.d.).

8.5.1 Deterministische en non-deterministische smart contracts

Er zijn twee verschillende categorieën van smart contracts: deterministische en non-deterministische smart contracts.



Afbeelding 85: Twee categorieën van smart contracts.

Een ***deterministisch smart contract*** heeft geen informatie van een externe partij van buiten de blockchain nodig om het contract te kunnen uitvoeren. Het smart contract kan alle informatie die noodzakelijk is voor de uitvoerbaarheid van het contract krijgen binnen het

blockchainnetwerk zelf. Een voorbeeld van een deterministisch smart contract is een peer-to-peerloterij waarbij:

1. Je een bepaalde tijd hebt om een getal te kiezen tussen 0 en 99.
2. Je een bepaalde hoeveelheid Ether kunt inzetten op het zelfgekozen getal, waarna de Ether wordt bewaard in een smart contract op het Ethereum-netwerk.
3. De loterij sluit nadat een bepaalde tijd is verstreken en er een willekeurig winnend getal wordt aangekondigd.
4. De deelnemers die het winnende getal hebben gekozen automatisch middels een smart contract hun beloning krijgen uitgekeerd op hun Ethereum-adressen.

Het is bij een dergelijke loterij belangrijk dat het winnende getal willekeurig is gekozen. Liefst wordt het winnende getal gegenereerd door een onafhankelijke partij. Eén manier om willekeurigheid en onafhankelijkheid te garanderen, is om te kijken naar de blok hash. Je kunt bijvoorbeeld stellen dat de loterij sluit bij blok #1.000 en dat de laatste twee decimale getallen van de hash van het desbetreffende blok bepalen wat het winnende getal is. Stel dat de hash als volgt is:

0x4ff4a38b278ab49f7739d3a4ed4e12714386a9fdf72192f2e8f7da7822f1**0**b**4**d

Als het winnende getal de laatste twee decimale getallen betreft, is het winnende getal 04. Het getal is voor iedereen verifieerbaar en het smart contract keert automatisch de beloning uit naar iedereen die dit getal heeft gekozen. Omdat dit willekeurige getal binnen in de blockchain is gegenereerd en op zich voldoende is om het smart contract te activeren, is er sprake van een deterministisch smart contract.

Een ***non-deterministisch smart contract*** heeft daarentegen wel informatie van een externe partij buiten de blockchain nodig. (Atzei et al, 2017) Een dergelijke partij wordt ook wel een orakel genoemd. De behoefte om gebruik te maken van orakels kan leiden tot het orakelprobleem.

8.5.2 Orakels en het orakelprobleem

Blockchains en smart contracts kunnen uit zichzelf geen data van buiten hun netwerk benaderen. In het voorbeeld van Fizzy maakt het smart contract gebruik van data die afkomstig is van de databases van het globale luchtverkeer. Een externe bron die het smart contract voedt met informatie die relevant is voor de contractuele overeenkomst wordt ook wel een

orakel genoemd. Dit kan allerlei typen informatie zijn, zoals bijvoorbeeld temperatuur, de prijs van een product, de hoeveelheid regenval, etc. Orakels zijn belangrijk in de verbinding van de blockchain met de reële wereld en activeren smart contracts wanneer er aan bepaalde condities van het contract is voldaan.

Er zijn talloze toepassingen mogelijk als smart contracts informatie kunnen opnemen buiten de blockchain voor de automatische uitvoering van overeenkomsten. Het introduceert echter wel een element van vertrouwen in orakels, terwijl blockchain in eerste instantie het vertrouwen in derde partijen wilde vermijden. (Thevenard, 2019) Het probleem waarbij er vertrouwd moet worden op derde partijen om het smart contract te voeden met externe data staat bekend als het ***orakelprobleem***.

Er zijn verschillende manieren waarop je kan omgaan met het orakelprobleem. Wij bespreken hieronder enkele voorbeelden. Het doel is om de integriteit van orakels te verzekeren, zodat er alleen correcte data-input wordt opgenomen in de blockchain.[99]

Gebruik van meerdere databronnen

Eén manier om te voorkomen dat valse data wordt geïnjecteerd in de blockchain, is door gebruik te maken van meerdere databronnen. Om de data te corrumperen zal de meerderheid van de databronnen of het orakel zelf, dat in wezen een Single Point of Failure is, moeten worden gecompromitteerd. (Thevenard, 2019)

Gebruik van meerdere databronnen met behulp van Schelling points

De kans dat er malafide informatie in de blockchain wordt opgenomen, kan ook worden verkleind door gebruik te maken van meerdere orakels. Het systeem blijft daardoor veilig, zolang de meerderheid betrouwbare informatie levert. Buterin (2014) schreef over hoe een dergelijk systeem zou kunnen werken door middel van ***Schelling points***.

Het concept Schelling points werd voor het eerst geïntroduceerd door Thomas Schelling in zijn boek *The Strategy of Conflict* (1960).[100] In het boek omschrijft Schelling het als een “focal point”

[99] Er wordt weleens gezegd dat blockchain een ‘waarheidsmachine’ (truth machine) is waarbij je zeker weet dat de gegevens die erop staan correct zijn. Dit is echter niet waar. De uitdaging is om mensen zo te stimuleren dat ze geen onjuiste data schrijven naar de blockchain. Slechte input in de blockchain leidt namelijk altijd tot slechte output. Dit staat ook wel bekend als garbage in, garbage out.

[100] Thomas Schelling ontving in 1995 de Nobelprijs voor economie voor zijn bijdragen aan de speltheorie.

voor iedere persoonsverwachting van wat de ander verwacht dat hij verwacht wat er wordt verwacht te doen (p. 57). Het werkt als volgt. Stel je voor dat jij en een andere gevangene in aparte ruimtes worden gehouden. Ieder van jullie ontvangt twee identieke papieren waar acht getallen op zijn geschreven:

14237 59049 76241 81259 90215 100000 132156 157604

Jullie mogen beiden één getal uitkiezen. Mochten jullie beiden exact dezelfde getal kiezen, dan worden jullie vrijgelaten. Mochten jullie beiden andere getallen kiezen, dan worden jullie voor de rest van jullie leven gevangen gehouden. In theorie zou je kunnen zeggen dat er een kans van 1 op 8 is dat jullie allebei hetzelfde getal kiezen. Er zijn immers slechts acht mogelijkheden. Echter, in werkelijkheid is de kans veel hoger, omdat het nummer 100000 'speciaal' is en duidelijk uit het oog springt, waardoor het een focal point wordt. Elk van jullie verwacht dat de ander het getal 100000 kiest en verwacht dat de ander verwacht dat jullie allebei het verwachten.[101] (Buterin, 2014) Een dergelijk concept kan ook worden toegepast om orakels te stimuleren juiste data in de blockchain in te voeren. We zouden bijvoorbeeld alle orakels kunnen vragen om de huidige prijs van Apple (AAPL) aandelen in de blockchain in te voeren en na te gaan wat de orakels denken dat de huidige prijs is. Er kan worden afgesproken dat alleen de mediane input, de correcte input is.[102] (Chan, 2018)

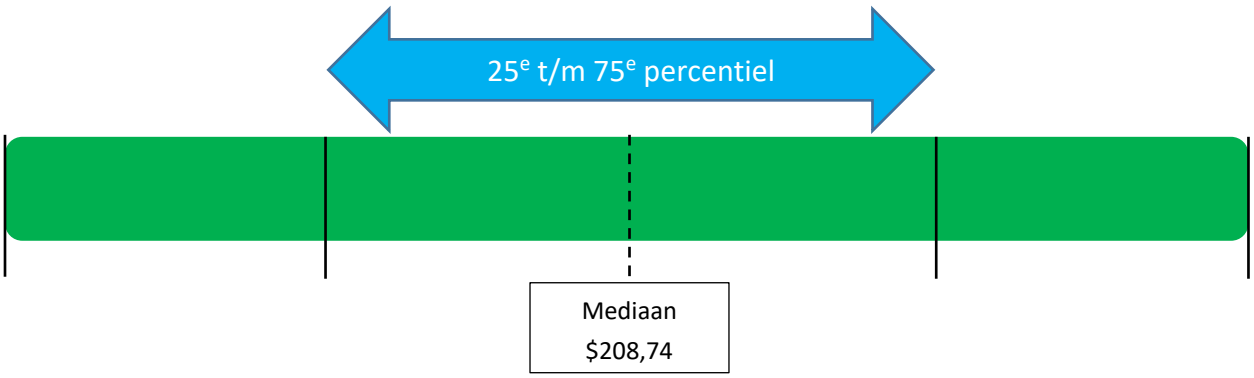
Gebruik van een beloningssysteem

Naast eerdergenoemd gebruik van Schelling points kan ook worden afgesproken dat elk orakel dat een prijs heeft ingediend die valt binnen het 25^{e} en 75^{e} percentiel een beloning ontvangt in bepaalde tokens. Zo zouden nodes binnen een gedecentraliseerd orakelnetwerk kunnen worden gevraagd om een bepaald aantal coins als onderpand te leggen om de dienst van een orakel te mogen uitvoeren. Als zij hun werk goed uitvoeren, worden zij beloond. Mochten zij hun werk als orakel niet goed uitvoeren, dan zou er een percentage van hun onderpand kunnen worden ingenomen.

[101] Zie 'SchellingCoin: A Minimal-Trust Universal Data Feed' van Vitalik Buterin (2014) voor een uitgebreidere beschrijving van Schelling points en wat de zwakheden van een dergelijk systeem zijn.

[102] De mediaan is het midden van een gegevensverzameling. Als er 13 getallen zijn die worden gerangschikt van laag naar hoog, dan is het 7^{e} getal de mediaan. Als er een even aantal getallen zijn die worden gerangschikt van laag naar hoog, dan wordt het gemiddelde genomen van de middelste twee data. Bij 12 getallen worden het 6^{e} en 7^{e} getal gemiddeld.

Een systeem bestaande uit een combinatie van Schelling points en een beloningssysteem vertrouwt erop dat de orakels worden gestimuleerd correct te gissen wat de andere orakels als data-input zullen geven aan de blockchain. Het insturen van accurate informatie is hierbij de beste strategie om het mediane getal op te leveren en beloond te worden.



Afbeelding 86: Orakels sturen de prijs van Apple (AAPL) aandelen naar de blockchain. Het mediane getal wordt door de blockchain aangenomen als de ware prijs van een Apple-aandeel. Orakels die het getal tussen de 25e en 75e percentiel inzenden, worden beloond.

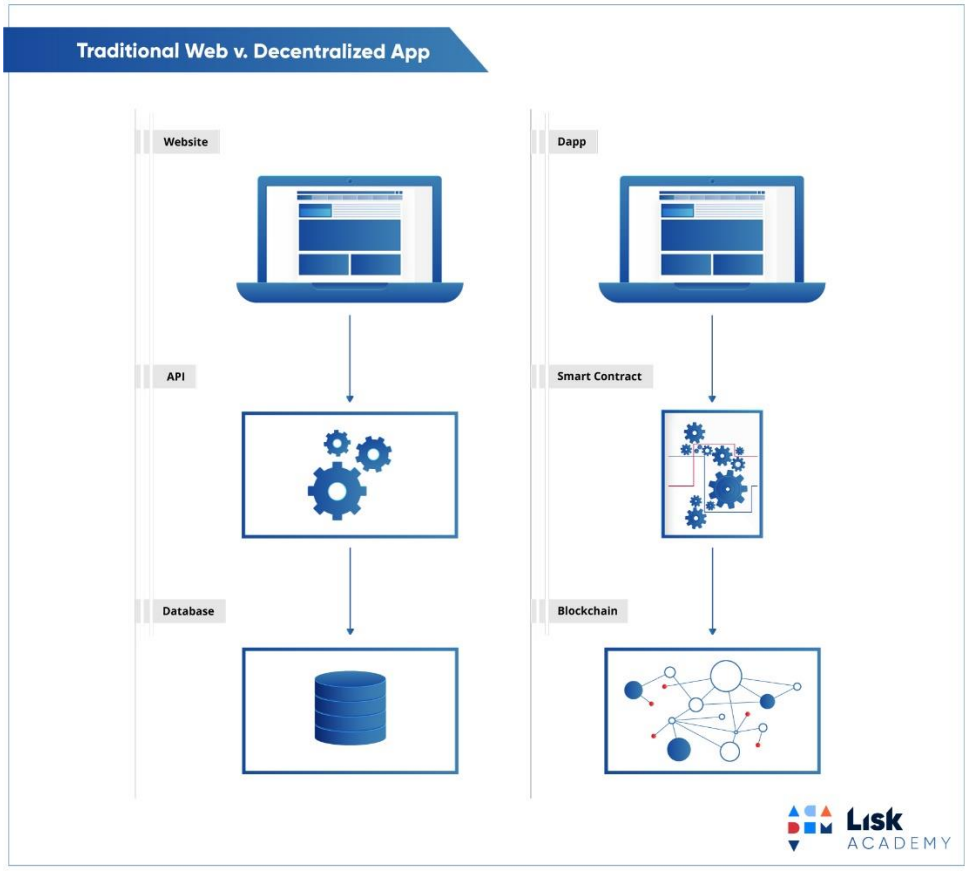
Er bestaat in het vorige voorbeeld echter nog wel het risico dat een meerderheid van de orakels in handen is van een enkele entiteit, of van een kartel dat valse data naar de blockchain stuurt. Met andere woorden, het eigenaarschap van orakels kan alsnog te gecentraliseerd zijn. Voorbeelden van projecten die momenteel werken aan een gedecentraliseerd orakelsysteem om het orakelprobleem op te lossen, zijn ChainLink, Witnet en Oraclize.[103]

8.6 Gedecentraliseerde applicaties

Er is geen eenduidige definitie van wat een ***gedecentraliseerde applicatie*** (dApp) behelst. Wij definiëren een dApp als een applicatie die gebruikmaakt van de gedecentraliseerde dataopslag van een blockchain. Hierbij wordt de applicatie niet uitgevoerd via een centrale server, maar via een gedecentraliseerd netwerk van nodes. Het heeft net als een normale applicatie vaak een front end en een user interface. De interface biedt de gebruiker een makkelijkere interactie met smart contracts en de blockchain. Door de smart contracts die de kerncode uitmaakt van een dApp op decentrale wijze op te slaan en uit te voeren, is er geen Single Point of Failure. De werking van de applicatie en de data van de applicatie zijn niet zomaar te censureren of te verwijderen.

[103] Op 13 juni kondigde ChainLink aan dat Google de ChainLink-technologie gaat gebruiken voor hun cloud services (Day, 2019).

De website van Lisk (2019), net als Ethereum een blockchainplatform dat ontwikkeld is om smart contracts en dApps op te bouwen, vergelijkt een dApp ook wel met een website die middels een ***application programming interface*** (API) bepaalde data uit een database aanroept. De API is een communicatieprotocol waarmee de webapplicatie en de server databerichten met elkaar kunnen delen. Hierbij wordt de volgende vergelijking gemaakt tussen een traditionele website en een dApp.



Afbeelding 87: Vergelijking tussen het traditionele web en een gedecentraliseerde applicatie.

In de Ethereum white paper wordt onderscheid gemaakt tussen drie typen dApps. De eerste categorie bestaat uit financiële dApps die je geld helpt beheren en je in staat stelt om met je geld contracten af te sluiten. Voorbeelden hiervan zijn cryptovaluta en financiële derivaten. De tweede categorie bestaat uit semi-financiële dApps waar ook geld bij betrokken is, maar waar daarnaast een gewichtige niet-monetaire zijde aan vasthangt. Denk hierbij bijvoorbeeld aan een verzekeringsapplicatie zoals die van Fizzy. De derde categorie bestaat uit dApps die totaal niet financieel van aard zijn. (Buterin, p. 19, 2014)

DApps kunnen dus zeer divers van aard zijn. Als voorbeeld worden de volgende twee Ethereum dApps behandeld die je momenteel al kunt gebruiken: Golem en Ethlance.

8.6.1 Golem

Golem is een project op Ethereum dat mensen de mogelijkheid biedt om hun overtollige computerkracht peer-to-peer te delen met anderen. De computerkracht kan worden gebruikt voor verscheidene doeleinden. Mensen kunnen het huren voor bijvoorbeeld CGI-rendering, voor machine learning of voor het uitvoeren van ingewikkelde wetenschappelijke berekeningen. Iedereen die zijn computerkracht beschikbaar stelt, wordt beloond in Golem Network Tokens (GNT). Je kunt Golem zien als een open marktplaats voor het huren en verhuren van computerkracht. Het heeft de ambitie om een supercomputer te zijn, die voor iedereen toegankelijk is.

8.6.2 Ethlance

Ethlance is een andere dApp die is ontwikkeld op Ethereum. Het is een marktplaats voor freelancers die werk willen verrichten voor Ethers. Het platform neemt geen percentage van het bedrag dat je krijgt van de werkgever en er zijn geen lidmaatschapskosten. Het maakt gebruik van een transparant reviewsysteem en freelancers en potentiële klanten kunnen op transparante wijze zien wat hun vorige activiteiten waren, voordat zij een zakelijke relatie aangaan.[104]

Een interessante subgroep van een dApp is een gedecentraliseerde autonomie organisatie (DAO) en een gedecentraliseerde autonome corporatie (DAC).

[104] Voor meer informatie over Ehtlance, zie: https://ethlance.com/.

Intermezzo: Winstgevende dApps

Een belangrijke vraag met betrekking tot dApps is hoe je er als ontwikkelaar van de dApp geld mee kunt verdienen. Volgens Siraj Raval (2016) dient een dApp die winstgevend wil zijn te voldoen aan de volgende vier eigenschappen:

1. Open source.
2. Interne valuta.
3. Gedecentraliseerde consensus.
4. Geen Single Point of Failure.

Open source

Hoewel het goed mogelijk is om closed source dApps te ontwikkelen, roepen dergelijke dApps veel wantrouwen op. Als de code niet transparant voor iedereen in te zien is, is het mogelijk dat de ontwikkelaars de dApp zodanig hebben ontworpen, dat ze de data kunnen censureren. Dit gaat in tegen het initiële principe van Bitcoin en andere open source blockchains om vertrouwen in tussenpartijen te minimaliseren. Echter, als het open source is, zouden mensen de applicatie kunnen kopiëren en aanpassen met eigen logo's.

Interne valuta

De ontwikkelaar kan een schaars token, de appcoin, introduceren in de applicatie. Om gebruik te mogen maken van het blockchainnetwerk waarop de applicatie draait, dient deze appcoin te worden gebruikt. Gebruikers die een dienst leveren aan de applicatie of het netwerk waar de applicatie op draait, kunnen bijvoorbeeld uitbetaald worden in deze appcoins. Als de appcoins een monetaire waarde vertegenwoordigen stimuleren ze het gebruik van de dApp.

Gedecentraliseerde consensus

Er dient ook consensus te zijn binnen het gedecentraliseerde netwerk over wat de staat van de data is. Elke node op het netwerk moet er dus over eens zijn dat jouw gebruikersnaam en private key horen bij jouw account en dat jij daarmee kunt inloggen in de dApp.

Geen Single Point of Failure

Doordat de data in een dApp zijn gedecentraliseerd over een groot netwerk van nodes, kan een dApp niet makkelijk worden gesloten. Als één node faalt, zijn er nog andere nodes die het netwerk kunnen draaien.

8.7 Gedecentraliseerde autonome organisatie (DAO)

Gedecentraliseerde autonome organisaties (DAO's) worden soms ook wel ***gedecentraliseerde autonome corporaties*** (DAC's) genoemd. Vitalik Buterin ziet de DAC echter als een subklasse van de DAO.[105] Hij beschrijft de DAO als een autonome entiteit, die ook afhankelijk is van het inhuren van individuen. Deze individuen kunnen bepaalde noodzakelijke taken vervullen die de entiteit niet kan. De DAO heeft hiervoor intern kapitaal tot zijn beschikking, waarmee bepaalde activiteiten van deze individuen kunnen worden beloond. (Buterin, 2014) Wat een DAO wezenlijk anders maakt van een gecentraliseerde organisatie is dat het geen top managementteam of een CEO heeft. Het heeft ook geen vestigingen, werknemers, of dochtermaatschappijen. In plaats daarvan bestaat een DAO op een gedecentraliseerd netwerk van gebruikers en nodes die transacties verzamelen, verifiëren en updaten op een blockchain. Beslissingen over wijzigingen aan de code worden gemaakt door democratische stemprocessen. Het is dus een radicaal andere manier om een bedrijfsorganisatie in te richting. Bitcoin kan vanwege zijn autonome karakter – het is immers een zelfvoorzienend en zelforganiserend systeem – worden gekenmerkt als een DAO, omdat het (a) een betaalsysteem draait, (b) subcontractors in dienst heeft die als mijners werken en (c) deze subcontractors betaalt met nieuw uitgekeerde Bitcoins (Vigna & Casey, 2015, p. 229). Daarnaast kunnen mijners stemmen op verbetervoorstellen aan het protocol door middel van hun computerkracht. DAO's zijn dus organisaties waarvan de organisatieregels zijn uitgedrukt in een volkomen transparant computerprogramma. Ze worden beheerd door een collectief besluitvormingsproces van stakeholders via een gedecentraliseerd protocol en worden niet beïnvloed door een centraal bestuursorgaan.

Definitie van DAO
Een DAO kan worden gedefinieerd als een non-hiërarchische organisatie die routinetaken uitvoert en registreert op een blockchain. De regels waaraan de DAO zich houdt, staan ook vastgelegd op de blockchain. Daarnaast is de DAO afhankelijk van vrijwillige bijdragen van interne stakeholders om de organisatie door middel van een democratisch consultatieproces te begeleiden. (Hsieh et al., 2018, p. 2)

[105] Daniel Larimer, de oprichter van onder andere EOS, Steem en BitShares, heeft het concept van een DAC geïntroduceerd. Buterin beschrijft een DAC als een subklasse van DAO's. Een DAC heeft aandelen en keert dividend uit aan aandeelhouders. (Buterin, 2014)

Eén goed voorbeeld van een DAO op het Ethereum-netwerk was de mislukte Genesis DAO, ook wel kortweg de DAO genoemd. Het was bedoeld als zijnde een venture capital fund voor de cryptowereld.

Afbeelding 88: Logo van de Genesis DAO op het Ethereum-netwerk.

De DAO zou als volgt werken:

1. Een developers team van Slock.IT programmeert de DAO.
2. Er is een vooraf vastgestelde periode waarin het publiek kan investeren in het fonds. In ruil voor de investering ontvangen investeerders DAO-tokens. Deze tokens representeren eigendomsrecht van de DAO. Je kunt het vergelijken met aandelen. Het investeringsproces kun je vergelijken met een crowdsale of een ***Initial Coin Offering*** (ICO). ICO's worden in paragraaf 10.4 gedetailleerder besproken.
3. Wanneer de investeringsperiode afgelopen is, start de DAO met zijn operaties.
4. Mensen kunnen dan een projectplan indienen bij de DAO voor financieringsaanvragen. De DAO-tokenhouders kunnen dan door middel van een stemproces stemmen op projectplannen. Plannen met voldoende stemmen krijgen financiering en de DAO-tokenhouders ontvangen beloningen als de projecten winst maken.

De DAO kan dus worden gezien als een investeringsfonds zonder traditionele investeringsmanagers. In plaats van managers die fondsen beheren, worden de fondsen middels een democratisch proces beheerd door de community van DAO-tokenhouders.

De DAO werd gelanceerd op 30 april 2016 en de crowdsale zou vier weken lang duren. Uiteindelijk werd er 12,7 miljoen Ether geïnvesteerd in het project wat toentertijd, bij de prijs van $20 USD per Ether, gelijkstond aan ongeveer $250 miljoen USD. Echter, werd er op 17 juni 2016 een hack in de code geëxploiteerd, waardoor de hacker het fonds van de DAO kon leegtrekken. Binnen enkele uren werd 3,6 miljoen Ether gestolen, wat toentertijd gelijkstond aan iets meer dan $70 miljoen USD. Het is hierbij belangrijk om te weten dat het Ethereum-protocol nooit is gehackt. De hack betreft alleen de DAO-applicatie. Om het gestolen fonds

weer terug te laten keren naar de investeerders werd er een hard fork voorgesteld en geïmplementeerd. Het voorstel was om de staat van de blockchain terug te draaien naar een moment van voor de hack, alsof de hack nooit heeft plaatsgevonden op de blockchain.[106]

Als je aan de potentie van DAO's denkt, dan moet je denken aan organisaties zonder centraal beslissingsorgaan, zoals een Facebook zonder een Raad van bestuur of een Amazon zonder Amazon CEO. Het sentiment omtrent de idealistische potentie van DAO's is goed verwoord door Vitalik Buterin (2015) met de woorden:

> "Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, Blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly."

Door het centrum – in dit geval een bedrijf als Uber – weg te halen, kunnen gebruikers direct economische en sociale interacties met elkaar aangaan. Een DAO is hiermee resistent tegen censuur van centrale tussenpartijen. Mocht er toch op de een of andere manier ongewenste censuur zijn, dan kan de DAO deze omzeilen met instrumenten als een hard fork.

Binnen een DAO kennen de deelnemers elkaar in beginsel niet allemaal. Dit maakt de DAO een interessant alternatief voor een vereniging of stichting. Afhankelijk van het DAO-protocol kunnen stakeholders anoniem stemmen en kunnen ze autorisatie aan anderen geven om in hun naam te stemmen. Stel je hierbij de situatie voor dat je afhankelijk van het onderwerp een ander de autorisatie geeft om te stemmen voor jou. De stemming zelf is transparant, snel en laagdrempelig vastgelegd op de blockchain.

[106] Zoals in een eerder hoofdstuk al is uitgelegd, zijn het de full nodes die transacties verifiëren en die updates doorvoeren. Zo zijn het ook de full nodes die, als zij consensus kunnen bereiken, transacties kunnen terugdraaien, veranderen en censureren. Middels deze methode werd de hack volledig teruggedraaid, waardoor er tegelijkertijd een splitsing kwam tussen de blockchain die deze hard fork wél heeft geïmplementeerd en de blockchain die deze hard fork niét heeft geïmplementeerd. Dit leidde dus tot twee verschillende versies van de Ethereum blokchain. De versie met de hard fork noem je de Ethereum blokchain met Ether als coin, die niet compatibel is met de oorspronkelijke Ethereum blokchain. De versie zonder de hard fork is de Ethereum Classic blockchain. Deze heeft de Ethereum Classic als coin. De Ethereum Classic coin is zelf ook niet compatibel met de Ethereum blokchain.

Bitcoin is de eerste DAO. Het heeft geen CEO of managers die de richting van de Bitcoin blockchain bepalen. Deelnemers kunnen verbetervoorstellen indienen en het netwerk kan erop stemmen door computerkracht te leveren voor de voorgestelde blockchain updates.

Sommige blockchains maken ook gebruik van ***worker proposals***. Dit zijn voorstellen die door mensen zijn ingediend om financiering te vragen voor een project, dat ten gunste is voor de desbetreffende blockchain. Zo kunnen ze bijvoorbeeld een marketingbureau inhuren of de eigen uren betaald krijgen ten bate van het initiatief. Naast technische comités gebruikt een DAO soms werkgroepen voor verschillende doelen, zoals het opzetten van documentatie, verrichten van onderzoek, en het verkrijgen van exchange listings.

Een DAO is geen perfect geregeld alternatief. Veel stakeholders zijn slechts vluchtig betrokken en lezen de voorstellen niet in detail. Het is ook niet altijd even praktisch om een hard fork te maken. Een DAO is echter wel weer een voorbeeld waarin blockchain helpt te innoveren.

Voorbeelden van bestaande DAO's op het Ethereum-platform zijn Aragon en DigixDAO. Aragon komt aan bod in het volgende intermezzo.

Intermezzo: Aragon

De ontwikkelaars van Aragon geloven in een toekomst waarbij organisaties autonoom en decentraal gerund kunnen worden. Door gebruik te maken van de blockchain, hoeven organisaties minder overheadskosten en administratieve kosten te maken.

Aragon is een platform waar je op laagdrempelige wijze DAO's kunt creëren. Hierbij maakt Aragon gebruik van Ethereum en ***InterPlanetary File System*** (IPFS), een peer-to-peernetwerk om data op te slaan en te delen.

Aragon is software dat je in staat stelt om op een laagdrempelige wijze een eigen organisatie op te richten en over grenzen heen samen te werken. Je kunt op Aragon in een mum van tijd een eigen organisatie starten met een aantal belangrijke organisatorische functies zoals identiteitsmanagement, modules om toegang en eigendom te controleren, beslissingsrechten, fondsenwerving en administratieve werkzaamheden. Doordat deze organisaties op een blockchain staan, kun je ze bureaucratievrij inrichten. Dit alles kun je regelen zonder programmeerkennis.

Aragon biedt momenteel een aantal templates aan van organisaties die je in een mum van tijd kunt opstarten. Voorbeelden van deze templates zijn:

1. Fondsenwerving om een transparante en verantwoordelijke crowdfundingcampagne te starten voor je eigen organisatie.
2. Open Enterprise waarbij je apps kunt gebruiken om projectmanagement, budgetplanning en beloningen in te zetten voor je eigen organisatie.
3. Reputatiesysteem om middels democratische stemmen beslissingen te nemen binnen je organisatie. Het gewicht van de stemmen worden gelinkt aan reputaties.
4. Een aandelensysteem waarbij je eigenaarschap binnen je organisatie kunt vastleggen en verdelen. Beslissingen worden hierbij genomen op basis van democratische stemmen. De stemmen worden gelinkt aan het gewicht van de stake die een aandeelhouder heeft. Daardoor hebben grotere aandeelhouders meer invloed.
5. Ledensysteem waarbij beslissingen binnen de organisatie gebeuren op basis van een één-lid-één-stemprincipe.

Je kunt op het testnet van Aragon, https://rinkeby.aragon.org/, experimenteren met het aanmaken en inrichten van DAO's.

8.7.1 De toekomstvisie van DAO's en autonome agenten

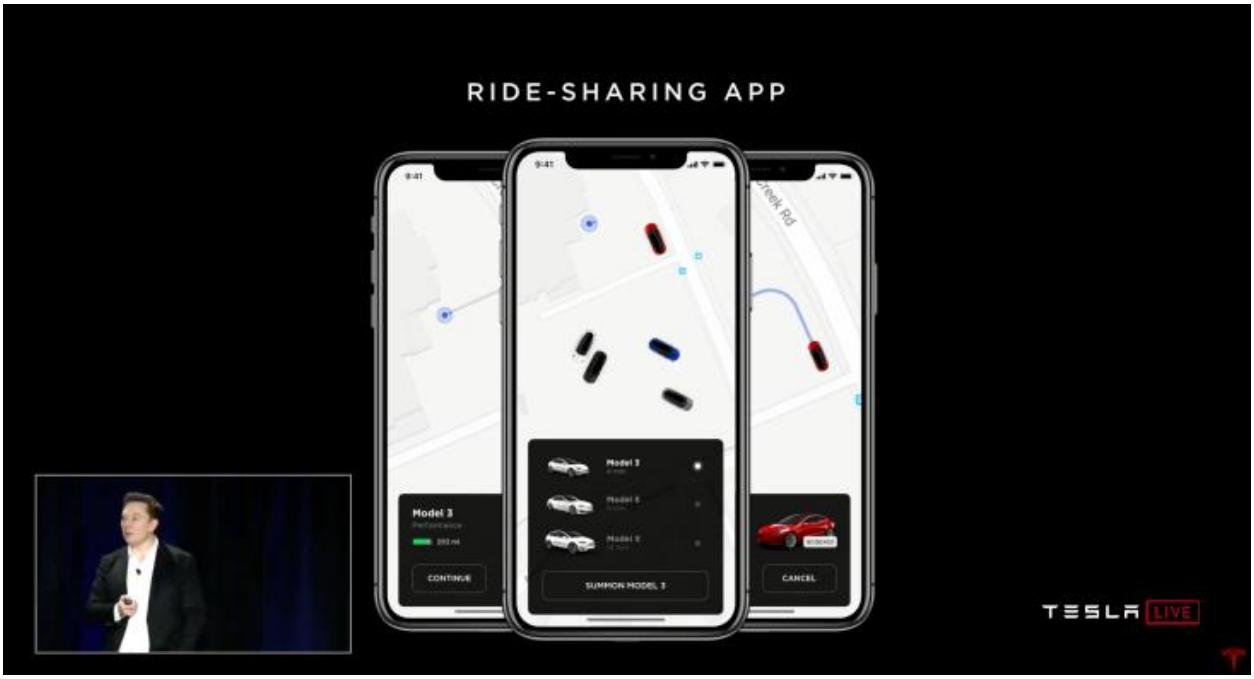
Een voorbeeld van een verder geëvolueerde DAO, die we wellicht in de nabije toekomst zullen zien, is een machine die volledige autonomie heeft over zichzelf. David Irvine (2014), uitvinder van het SAFE Netwerk, schetst een intrigerend toekomstperspectief, waarin dergelijke machines een plek hebben in onze sociale en economische wereld.[107] Stel je voor dat er een robot-ober wordt ontwikkeld met kunstmatige intelligentie. De robot serveert eten en drinken in een restaurant en heeft dingen nodig als elektriciteit en reparaties. Hij krijgt betaald in een cryptovaluta als bijvoorbeeld Ether door klanten die eten en drinken bij hem bestellen. De Ether bewaart hij in zijn cryptowallet. Daarnaast kan de robot zichzelf ook aansluiten aan een stopcontact om zich op te laden. Voor het opladen betaalt hij de elektriciteitsaanbieder Ether. Als de robot is versleten en een reparatie nodig heeft, gaat hij naar een reparatiewinkel en betaalt hij de monteur in Ether. Uiteraard bevat de robot voldoende mechanismen waarmee zijn cryptowallet is beveiligd tegen diefstal.

Deze robot is geen traditionele DAO meer, omdat er geen groep is die gezamenlijk zeggenschap heeft over de robot. Ook is het niet noodzakelijk dat de software van de robot op een blockchain is geplaatst. Vitalik Buterin (2014) noemt een dergelijke entiteit die geen betrokkenheid van mensen behoeft om zichzelf draaiende te kunnen houden en te kunnen manoeuvreren in de wereld een ***autonome agent*** (AA). Een andere voorbeeld van een autonome agent die al bestaat, is een computervirus. Het virus overleeft door zichzelf te blijven repliceren van machine tot machine, zonder menselijke tussenkomst.

Een toekomstperspectief dat dichterbij lijkt dan het bovenstaande voorbeeld van de robot is een zelfrijdende auto, die zelf ritjes aanbiedt tegen betaling en die via smart contracts zijn opbrengsten verdeelt over zijn eigenaren. Elon Musk zei in april 2019 dat hij de eerste robotaxi's verwacht uit te rollen in 2020 (Korosec, 2019). Tesla auto's bezitten momenteel al over voldoende kunstmatige intelligentie dat ze zelfrijdend zijn. Het enige wat nog ontbreekt is een smart contract waarmee de opbrengsten van de robotaxi automatisch, eventueel ook zonder tussenkomst van een derde partij als een financiële instelling, zijn winsten deelt met zijn eigenaar. Als een community besluit om gezamenlijk te investeren in een dergelijke robotaxi in ruil voor aandeeltokens en het beheer ervan transparant op een blockchain wordt vastgelegd, waardoor de rechten van iedereen inzichtelijk zijn, dan is het al een DAO. De mede-eigenaren

[107] Het SAFE Netwerk is een autonoom peer-to-peer netwerk dat is ontwikkeld door MaidSafe. SAFE staat voor Secure Access For Everyone.

kunnen bijvoorbeeld met hun aandeeltokens voorstellen indienen voor bepaalde updates aan de taxi en op decentrale wijze stemmen over welke updates moeten worden doorgevoerd. Daarnaast keert de robotaxi al zijn eigenaren, naar verhouding van hun geïnvesteerde geld, de winsten uit.



Afbeelding 89: Elon Musk, CEO van Tesla, voorspelt dat de eerste autonome robotaxi's van Tesla in 2020 op de markt komen. Volgens Musk is de software al klaar. Het enige wat nog ontbreekt, is regulatoire toestemming. (Korosec, 2019).

8.8 Samenvatting, begrippen en bronnen

Samenvatting

De eerste generatie applicaties concentreerde zich voornamelijk op digitaal geld. De generatie blockchains waar deze applicaties op werden gebouwd, wordt ook wel blockchain 1.0 genoemd. Hoewel Bitcoin een geldmiddel is en voornamelijk wordt gebruikt als cryptovaluta waarbij diensten en goederen kunnen worden verhandeld, is het ook mogelijk om de scriptingtaal van Bitcoin te gebruiken voor de opslag van kleine hoeveelheden metadata in de transacties. Hierdoor zou je bijvoorbeeld in een Bitcoin-transactie een script mee kunnen geven dat er 1.000 eenheden van een nieuwe activa zijn uitgegeven en dat ze zijn toegekend aan een bepaald Bitcoin-adres. Deze eenheden kunnen worden gezien als nieuwe coins. Dergelijke coins worden colored coins genoemd.

Later zijn er blockchains opgekomen met als doel om op makkelijkere wijze nieuwe typen applicaties te ontwikkelen dan alleen een nieuw geldsysteem. Deze blockchains worden ook wel 2e generatie blockchains genoemd: blockchain 2.0.

Een voorbeeld van blockchain 2.0 is Ethereum. Het doel van Ethereum is om ontwikkelaars de mogelijkheid te bieden om smart contracts en applicaties te ontwikkelen met arbitraire condities en voorwaarden. Een smart contract is een vorm van decentrale automatisering en is een contract met bepaalde condities en voorwaarden die zijn vastgelegd in code. Het contract is zelfuitvoerend, omdat het zelf de juiste corresponderende acties uitvoert wanneer er aan de condities en voorwaarden wordt voldaan.

Er zijn twee verschillende categorieën van smart contracts: deterministische en non-deterministische smart contracts. Een deterministisch smart contract heeft geen informatie van een externe partij van buiten de blockchain nodig om het contract te kunnen uitvoeren. Het smart contract kan alle informatie die noodzakelijk is voor de uitvoerbaarheid van het contract krijgen binnen het blockchainnetwerk zelf. Een non-deterministisch smart contract heeft daarentegen wel informatie van een externe partij buiten de blockchain nodig. Een dergelijke partij wordt een orakel genoemd.

De behoefte om gebruik te maken van orakels kan leiden tot het orakelprobleem – het probleem waarbij er vertrouwd moet worden op derde partijen om het smart contract te voeden met externe data. Er zijn verschillende manieren om het orakelprobleem het hoofd te bieden. Enkele voorbeelden zijn:

1. Het gebruikmaken van meerdere databronnen.
2. Het gebruikmaken van meerdere databronnen met behulp van Schelling points.
3. Het gebruikmaken van een beloningssysteem.

Met de smart contracts kunnen er gedecentraliseerde applicaties (dApps) worden ontwikkeld. Wij definiëren een dApp als een applicatie die gebruikmaakt van de gedecentraliseerde dataopslag van een blockchain.

Naast dApps kunnen er ook gedecentraliseerde autonome organisaties (DAO's) en gedecentraliseerde autonome corporaties (DAC's) worden ontwikkeld. Een DAO kan worden gedefinieerd als een non-hiërarchische organisatie die routinetaken uitvoert en registreert op een blockchain. De regels waaraan de DAO zich houdt, staan ook vastgelegd op de blockchain.

Daarnaast is de DAO afhankelijk van vrijwillige bijdragen van interne stakeholders om de organisatie door middel van een democratisch consultatieproces te begeleiden. Een DAC is een subklasse van DAO's. Een DAC heeft aandelen en keert dividend uit aan aandeelhouders.

Opmerkingen die je nu kunt uitleggen

- Blockchain 2.0 biedt ons andere applicaties op de blockchain dan alleen een nieuw geldsysteem.
- Je kunt smart contracts ontwikkelen op Ethereum waarbij de condities en voorwaarden zo duidelijk zijn vastgelegd in de code dat er bij contractbreuk geen interpretatie van derde partijen meer nodig is.
- Bitcoin is een first-to-file-systeem.
- Ethereum is ontstaan, omdat het bij Bitcoin haast niet mogelijk is om een stuk logica mee te geven aan een transactie die bijvoorbeeld zegt dat een persoon automatisch zijn BTC ontvangt nadat hij een tegenprestatie heeft geleverd.
- Ethereum is Turing-compleet.
- Non-deterministische smart contracts kunnen lijden aan het orakelprobleem.
- Bitcoin is de eerste gedecentraliseerde autonome organisatie (DAO).

Verklarende begrippenlijst

Application Programming Interface (API): Een communicatieprotocol waarmee de webapplicatie en de server databerichten met elkaar kunnen delen.

Autonome agent (AA): Een entiteit die geen betrokkenheid van mensen behoeft om zichzelf draaiende te kunnen houden en te kunnen manoeuvreren in de wereld.

Bitcoin 2.0: Een nieuwere generatie van Bitcointechnologie die bedoeld is om andere toepassingen dan alleen cryptovaluta mogelijk te maken.

Blockchain 1.0: De eerste generatie blockchains die voornamelijk gebruikt zijn om cryptovaluta's op te draaien.

Blockchain 2.0: De tweede generatie blockchains die meer gericht zijn op het mogelijk maken van smart contracts, dApps en DAO's.

Blockchain 3.0: De derde generatie blockchains die een cluster van issues waar blockchain 2.0 nog mee kampt, hebben opgelost. Voorbeelden van zulke issues zijn schaalbaarheid, interoperabiliteit, privacy, duurzaamheid en governance. Blockchains die zichzelf scharen onder 3.0 zijn bijvoorbeeld EOS en Cardano.

Colored coins: Coin, vaak één satoshi, waar je bepaalde eigenschappen aan kunt toekennen zodat ze verscheidene dingen kunnen representeren, zoals bijvoorbeeld aandelen, obligaties, eigendomsrechten op onroerend goed, coupons en alternatieve cryptovaluta. Er is een periode geweest waarin veel onderzoek is gedaan naar de mogelijkheden van colored coins op de Bitcoin blockchain.

Deterministisch smart contract: Smart contract die geen informatie nodig heeft van een externe partij van buiten de blockchain om het contract te kunnen uitvoeren.

Gas: Transactiekosten die je betaalt om een transactie op de Ethereum blockchain uit te voeren.

Gedecentraliseerde applicatie (dApp): Een applicatie die gebruikmaakt van de gedecentraliseerde dataopslag van een blockchain. Hierbij wordt de applicatie niet uitgevoerd via een centrale server, maar via een gedecentraliseerd netwerk van nodes. Het heeft net als een normale applicatie vaak een front end en een user interface.

Gedecentraliseerde autonome corporatie (DAC): Een subklasse van DAO's. Een DAC heeft aandelen en keert dividend uit aan aandeelhouders.

Gedecentraliseerde autonome organisatie (DAO): Een autonome entiteit, die ook afhankelijk is van het inhuren van individuen. Deze individuen kunnen bepaalde noodzakelijke taken vervullen die de entiteit niet kan. De DAO heeft hiervoor intern kapitaal tot zijn beschikking, waarmee bepaalde activiteiten van deze individuen kunnen worden beloond. Wat een DAO wezenlijk anders maakt van een gecentraliseerde organisatie is dat het geen top managementteam of een CEO heeft. Het is een non-hiërarchische organisatie.

ICO: Zie Initial Coin Offering.

Initial Coin Offering (ICO): Fondsverwerving waarbij tokens worden gecreëerd en verkocht door een bedrijf of project.

InterPlanetary File System (IPFS): Een peer-to-peernetwerk om data op te slaan en te delen. Veel dApps maken naast de blockchain ook gebruik van IPFS.

IPFS: Zie InterPlanetary File System.

Non-deterministisch smart contract: Smart contract die wel informatie nodig heeft van een externe partij van buiten de blockchain om het contract te kunnen uitvoeren.

Orakel: Een bron buiten de blockchain die een smart contract voedt met relevante externe informatie zodat het smart contract arbitraire condities kan checken.

Orakelprobleem: Het probleem waarbij er vertrouwd moet worden op derde partijen om het smart contract te voeden met externe data.

Schelling points: Een 'focal point' voor iedere persoonsverwachting van wat de ander verwacht dat hij verwacht wat er wordt verwacht te doen.

Smart contract: Een contract met bepaalde condities en voorwaarden die zijn vastgelegd in code. Het contract is zelfuitvoerend, omdat het zelf de juiste corresponderende acties uitvoert wanneer er aan de condities en voorwaarden wordt voldaan. Het contract moet hiervoor wel voldoende informatie bevatten van elke partij die betrokken is bij het contract, zodat het het vermogen ontneemt van partijen om het contract te verbreken. Er zijn twee typen smart contracts: deterministische en non-deterministische.

Solidity: De programmeertaal die specifiek voor Ethereum is ontwikkeld om smart contracts mee te schrijven.

Turing-compleet: Elke berekening of gegevensbewerking die geprogrammeerd kan worden, kan in een Turing-compleet systeem ook geprogrammeerd worden.

Worker proposal: Een voorstel dat wordt ingediend om financiering te vragen voor een project, dat ten gunste is voor de desbetreffende blockchain. Zo kunnen ze bijvoorbeeld een marketingbureau inhuren of de eigen uren betaald krijgen ten bate van het initiatief.

Bronnen

Ackermann, J. & Meier, M. (2018). Blockchain 3.0: The next Generation of Blockchain Systems. *Advanced Seminar Blockchain Technologies, Summer Term 2018*, Technical University Munch.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). *Lecture Notes in Computer Science*, 164–186. https://doi.org/10.1007/978-3-662-54455-6_8

AXA. (z.d.). fizzy by AXA. Geraadpleegd op 27 december 2019, van Fizzy.axa website: https://fizzy.axa

Buterin, V. (2013). *Ethereum white paper: a next generation smart contract and decentralized application platform* [White paper]. Geraadpleegd op 27 december 2019, van Blockchainlab: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, 6 mei). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. Geraadpleegd op 27 december 2019, van Ethereum.org website: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

ChainTrade. (2017, 27 december). 10 Advantages of Using Smart Contracts. Geraadpleegd op 27 december 2019, van Medium website: https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a

Chan, K. (2018, 9 november). Keeping Honest - Solving the Oracle Problem. Geraadpleegd op 27 december 2019, van Medium website: https://medium.com/@kenchangh/keeping-honest-solving-the-oracle-problem-714addc06e53

Clement, A. (2019, 24 mei). fizzy by AXA: Ethereum Smart Contract in details. Geraadpleegd op 27 december 2019, van Medium website: https://medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0

Colored-Coins. (2017, 5 juni). Colored Coins. Geraadpleegd op 27 december 2019, van GitHub website: https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Faq#coloring-satoshis

Day, A. (2019, 13 juni). Building hybrid blockchain/cloud applications with Ethereum and Google Cloud | Google Cloud Blog. Geraadpleegd op 27 december 2019, van Google Cloud Blog website: https://cloud.google.com/blog/products/data-analytics/building-hybrid-blockchain-cloud-applications-with-ethereum-and-google-cloud

Ethereum Foundation. (2014, 28 maart). SchellingCoin: A Minimal-Trust Universal Data Feed. Geraadpleegd op 27 december 2019, van Ethereum.org website: https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

Etherscan.io. (z.d.). Fizzy contract. Geraadpleegd op 27 december 2019, van Etherscan.io website: https://etherscan.io/address/0xe083515d1541f2a9fd0ca03f189f5d321c73b872

Ethlance. (z.d.). Ethlance - hire or work for Ether cryptocurrency. Geraadpleegd op 27 december 2019, van Ethlance.com website: https://ethlance.com/

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, *7*(1). https://doi.org/10.1186/s41469-018-0038-1

Irvine, D. (2014, 19 februari). Machines that own themselves in bitcoin. Geraadpleegd op 27 december 2019, van Metaquestions website: https://metaquestions.me/2014/02/19/machines-that-own-themselves-in-bitcoin/

Korosec, K. (2019, 22 april). Tesla plans to launch a robotaxi network in 2020. Geraadpleegd van TechCrunch website: https://techcrunch.com/2019/04/22/tesla-plans-to-launch-a-robotaxi-network-in-2020/

Raval, S. (2016). *Decentralized applications: harnessing Bitcoin's Blockchain technology*. Sebastopol, Calif.: O'reilly.

Rosenfeld, M. (2012). *Overview of Colored Coins*. Geraadpleegd op 27 december 2019, van https://bitcoil.co.il/BitcoinX.pdf

Schelling, T. C. (1960). *The strategy of conflict*. Whitefish, Montana: Literary Licensing.

Thevenard, J. (2019, 15 januari). Decentralised Oracles: a comprehensive overview. Geraadpleegd op 27 december 2019, van Medium website: https://medium.com/fabric-ventures/decentralised-oracles-a-comprehensive-overview-d3168b9a8841

Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order*. New York, N.Y.: Picador/St. Martin's Press.

Young, S. (2018). Enforcing Constitutional Rights Through Computer Code. Geraadpleegd van CUA Law Scholarship Repository website: https://scholarship.law.edu/jlt/vol26/iss1/5/

9. Blockchain governance en wie met welke rol mag deelnemen

"The first point is that transnational organizations need transnational governance structures. The reach, accessibility, and transparency of blockchain technology could be an effective transnational governance structure. Blockchain governance is more congruent with the character and needs of transnational organizations than nation-states. The second point is that not only is the transnational governance provided by the blockchain more effective, it is fairer. There is potentially more equality, justice, and freedom available to organizations and their participants in a decentralized, cloud-based model. This is provided by the blockchain's immutable public record, transparency, access, and reach."

- Melanie Swan (2015)

9.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Dat een blockchain verschillende governancestructuren kan hebben.
- Dat er voorwaarden kunnen worden gesteld waaraan je moet voldoen voordat je kunt deelnemen aan een blockchain.
- Dat deelnemers verschillende rollen in kunnen nemen.
- Dat de voorwaarden die worden gesteld om een rol te verkrijgen per samenwerkingsvorm op de blockchain kunnen verschillen.
- Dat een centrale versus een decentrale besturing van die samenwerkingsvormen impact heeft op deelnemers binnen de blockchain.
- Dat hierbinnen het verschil tussen een permissionless en een permissioned blockchain belangrijk is.
- Dat het verschil tussen een publieke en een private blockchain ook belangrijk is.

Inleiding

Een blockchain heeft zoals elk samenwerkingsverband een manier nodig om te worden bestuurd. De besturing wordt ook wel blockchain governance genoemd. De invulling van een besturingsvorm hangt samen met de doelen die het verband nastreeft. In dit hoofdstuk wordt er voornamelijk gekeken naar het verschil in besturingsvorm tussen enerzijds centraler gedreven blockchains en anderzijds decentraler gedreven blockchains zoals het Bitcoin-netwerk. Concreet richten we ons op het verschil tussen publieke en private blockchains en de tussenvorm hiervan, consortium. Uit een besturingsvorm van een blockchain vloeit mede voort wie mag deelnemen aan de blockchain. Als duidelijk is wie mag deelnemen, kun je kijken wie bijvoorbeeld als validator mag optreden om het netwerk te helpen onderhouden, wie mag beslissen over de hardware en software van het systeem en wie de strategie mag helpen uitzetten. Is er een open toegang voor iedereen om gebruik te mogen maken van de blockchain en deel te nemen aan de besturingsvorm of worden sommigen afgesloten van deelname?

Nadat we eerst de definitie van blockchain governance hebben besproken in paragraaf 9.2, maken we een kernonderscheid tussen een systeem waar iedereen het consensusmechanisme onderhoudt versus een systeem waar slechts een selecte groep dit kan doen. Dit is het verschil tussen permissionless en permissioned (paragraaf 9.3). In paragraaf 9.4 wordt verder onderscheid gemaakt tussen publieke, private en consortium blockchains. Dezelfde paragraaf wordt afgesloten met een overzicht van de verschillende typen blockchains, gebaseerd op de onderscheidingen in permissionless, permissioned, publiek, privaat en consortium. In paragraaf 9.5 wordt een samenvatting gemaakt van het hoofdstuk en worden de gebruikte termen en bronnen genoemd.

9.2 Governance

Blockchains worden vanuit verschillende redenen opgezet en kunnen van daaruit een eigen governance aannemen. ***Governance*** wordt gedefinieerd door Peter Weill als het raamwerk van besluitrechten en verantwoordelijkheden om gewenst gedrag te stimuleren (2004, p. 3). Hieronder vallen de volgende drie belangrijke elementen:

1. Rechten op besluitvorming.
2. Accountability.
3. Stimulansen.

9.2.1 Rechten op besluitvorming

Onder de rechten op besluitvorming vallen het recht om besluitvoorstellen in te dienen, uit te voeren en te monitoren. Deze rechten kunnen zowel centraal als decentraal worden ingericht. (Beck & Müller-Block, pp. 10-11). Met andere woorden, is de macht op besluitvorming geconcentreerd binnen één partij, een kleine groep partijen of is het verspreid over een volledig gedecentraliseerd netwerk? De vraag over hoe gedecentraliseerd je deze rechten wil inrichten, heeft impact op de keuze tussen een publieke, private of consortium blockchain.

9.2.2 Accountability

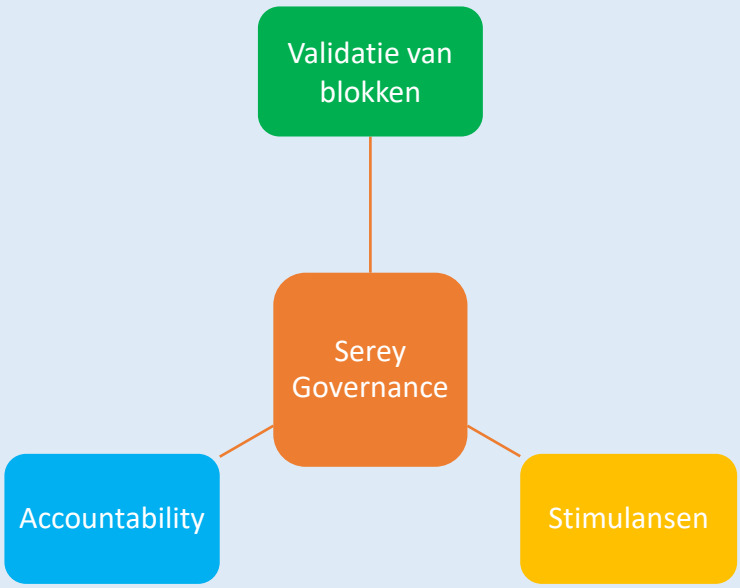
Accountability is gelinkt aan het recht om besluiten en gedragingen te mogen monitoren en op basis hiervan aangesproken te kunnen worden op je verantwoordelijkheden. Accountability wordt uitgeoefend door middel van contracten en gedragsprotocollen die bijvoorbeeld in blockchainsystemen worden vastgelegd. (Beck & Müller-Bloch, 2018, p. 11)

9.2.3 Stimulansen

Deelnemers aan een blockchain kunnen worden aangemoedigd om deel te nemen of zelfs de blockchain te helpen onderhouden door middel van monetaire en non-monetaire stimulansen. Een voorbeeld van een non-monetaire stimulans is het verkrijgen van privileges bij het vertonen van goed gedrag. Andere voorbeelden zijn dat je bij goed gedrag kunt genieten van een grotere zichtbaarheid binnen het systeem en dat je reputatie omhoog gaat. Een blockchain met een goed ontwikkelde structuur van stimulansen moedigt mensen aan om gebruik te maken van de blockchain en zich zo te gedragen dat hun acties in lijn zijn met de doelen van het systeem. (Beck & Müller-Bloch, 2018, pp. 11-12)

Intermezzo: Hoe de governance van Serey eruitziet

Serey.io is een social media blockchainplatform dat afgeleid is van Steemit. Het is het eerste blockchainproject in Cambodja en heeft als ambitie om Cambodjanen te stimuleren om meer te schrijven. Serey gelooft dat schrijven één van de beste manieren is om je intellectueel te ontwikkelen. Door te schrijven, word je gedwongen om te reflecteren op je eigen denken en cultiveer je je verbeeldingskracht. Daarnaast slaat Serey net als Steemit alle inhoud van een post op op de blockchain, waardoor het onmogelijk is om de inhoud te censureren. Het is hiermee ook een instrument om vrijheid van meningsuiting te bevorderen – iets wat in veel landen op de wereld nog niet geaccepteerd wordt. Het woord "Serey" betekent in het Cambodjaans dan ook toepasselijk "vrijheid".



Afbeelding 90: De aspecten van de governance bij Serey.

De governance van Serey draait om democratische participatie. Het bevat de volgende drie aspecten:

1. *Het recht om de Serey blockchain te onderhouden.* Iedereen die de blockchain draait, ook wel witnesses genoemd, zijn democratisch gekozen door de community om nieuwe posts toe te voegen aan de blockchain.
2. *Deelnemers aan de blockchain worden accountable gesteld voor hun gedragingen*. Dit aspect is in lijn met punt 3. Gebruikers die slechte posts plaatsen, kunnen worden gedownvote. Downvotes maken de post minder zichtbaar en zorgen ervoor dat de post ook minder monetaire beloningen ontvangt. De beloningen vinden plaats in Serey coins.

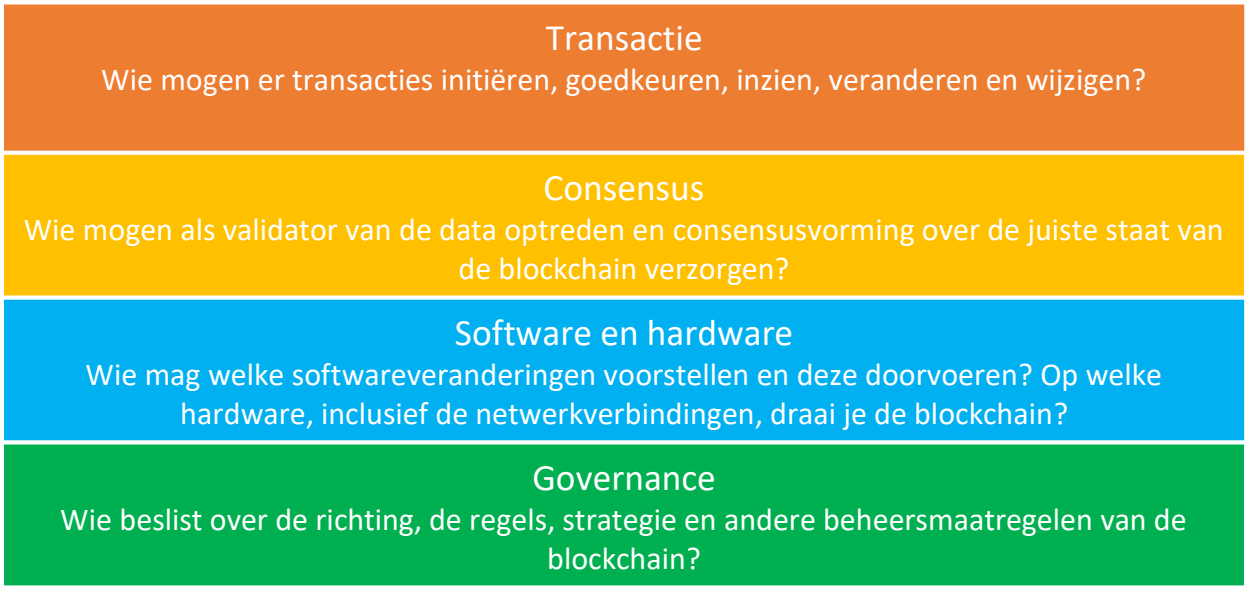
3. *Systeem van stimulansen*. Gebruikers worden gestimuleerd om posts te plaatsen die de community waardevol acht, omdat zulke posts meer upvotes krijgen. Upvotes leiden tot zowel monetaire als non-monetaire beloningen. Posts met meer upvotes krijgen meer rewards in Serey coins. Daarnaast zorgen upvotes ervoor dat de reputatiescore van de gebruiker omhooggaat en de posts zichtbaarder worden. Tot slot hebben de stemmen van gebruikers met meer Serey coins ook meer gewicht. Een stem van iemand met 1.000 Serey coins heeft meer impact dan een stem van iemand met slechts 1 Serey coin.

Afbeelding 91: Serey logo.

Het governancesysteem stimuleert gebruikers ook om op een beschaafde wijze met elkaar in discussies te treden. Trollen wordt ontmoedigd, omdat ze kunnen worden gedownvote. Door de downvotes worden trollen minder zichtbaar en krijgen ze een lagere reputatiescore die voor iedereen zichtbaar is.

9.3 Wie mag toetreden met welke rol?

Een blockchain hoeft niet altijd toegankelijk te zijn voor iedereen. Een blockchain kan bepaalde regels hebben, zodat alleen mensen die voldoen aan bepaalde criteria mogen deelnemen. Deze deelnemers kunnen bepaalde rollen vervullen die grofweg te verdelen zijn in de volgende vier aspecten: transactie, consensus, software en hardware en governance.



Afbeelding 92: De vier aspecten waaraan je kunt deelnemen binnen een blockchain.

9.3.1 Rollen

Je kunt uit elk aspect bepaalde bevoegdheden nemen en deze combineren tot een rol. Je kunt bijvoorbeeld een rol maken waarin iemand transacties kan inzien, kan meedoen met consensusvorming en software updates kan voorstellen.

9.3.2 Permissionless

Eén kernonderscheid dat wordt gemaakt tussen blockchains vindt plaats op het niveau van consensus. Als een blockchain iedereen toestaat om deel te nemen aan het valideren van data en consensusvorming, wordt er gesproken van een ***permissionless blockchain***. Dergelijke blockchains zijn van nature open. Voorbeelden van een permissionless blockchain zijn Bitcoin en Ethereum. Iedereen mag een full node draaien, waarmee alle transacties kunnen worden gevalideerd en iedereen ook mag deelnemen aan het proces om nieuwe blokken te produceren en toe te voegen aan de blockchain. De enige restrictie is dat je wel moet beschikken over hardware die geschikt is om de blockchain op te draaien en, in het geval van Proof-of-Work, moet je voldoende computerkracht hebben, zodat je daadwerkelijk geldige blokken kunt

produceren. Dit is echter geen restrictie op wie de persoon zelf is. Iedereen – het maakt niet uit hoe oud je bent, waar je vandaan komt, waar je woont, wat je status in de samenleving is of welk geslacht je hebt – mag deelnemen aan consensus. Het is belangrijk om hierbij te beseffen dat we het over consensusvorming op netwerkniveau bedoelen. Het is namelijk nog steeds mogelijk om bijvoorbeeld een smart contract of dApp op Ethereum te ontwikkelen waarin bepaalde permissies zijn vastgelegd over wie wel of niet gebruik mogen maken van het smart contract of de dApp.

Als iedereen een full node mag draaien, kan iedereen ook potentieel alle data in de blockchain inzien. Het afschermen van data dient dan te gebeuren met anonimiteitstechnologieën als bijvoorbeeld Zero-Knowledge Proofs.[108]

9.3.3 Permissioned

Bij een ***permissioned blockchain***, daarentegen, mag er slechts een geselecteerd groepje deelnemers data in een blockchain helpen valideren en op die manier bijdragen aan consensusvorming. Er is een autoriteit die eerst toestemming moet verlenen of je als validator mag fungeren. Met andere woorden, niet iedereen mag zomaar een node zijn op het netwerk die de blockchain helpt onderhouden. In een permissioned blockchain zijn alle validators dus bekend bij de autoriteit. Een permissioned blockchain vertrouwt dus niet op volledige decentralisatie waarbij iedereen kan deelnemen in consensusvorming. Dergelijke blockchains zijn van nature meer gesloten en vereisen vaak dat de validator zijn identiteit bekendmaakt aan zij die beslissingen mogen maken op governanceniveau.

9.3.4 Redenen om te kiezen voor permissionless of permissioned

Er zijn verschillende redenen waarom je zou willen kiezen voor een permissionless over een permissioned blockchain en vice versa.

In de eerste plaats is het makkelijker om bij permissionless meerdere bevoegdheden te combineren. Bij een permissioned blockchain is de kans groter dat in lijn met een bestaande organisatiegraad de bevoegdheden meer worden gesplitst. Je kan het initiëren van een transactie bij een permissioned blockchain bijvoorbeeld scheiden van het inzien van de transactie, of iemand zelfs de bevoegdheid geven om de transactie achteraf te corrigeren of te verwijderen. Het gevolg van een subtielere rolverdeling kan leiden tot

[108] Zero-Knowledge Proofs worden behandeld in hoofdstuk 5.

performanceoptimalisatie van de blockchain. Zo kan een kleiner netwerk van validators en meer centrale controle van de governance meer transacties per seconde verwerken en kan er sneller strategische besluiten worden genomen. Aan de andere kant kan het vertrouwen in een gedecentraliseerder systeem ook de kans bieden om bevoegdheden verder te decentraliseren, zodat er minder complianceprocedures als interne controles nodig zijn.

Een tweede verschil is dat je identiteitsbeheer centraler zet in een permissioned blockchain. Rollen en bevoegdheden en voorwaarden om deze rollen te verkrijgen, kunnen worden opgezet, zoals bedrijven dat kennen bij huidige ERP-systemen. Er kan hierbij ook geëxperimenteerd worden met nieuwe efficiëntere consensusmechanismen. Zo kun je bijvoorbeeld besluiten om de groep validators klein te houden en afspreken dat slechts 5 van de 7 validators een blok moeten goedkeuren. Bijkomend kun je de regel ook zo vastleggen dat er van deze 5 altijd een specifieke subgroep van 3 is die toestemming moeten geven voor elke transactie. Een andere eis kan zijn dat de groep validators altijd over de nieuwste en snelste hardware moet beschikken.

Een derde verschil is dat je bij een permissioned blockchain vertrouwen verschuift van een gedecentraliseerd systeem naar de mensen die je hebt geautoriseerd deel te mogen nemen. In lijn hiermee kun je besluiten de transparantie van gegevens ook meer af te schermen van andere gebruikers, omdat je als bedrijf niet alles wil of kunt delen. Het gevolg van een minder gedecentraliseerde opzet is dat het systeem gevoeliger kan zijn voor fouten, fraude, spam en distributed-denial-of-service (DDoS) aanvallen.

Een vierde noemenswaardig verschil tussen een permissionless en permissioned blockchain is het mogelijk gebruik van ***cryptotokens*** binnen de cryptoeconomie.[109] Om deelnemers te stimuleren samen te werken, kunnen deelnemers een beloning verdienen in bijvoorbeeld monetaire tokens, meer zichtbaarheid of meer reputatie. Permissionless blockchains maken veelal gebruik van cryptotokens om te kunnen functioneren. Bij permissioned netwerken is dit niet altijd nodig, omdat de participanten als onderdeel van systeembeleid op andere manieren kunnen worden gemotiveerd het juiste gedrag te vertonen. Als het permissioned netwerk bijvoorbeeld dat van een bedrijf is, kun je het gedrag van deelnemers sturen met instrumenten als beloningsstructuren, kansen op promotie of verbetering van secundaire arbeidsvoorwaarden.

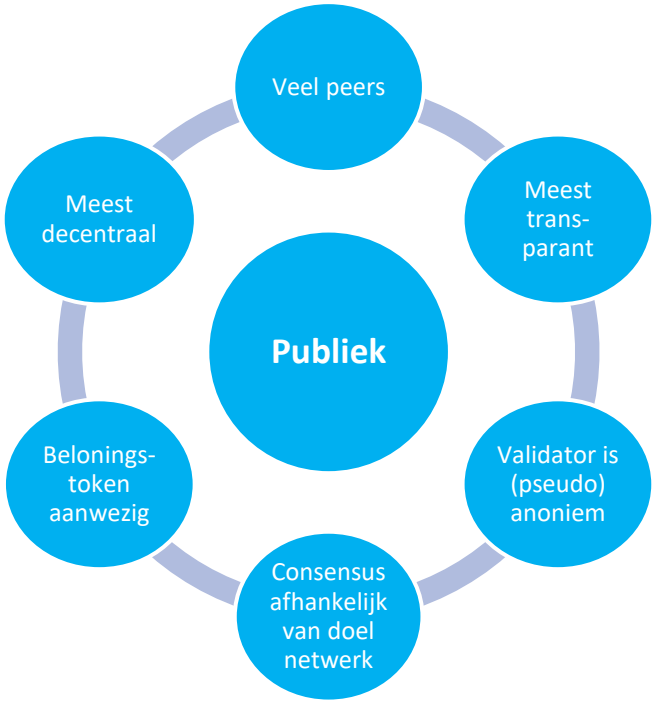
[109] Cryptoeconomie komt uitgebreider aan bod in hoofdstuk 10.

9.4 Publiek, privaat en consortium blockchains

Naast het onderscheid tussen permissionless en permissioned is er ook een onderscheid tussen publieke, private en consortium blockchains. Dit onderscheid is gebaseerd op de vraag of iedereen mag deelnemen aan een blockchain of niet.

9.4.1 Publieke blockchain

Als iedereen mag deelnemen aan een blockchain, in welke rol dan ook, dan wordt er gesproken over een ***publieke blockchain***. Een kenmerk van publieke blockchains is dat het niet van belang is wie er data schrijft naar de blockchain, wie er data leest van de blockchain en wie de blockchain mogen onderhouden. Dat laatste zorgt ervoor dat de meeste publieke blockchains ook permissionless zijn. Dergelijke blockchains zijn door de lage drempel om deel te nemen aan het netwerk het meest gedecentraliseerd.



Afbeelding 93: Aspecten van een publieke blockchain.

Bij publieke blockchains is er een sterk vertrouwen in decentralisatie en minder vertrouwen in een autoriteit die de governance van een blockchain op zich neemt. Het systeem zelf dwingt vertrouwen af door middel van overeengekomen protocollen. In het verlengde hiervan geldt dat als het niet belangrijk is om te weten wie er deelneemt aan het netwerk, je ze net zo goed (pseudo)anonimiteit kunt verlenen binnen de blockchain. Een publieke

blockchain, waar iedereen gelijk wordt behandeld, gebruik je vooral als je een groep gelijkgestemden met elkaar samen wil laten werken. De samenwerking wordt hierin gewaarborgd door het consensusmechanisme. Een blockchain waarbij er geen centrale partij aanwezig is om te bepalen wie mogen deelnemen aan het netwerk wordt ook wel een ***open blockchain*** genoemd. De deelnemers bepalen de werking van de blockchain in lijn met groepsmotieven als openheid, neutraliteit en vrijheid. Binnen de publieke blockchain kan iedereen ook meebeslissen over alle governance vraagstukken. Daarnaast zijn dergelijke blockchains ook meer gericht om innovaties te stimuleren, zonder daarbij de belangen van één partij of organisatie in ogenschouw te nemen. Veel van de publieke blockchains zijn vanwege hun innovatiegedreven karakter vaak open source. Om iedereen te stimuleren om deel te nemen aan het netwerk en goed gedrag te vertonen, die in overeenstemming is met de doelen van het systeem, bevat een publieke blockchain vaak ook een beloningstoken. Bij Bitcoin zijn dit de nieuw gecreëerde Bitcoins en de transactiefees die aan mijners worden uitgekeerd nadat zij een geldige blok hebben geproduceerd met de computerkracht die ze leveren aan het netwerk.

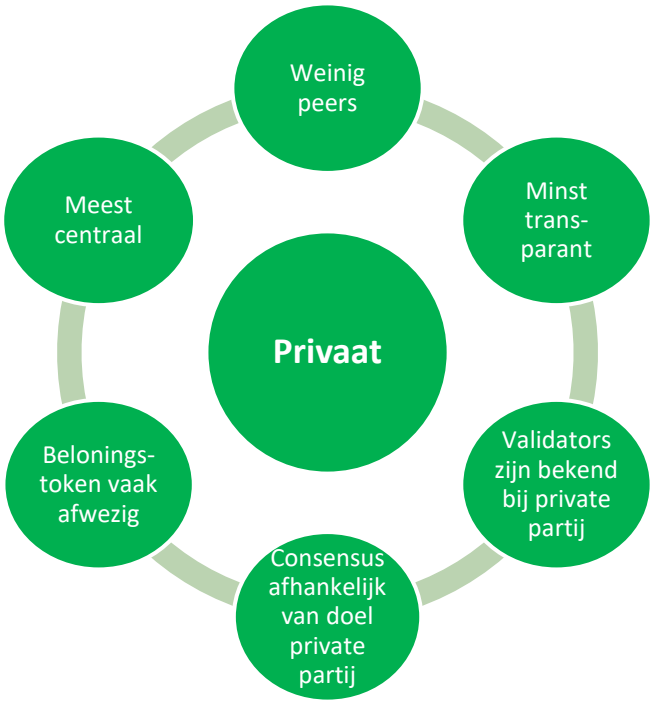
Publieke blockchains proberen zoveel mogelijk tussenpartijen buitenspel te zetten. Veel tussenpartijen, zoals een kadaster of notaris, opteren eerder voor private blockchaininitiatieven waarin zij een rol als tussenpartij kunnen innemen. Daarnaast is een publieke blockchain bij veel bedrijven niet altijd wenselijk, zeker niet in een meer gereguleerde omgeving waarin er onder andere wordt verwacht dat ze de identiteit van alle partijen die data schrijven naar de blockchain kennen.

9.4.2 Private blockchain

Als je niet vertrouwt dat de blockchain software gedragen kan worden door een decentraal netwerk van (pseudo)anonieme gelijkgestemden, zul je een deel van je vertrouwen bij de deelnemers willen leggen die je zelf kent en zelf hebt uitgekozen om deel te nemen. Je zult dus invloed uit willen oefenen op wie mag deelnemen in vraagstukken rondom governance, software en hardware, consensus en transacties. Een blockchain waarbij een centrale partij invloed kan uitoefenen op het eigen blockchainnetwerk wordt een ***private blockchain*** genoemd. Deze centrale partij heeft vaak een aantal nodes opgezet die hij zelf beheert en die samen met elkaar de blockchain draaiende houden. In het extreemste geval heeft de partij één enkele node waarop de blockchain draait. Dit geeft echter geen voordelen ten opzichte van een gecentraliseerd netwerk die ook een SPOF is.

Er wordt ook weleens gesproken over een ***gesloten blockchain*** als deze centrale partij beslist wie wel en wie niet mag deelnemen. Een open versus gesloten blockchain gaat enkel over deelname en is het gevolg van het hebben van een publiek of privaat systeem. De centrale partij kan een bedrijf zijn dat een eigen blockchain ontwikkelt. Dit bedrijf zal zodoende niet alleen de toetreding, maar ook het werk dat deelnemers in het systeem verrichten, willen beheersen. Voor verdere beheersing van de blockchain stelt het bedrijf regels op omtrent:

1. Waar een deelnemer aan moet voldoen.
2. Welke rollen je nodig hebt om de blockchain technisch te onderhouden.
3. Welke rollen je nodig hebt om transacties te verrichten, in te zien en aan te passen.
4. Welke rollen je nodig hebt om het gehele consensusmechanisme te laten werken.



Afbeelding 94: Aspecten van een private blockchain.

De centrale partij, bedrijfseigenaren of het managementteam, nodigt specifieke deelnemers uit en deelt ze een specifieke rol toe. Deze deelnemers zijn onder andere eigen werknemers en de rollen zijn gemaakt in lijn met de bestaande management control systemen. Als je weet wie iemand is ga je ervan uit dat ze zich niet misdragen. Je controleert immers met je management control systeem ook wat ze doen waardoor misdragingen kunnen worden opgevolgd met maatregelen. Zodoende ondersteun je ook de wetgever en auditors. Daarnaast kan een centraal geleide organisatie sneller beslissingen nemen, omdat het met

minder partijen overleg heeft. Deze beslissingen kunnen gaan over de vier eerder genoemde aspecten: governance, software en hardware, consensus en transacties.

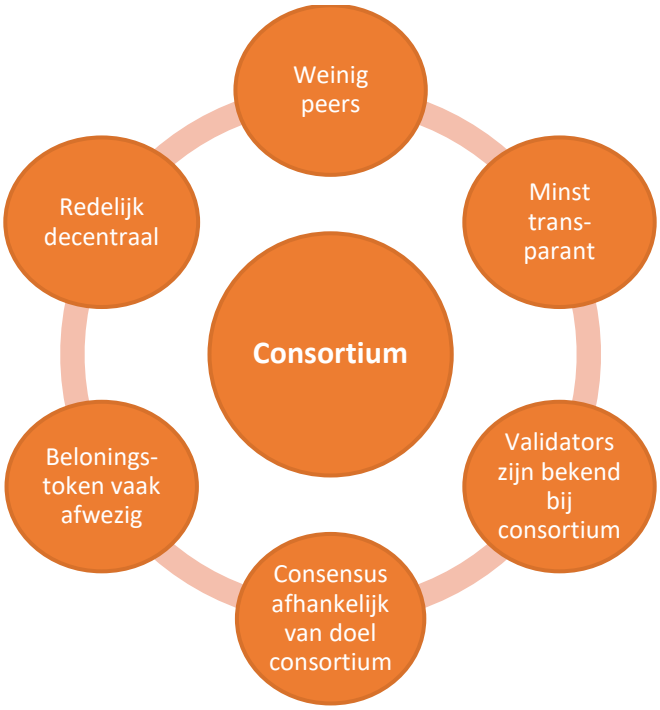
Denk bij een privaat systeem aan een intranet waarin je de nodes, data en de source code controleert. Je kent iedereen en alle transacties zijn in te zien als dit nodig is, maar je schermt mensen ook af van het verifiëren of zien van bepaalde transacties. Dat is handig wanneer de gegevens bedrijfsgevoelig zijn. In een publiek systeem is het ook mogelijk om dit technisch in te bouwen, maar dit blijkt in de praktijk vooralsnog lastig en duur te zijn.[110]

9.4.3 Consortium blockchain

Een tussenvorm van een publieke en een private blockchain is er één waarin meerdere organisaties samenwerken om een blockchain op te zetten. Dit wordt een ***consortium blockchain*** of ***federated blockchain*** genoemd. De consensus wordt hierbij beheerd door een selectie van nodes. Een voorbeeld van een consortium is 15 financiële instellingen die ieder een node draait. Van deze 15 nodes moeten er dan minimaal 10 een blok goedkeuren. (Buterin, 2015) Dit betreft dus een gesloten blockchain waar het consortium voor het gehele netwerk besluit wie met welke rol mogen deelnemen, welke transacties openlijk te zien zijn, welke transacties afgeschermd blijven en hoe de governance dient te worden ingericht. Het consortium kan overigens wel besluiten om het recht om de blockchain te lezen publiekelijk te maken.

Libra, de blockchain die onder andere is ontwikkeld door Facebook om de Libra coin te faciliteren, is een voorbeeld van een consortium blockchain. Naast Facebook zal deze onder andere worden beheerd door een netwerk van andere partijen zoals Uber, Xapo, Spotify, Coinbase en Vodafone. Doordat de beheerstructuur van blockchain niet in handen is van slechts één partij, maar in handen van meerdere voor elkaar bekende partijen is het gecentraliseerder dan een publieke blockchain en meer gedecentraliseerd dan een private blockchain.

[110] Ernst & Young (2019) heeft onderzoek gedaan naar de transactiekosten binnen een private blockchain en een publieke blockchain die gebruik maakt van Zero-Knowledge Proofs. Zij concluderen dat de transactiekosten van Zero-Knowledge Proofs bij publieke blockchains op korte termijn goedkoper zullen worden dan privacy transacties op een private blockchain. (p. 14)



Afbeelding 95: Aspecten van een consortium blockchain.

Partijen kunnen verschillende belangen hebben binnen een consortium blockchain. Een consortium supply chain blockchain kan bijvoorbeeld bestaan uit transporteurs, overheden en financiële instellingen die decentraal samenwerken. In een consortium kun je daarnaast je eigen transacties afschermen van andere deelnemers. Dit is bijvoorbeeld handig in het communiceren van bedrijfsgeheimen of wanneer twee klanten een prijsafspraak maken via de blockchain. Volledige transparantie van de gegevens, zoals we dat kennen van publieke blockchains en anonimiteit van deelnemers, staat meestal niet op de agenda. Anderzijds zul je wel publiekelijk inzicht willen geven in bepaalde transacties om de integriteit van het systeem aan te tonen en om bepaalde data te overleggen aan bijvoorbeeld auditors.

Intermezzo: Facebooks cryptomunt, de Libra

Na zich jarenlang afzijdig te hebben gehouden van de cryptowereld wil een consortium van grote ondernemingen en social impact organisaties, onder leiding van Facebook, binnenkort hun entree maken. Het originele plan was om de toekomstige cryptomunt, de Libra, te introduceren in de eerste helft van 2020. De Libra White Paper (2019) beschrijft de Libra als een cryptomunt met lage volatiliteit die zal draaien op de Libra blockchain.

Doel van Libra

Het doel is om van Libra een stabiele munt te maken die is gebouwd op een goed beveiligde en stabiele open source blockchain. Om de munt stabiel te houden, zal hij volledig gedekt worden door Libra-reserves – een mandje van reële activa, zoals bankdeposito's en kortlopende overheidsobligaties in de volgende valuta: USD, GBP, EUR en JPY. In dat opzicht is Libra vergelijkbaar met de Special Drawing Rights (SDRs) die door het Internationaal Monetair Fonds is ingevoerd in 1969 om andere reserves van deelnemende landen aan te vullen. SDRs zijn ook gekoppeld aan een mandje van verschillende valuta, namelijk de USD, EUR, CNY, JPY en GBP.

De reden om de Libra te koppelen aan een collectie van verscheidene activa is om de koersschommelingen minder afhankelijk te maken van één activa. Deze activa zullen worden gehouden over een globaal netwerk van beheerders die alleen een full node mogen draaien. Hierdoor zal Libra genieten van de voordelen van stabiele traditionele overheidsgeld en de voordelen van cryptogeld. Zo zal Libra op een veilige manier tegen lage transactiekosten vrijwel onmiddellijk kunnen worden overgemaakt naar zowel binnen- als buitenland.

De hoop is dat financiële diensten beter en goedkoper worden en op die manier toegankelijker zijn voor iedereen.

Overwegingen voor de inrichting van de Libra blockchain

De Libra blockchain is ontwikkeld met de volgende drie vereisten in het achterhoofd:

1. Het moet op te schalen zijn naar miljarden accounts met een hoge transactieverwerking en snelheid.
2. De fondsen en financiële data moeten sterk beveiligd zijn.
3. Het moet dusdanig flexibel zijn dat het toekomstige innovaties aan het netwerk en de financiële dienstverleningen mogelijk maakt.

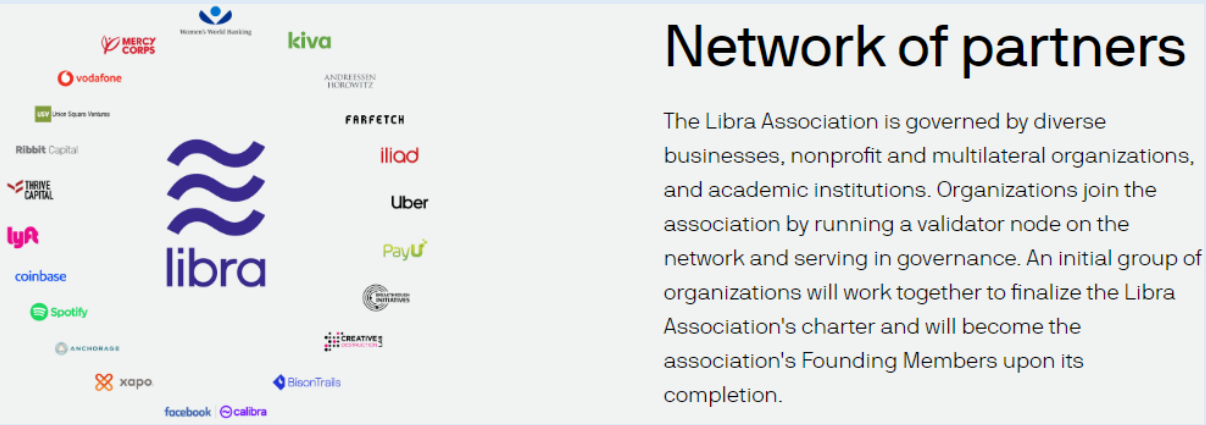
Hiervoor is er gekozen om:

1. Een nieuwe programmeertaal, genaamd Move, te introduceren. Het doel van Move is om het ontwikkelen van smart contracts en transactielogica op de blockchain veiliger te maken, dus met minder risico's dat de softwareontwikkelaar fouten in de code schrijft die leiden tot onvoorziene bugs en ongewenst gedrag van de software.
2. Daarnaast is er gekozen voor een Byzantine Fault Tolerance consensusprotocol dat geschikt is voor een hoge transactieverwerking, weinig netwerkvertraging heeft en energie efficiënter is dan het Proof-of-Work consensusmechanisme van bijvoorbeeld Bitcoin. Het consensusprotocol is de set aan regels die bepaalt hoe er binnen een blockchainnetwerk consensus wordt bereikt over de juiste staat van de blockchain en wat de voorwaarden zijn voor een transactie om te worden goedgekeurd.
3. Verder is de blockchain volgens de White Paper pseudoanoniem en biedt het gebruikers de mogelijkheid om meerdere adressen aan te maken die niet gelinkt worden aan hun wereldse identiteiten.

De Libra Association

De Libra Association zal bestaan uit een consortium van founding members, bestaande uit onder andere Uber, Xapo, Spotify, Coinbase en Vodafone. Om in het consortium te komen, hebben zij $10 miljoen USD moeten bijleggen voor de Libra Reserve. Daarnaast zitten er ook social impact organisaties bij als Women's World Banking en Kiva. De deelnemers van het consortium zullen Libra Investment Token (LIT) krijgen, waarmee zij kunnen deelnemen in de governance van de Libra Association. Het is ook mogelijk dat ze in LIT worden beloond voor het onderhoud van de blockchain en voor het valideren van transacties.

De Libra Association zal de Libra Reserve managen ten gunste van de stabiliteit en groei van de Libra-economie. De rente die wordt verkregen op de Libra Reserve zal worden gebruikt om de kosten te dekken. De Libra Association zal de enige partij zijn die nieuwe Libra kan creëren en vernietigen. Nieuwe Libra wordt gecreëerd wanneer geautoriseerde resellers Libra hebben gekocht van de Libra Association met fiatgeld om de nieuw uitgegeven Libra te dekken. Libra zal alleen worden vernietigd wanneer de geautoriseerde resellers hun Libra verkopen aan de Libra Association in ruil voor de onderliggende activa. De Libra Reserve ageert hierdoor als de 'buyer of last resort'.



Afbeelding 96: Libra consortium (Libra.org, 2019).

Het beleid van de Libra Association kan alleen worden gewijzigd als er een meerderheid is bereikt onder de deelnemers. Hoeveel consensus er moeten worden bereikt is nog onduidelijk. Ook is het onduidelijk hoeveel consensus er dient te worden bereikt om een transactie goed te keuren. Naar verwachting is net als bij de meeste andere Byzantine Fault Tolerance protocollen 67% consensus nodig voor de goedkeuring van transacties. Een ander doel van de Libra Association is om een standaard te ontwikkelen voor open digitale identiteiten. Dergelijke identiteiten zijn volgens de Libra Association een voorwaarde voor financiële inclusie.

Permissioned blockchain

Dat niet iedereen de blockchain kan draaien op hun eigen computer, betekent dat het een permissioned blockchain is. Echter, is het de bedoeling dat ze binnen 5 jaar de transitie inzetten naar een permissionless omgeving, waardoor iedereen ook een node kan draaien, om zo het netwerk te helpen onderhouden.

Calibra wallet

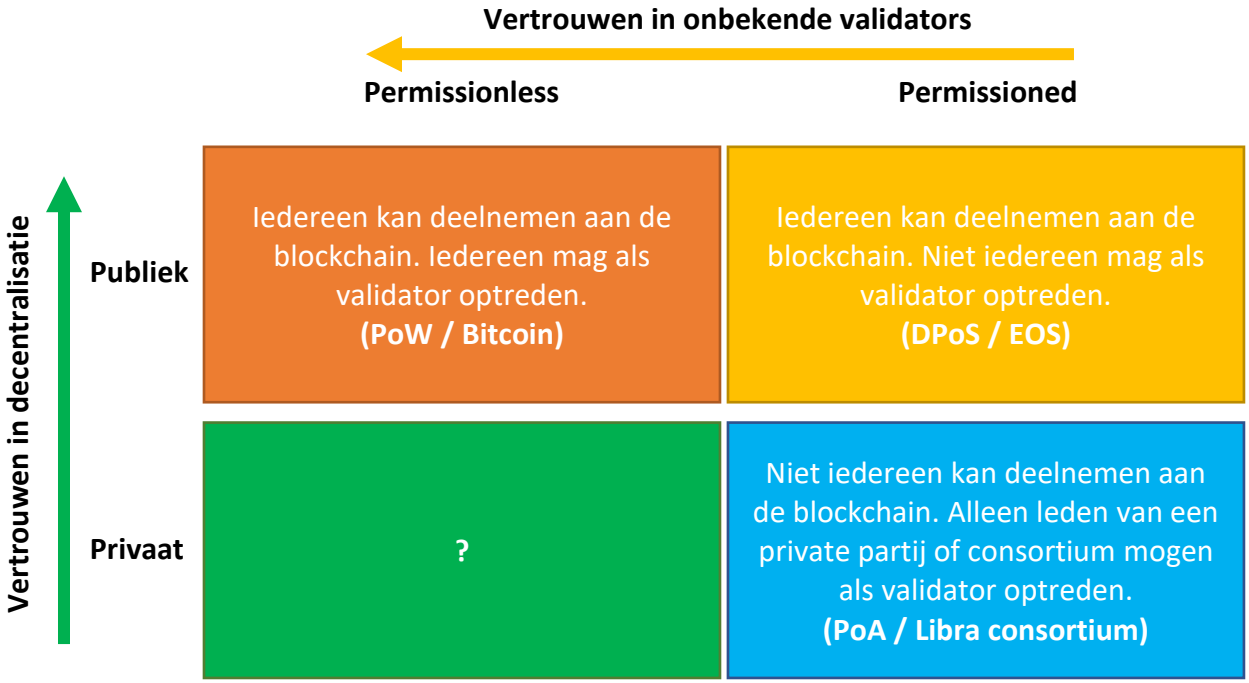
Libra zal worden geïmplementeerd in het ecosysteem van Facebook en dus ook in applicaties als Messenger, WhatsApp en Instagram. De wallet waarin Libra zal worden bewaard, heet de Calibra wallet.

Wat zal Libra tot gevolgen hebben?

Het is lastig te voorspellen wat de gevolgen van Libra zullen zijn voor de crypto- en financiële wereld, zeker ook omdat nog niet alle details en regelgeving omtrent Libra bekend zijn.

9.4.4 Overzicht van Permissionless vs Permissioned vs Publiek vs Privaat

Het is belangrijk om te beseffen dat een blockchain verschillende vormen kan aannemen. Uit alle eerder besproken verschillen tussen permissionless, permissioned, publieke en private blockchains komt naar voren dat bouwstenen van blockchain op andere manieren kunnen worden gebruikt of kunnen worden aangepast, afhankelijk van de doelen die het samenwerkingsverband nastreeft.[111] Het staat enig bedrijf vrij om te experimenteren met de techniek en daar de voor- en nadelen van te ondervinden. De volgende tabel vat de verschillende blockchains, zoals we die eerder hebben onderscheiden van elkaar, samen.



Afbeelding 97: Een overzicht van verschillende typen blockchains, uitgedrukt in permissionless, permissioned, privaat en publiek.

Keuzes tussen de verschillende typen blockchains raken de beheersing van de organisatie. Hoe meer vertrouwen er is in het decentrale karakter van de blockchain, hoe makkelijker het is om deel te nemen. Hoe meer vertrouwen er is dat validators als onbekenden mogen deelnemen aan consensusvorming, hoe transparanter het systeem. Iedereen kan dan immers een full node draaien en alle data helpen valideren. Dergelijke systemen hebben door het decentrale karakter vaak veel validators en kampen mede daardoor nog met

[111] De bouwstenen van blockchain zijn de volgende eigenschappen: gedecentraliseerd netwerk, geen Single Point of Failure, peer-to-peer, onwijzigbaarheid van transacties, cryptografie en consensusmechanisme.

schaalbaarheidsproblemen. Ook zijn dergelijke blockchains relatief gezien duurder dan de minder gedecentraliseerde en permissioned varianten. Op de lange termijn, echter, wordt verwacht dat een permissionless publieke blockchain steeds efficiënter wordt, zodat meer professionele partijen zullen opteren voor dergelijke blockchains. Deze blockchains moeten dan wel zodanig worden ingericht dat de rollen die deelnemers kunnen innemen voor bedrijfsapplicaties goed afgebakend zijn en voldoen aan bedrijfsvereisten. Zo kunnen bedrijven op permissionless publieke blockchains bijvoorbeeld gegevens anonimiseren door middel van Zero-Knowledge Proofs en kunnen deelnemers op applicatieniveau worden gevraagd om hun identiteit te tonen.

Internet of Blockchains

Het ***internet of blockchains*** is een netwerk van verschillende blockchains die onderling communiceren en data uitwisselen. Dit wordt ook wel ***interoperabiliteit*** genoemd. Private blockchains vragen bijna automatisch om meerdere blockchains die data met elkaar uitwisselen. Bijvoorbeeld eentje voor je identiteit, eentje voor je bezittingen en eentje voor je social media. Er zullen smart contracts en interfaces komen waarmee gegevens uitgewisseld kunnen worden tussen verschillende blockchains.

9.5 Samenvatting, begrippen en bronnen

Samenvatting

Een blockchain heeft zoals elk samenwerkingsverband een manier nodig om te worden bestuurd. De besturing wordt ook wel blockchain governance genoemd. Dit bestaat uit:

1. Rechten op besluitvorming.
2. Accountability.
3. Stimulansen.

De invulling van deze elementen hangt samen met de doelen die het verband nastreeft.

Om deel te nemen aan een blockchain heb je toegang nodig. Het kan zijn dat centrale autoriteiten je eerst toegang moeten verlenen. Dit heet een private blockchain. Als de toegang voor iedereen is geregeld, heet het een publieke blockchain.

Als je eenmaal toegang hebt, ben je als gebruiker in staat om verschillende rollen aan te nemen die te verdelen zijn in de aspecten; transactie, consensus, software en hardware, en governance. Hierbij is de rol tot het onderhouden van het consensusmechanisme belangrijk. Als iedereen dit mag, is het een permissionless blockchain. Als de rol echter voor een selecte groep is weggelegd, spreken we over een permissioned blockchain.

Het al dan niet willen beslissen over de toegang of de rol door een organisatie leidt tot vier verschillen tussen een permissionless en permissioned blockchain. Ten eerste kan een bedrijf door de rollen op te splitsen de onderliggende organisatiestructuur min of meer in stand houden. Ten tweede kun je het beheer van identiteiten binnen een eigen blockchain versterken als je alle rollen en personen aan wie je het geeft in de hand houdt. Ten derde verleg je het vertrouwen niet naar het systeem, maar beheers je je organisatie naast de blockchain ook op andere manieren zoals met personeelsmanagement en afdelingsmanagers. Dit is waarom je, ten vierde, binnen een permissionless systeem vaak gebruik maakt van cryptotokens om samenwerking te stimuleren.

Dit laatste is ook een reden dat er bij publieke blockchains meer vertrouwen is in decentralisatie en het systeem, en minder in een autoriteit die de governance van een blockchain op zich neemt. Andere redenen zijn onder andere de gebruikte consensusprotocollen, het open source karakter en de transparantie van besluitvorming. Dit leidt ertoe dat je meer vertrouwen hebt in het toetreden en deelnemen van onbekenden. Het vertrouwen ligt immers in het systeem en niet in de gebruiker.

Opmerkingen die je nu kunt uitleggen

- In een publiek netwerk wordt er in beginsel meer vertrouwd op het blockchainsysteem zelf.
- In een privaat netwerk leidt de behoefte aan centrale controle en het kennen van de eigen deelnemers tot een situatie waarin er minder op blockchain hoeft te worden gesteund en meer op het eigen management control systeem.
- Een bedrijf dat geneigd is naar een private blockchain, zal in beginsel willen weten wie er in het blockchainsysteem zit en aan de hand daarvan eerder specifieke rollen toebedelen.
- Een groter aantal nodes helpt vertrouwen in het blockchainsysteem in de hand.
- Toetreding tot en rollen van deelnemers in een blockchain hangen samen met de anonimiteit van de deelnemers en het vertrouwen in de deelnemers.

Verklarende begrippenlijst

Accountability: De plicht om op basis van het vertoonde gedrag aangesproken te worden op verantwoordelijkheden.

Consortium blockchain: Een verband waarin meerdere organisaties een permissioned blockchain opzetten. Dit wordt ook wel een federated blockchain genoemd.

Cryptotoken: Een token op een blockchain dat een digitaal of fysiek bezit representeert.

Federated blockchain: Zie consortium blockchain.

Gesloten blockchain: Een blockchain waarbij een centrale partij bepaalt wie mogen deelnemen aan het netwerk.

Governance: Het raamwerk van besluitrechten en verantwoordelijkheden om gewenst gedrag te stimuleren.

Internet of blockchains: Een netwerk van blockchains die met elkaar communiceren en informatie delen.

Interoperabiliteit: Zie internet of blockchains.

Open blockchain: Een blockchain waarbij er geen centrale partij aanwezig is om te bepalen wie mogen deelnemen aan het netwerk.

Permissioned blockchain: Een systeem waarbij een autoriteit toestemming verleent wie op de blockchain mag valideren. De validators zijn hierbij bekend.

Permissionless blockchain: Een blockchain zonder autoriteit. Iedereen kan toetreden en de rol van validator vervullen. De validators hoeven hierbij niet bekend te zijn.

Private blockchain: Een blockchain waarbij een centrale partij invloed uitoefent op toetreders en rollen van het eigen blockchainnetwerk.

Publieke blockchain: Een blockchain waar het publiek, in plaats van een centrale partij, samen beslist over toetreders en rollen van het blockchainnetwerk.

Bronnen

Beck, R., & Müller-Bloch, C. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19(10), 1020-1034. Doi: 10.17705/1jais.00518

Buterin, V. (2015, 6 augustus). On Public and Private Blockchains. Geraadpleegd op 22 december 2019, van Ethereum website: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

ConsenSys (2018, 12 december). 5 Reasons Why Enterprise Ethereum Is so Much More Than a Distributed Ledger Technology. Geraadpleegd op 22 december 2019, van Consensys website: https://media.consensys.net/5-reasons-why-enterprise-ethereum-is-so-much-more-than-a-distributed-ledger-technology-c9a89db82cb5

Ernst & Young (2019). *Total cost of ownership for blockchain solutions*. Geraadpleegd van https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf

Libra Association Members. (2019). *An introduction to Libra* [White paper]. Geraadpleegd van https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive*, 3(1), 1-17.

Zhang, R., Xue, R., Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, 1(1), 1-35.

10. Cryptoeconomics en de relevantie van cryptografische tokens

"This Cambrian explosion of cryptoassets will precipitate one of the greatest reorganizations of wealth and transformations to the global economy in our history. This represents a second kick at the can – an opportunity to assure that everyone has the ability to benefit from the prosperity of the digital age.
To truly realize that promise, however, it's time we looked at cryptoassets not just as 'digital gold', but of digital everything."
- Alex Tapscott (2018)

10.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat tokens zijn en hoe ze zich verhouden tot cryptovaluta.
- Wat cryptoeconomics is en welke rol een token hierbinnen kan spelen.
- Wat het verschil is tussen tokens ten bate van de applicatie en tokens als bezit.
- Wat inwisselbare en niet-inwisselbare tokens zijn en hoe deze de cryptoeconomie ondersteunen.
- Hoe tokens kunnen worden ingezet voor fondsverwerving.

Inleiding

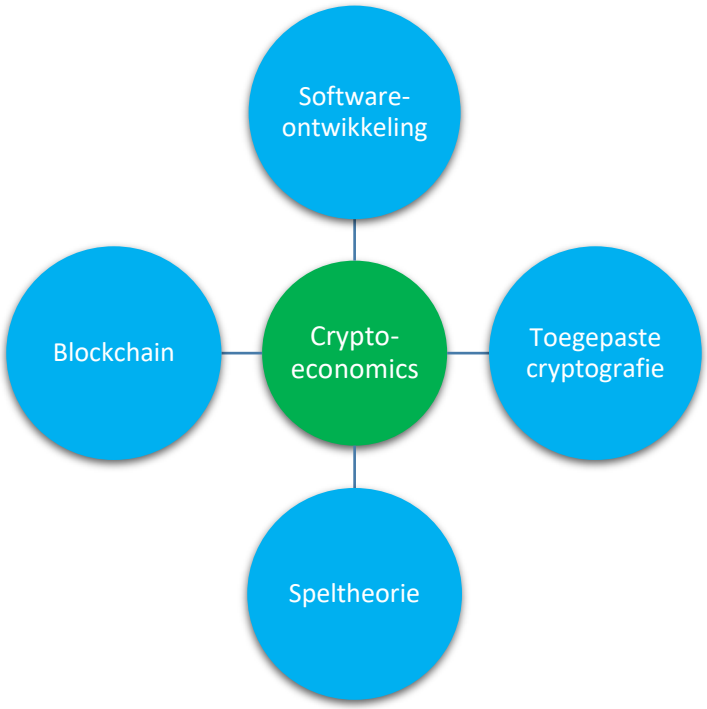
Eén van de grote vindingen van Satoshi Nakamoto is het combineren van reeds bestaande technologieën met een beloningssysteem dat een decentraal netwerk in de lucht houdt. Zoals eerder vermeld, wordt de beloning in Bitcoins uitgekeerd aan de mijner die een blok produceert.

Tokens in onze huidige samenleving zijn bekend als onder andere bonnen en munten – bijvoorbeeld spaarpunten, casinomunten en geschenkkaarten. Ook kennen we tokens in de IT die toegangsrechten verschaffen tot een netwerk om een taak te mogen verrichten of als representaties van rechten op onderliggende bezittingen. Een Bitcoin, wat je ook zou kunnen zien als een cryptografisch token, verschilt met de voorgaande genoemde tokens in de zin dat het waarde representeert. Cryptografische tokens kunnen voor velerlei redenen worden ingezet. Ze dienen in het blockchainlandschap vooral het Internet of Value.

Met cryptografische tokens zoals Bitcoin kun je betalen of sparen, maar je kunt er ook een stap verder mee gaan. Bitcoin kun je bijvoorbeeld verdienen door computerkracht te leveren om nieuwe blokken te produceren. Zodoende creëert het een economie waarbij verschillende deelnemers worden aangemoedigd om het netwerk te helpen beveiligen in ruil voor cryptovaluta. Het inzetten van cryptografische tokens om bepaald gedrag van participanten te stimuleren en verkeerd gedrag af te straffen door een consensusprotocol, is onderdeel van cryptoeconomics.

In dit hoofdstuk wordt in 10.2 eerst beschreven wat cryptoeconomics is. Vervolgens wordt in 10.3 behandeld hoe tokens in te delen zijn. Hierbij komen onder andere dApp-tokens en cryptovaluta naar voren, maar ook het verschil tussen inwisselbare en niet-inwisselbare tokens. Het hoofdstuk wordt in paragraaf 10.4 vervolgd met een overzicht van hoe tokens kunnen worden ingezet voor fondsverwerving door een Initial Coin Offering, Security Token Offering en Initial Exchange Offering. In 10.5 wordt een samenvatting gemaakt van het hoofdstuk en worden de gebruikte termen en bronnen genoemd.

10.2 Cryptoeconomics



Afbeelding 98: Multidisciplinaire aspecten van cryptoeconomics.

Cryptoeconomics is een nieuwe discipline die is opgekomen door de komst van blockchain. Het houdt zich bezig met de productie, consumptie en welvaartsoverdracht door middel van computernetwerken, cryptografie, speltheorie en softwareontwikkeling. De fundamenten van cryptoeconomics zijn dus sterk multidisciplinair. (Sultan et al., 2018) Deze computernetwerken kunnen worden gezien als systemen waarbinnen waarde kan worden uitgewisseld tussen verschillende personen. Wat als waarde wordt gedefinieerd, kan verschillen van persoon tot persoon en is volledig subjectief. Waarde kan bijvoorbeeld gerepresenteerd worden in een cryptotoken, een dienst of bepaalde informatie. De computernetwerken zijn ontworpen met bepaalde regels die als een soort wetten fungeren voor iedereen die deelneemt. Het eerste verschil met wetten, zoals we die kennen in natiestaten, is dat ze niet worden ontworpen door een overheid. Regels worden ontworpen door een private partij als het een private blockchain betreft. Bij een publieke blockchain worden de regels bepaald door een community die samen consensus bereikt over de regels. Een tweede verschil is dat er vertrouwen is dat de software de regels forceert, in plaats van de overheid.

Tijdens het ontwikkelen van de regels worden er bepaalde assumpties gemaakt over hoe deelnemers zich kunnen gedragen en misdragen binnen het netwerk. Het centrale idee achter cryptoeconomics binnen blockchain is dat er dan protocollen worden ontwikkeld die mensen stimuleren om zodanig deel te nemen aan het netwerk dat de waarde van het netwerk wordt gemaximaliseerd voor de deelnemers. Netwerkwaarde kan alleen worden gemaximaliseerd als het netwerk en de transacties die daarin plaatsvinden zelf ook beveiligd zijn. Om dit te bewerkstelligen wordt cryptografie toegepast voor beveiliging van transacties binnen het netwerk en worden er beloningen uitgekeerd aan deelnemers die het netwerk, bijvoorbeeld door mijnen of staking, helpen beveiligen. Zo wordt er bijvoorbeeld gebruikgemaakt van hash-functies, digitale handtekeningen, blokbeloningen, cryptotokens en consensusmechanismen. Het protocol dient aldus te leiden tot een aantal dingen als:

1. Deelnemers kunnen erop vertrouwen dat hun transacties daadwerkelijk worden uitgevoerd.
2. Transacties worden snel en onherroepelijk uitgevoerd.
3. Transacties zijn goedkoop.
4. Iedereen heeft toegang tot de broncode binnen een publieke blockchain.
5. Er is geen centrale autoriteit die het protocol en het netwerk controleert binnen een gedecentraliseerde blockchain. (Nguyen, 2018)

Als we kijken naar peer-to-peer filesharing programma's zoals Bittorent en Napster, dan zien we dat ze extra economische stimulansen missen die bijvoorbeeld de Bitcoin blockchain wel

biedt. Mensen die Bittorent en Napster gebruiken, bewaren bestanden op hun harde schijf die zij ter download beschikbaar stellen aan de rest van het netwerk, zonder dat zij ervoor worden beloond. Bij Bitcoin worden mijners gestimuleerd om het netwerk te helpen onderhouden en te beveiligen, doordat ze hiervoor een beloning in de vorm van waardevolle Bitcoins kunnen ontvangen. De achterliggende gedachte van een goed ingericht cryptoeconomisch systeem is dat het houdbaar en het liefst een zelforganiserend systeem wordt, zonder centrale partijen die mensen aansporen om op een bepaalde manier te ageren.

10.2.1 Speltheorie

Speltheorie is een formele studie naar besluitvorming waar verscheidene spelers keuzes moeten maken die potentieel het belang van andere spelers raken. Bij speltheorie gaat het erom dat je in een competitieve omgeving zoekt naar optimale besluiten.[112] Een cryptoeconomisch systeem dient zodanig te zijn ingericht dat deelnemers in hun keuzevrijheden altijd ervoor kiezen om goed gedrag te tonen, omdat dit tot meer profijt leidt dan slecht gedrag. Met andere woorden, het slechte gedrag dient zodanig zwaar te worden afgestraft dat een speler het niet waagt. Binnen het Proof-of-Work cryptoeconomisch systeem betekent dit bijvoorbeeld dat wanneer een mijner probeert een transactie te double-spenden in een malafide blok, zijn malafide blok niet zal worden geaccepteerd door het netwerk. Met andere woorden, zijn blok wordt een orphaned blok en hij krijgt geen beloning voor het werk dat hij heeft verricht. De mijner heeft voor niets zijn computerkracht geconcentreerd op het aanmaken van een malafide blok, terwijl hij wel elektriciteitskosten heeft betaalt voor de productie van het blok.

Centraal binnen cryptoeconomics is dus dat goed gedrag van deelnemers wordt beloond en slecht gedrag wordt afgestraft. Een manier om deelnemers te stimuleren op goed gedrag is door beloningen in cryptotokens.

[112] Speltheorie wordt ook wel gedefinieerd als een theorie die ervan uitgaat dat de mens rationeel – homo rationalis – is. Er wordt verondersteld dat hij altijd doelbewust en logisch ageert om zijn doelen zo dicht mogelijk te benaderen. (Bonanno, 2015, p. 2)

10.3 Indeling van blockchaintokens

Coins of tokens?
Wat is het verschil tussen coins en tokens? De initiële term was coin. Vandaar ook Initial Coin Offering. Deze coin was vooral bedoeld om weer te geven dat het een munt betreft als in 'valuta'. Sindsdien kwamen onder andere Ethereum op met ERC-20 tokens, waarop de term token in zwang raakte. Hoewel tokens niet per se zijn ontwikkeld als een valuta bieden ze wel deze, en andere, mogelijkheden. Hierdoor dekt de term token dus een bredere lading en is het passender binnen de huidige ontwikkelingen van blockchain.

Initieel was internet opgezet om onderling informatie uit te wisselen. Dit wordt ook wel een ***Internet of Information*** genoemd. Hierbinnen is het lastig om waarde op te slaan en te verplaatsen zonder een vertrouwde tussenpartij (Tapscott, 2016). De rol van de tussenpartij is voornamelijk om te kijken of waarde, bijvoorbeeld een euro, niet dubbel wordt uitgegeven (Satoshi, 2008, p. 2). Met de komst van blockchain kun je de nood tot tussenpartijen omzeilen en waarde direct peer-to-peer verhandelen.[113] Dit wordt ook wel het ***Internet of Value*** genoemd. Hiervoor wordt er gebruikgemaakt van cryptotokens. Een cryptotoken kan worden gecreëerd op een blockchain en ook een verhandelbare activa representeren. Soms worden tokens aangemaakt in een ICO of een STO om een project te kunnen financieren. Het proces van tokencreatie wordt ***tokenization*** genoemd. Door deze tokens te verhandelen, kun je het eigendom op de onderliggende activa overdragen.

Er zijn verschillende perspectieven van waaruit je naar cryptotokens kunt kijken. Gezien het veld zich nog flink ontwikkelt, is er momenteel nog geen eenduidige en universeel gehanteerde indeling van tokens. De volgende indeling is tweeledig en gericht op de toekomstige grote rol van tokens in een Internet of Value:

1. In de eerste plaats zijn er ***tokens ten bate van het onderhouden van een applicatie*** die ervoor zorgen dat mensen worden gestimuleerd deel te nemen binnen een blockchainapplicatie. Deze tokens worden dan als beloning ingezet. Doordat deze tokens een waarde vertegenwoordigen, helpen ze deelname in te hand. Deze tokens worden onderscheiden van ***tokens als bezit***. Tokens als bezit vertegenwoordigen ook

[113] Met een soevereine identiteit wordt de barrière om waarde naar elkaar te versturen tevens aanzienlijk verlaagd. Zodoende kun je nog betrouwbaarder geld, aandelen of eigendomsrechten op onroerend goed naar elkaar sturen.

een waarde, maar dan vooral om het bezit van deze waarde aan te tonen en het recht op dit bezit te kunnen overdragen.

2. In de tweede plaats is er dan de vraag hoe cryptotokens in een economisch systeem toe te passen zijn. Een manier hiervoor is om te kijken naar de inwisselbaarheid van tokens. Sommige zijn inwisselbaar tegen elkaar en sommige zijn juist uniek. Deze unieke tokens kunnen een minuscule waarde vertegenwoordigen en toch efficiënt worden vastgelegd en verhandeld op de blockchain.

Deze indeling kan in onderstaand diagram worden samengevat en wordt vervolgens verder uitgelegd:

Toepassing	Token ten bate van de applicatie	Token als bezitting
Inwisselbare tokens	Netwerk: Ether dApp: Augur	Asset: goud Security: aandeel Shell Cryptovaluta: Bitcoin
Niet-inwisselbare tokens		Asset: geboortecertificaat Security: persoonlijke lening

Afbeelding 99: tweeledige indeling van tokens. Enerzijds, om tokens te onderscheiden die worden gebruikt om een blockchainnetwerk te onderhouden vs bezit aan te tonen en over te dragen. Anderzijds, om tokens te onderscheiden die inwisselbaar vs niet inwisselbaar zijn.

10.3.1 Tokens ten behoeve van de applicatie versus tokens als bezitting

Zoals vermeld in hoofdstuk 10 zijn er verschillende deelnemers en rollen binnen een blockchain. Om ervoor te zorgen dat mensen het gewenste gedrag vertonen, kunnen tokens met een bepaalde waarde worden ingezet om het gewenste gedrag te belonen. De waarde van de token is afhankelijk van vraag aanbod op de markt. Om de vraag op te schroeven, zou je kunnen proberen het gebruikersgemak en het gewenste nut van het netwerk beter te communiceren, zodat er een netwerkeffect ontstaat waarbij meer mensen er gebruik van gaan

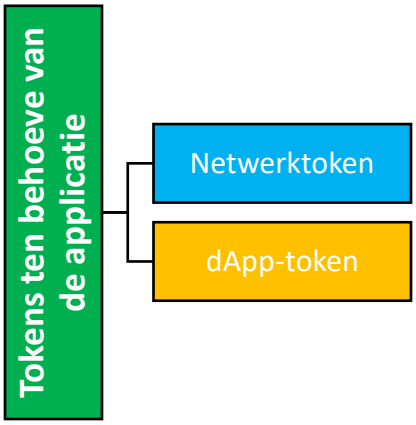
maken.[114] Binnen private blockchains is het inzetten van een token als beloning niet zo zinvol, omdat een centrale partij, zoals het bedrijfsmanagement, alle deelnemers binnen het netwerk al kent en de samenwerking reguleert. Deelnemers worden toch al beloond met bijvoorbeeld een salaris en vertrouwen wordt al afgedwongen door de centrale partij. Binnen een publieke omgeving kennen de verschillende partijen van het netwerk elkaar niet.

Let erop dat een token meerdere doelen tegelijkertijd kan dienen. Bitcoin wordt bijvoorbeeld gebruikt als netwerk- of applicatietoken en een bezitting. Dit wordt ook wel een ***dual token structure*** genoemd.

10.3.2 Tokens ten behoeve van de applicatie

Deze tokens worden op het meest basale niveau gebruikt om te stimuleren dat het netwerk in de lucht wordt gehouden. Dit netwerk kan als platform dienen waarop decentrale applicaties, dApps, draaien.

Tokens ten behoeve van de applicatie kunnen als volgt worden ingedeeld.



Afbeelding 100: Onderverdeling van tokens ten behoeve van de applicatie.

Netwerktoken

Netwerktokens worden ingezet om deelnemers te belonen voor het werk dat ze verrichten om het netwerk te helpen onderhouden. Andere namen voor deze netwerktokens zijn *intrinsieke*,

[114] Een netwerkeffect is het effect dat ervoor zorgt dat een product of dienst waardevoller wordt wanneer er meer gebruikers van het product of de dienst zijn. Als er maar één gebruiker binnen een telefoonnetwerk is met een telefoon, heeft het hebben van een telefoon weinig waarde voor de ene gebruiker.

native, *built-in* of *system incentive* tokens. Ze nemen een centrale plek in binnen een blockchain, omdat ze als organisatorisch idee een gedistribueerd vertrouwd netwerk ondersteunen en daarmee vorm geven aan het cryptoeconomische systeem van een blockchain. Een netwerk kan naast een applicatie ook een platform zijn. Dit zijn netwerken die dienen als besturingssysteem waarop dApps worden gedraaid – vergelijkbaar met Windows of iOS waar applicaties op draaien. Het platform ondersteunt dan bijvoorbeeld in het verifiëren van transacties en het voorkomen van spam. Een voorbeeld van een platform is Ethereum met het Ether-token (ETH). Ethereum maakt net als Bitcoin gebruik van het Proof-of-Work consensusmechanisme, waarbij de mijner die de juiste blok header hash genereert ook wordt beloond in ETH. Daarnaast krijgt de mijner ook de fees van de transacties.

Vier voorbeelden van platformtokens zijn:

1. EOS-tokens van het EOS-netwerk.
2. NEO-tokens van het NEO-netwerk.[115]
3. ADA-tokens van het Cardano-netwerk.[116]
4. MIOTA-tokens van IOTA.

Bij IOTA is het ook zo dat deelnemers aan het netwerk zonder vergoeding het netwerk kunnen gebruiken zolang ze computerkracht of ruimte beschikbaar stellen, waarmee twee voorgaande transacties worden geverifieerd in plaats van het gebruik van het MIOTA-token als beloning.[117] IOTA gebruikt geen blokken en heeft een lage drempel om de data-infrastructuur draaiende te houden in verband met het gebruik van IOTA-gebaseerde Internet of Things-sensoren. IOTA richt zich namelijk op de Machine2Machine-communicatie (M2M) en daarmee op het Internet of Things (IoT).[118]

---

[115] NEO staat ook wel bekend als het Chinese Ethereum. NEO naast de NEO-tokens ook GAS-tokens die worden gebruikt om transactiekosten in te verrekenen en ONT-tokens waarmee de tokenhouders kunnen meebeslissen in bijvoorbeeld upgrades van het netwerk. Voor meer informatie over NEO, zie https://neo.org/.

[116] De voornaamste kartrekker van Cardano is Charles Hoskinson, medeoprichter van Ethereum. Voor meer informatie over Cardano, zie https://www.cardano.org/.

[117] Meer informatie over dit 'pay-it-forward'-systeem en hoe IOTA werkt, is te vinden op https://www.iota.org/get-started/what-is-iota.

[118] Als IOTA geen gebruikmaakt van blokken, kun je je afvragen of het wel een blockchain is. Op de IOTA-website valt te lezen dat zijn datastructuur, genaamd de Tangle, geen gebruikmaakt van een blockchain, maar van 'Directed Acyclic Graphs' om het grootboek in op te slaan. Dit komt de schaalbaarheid ten goede. Hoewel het geen gebruikmaakt van blockchain, is IOTA toch wel relevant binnen het blockchainlandschap, omdat het bepaalde eigenschappen van traditionele blockchains, zoals platformtokens, bevat. Daarnaast is het ook een relevante ontwikkeling van blockchainalternatieven. Voor meer informatie over Tangle, zie

dApp-token

dApp-tokens worden ook wel ***utility token*** genoemd, omdat ze alleen nut hebben binnen hun eigen applicatie en ze worden gebruikt om toegang te krijgen tot dit nut. Buiten die applicatie hebben ze geen nut. Je kunt ze natuurlijk buiten de applicatie wel verhandelen. Ze zijn echter niet altijd geprogrammeerd als valuta of aandeel in een netwerk. Een voorbeeld van een dApp-token is Siacoin (SC). Siacoin is daarnaast ook de naam van het onderliggende cloudopslagnetwerk. Binnen Siacoin kunnen mensen hun vrije schijfruimte ter beschikking stellen voor anderen in het netwerk. Als beloning voor het aanbieden van schijfruimte verdienen zij Siacoin.

Twee public chain voorbeelden van dApp-tokens zijn:

1. Golem Network Tokens (GNT) die draaien op Ethereum. Met GNT-tokens krijg je toegang tot een marktplaats voor computerkracht. Mensen die hun computerkracht delen met het Golem-netwerk, worden beloond in GNT. GNT kan daarnaast ook worden gebruikt om computerkracht van een ander te huren.[119]
2. Reputation tokens (REP) van Augur waarmee je kunt deelnemen aan een gedecentraliseerd voorspellingsmarkt. Mensen kunnen met REP een voorspellingsmarkt openen voor een bepaalde gebeurtenis. Anderen kunnen dan hun REP staken en daarmee wedden of de gebeurtenis zal uitkomen of niet. Augur is gebouwd op het Ethereum-netwerk.[120]

De dApp-tokens op Ethereum zijn gemaakt volgens het ***Ethereum Request For Comments 20*** (ERC-20) protocol. Het protocol definieert bepaalde regels en standaarden met betrekking tot het uitgeven van tokens op het Ethereum-netwerk. Alle dApp-tokens gemaakt volgens ERC-20 zijn uniek voor hun applicatie en kunnen onderling worden verhandeld binnen het Ethereum-netwerk.

Sommige tokens die initieel als utility token werden aangemaakt, worden nu aangemerkt als security tokens. Security tokens komen later in dit hoofdstuk aan bod.

---

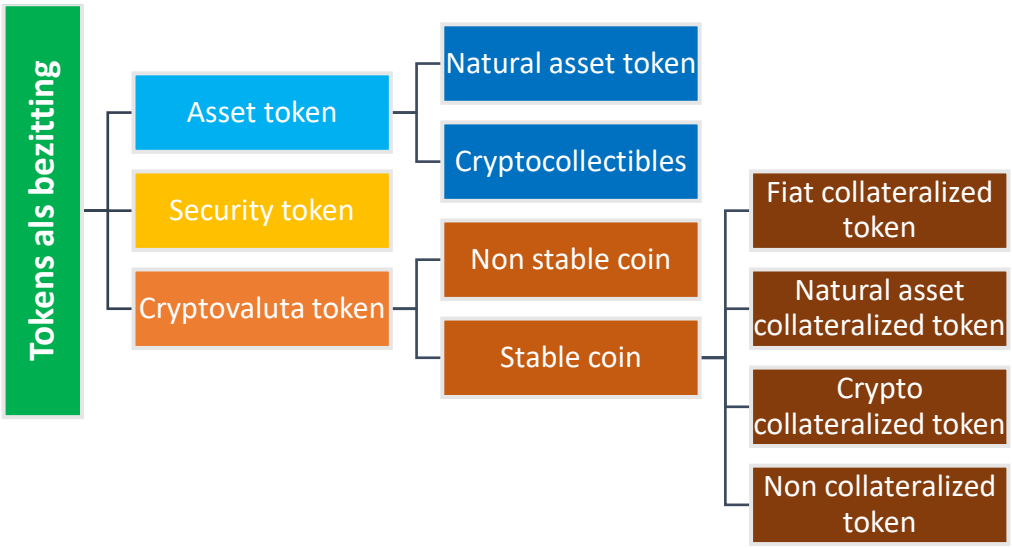
https://www.iota.org/research/meet-the-tangle. Volgens de IOTA foundation zullen mensen uiteindelijk minder dan 1% aan al het internetverkeer deelnemen. Het IoT zal de rest van het verkeer uitmaken.

[119] Voor meer informatie over Golem, zie https://golem.network/.

[120] Zie de white paper voor meer informatie over Augur: https://www.augur.net/whitepaper.pdf.

10.3.3 Tokens als bezitting

Tokens ten bate van applicaties verschillen van tokens die draaien om het vastleggen en uitwisselen van waarde binnen de blockchainapplicaties, tokens als bezitting. Deze klasse van tokens kan als volgt verder worden onderverdeeld.



Afbeelding 101: Onderverdeling van tokens als bezitting.

Asset tokens

Indien alle rechten en plichten tot het onderliggende bezit worden vastgelegd in het token, is de waarde van het token hetzelfde als het onderliggende bezit. Als je token bijvoorbeeld een digitale representatie is van het eigendom over je huis, dan is het token evenveel waard als je huis. Het digitaliseren van eigendom vergemakkelijkt de overdracht binnen een blockchain aanzienlijk. Dergelijke tokens met een onderliggende waarde in de werkelijke wereld worden ***asset-backed tokens*** genoemd. Een belangrijke voorwaarde bij asset tokens is dat de identiteit van de eigenaar vast kan worden gesteld.

Er worden binnen asset tokens ook nog onderscheid gemaakt in verschillende typen. ***Natural asset tokens*** hebben als onderliggende waarde bijvoorbeeld goud, olie, CO_2 en water. ***Cryptocollectibles*** zijn tokens die unieke digitale objecten zoals CryptoKitties of e-Sportskaarten of een avatar binnen een spel representeren.

Asset cryptotokens brengen in potentie andere voordelen met zich mee:

1. Je kunt het assetbezit eenvoudig opdelen en in kleine eenheden beschikbaar maken aan bedrijven, gebruikers en investeerders. Dit wordt ook wel ***fractioneren*** genoemd. Zo zou je bijvoorbeeld het eigendom van de Mona Lisa kunnen laten representeren door 1.000 tokens en deze tokens op de markt verkopen. Mensen die 1 token hebben, bezitten dan 1/1000^{e} van de Mona Lisa.
2. Je kunt rechten programmeren aan het cryptografische token en deze via smart contracts afdwingen. Je kunt bijvoorbeeld instellen dat je Mona Lisa token alleen aan non-profit instellingen mag worden verkocht of dat het alleen binnen een tijdsbestek van nu en drie maanden kan worden verkocht aan mensen die kunnen bewijzen minimaal drie maal per jaar naar een schildersmuseum te gaan.
3. Je vermindert, mede door de snelle en goedkope microtransacties, de frictie van aan- en verkoop aanzienlijk.[121] Zo kan een smart koelkast constant scannen waar de goedkoopste elektriciteit op een bepaald moment is en het ene uur hier en het andere uur weer daar elektriciteit inkopen.
4. Je kunt alle relevante informatie voor de onderliggende activa in de token vastleggen. Je kunt bijvoorbeeld inzien wie de vorige eigenaren zijn geweest van een tweedehandse machine die je hebt gekocht. Zodoende kan de deeleconomie een injectie krijgen.
5. Je kunt laagdrempelig zelf een asset aanmaken, zoals een toegangsticket voor een thuisconcert. Een voorbeeld van netwerken waarbij je asset tokens kunt creëren is BitShares. Zo kun je op BitShares bijvoorbeeld een token aanmaken die een aandeel binnen je bedrijf representeert. Dergelijke tokens worden ook wel security tokens genoemd.

Security tokens

Security tokens zijn tokens die obligaties, aandelen, leningen, futures, opties en andere verhandelbare financiële bezittingen representeren. Hoewel ze behoren tot de asset tokens, worden ze vaak toch nog apart genoemd. Security tokens worden ook wel een ***stake*** of ***membership token*** genoemd. Aan security tokens kunnen allerlei rechten worden meegegeven. Zo kan het recht worden verleend om elk moment van de dag de omzet of winst tot dat moment in te zien en dividend te ontvangen. Ook kan het recht bieden om de security niet aan iedereen door te verkopen, of om je stemrecht over de richting van het bedrijf tijdelijk aan iemand te kunnen uitlenen. Houders van security tokens richten zich op het vergroten van de waarde hiervan. Dit kunnen ze doen door fondsen te werven, het netwerk uit te breiden, te stemmen over welke ontwikkelaars welke initiatieven nemen ten aanzien van het netwerk en de dApp commercieel te benutten.

[121] Microtransacties zijn betalingen ten bedrage van centen. Dit is mogelijk met blockchain.

Enkele publieke blockchainvoorbeelden van netwerken die security tokens creëren binnen hun ecosysteem zijn Waves en NXT. Binnen Ethereum worden ze aangemaakt als ERC-1404 tokens. Voorbeelden in de private equity sfeer zijn JP Morgan's Quorum dat op Ethereum draait en Bakkt, een exchange die is gelinkt aan bestaande non-cryptomarkten.

Cryptovaluta tokens

Cryptovaluta tokens behoren ook tot de asset tokens en worden door de verwachte financieel-economische impact toch nog apart behandeld. Bitcoin is het bekendste voorbeeld van een cryptovaluta. In dit geval is de token bedoeld om als geld te fungeren. De wijze waarop Bitcoin het valutadoel nastreeft, is bekend. Andere voorbeelden van cryptovaluta zijn Bitcoin Cash (BCH), Litecoin (LTC) en Zcash (ZEC).

Ook worden ***stable coins*** in deze indeling bij de cryptovaluta tokens gevoegd. Deze zijn bedoeld om de volatiliteit van de waarde van cryptokens te overwinnen. Stable coins hebben als doel een stabiele waarde te vertegenwoordigen. Dit gebeurt door bijvoorbeeld fysieke bezittingen, zoals fiat of goud in onderpand, aan te houden, zoals bij Tether (USDT) en USDVault. Tether is ***fiat collateralized*** en USDVault is ***natural asset collateralized*** met goud als onderpand. Dit onderpand wordt in escrow gelegd bij een derde partij, vaak een private bank, terwijl het houden van dit onderpand wordt afgedwongen via audits die liefst inzichtelijk voor iedereen beschikbaar is.

Cryptofiattokens bieden de blockchainvoordelen van onder meer een efficiënt, cryptografisch beveiligd en snel betaalmiddel met lage transactiekosten. Er zijn vele centrale banken, waaronder de Europese Centrale Bank (ECB), die de cryptofiatontwikkeling in de gaten houden. Als een centrale bank zelf een cryptovaluta uitgeeft, dan spreken we conceptueel over een ***Central Bank Digital Currency*** (CBDC). Hoewel de CBDC elementen van blockchain kan gebruiken, is het niet noodzakelijk een toepassing van blockchain. Dit staat lijnrecht tegenover de ontstaansredenen van Bitcoin, aangezien dit een centraal gereguleerde valuta is.

Een cryptofiat kan ook cryptoactiva in onderpand hebben. Ze worden ***crypto collateralized tokens*** genoemd. Voorbeelden hiervan zijn DAI en BitUSD. Het risico met dergelijke tokens is dat de onderliggende cryptoactiva zodanig waarde verliest, dat de bovenliggende stable coin de waarde ook niet meer vast kan houden.

Tot slot zijn er ook cryptovaluta's zonder enig onderpand. Deze worden ***non collateralized tokens*** genoemd en behouden door algoritmes hun stabiele waarde.

10.3.4 Blockchain belooft om laagdrempelig unieke objecten vast te leggen

Tokens kunnen ook worden ingedeeld op basis van de mate waarin ze inwisselbaar (fungible) zijn of niet (non-fungible).

Inwisselbare tokens

Een pak bloem van 1 kg is inwisselbaar voor een ander pak bloem van 1 kg. Een biljet van €10 is daarnaast ook inwisselbaar voor twee biljetten van €5. Hetzelfde geldt voor ***inwisselbare tokens***: de afzonderlijke eenheden zijn niet te onderscheiden van elkaar en zijn met elkaar in te wisselen. Een voorbeeld is Bitcoin. 1 Bitcoin is in te wisselen voor een andere Bitcoin en twee halve Bitcoins zijn in te wisselen voor 1 hele Bitcoin.[122]

Niet-inwisselbare tokens

Tegenover inwisselbare, staan de ***niet-inwisselbare tokens***. Deze zijn uniek en daarmee schaars. Denk bijvoorbeeld aan personen, land en geboortecertificaten die niet inwisselbaar zijn tegen andere personen, land en geboortecertificaten. Het onderliggende bezit kun je wel fractioneren. Blockchain staat het toe om de authenticiteit van niet-inwisselbare tokens op een toegankelijke, snelle, goedkope manier vast te leggen. Dit is van groot belang, omdat juist in een digitale wereld een kopie van een digitaal goed makkelijk is gemaakt. Dus in het hebben van een token als representatie, ligt niet alleen een mogelijkheid om zomaar goederen uit de echte wereld makkelijk met elkaar te verhandelen. Het geeft je ook de mogelijkheid elk fysiek goed een authentieke digitale representatie te geven, hoe klein of onbenullig dat goed ook mag zijn, en dat te verhandelen. Daarnaast is het creëren van een schaarse token ook economisch interessant als je de prijs hoog wil houden. De prijs van een product komt in een competitieve markt onder invloed van kopers en aanbieders tot stand. Hoe lager het aanbod, hoe groter de schaarste en daarmee de kans op een hogere prijs.

---

[122] Echter, wat als je bijvoorbeeld weet dat de cryptovaluta die je hebt ooit is buitgemaakt door de politie in verband met een moord? Dan zou je persoonlijk misschien een andere waarde geven aan het token. Hetzelfde geldt trouwens ook voor fiatgeld. Als je weet dat je een euromunt in handen hebt die in verband is gebracht met een voor jou onethische zaak, dan zou je wellicht die specifieke euromunt anders waarderen. Verder is het ook mogelijk dat tokens die middels blockchainanalyse voor criminele doelen blijken te zijn gebruikt, op een zwarte lijst worden geplaatst.

ERC-721 tokens – cryptogoods

De ***ERC-721*** standaard op het Ethereum-netwerk staat niet-inwisselbare tokens toe. Je kunt hier naast tokendata als naam en symbool ook data erin zetten die unieke eigendomsdetails weergeven. Dit is belangrijk omdat een niet-inwisselbare token niet hetzelfde is als een andere niet-inwisselbare token. De ene CryptoKitty is zeg maar niet hetzelfde als een andere CryptoKitty. Deze data zijn betrouwbaar gevalideerd door de blockchain.

Smart contracts helpen tokenization verder in de hand, doordat ze gebruikers de instrumenten bieden om zelf verdere rechten en plichten aan hun bezittingen te geven. Zo kan er geprogrammeerd worden dat een kunstwerk bij de eerste verkoop wordt verkocht met 10% commissie en de daaropvolgende doorverkopers 2% ontvangen.

Tot zover de indeling van tokens. Vervolgens is het belangrijk te begrijpen hoe tokens worden gecreëerd voor fondsverwerving en hoe ze gebruikt kunnen worden binnen het blockchaindomein.

Intermezzo: Paradigmaverschuiving door tokenization

Al met al lijkt tokenization tot een paradigmaverschuiving te gaan leiden. Tokens bieden een flexibele gevarieerde manier om waarde, informatie, ideeën, rechten en plichten op snelle, transparante en veilige wijze over te dragen of vast te leggen tussen meerdere partijen. Ze kunnen ook worden ingebed in smart contracts. Je creëert met de ***smart tokens*** zogenaamde ***smart assets***. Je kunt hierdoor bijvoorbeeld opvolgen waar een goed vandaan komt of hoe het wanneer door wie is verzekerd of gerepareerd. Een voorbeeld hiervan zijn impact tokens waarin partijen als overheid, beleggers en instanties samenwerken om impactbeleggen te ondersteunen. Met een impact token als een SolarCoin kun je de productie van je eigen zonne-energie verifiëren. Meerdere SolarCoins kunnen zicht geven op waar zonne-energie wordt opgewekt en verbruikt, waardoor je impactmeting kunt automatiseren. Beleggers kunnen de coins gebruiken om de beleggingsportefeuille te verduurzamen. Ook wordt je bezit zelf op laagdrempelige wijze een handelsmiddel. Dat handelsmiddel kun je gefractioneerd ruilen of gefractioneerd inzetten als waarborg voor een lening. Dus een deel van je huis of aandeel zou theoretisch kunnen worden verkocht en gebruikt worden om boodschappen te doen naast je gebruikelijke valuta. Tokenization kan hierdoor nieuwe bedrijfsmodellen doen ontstaan.

Tokenization zorgt er ook voor dat de drempel om transacties te verrichten aanzienlijk wordt verlaagd door bijvoorbeeld de lage transactiekosten en de snelle settlementtijd. Het roept verder ook de volgende interessante vragen op over geld. Als een aandeel in een onderneming een security token is die je vervolgens inzet om boodschappen mee te kopen, is het aandeel dan een vorm van geld geworden? Kunnen we zeggen dat we een terugkeer krijgen naar een situatie waarin middelen worden geruild zonder betrokkenheid van een medium als geld? Voor de wetgeving en controlerende en uitvoerende instanties zal dit voorlopig nog even een diffuse situatie blijven.

Intermezzo: Central Bank Digital Currencies

De discussies over de gevolgen van cryptovaluta als Bitcoin en Libra voor natiestaten en financiële dienstverleners raakten de laatste jaren in een stroomversnelling. Nieuwe cryptomunten vinden gebruik in de echte wereld en kunnen een alternatief zijn voor een nationale fiat geld. Vandaar dat centrale banken meerdere onderzoeken en acties zijn gestart om de verantwoordelijkheid van het monetair systeem en de nationale valuta bij de natiestaat te houden. Hierbij hebben zij ook gekeken naar de potentiële gevolgen van een zelfgemaakte ***Central Bank Digital Currency*** (CBDC). Een CBDC is een cryptovaluta gebaseerd op centraal gecontroleerde blockchaintechnologie of een andere vorm van Distributed Ledger Technologie (DLT). (Lietuvos Bankas, 2019)

Voordelen en risico's

Enkele potentiële voordelen van een CBDC zijn:

1. Het is een kostenefficiënt en snel systeem dat internationale betalingen vergemakkelijkt en het betalingsrisico verlaagt. Zodoende kan het de concurrentiepositie van nationale ondernemingen en valuta verbeteren.
2. Het kan een koppeling verzorgen aan digitale identiteiten van burgers, organisaties en apparaten.
3. Transacties met CBDC worden versleuteld binnen een blockchain of gedistribueerd grootboek en zijn daarmee beter beveiligd**.**
4. Er wordt een fundering gelegd voor verdere digitale innovatie, zoals programmering van de munt. Zo is het mogelijk om automatische belastingbetalingen te programmeren in de CBDC en het reguleren van het aanbod van de CBDC.
5. Het valt binnen de vertrouwde omgeving van nationale valuta en haalt daarmee grotendeels concurrentie van digitale munten die niet volgens de nationale wetgeving zijn gecreëerd weg.
6. Het staat ook toe dat binnen de nationale wetgeving andere digitale munten worden gecreëerd door private of publieke partijen die samenwerken met de CBDC.
7. Het is lastiger om de CBDC illegaal te dupliceren of illegaal te gebruiken.

Deze voordelen worden in dit intermezzo los gezien van de discussie over in hoeverre een natiestaat een monopolie op een valuta moet hebben. Deze discussie wordt immers apart gevoerd in hoofdstuk 13 van deel II.

Tegenover de voordelen van een CBDC staat volgens Banque de France en de Nationale Bank van België het risico dat de laagdrempeligheid ervoor zorgt dat een grote partij burgers

massaal hun geld bij een financiële instelling weghalen (Pfister, 2017). Hierop antwoordde de Bank of England dat banken kunnen worden beschermd door ze niet te verplichten op aanvraag hun deposito´s in CBDC om te wisselen (Kumhof & Noone, 2018).

Mocht het na afweging van deze voordelen en risico's komen tot een CBDC, dan vergt de implementatie hiervan een publiek private samenwerking die er goed aan doet aandacht te besteden aan thema's als:

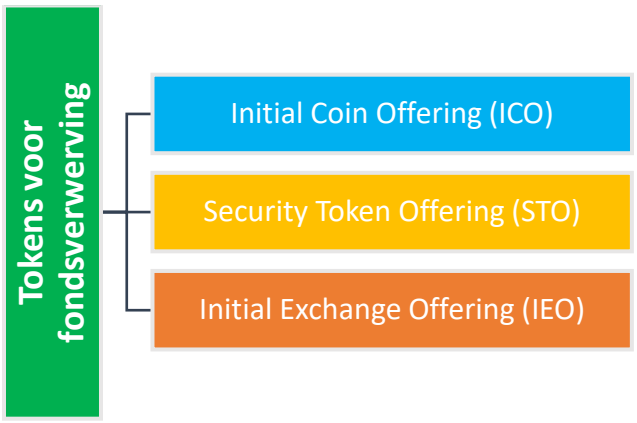
1. Het coördineren van belangen en acties van verschillende partijen, waaronder nationale banken, overheden, de Europese Unie en de ECB via een consortium.
2. Het invoeren van wetgeving die de digitale identiteit van de burger en apparaten reguleert.
3. Het invoeren van wetgeving die het verwerken van de digitale informatie rondom het gebruik van een CBDC reguleert.
4. Het invoeren van wetgeving die consumenten en bedrijven beschermt in geval van gebruik van een CBDC.
5. Het reguleren en invoeren van pan-Europese betalingsoplossingen. (Bankenverband.de, 2019)

Toekomst

Het is de verwachting dat CBDC's al op de korte termijn worden gelanceerd. China is onlangs gestart met een pilot van hun CBDC. Hierbij zijn 4 grote banken, 3 grote telecombedrijven en Huawei betrokken (Ledger Insights, 2019). De Franse centrale bankier, Francois Villeroy, heeft de ECB ook al aangemoedigd om een eigen CBDC uit te geven en wil dat Frankrijk al in 2020 een pilot start met een CBDC (Jakobson, 2019).

10.4 Tokens voor fondsverwerving

Er zijn over het algemeen drie manieren om door middel van tokenverkopen fondsen te verwerven: Initial Coin Offerings, Security Token Offerings en Initial Exchange Offerings.



Afbeelding 102: Drie manieren om door tokenverkopen fondsen te verwerven.

10.4.1 Initial Coin Offering (ICO)

Eén van de eerste instrumenten voor fondsverwerving binnen blockchain was de ***Initial Coin Offering*** (ICO), waarbij er op een blockchaintokens werden gecreëerd en werden verkocht. Ethereum staat bekend als de voornaamste blockchain waarop ICO's werden gedaan. Een groot aantal ICO's vond plaats buiten de bescherming van de nationale wet- en regelgeving. Zodoende was er onduidelijkheid over vragen als: 'Welk stemrecht koop ik als investeerder?' en 'Heb ik een deel van het bedrijf in handen?' Ook werd er vaak geen financiële verantwoording naar de aandeelhouder verzorgd, omdat er geen officiële aandelen uitgegeven zijn. Dit heeft geleid tot veel misbruik, waarbij fondsen werden verworven voor ideeën zonder dat er enige code was geschreven en er ook geen intentie was om daadwerkelijk een product op te leveren. Op Ethereum zijn er inmiddels meer dan 150.000 coins beschikbaar.[123]

10.4.2 Security Token Offering (STO)

Als opvolger op de ICO is er de ***Security Token Offering*** (STO).[124] Deze dient hetzelfde doel als een ICO. Maar nu participeer je wel in de activiteiten van een bedrijf via zijn effecten, zoals aandelen. Daarnaast heb je stemrecht en mogelijk ook recht op dividend. Bedrijven als Securitize en Polymath hebben hiervoor standaardprotocollen geschreven, waarmee je STO-

[123] Zie onder andere https://etherscan.io/tokens voor een lijst van verschillende tokens op Ethereum.

[124] Aan de naamgeving kun je zien dat er niet meer wordt gerefereerd naar coins (ICO), maar naar tokens (STO).

tokens kunt creëren, distribueren en houden met behulp van je wallet op bijvoorbeeld Coinbase.[125] Zodoende behoudt STO de voordelen van een snelle en goedkope manier om rechten en plichten over te dragen. Het security token zou binnen Nederland onder het toezicht van ***AFM*** en ***DNB*** en wet- en regelgeving, zoals ***EMIR***, ***PRIIPS***, ***AMLD5*** en ***MiFID II***, vallen. Binnen de Nederlandse wet dient de investeerder wel een KYC-proces te hebben afgerond. In de Verenigde Staten wordt de ***Howey test*** gebruikt om te zien of een token een security is of niet. Als het een security betreft, dan valt deze onder de bevoegdheid van de ***Securities and Exchange Commission*** (SEC) in de Verenigde Staten. Hierbij wordt de vraag gesteld of er een investering is gemaakt in USD binnen een samenwerkingsverband waarbij de inzet van een persoon verwacht tot winsten te leiden. Met andere woorden, de token is een security wanneer het voldoet aan de volgende eisen:

1. Het is een investering van geld.
2. Er is een winstverwachting door werk van een derde partij.
3. Er is geïnvesteerd in een gemeenschappelijke onderneming.

10.4.3 Initial Exchange Offering (IEO)

Een andere ontwikkeling is dat ICO's en STO's steeds vaker via ***Initial Exchange Offering***-platformen zoals Bitfinex en Binance worden verricht. Hierin verkrijgt een startup crowdfunding met als tussenpartij een cryptobeurs die meestal KYC- en AML-checks op zich neemt. De fondsen worden vaak verkregen in het eigen netwerktoken van het platform, bijvoorbeeld de Binance Coin (BNB).

[125] Coinbase is een handelsbeurs voor cryptocoins.

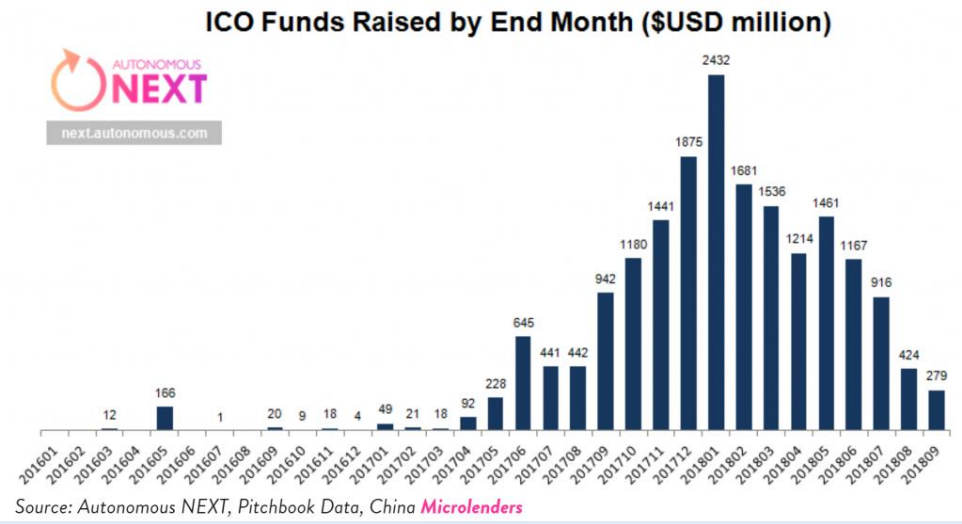
Intermezzo: ICO bubbel

Gedurende 2017 en 2018 vond een run op ICO's plaats. Dit leidde tot een beleggingsbubbel in de ICO-markt. Deze bubbel werd veroorzaakt door de toenemende aandacht voor Bitcoin en andere cryptotokens en de mogelijkheden van blockchaintechnologie.

Het begin van de bubbel

Voordat de bubbel plaatsvond, stond Bitcoin bekend als een redelijk obscure digitale munt. Met initiatieven zoals Ethereum werd duidelijk dat de onderliggende blockchaintechnologie ook voor andere doeleinden kon worden gebruikt. Dit leidde tot gespannen verwachtingen voor de jonge technologie. Deze verwachtingen, samen met de laagdrempeligheid van het maken van een investering, het financiële karakter van de Bitcoin en de historie van een eerdere speculatieve bubbel van Bitcoin, waren de voornaamste redenen voor een massieve toename van investeringen in de blockchainmarkt.

Dit leidde tot een hogere waarde van Bitcoin en andere publieke systemen. Daarnaast leidde het ook tot meer blockchaininvesteringen door bedrijven en organisaties in private systemen. Dit op zijn beurt zwengelde aandacht en investeringen in ICO's verder aan, met als gevolg een almaar toenemende instroom van nieuw geld in de markt. Het investeringsfenomeen ***FOMO*** (Fear of Missing Out) valt hier vaak: de angst dat je waardevermeerdering van je investeringsportefeuille mist als je niet investeert in een opgaande investeringsbubbel. Deze bubbel was tweeledig, enerzijds namen de investeringen in het steeds groter wordende aantal ICO's toe. Zo begon het ICO fenomeen pas in 2013, maar hadden de ICO's tussen 2014 en 16 december 2017 een waarde van $27 mrd USD. (icobench.com, 2019)



Anderzijds was er meer interesse in blockchain in het algemeen, en dan vooral in bestaande tokens als Bitcoin en aanverwanten. De totale marktkapitalisatie explodeerde tijdens de bubbel dan ook van $18 mrd USD in januari 2017 naar $830 mrd USD in januari 2018, een vermenigvuldiging van 46 keer in één jaar tijd. De $27 mrd USD aan ICO's-opbrengsten is hiermee vergeleken bescheiden. Echter, als snelle toegankelijke en in het begin heel succesvolle toepassing van een blockchain was het een symbool van reeds ingeloste verwachtingen van de blockchaintechnologie.

De eerste ICO's begonnen in juli 2013 met de introductie van Mastercoin. Vervolgens versnelde het fenomeen met de komst van Ethereum in 2014, toen het op één na grootste ICO-project. Ethereum bood namelijk met het ERC-20-standaardprotocol een kans om op laagdrempelige wijze een token te creëren als nieuw digitaal bezit. Hierdoor nam het aantal ICO's toe tot een aantal van 5.655 tussen 2014 en 16 december 2019 (https://icobench.com). Het fenomeen werd zo stevig dat zelfs toen de bubbel leegliep in 2018, nog steeds de twee grootste ICO's tot nu toe plaats konden vinden; die van EOS en Telegram. (https://www.coinist.io). Een ander fenomeen uit deze tijd was de ***airdrop***. Hierbij worden tokens vrij gedistribueerd om de promotie van deze tokens te ondersteunen.

De langzaam groter wordende risico's van ICO's

Met de versnellende marktgroei namen ook de risico's op verlies en schandalen omtrent de ICO's toe. Ten eerste bleek dat de nieuwe technologie de verwachtingen niet kon waarmaken, zeker niet op een dergelijke korte termijn. Dit terwijl ruwweg de helft van de ICO's nog gedurende de hoogtepunten van de markt al failliet gingen. (Sedgwick, 2018) Dit had mede te maken met de onervarenheid van de ondernemers, die als ontwikkelaar wellicht wel de kennis in huis hadden, maar als businessmanager of financiële professional niet. Ethereum had de drempel om een eigen token aan te maken immers dusdanig verlaagd dat het makkelijk was om zelf een ICO beginnen. (Kauflin, 2018) Daarnaast namen de schandalen omtrent ICO's toe. Zo werden investeerders voorgelogen in scams, waar onbekende ondernemers met het geld gingen lopen. Ook was er sprake van diefstal bij databases van centrale exchanges of bij de eerder genoemde Ethereum Genesis DAO (zie hoofdstuk 8.7). Ook werd er breeduit geschreven over marktmanipulatie van verschillende tokens, zoals bij ***pump and dump***. Hierbij worden substantiële hoeveelheden van een token gekocht door een partij om anderen te stimuleren ook te gaan kopen. Vervolgens probeert dezelfde partij de tokens op een hogere prijs te verkopen.

Een andere methode van marktmanipulatie is om valse informatie te verspreiden over een token om de prijs naar beneden te brengen. Dit wordt met ***FUD*** aangeduid, wat staat voor het verspreiden van “Fear, Uncertainty and Doubt”.

Het grote deel van deze investeerders dat de problemen ervaarde, bestond hierbij uit onervaren kleine investeerders (De Vries & Wassink, 2018). Deze investeerders kwamen pas langzaam tot het besef dat ze in al deze gevallen geen legale middelen hadden om hun rechten af te dwingen. Ook vertegenwoordigden de tokens zelf geen legaal bezit, of gaven ze geen recht op mogelijke dividenden. De nationale aandacht voor de gebreken van deze investeringen leidde tot ingrijpen van nationale overheden. Om deze investeerders te beschermen, werden burgers gewaarschuwd voor de hoge risico’s van de investeringen. In vele landen zijn ICO’s sterk gereguleerd of zelfs verboden. (Russell, 2017)
Ondanks de sterke fluctuaties van de prijzen werd de term ***HODL*** breeduit gebruikt. Hierbij behoudt de investeerder het token voor de lange termijn, ondanks dat het aan waarde verliest.

De leeglopende bubbel

Gedurende 2018 liep de bubbel leeg. De totale marktkapitalisatie is met $195 miljard USD op 16 december 2019 nog steeds bijna 11 keer zo hoog als begin 2017. In die zin heeft de grotere aandacht voor de cryptomarkt een tot op heden blijvende invloed gehad. Binnen deze kapitalisatie neemt Bitcoin nog steeds de meeste waarde in.

Afbeelding 103: Marktkapitalisatie van de cryptomarkt van 1 januari 2017 tot 16 december 2019.

Echter, andere initiatieven waar je ICO’s op kunt uitvoeren, als Ethereum en EOS, staan hier ook tussen als goed gefinancierde blockchainorganisaties. Ondertussen is het begrip ICO zelf zich verder aan het ontwikkelen met behulp van ideeën als onder andere Security Token Offerings (STO’s), Digital Security Offerings (DSO’s), Initial Exchange Offerings (IEO’s) en tokenized IPO’s.

Intermezzo: Atomic Swaps

Als je cryptovaluta's wil verhandelen, gebruik je hier vaak een ***handelsplatform*** (exchange) voor. Dit platform is of gecentraliseerd of gedecentraliseerd. Het nadeel van een handelsplatform is dat niet altijd alle beschikbare cryptovaluta's te verhandelen zijn. Daarnaast kun je niet altijd direct de ene cryptovaluta omwisselen voor een andere. De handel gaat vaak nog via Bitcoin en Ethereum. Als je bijvoorbeeld Zcash wil omwisselen voor Litecoin, moet je eerst ZCash omwisselen voor Bitcoin en daarna omzetten in Litecoin. De tussenwissel gaat gepaard met wisselkosten.

Daar komen bij gecentraliseerde platformen specifieke nadelen bij. Zo zijn de private keys in handen van de eigenaar van dit platform. Dit vormt zodoende een Single Point of Failure. Dit maakt het platform gevoelig voor hacks. Daarnaast vragen de centrale platformen vaak hogere tarieven in vergelijking met decentrale platformen om kosten te dekken en winst te maken. Decentrale handelsplatformen (***decentralized exchange*** of ***DEX***) kennen deze nadelen niet, maar wel weer andere nadelen. Zo hebben decentrale platformen vaak kleinere handelsvolumes om voor elke cryptovaluta een markt of een goede prijs te bieden.

Om deze nadelen van handelsplatformen te omzeilen, wijken mensen die cryptovaluta's willen verhandelen ook wel uit naar een peer-to-peeroplossing buiten exchanges om. Hier ben je echter niet altijd zeker dat de andere partij ook daadwerkelijk de cryptovaluta's levert. Dit wordt ook wel ***counterparty risk*** genoemd.

Een ***atomic swap*** biedt een oplossing voor deze nadelen door een directe transactie tussen twee wallets op te zetten. Zo kun je cryptovaluta's van verschillende blockchains omwisselen met lage tarieven, zonder tussenpartij en met garantie op wederzijdse levering. Atomic swaps gebruiken hiervoor smart contracts. Het woord atomic geeft aan dat de uitwisseling of helemaal gebeurt, of helemaal niet gebeurt. Hiermee is atomic swap een belangrijke ontwikkeling om de handel van cryptovaluta's veiliger te maken. (Van der Hoeff, 2018) Deze methode werd als eerste door Sergio Demian geopperd in juli 2012. In 2013 werd het verder uitgewerkt door Tier Nolan. Atomic swaps raakten bekender toen er op 19 september 2017 voor het eerst werd getweet over een werkende swap tussen Decred and Litecoin.

Een voorbeeld van hoe een atomic swap werkt

Bob en Alice willen hun Litecoin en Bitcoin wisselen via een atomic swap en spreken een hoeveelheid en prijs af. Vervolgens gaan ze een Hashed TimeLock Contract (HTLC) aan, een soort virtuele kluis die alleen te openen is met twee sleutels:

1. Een HashLock-sleutel die cryptovaluta's alleen tussen de handelaars verdeelt nadat zij de transactie hebben getekend met een geheime code.
2. Een TimeLock-sleutel die de cryptovaluta's terugstuurt naar de oorspronkelijke handelaars als de omwisseling niet binnen een bepaalde tijdsperiode plaatsvindt.

Alice opent hiervoor een contract, waarmee haar Litecoin op een HTLC -adres, de kluis, wordt gezet en er een geheime code wordt gecreëerd, een preimage. Dit preimage wordt gebruikt om een cryptografische hash te maken die Alice naar Bob stuurt. Deze hash heeft Bob nodig om zijn Bitcoin ook op een HTLC-adres, de kluis, te zetten. Bob gebruikt hiervoor dus dezelfde hash die is gebaseerd op dezelfde geheime code als die van Alice.
Nu weet Alice in welke kluis, HTLC-adres, de Bitcoins zich bevinden en kan zij het slot hiertoe opendraaien met haar eigen digitale handtekening en de preimage. Hierop wordt de preimage transparant op de blockchain gezet, zodat Bob deze kan gebruiken om het slot aan zijn kant open te draaien. Als beide sloten zijn opengedraaid, gaan de deuren van de kluis open en kunnen Alice en Bob de Bitcoin en Litecoin eruit nemen. Daarmee is ook het smart contract vervuld en wordt het beëindigd.

Mochten Alice en/of Bob op enig moment alsnog besluiten af te zien van de wissel, dan kunnen ze besluiten hun eigen slot niet open te draaien. In dat geval krijgt niemand de cryptovaluta van de ander. (Nolan, 2013)

De cryptovaluta's worden hier dus uitgewisseld tussen twee verschillende blockchains, hoewel je een swap natuurlijk ook kunt doen binnen eenzelfde blockchain. Een swap tussen twee verschillende chains wordt ook wel een ***cross-chain*** swap genoemd. Voor twee verschillende blockchains dien je een betalingskanaal tussen elkaar op te zetten, waarin je meerdere bedragen naar elkaar over kunt sturen via een smart contract, met als resultaat dat alleen de eindbalans van alle transacties op een blockchain wordt geschreven. Dit scheelt ruimte en tarieven om de informatie in blocks op te nemen. (OAX, 2018) Deze betalingskanalen worden onder andere ondersteund door het Lightning netwerk van Bitcoin.

Toekomst

Er zijn echter nog wat technische beperkingen die de ontwikkeling van atomic swaps tegenhouden. Zo wordt gezocht naar mogelijkheden om de verschillende hash algoritmes die blockchains gebruiken op elkaar af te stemmen, de snelheid te vergroten en te voorkomen dat een blockchain verplicht smart contracts moet ondersteunen om met atomic swaps te werken. Tevens mist de toepassing nog wat liquiditeit om efficiënt te werken, mede omdat atomic swaps nog een opkomende technologie is die nog aan schaal moet winnen. Door dit in de toekomst op te lossen, is te verwachten dat atomic swaps de veiligheid, schaalbaarheid en interoperabiliteit van blockchains verder verbeteren. Hier bovenop maken ze het blockchain ecosysteem meer valuta-agnostisch wat wellicht kleinere blockchains ten goede komt. (Uczciwek, 2018)

Tegenwoordig zijn er al handelsplatformen die volledig werken op atomic swaps. Eén daarvan is Atomic DEX. Voor meer informatie over dit handelsplatform, zie https://atomicdex.io/.

10.5 Samenvatting, begrippen en bronnen

Samenvatting

Cryptografische tokens dienen vele doelen zoals toegang verschaffen tot een systeem of het representeren van informatie van een fysiek object. Hiermee verschaffen de tokens waarde die je binnen een blockchain uit kunt wisselen tussen verschillende partijen. Deze welvaartsoverdracht door middel van computernetwerken, cryptografie, speltheorie en softwareontwikkeling is samen met welvaartscreatie- en consumptie onderdeel van cryptoeconomics. Een belangrijke rol van Bitcoin als token is dat het mensen stimuleert samen te werken en daarmee een zelforganiserend cryptoeconomisch systeem helpt te onderhouden.

Tokens worden in het boek op twee manieren ingedeeld. Enerzijds als tokens ten behoeve van de applicatie (netwerk/dApp) versus tokens als bezitting zoals activa en cryptovaluta. Anderzijds om ze in een economisch systeem in te passen door te kijken in hoeverre een token inwisselbaar is. Blockchain kan deze tokens bijzonder efficiënt vastleggen en verhandelen, zelfs als ze een minuscule waarde vertegenwoordigen en/of uniek in hun soort zijn.

In het boek wordt tevens gerefereerd aan de laagdrempelige snelle wijze waarmee financiële fondsen kunnen worden verworven om initiatieven te ondersteunen. Hierbij worden Initial Coin Offerings, Security Token Offerings en Initial Exchange Offerings als manieren van fondsverwerving genoemd. De trend hierbij is dat deze tokens steeds meer op een georganiseerde, door overheden en regelgeving ondersteunde, wijze worden aangeboden en verhandeld.

Opmerkingen die je nu kunt uitleggen

- Om een blockchain te draaien, heb je geen token nodig.
- Tokenization is één van de belangrijkste bijdragen van blockchain aan cryptoeconomics.
- Cryptoeconomics is een nieuwe discipline die is opgekomen door de komst van blockchain en omvat de studie van computernetwerken, cryptografie, speltheorie en softwareontwikkeling.
- Smart tokens dragen waarde, informatie, ideeën, rechten en plichten laagdrempelig over door middel van smart contracts.
- Elke bezitting kan in principe binnen de blockchain een token krijgen, tot aan individuele paperclips toe.
- In de toekomst kun je theoretisch elke bezitting die je hebt, tokenizen en deze tokens al dan niet gefractioneerd gebruiken als betaal- of financieringsmiddel.

- Centrale banken volgen de ontwikkelingen van cryptovaluta's zeer goed en sommige experimenteren al met Central Bank Digital Currencies (CBDCs).
- Er zijn verschillende manieren om met behulp van tokens fondsen te verwerven. De meest gangbare manieren zijn Initial Coin Offerings, Security Token Offerings en Initial Exchange Offerings.

Verklarende begrippenlijst

Autoriteit Financiële Markten (AFM): De Nederlandse toezichthouder op de financiële markten.

Airdrop: Gratis distributie van tokens om de promotie van deze tokens te ondersteunen.

AMLD4/5: De vierde en vijfde EU Anti-Money Laundering Directive. Dit staat voor de EU anti-witwas richtlijn.

Asset-backed token: Refereert hier aan een stable coin die als onderpand bezittingen in bewaring heeft.

Atomic Swap: Een directe swap tussen twee verschillende cryptovaluta's. Atomic swaps maken gebruik van Hashed TimeLock Contracts.

Central Bank Digital Currency (CBDC): Cryptovaluta uitgegeven door een centrale bank.

Counterparty risk: Het risico dat de ander met wie je een transactie aangaat zijn contractuele plicht niet vervult.

Cross-chain: Tussen twee verschillende blockchains. Een cross-chain swap is een wissel tussen cryptovaluta's van twee verschillende blockchains.

Crypto collateralized tokens: Refereert hier aan een stable coin die cryptobezit als onderpand heeft.

Cryptocollectibles: Tokens die unieke digitale objecten zoals CryptoKitties of e-Sportskaarten of een avatar binnen een spel representeren.

Cryptoeconomics: Een nieuwe discipline die is opgekomen door de komst van blockchain en de studie omvat van computernetwerken, cryptografie, speltheorie en softwareontwikkeling. Binnen cryptoeconomics wordt er onderzocht hoe een gedecentraliseerd netwerk moet worden ingericht om deelnemers zoveel mogelijk te stimuleren goed gedrag te vertonen.

Decentralized Exchange (DEX): Een handelsplatform dat wordt ondersteund door een publieke blockchain zonder centrale partij.

De Nederlandsche Bank (DNB): De Nederlandse centrale bank.

Dual token structure: Een structuur waarbij een token meerdere doelen tegelijkertijd dient. Bitcoin wordt bijvoorbeeld gebruikt als netwerk- of applicatietoken en een bezitting.

European Market Infrastructure Regulation (EMIR): EU regelgeving omtrent derivaten.

Ethereum Request for Comments 20 (ERC-20) protocol: Het protocol definieert bepaalde regels en standaarden met betrekking tot het uitgeven van tokens op het Ethereum-netwerk.

Ethereum Request for Comments 721 (ERC-721) protocol: Het protocol voor niet-inwisselbare tokens op het Ethereum-netwerk.

Fiat collateralized token: Refereert hier aan een stable coin die als onderpand fiat valuta in bewaring heeft.

FOMO: Fear of Missing Out. De angst om waardevermeerdering van een token mis te lopen.

Fractionering: Het in kleine eenheden opdelen van eigendomstokens.

FUD: Fear, Uncertainty en Doubt.

Fungible tokens: Tokens die niet van elkaar te onderscheiden zijn en die met elkaar in te wisselen zijn. Een voorbeeld hiervan is Bitcoin.

Handelsplatform: Een platform waarop tokens kunnen worden verhandeld.

HODL: De investeerder behoudt het token voor de lange termijn, ondanks dat het aan waarde verliest.

Howey test: Amerikaanse test om te zien of een token een security is of niet. Als het wel een security is, dan valt het onder de toezicht van de Security and Exchange Commission.

Initial Coin Offering (ICO): Fondsverwerving waarbij tokens worden gecreëerd en verkocht door een bedrijf of project.

Initial Exchange Offering (IEO): Fondsverwering met als tussenpartij een cryptobeurs die meestal KYC- en AML-checks op zich neemt. De verwerving wordt vaak verkregen in het eigen netwerktoken van het platform.

Internet of Information: Eerst verschijningsvorm van internet waarin internet vooral bedoeld was om informatie uit te wisselen.

Internet of Value: Het internet waarbij naast informatie ook waarde veilig kan worden uitgewisseld.

Inwisselbare token: Zie fungible token.

Membership token: Zie security token.

Markets in Financial Instruments Directive (MiFID II): EU richtlijn gericht op harmonisatie van financiële markten binnen de EU en het beschermen van de investeerder.

Natural asset collateralized token: Refereert hier aan een stable coin die als onderpand natuurlijk eigendom in bewaring heeft.

Netwerktoken: Token dat wordt ingezet om deelnemers te belonen voor het werk dat ze verrichten om het netwerk te helpen onderhouden.

Non-Fungible Token (NFT): Niet-inwisselbare token. Ze zijn niet uniek. Dit in tegenstelling tot een fungible token zoals jouw fiets met geregistreerd framenummer.

Niet-inwisselbare token: Zie Non-Fungible Token.

Non collateralized token: refereert hier aan een stable coin waarbij geen onderpand in bewaring is om de waarde van het token te ondersteunen.

Packaged Retail Investment and Insurance-Based Products (PRIIPS): EU regelgeving omtrent alternatieve spaarproducten.

Pump and dump: Een investeerder koopt substantiële hoeveelheden van een token en stimuleert vervolgens anderen om ook te gaan kopen zodat de prijs stijgt. Daarna probeert dezelfde investeerder de tokens op een hogere prijs te verkopen.

Securities and Exchange Commission (SEC): Amerikaanse tegenhanger van de AFM.

Security token: Token die obligaties, aandelen, leningen, futures, opties en andere verhandelbare financiële bezittingen representeren. Security tokens worden ook wel een stake of membership token genoemd.

Smart asset: Een token dat een activa representeert en wordt gedefinieerd door de regels van smart contracts.

Smart token: Token dat je kunt programmeren. Zo kun je bijvoorbeeld het gebruiksrecht van digitale muziek binnen een vooraf afgesproken periode vastleggen.

Speltheorie: Een formele studie naar besluitvorming waar verscheidene spelers keuzes moeten maken die potentieel het belang van andere spelers raken.

Stable coin: Een blockchaintoken die relatief stabiel in waarde blijft. De bedoeling is de stabiliteit van fiat valuta als bijvoorbeeld de EUR en USD te verkrijgen.

Stake: Zie security token.

Security Token Offering (STO): Een STO dient hetzelfde doel als een ICO, maar nu participeer je wel in de activiteiten van een bedrijf via zijn effecten, zoals aandelen.

Tokenization: Het proces van tokencreatie.

Token als bezit: Token dat een bezit vertegenwoordigt.

Token ten bate van het onderhouden van een applicatie: token dat mensen stimuleert deel te nemen binnen een blockchainapplicatie.

Utility token: Token dat wordt gebruikt om gebruik te mogen maken van een dApp.

Bronnen

Aggarwal, V., & Tan, Y. (2019). A Structural Analysis of Bitcoin Cash's Emergency Difficulty Adjustment Algorithm. *SSRN Electronic Journal*. 1-36. Doi: 10.2139/ssrn.3383739

Autonomous Next (2018, 8 oktober). CRYPTO: September ICOs 90% Down from January, but Venture Funding is Ray of Hope. Geraadpleegd van https://next.autonomous.com/thoughts/crypto-september-icos-90-down-from-january-but-venture-funding-is-ray-of-hope

Bankenverband (2019, 30 oktober). German banks say: The economy needs a programmable digital euro! Geraadpleegd van https://en.bankenverband.de/newsroom/comments/programmable-digital-euro/

Bonanno, G., (2015). Game Theory: An open access textbook with 165 solved exercises. *eScholarship, University of California*. Doi 10.13140/RG.2.1.3369.7360

Chan, W. (2018, 18 september). Atomic swaps, cross chain swaps, on chain, off chain. Geraadpleegd van https://medium.com/@OAX_Foundation/tl-dr-atomic-swaps-cross-chain-swaps-on-chain-off-chain-f428512e1d2a

Cointelegraph. (n.d.) Difference between Bitcoin and Bitcoin Cash. Geraadpleegd van https://cointelegraph.com/bitcoin-cash-for-beginners/btc-bch-differences

Colloquium of the Belgian Financial Forum in cooperation with SUERF & The European Money and Finance Forum & Eggsplore, Smets. J. (2016). Fintech and Central Banks. Geraadpleegd van https://www.suerf.org/docx/l_ec5decca5ed3d6b8079e2e7e7bacc9f2_9467_suerf.pdf

Crypto Gibraltar (2019, 25 maart). Interview with Komodo's CTO, How Atomic Swaps Will Change How Cryptocurrency is Traded. Geraadpleegd van http://www.cryptogib.gi/interview-with-komodos-cto-how-atomic-swaps-will-change-how-cryptocurrency-is-traded/

Decred. [@decred]. (2017, 19 september). [Tweet] Geraadpleegd van https://twitter.com/decredproject/status/910224860625780736

Finextra (2019, 31 oktober). German banks call for digital euro. Geraadpleegd van https://www.finextra.com/newsarticle/34677/german-banks-call-for-digital-euro

Frankenfield, J. (2019, 25 juni). Atomic Swaps Defined. Geraadpleegd van https://www.investopedia.com/terms/a/atomic-swaps.asp

van der Hoeff, M. (2018, 20 april). Atomic Swaps Simply Explained: How to Swap Cryptocurrencies without a Middleman. Geraadpleegd van https://hackernoon.com/atomic-swaps-simply-explained-how-to-swap-cryptocurrencies-without-a-middleman-6cd29680c32e

Mayer, T. (2019). A digital euro to save EMU. Geraadpleegd van https://voxeu.org/article/digital-euro-save-emu

Jakobson, L. (2019, 5 december). France: 2020 national digital currency bridge to e-euro. Geraadpleegd van https://modernconsensus.com/cryptocurrencies/france-2020-national-digital-currency-bridge-to-e-euro/

Juškaitė, A., & Šiaudinis, S., & Reichenbachas, T. (2019). CBDC – in a whirlpool of Discussion. Geraadpleegd van https://www.lb.lt/uploads/publications/docs/23917_e0ae2c863fbc83cc688dac638fb16455.pdf

Kauflin, J. (2018, 29 oktober). Where Did The Money Go? Inside the Big Crypto ICOs of 2017. Geraadpleegd van https://www.forbes.com/sites/jeffkauflin/2018/10/29/where-did-the-money-go-inside-the-big-crypto-icos-of-2017/

Kharif, O. (2018, 9 juli). Half of ICOs Die Within Four Months After Token Sales Finalized. Geraadpleegd van https://www.bloomberg.com/news/articles/2018-07-09/half-of-icos-die-within-four-months-after-token-sales-finalized

Kumhof, M., & Noone, C. (2018). Staff Working Paper No. 725. Central bank digital currencies - design principles and balance sheet Implications. Geraadpleegd van https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/central-bank-digital-currencies-design-principles-and-balance-sheet-implications

Lannquist, A. (2019). *Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today?* [White paper] Geraadpleegd van http://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf

Leonard, S. (2017, juni 21). The Internet of Value: What It Means and How It Benefits Everyone. Geraadpleegd op 24 december 2019, van https://www.ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/

Levine, M. (2019, april 4). Money Stuff, Token Sales Have Some Rules Now. Geraadpleegd van https://www.bloomberg.com/opinion/articles/2019-04-04/token-sales-have-some-rules-now

MacIver, K. (2016, juli). From the internet of information to the internet of value. Geraadpleegd van https://www.i-cio.com/big-thinkers/don-tapscott/item/from-the-internet-of-information-to-the-internet-of-value

Mayer, T. (2019, 6 november). A digital euro to save EMU. Geraadpleegd van https://voxeu.org/article/digital-euro-save-emu

Nakamura, Y., & Kharif, O. (2017, 4 december). Battle for 'True' Bitcoin Is Just Getting Started. Geraadpleegd van https://www.bloomberg.com/news/articles/2017-12-04/battle-for-true-bitcoin-is-just-getting-started-quicktake-q-a

Nguyen, A., (2018, 9 september). Intro to Cryptoeconomics. Geraadpleegd van https://hackernoon.com/intro-to-cryptoeconomics-c984b020d186

Nolan, T. (2013, 2 mei). Alt chains and atomic transfers [Online forum comment]. Bericht geplaatst op https://bitcointalk.org/index.php?topic=193281.0

Peterson, J. Krug, J., Zoltu, M., Williams, A.K., Alexander, S.. Forecast Foundation. (1 november 2019). Augur: a Decentralized Oracle and Prediction Market Platform (v2.0). Bron: https://www.augur.net/whitepaper.pdf

Peterson, J.. & Krug, J., & Zoltu, M., & Williams, A.K., & Alexander, S. (2019). *Augur: a Decentralized Oracle and Prediction Market Platform (v2.0)* [White paper]. Geraadpleegd van https://www.augur.net/whitepaper.pdf

Pfister, C. (2017). Monetary Policy and Digital Currencies: Much Ado about Nothing? Geraadpleegd van https://publications.banque france.fr/sites/default/files/medias/documents/dt-642.pdf

Popper, N. (2017, 25 juni). Some Bitcoin Backers Are Defecting to Create a Rival Currency. Geraadpleegd van https://www.nytimes.com/2017/07/25/business/dealbook/bitcoin-cash-split.html

Russell, J. (2017, 4 september). China has banned ICOs. Geraadpleegd van https://techcrunch.com/2017/09/04/chinas-central-bank-has-banned-icos/

Sedgwick, K. (2018, 23 februari). 46% of Last Year's ICOs Have Failed Already. Geraadpleegd van https://news.bitcoin.com/46-last-years-icos-failed-already/

SFOX Edge (2019, 3 juni). Bitcoin Cash vs. Bitcoin SV: Six Months after the Hash War. Geraadpleegd van https://blog.sfox.com/bitcoin-cash-vs-bitcoin-sv-six-months-after-the-hash-war-e6d92a03b891

Sultan, K., & Runi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. *11th IADIS International Conference Information Systems 2018*. 49-57.

Tapscott, S. (2018, 25 juli). Beyond digital gold; Cryptocurrency is just one of seven types of cryptoassets you should know. Geraagdpleegd van https://qz.com/1335481/cryptocurrency-is-just-one-of-seven-types-of-cryptoassets-you-should-know/

Uczciwek, M. (2018). What Are Atomic Swaps? The Most Comprehensive Guide Ever! Geraadpleegd van https://blockgeeks.com/guides/atomic-swaps/

Wassink, S., de Vries, M., (2018). Onderzoeksrapport cryptocurrencymarkt: beleggingsbubbel of niet? En: In hoeverre is een beleggingsbubbel te voorspellen? Saxion University of Applied Sciences.

van Wirdum, A. (2018, 14 november). When the Fork Forks: What You Need to Know as Bitcoin Cash Goes to War. Geraadpleegd van https://bitcoinmagazine.com/articles/when-fork-forks-what-you-need-know-bitcoin-cash-goes-war/

11. Blockchain en de belofte van het internet (Web 3.0)

"The real promise of these new technologies, many of their evangalists believe, lies not in displacing our currencies but in replacing much of what we now think of as the internet, while at the same time returning the online world to a mere decentralized and egalitarian system."

- Steve Johnson (2018)

"We are concerned about the growing number of threats to the very existence of the open Web, such as censorship, surveillance, and concentrations of power. The Web that drives economic progress and knowledge, is the one where new businesses bloom, where government transparency is a reality, and where citizens document injustice."

- Tim Berners-Lee en Web We Want coalition (z.d.)

11.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Dat de blockchainontwikkeling logisch past binnen andere technologische ontwikkelingen, zoals die binnen de 3e en 4e industriële revolutie.
- Dat data centraal staan in de digitale revolutie.
- Dat interconnectiviteit grote kansen biedt tot verdergaande versnelling van technologieën.
- Hoe blockchain zich verhoudt als internettechnologie.
- Welke beloften internet maakte en blockchain nakomt.

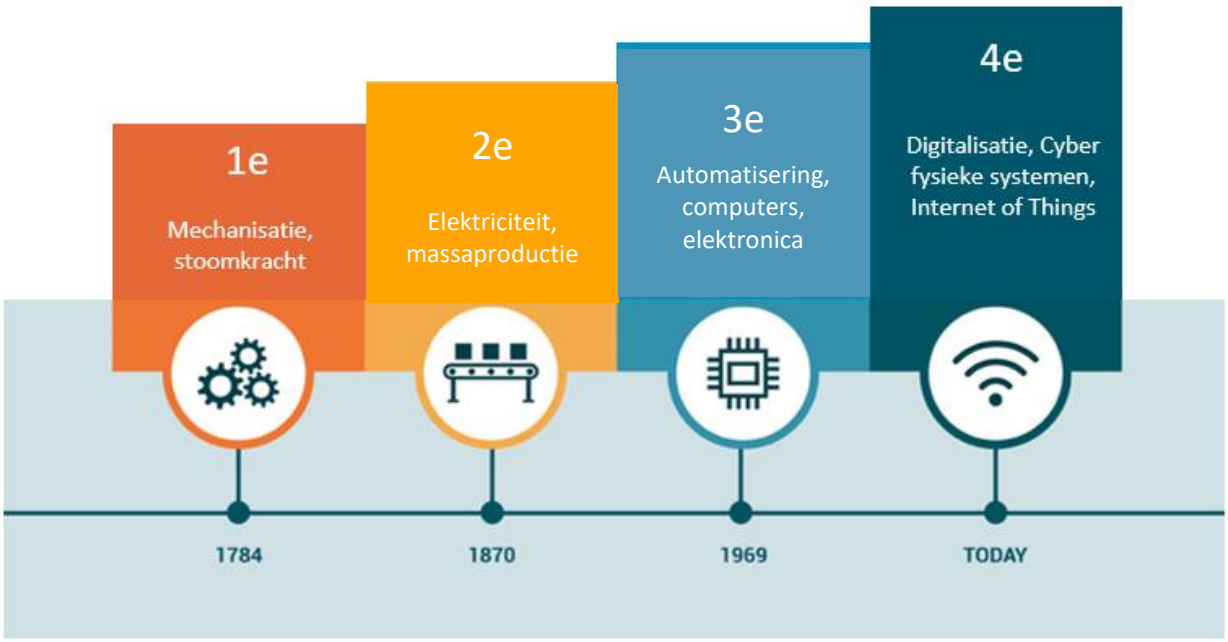
Inleiding

Technologische ontwikkelingen zijn inherent aan de mens. We leren van elkaar en de lessen die we leren worden van generatie op generatie aan elkaar overgedragen via informatiedragers als taal, kleitabletten, papyrus en databasesystemen. Dit is iets wat andere diersoorten niet of in mindere mate lijken te kunnen. Technologische ontwikkelingen raakten in een versnelling toen de mens in staat was om gigantische hoeveelheden energie op te wekken en te transporteren,

beginnend met de stoommachine. Dit was de ***1e industriële revolutie***. Elke industriële revolutie kenmerkt zich door de enorme veranderingen met betrekking tot hoe mensen zich onderling organiseren in bijvoorbeeld politieke, sociaaleconomische en militaire systemen. Industriële revoluties hebben deze impact mede veroorzaakt doordat er vanuit economisch perspectief flinke productiviteitsstappen worden gemaakt. Dit is altijd gepaard gegaan met de efficiëntere inzet van kapitaalmiddelen en een aanzienlijke verhoging van de welvaart.

De ***2e industriële revolutie*** kenmerkte zich door het vervangen van stoomkracht met elektriciteit wat op een mobielere manier opgewekt en gebruikt kon worden. Daarbovenop leidde de industriële toepassing van massaproductie tot verdere schaalvergroting en goedkopere producten. Het leidde ook tot vraagstukken omtrent urbanisatie, organisatie van infrastructuur, onderwijs, sociale innovatie en het milieu.

In de ***3e industriële revolutie*** werd productie aanzienlijk verder geautomatiseerd en groeide het aandeel van de dienstverlening in het bruto nationaal product dankzij de opkomst van elektronica, computers en het internet. Internet is belangrijk, omdat het mensen op een manier organiseert die voorheen niet mogelijk was. Binnen het internet zijn er drie stromen die Web 1.0, Web 2.0 en Web 3.0 worden genoemd. Deze stromen zijn relevant voor blockchain.



Afbeelding 104: Overzicht van de 4 industriële revoluties. De afbeelding is afkomstig van 'How Can Space Support the Fourth Industrial Revolution?' (*Tully, z.d.*).

Cybersecurity, Internet of Things, kunstmatige intelligentie, blockchain, robotisering, biotechnologie, quantum computing zullen in de ***4e industriële revolutie*** een grote rol spelen. De 4e industriële revolutie is voor een groot deel te danken aan de grotere capaciteit aan hardware, grotere beschikbaarheid van informatie en de grotere vooruitgang in algoritmes. Hierdoor kun je nog kleinere en complexere sensoren en machines maken. In de 4e industriële revolutie worden de mogelijkheden tot het genereren en analyseren van digitale data ook verder ontwikkeld. Deze digitale data ontstaan weer dankzij de vorige revolutie met onder andere computerisering, automatisering van processen en internet. Hiermee is het mogelijk om nog dieper te begrijpen hoe bijvoorbeeld een product of productieproces kan worden verbeterd, of hoe een mens te beïnvloeden is om een product of dienst te kopen.

In de volgende paragraaf wordt onder andere dieper ingegaan op de praktische applicaties die dankzij internet breeduit worden gebruikt, zoals social media, e-mail en e-commerce. Ook wordt ingegaan op hun invloed op de decentralisatie van onze samenleving. Dit gebeurt door eerst technologische ontwikkelingen te behandelen die internet mogelijk hebben gemaakt. Vervolgens wordt ingegaan op de drie ontwikkelingen van het Web: Web 1.0, Web 2.0 en Web 3.0.

In paragraaf 11.3 wordt beschreven hoe internet opnieuw vorm zou kunnen krijgen door er blockchain lagen in te bouwen, de blockchain stack. In paragraaf 11.4. wordt verder ingegaan op de beloften die internet indertijd deed, en de manier waarop blockchain deze beloften in zou kunnen willigen. Hierna wordt in paragraaf 11.5 dieper ingegaan op de verschillende technologische ontwikkelingen die tot blockchain hebben geleidt. Het hoofdstuk wordt afgesloten met een paragraaf waarin een samenvatting en de gebruikte begrippen en bronnen worden genoemd.

11.2 De technologische ontwikkeling van communicatiemiddelen en het internet

Internet is gebaseerd op communicatiesystemen als radiogolven en computers. Wat volgt is een overzicht van de technologische ontwikkelingen die hebben geleid tot het internet en die daarmee ook de grootschalige communicatie tussen individuen mogelijk hebben gemaakt.

1836	Morse, Henry en Vail ontwikkelen het telegrafiesysteem.
1876	Bell patenteert de elektrische telefoon.
1889	Hertz ontdekt elektromagnetische golven.
1902	Marconi stuurt met een telegraaf het eerste radiobericht over de Atlantische oceaan via elektromagnetische golven.
1941	Eerste elektrische computer wordt ontwikkeld.

Hiermee werden de condities gekweekt voor de ontwikkeling van het internet. Het internet zelf is een netwerk waarin apparaten met elkaar verbonden zijn en data met elkaar kunnen uitwisselen. Dit is iets anders dan de ontwikkeling van het ***World Wide Web***, ook wel WWW of het web genoemd. Deze laatste is een informatiemedium dat bereikbaar is via computers die met het internet zijn verbonden. Het internet kent een langere geschiedenis dan het web.

11.2.1 Internet

In de jaren 60 wordt internet als een decentrale technologie ontwikkeld om ervoor te zorgen dat het militaire communicatienetwerk snel gegevens uit kon wisselen op een manier die niet eenvoudig uit de lucht te halen was. Andere belanghebbenden pikten deze ontwikkeling op en verbreidden het netwerk van verbonden apparaten. Zo zagen wetenschappers en visionairs dat er meer potentie zat in een systeem waarin op decentrale wijze informatie kon worden uitgewisseld tussen iedereen die verbonden was. Hieronder volgt een lijst met enkele sleutelmomenten in de ontwikkeling van het internet.

1945	Vannevar Bush publiceert het idee van een memex waarin je brein linken legt tussen informatie door associatie met andere informatie, en niet door het opzoeken van informatie door bijvoorbeeld indexen. Het concept van de memex heeft de ontwikkeling van vroege hypertextsystemen beïnvloed. Het heeft dus indirect een invloed gehad op de creatie van het WWW.
1958	De Verenigde Staten zet het ***Advanced Research Projects Agency*** op (ARPA) om militaire technologieën te ontwikkelen.[126] ARPA is later de voornaamste aanjager van

[126] ARPA veranderde later in het Defense Advanced Research Projects Agency (DARPA).

internet, hoewel het idee mede door anderen buiten ARPA is ontwikkeld. ARPA heeft onder andere het initiatief genomen om mainframes van militaire instanties, militaire leveranciers, universiteiten en overheidsinstanties informatie met elkaar uit te laten wisselen. Het idee ontwikkelt zich gedurende de komende jaren tot een decentraal systeem waarbinnen informatiepakketten via de snelste route worden uitgewisseld.

1963 Ted Nelson ontwikkelt een model waarmee informatie wordt gemaakt en aan elkaar gelinkt. Hij noemt hier ook het begrip ***hypertext***, een manier om informatie met elkaar te delen.

1964 Paul Baran beschrijft een gedistribueerd netwerk als alternatief van een gecentraliseerd netwerk in het artikel, 'On Distributed Communications' (1964). Hierin stelt hij dat een gedistribueerd netwerk minder vatbaar is voor aanvallen en voorziet hij dat data in blokken opgedeeld kunnen worden alsvorens ze worden verstuurd door het netwerk.

1968 Douglas Engelbart demonstreert een computersysteem dat onder andere gebruik maakt van een grafische interface, video conferencing, muis, tekstverwerker en hypertext.

1969 Twee computers wisselen voor de eerste keer gegevens met elkaar uit wat heeft geleid tot ***ARPANET***, de eerste versie van internet. Het aantal verbonden militaire en universitaire computers neemt hierna gestaag toe. ARPA gebruikt het ook om onderzoekers van de ene instelling computerprogramma's van andere instellingen op afstand te laten gebruiken om samenwerkingskosten te drukken.

1971 Eerste microprocessor wordt in series geproduceerd. Microprocessoren zorgen ervoor dat computers goedkoper en kleiner kunnen worden gemaakt.

1971 De eerste e-mail wordt gestuurd over het ARPANET. E-mail wordt gezien als de killerapplicatie van het internet.

1973 Het woord "internet" wordt door Robert Kahn en Vinton Cerf genoemd als afkorting van inter-networking. Beiden werken aan ARPANET.

1974 Robert Kahn en Vinton Cerf ontwikkelen het ***Transmission Control Protocol*** (TCP) en het ***Internet Protocol*** (IP), samen bekend als TCP/IP. Met dit protocol worden gegevens in kleine pakketjes verstuurd naar een node die de pakketjes in de juiste volgorde plaatst om er een éénduidig informatiepakket van te vormen. TCP/IP wordt later een wereldwijde standaard waarmee op dezelfde manier data worden uitgewisseld over het internet.

1979 ***Usenet*** wordt ontwikkeld als netwerk voor de uitwisseling van berichten. Deze berichten zijn onderverdeeld in nieuwsgroepen.

1982 Carnegie Mellon University wetenschappers sluiten een lokale Coca-Cola machine aan het internet waardoor ze op afstand informatie kunnen ophalen over de voorraad en het tijdstip waarop nieuwe drank koud is om te drinken. Dit was de eerste realisatie van het Internet of Things.

Afbeelding 105: De eerste praktische applicatie van een IoT apparaat op Carnegie Mellon Universiteit (Maxey, 2016).

1983 Paul Mockapetris en Jon Postel ontwikkelen het Internet ***Domain Name System*** (DNS), een protocol om IP-adressen te vertalen naar makkelijk te onthouden domeinnamen.

1990 ARPANET wordt beëindigd.

11.2.2 Web 1.0

Wetenschappers en visionairs ondersteunden een decentrale ontwikkeling waarbij informatie gemakkelijk kon worden gedeeld met elkaar. Dit leidde tot ***Web 1.0***, een web dat voortkwam uit het gedachtegoed dat elk individu het recht heeft op vrijheid, zelfbeschikking en vrijheid van meningsuiting. Wat volgt zijn belangrijke ontwikkelingen binnen Web 1.0.

1990 Internet wordt tot dan toe vooral gebruikt door wetenschappers en bibliotheken om elkaars computers te bereiken. Dit gebeurde echter nog niet op een gebruiksvriendelijke manier. Grote bestanden konden daarnaast niet via e-mail of de dan bestaande netwerken worden verspreid, wel via diskettes. Om dit te overwinnen, ontwikkelt Tim Berners-Lee het World Wide Web (WWW). Het WWW is gebaseerd op de internetinfrastructuur die voornamelijk via ARPA was ontwikkeld. Berners-Lee koppelde standaarden als TCP/IP, hypertext en DNS aan zelf ontwikkelde universele standaarden zoals het ***Hypertext Transfer Protocol*** (HTTP). Dit protocol maakt het mogelijk voor een webbrowser om ***Hypertext Markup Language*** (HTML) documenten, een andere uitvinding uit 1992, op te vragen van een server. Er wordt

daarnaast ook gebruik gemaakt van ***Uniform Resource Identifiers*** (URI) die een unieke benaming van een bron of stuk informatie zijn. Een voorbeeld van een URI is de ***Uniform Resource Locator*** (URL) waar https://www.saxion.nl/onderzoek/meer-onderzoek/blockchain een voorbeeld van is. Daarnaast maakt het WWW mogelijk dat een server de opgevraagde HTML-documenten terugstuurt naar de client. Hiermee kan de overdracht en het vertonen van webpagina's worden georganiseerd. Door het intikken van webadressen in een webbrowser, krijg je webpagina's te zien. Door het klikken op links, surf je gebruiksvriendelijk naar andere informatie. Hierdoor kun je nu zonder veel technische kennis van het internet gebruikmaken. Deze gebruiksvriendelijkheid heeft ervoor gezorgd dat het aantal gebruikers sterk toenam.

Afbeelding 106: Het World Wide Web draaide op deze eerste NEXTcube webserver uit 1990 (CERN, z.d.).

Berners-Lee was zich bewust van de noodzaak tot samenwerking. Hij zag het WWW als een manier om informatie open en democratisch te verdelen zodat iedereen de vruchten kan plukken van samenwerking. Zijn werkgever, De Europese Raad van Kernonderzoek (***CERN***) ondersteunde dit en maakte de ontwikkelde internettechnologieën open source.

1991 Tim Berners-Lee maakt de eerste website. Hiermee ontstaat Web 1.0, wat gekenmerkt wordt door statische websites.

1992 Tim Berners-Lee ontwikkelt de programmeertaal, Hypertext Markup Language (HTML), om HTML-documenten op te maken zodat ze overzichtelijk kunnen worden gepresenteerd in een webbrowser. Webbrowsers vragen HTML-documenten van servers en geven deze weer in de vorm van webpagina's.

1993 Marc Andreessen en Eric Bina nemen het idee verder en organiseren grafische informatie, video's en geluid door bovenstaande en andere protocollen te laten samenwerken in de eerste grafische webbrowser - NCSA Mosaic. Mosaic, gevolgd door Netscape in 1994, was laagdrempelig om te gebruiken en open source. Hiermee

	werd het internet naar de massa gebracht. Nu kon iedereen eenvoudig van pagina naar pagina gaan. In lijn hiermee worden de eerste zoekmachines gebouwd.
1994	Oprichting van het ***World Wide Web Consortium*** (W3C) door onder andere Tim Berners-Lee, ***DARPA***, MIT en de Europese Commissie om webstandaarden te bevorderen. Deze standaarden zijn rechtenvrij zodat adoptie wordt bespoedigd. Het W3C is niet de eerste organisatie die probeert webstandaarden en protocollen af te spreken. De ***Internet Engineering Task Force*** (IETF) is sinds 1987 de prominentste ontwikkelaar en supporter van open standaarden.
1998	Vanaf het begin van ARPANET werd het vergeven van IP-adressen gecoördineerd door Jon Postel, een computer wetenschapper die mede betrokken was bij ARPANET. De organisatie waar Postel voor werkt, de non-profit ***Internet Corporation for Assigned Names and Numbers*** (ICANN), krijgt verantwoordelijkheid over de coördinatie van DNS-adressen en over de taken van het ***Internet Assigned Numbers Authority*** (IANA). De taken van IANA omvatten onder andere het onderhoud van een bestand met DNS-gegevens en de gerelateerde URL's verricht door de ICANN.
2016	In oktober worden de laatste IANA-functies overgedragen aan de globale internet gemeenschap.

11.2.3 Web 2.0

Vele webprotocollen die werden ontwikkeld, waren open en werden gebruikt voor de ontwikkeling van ***Web 2.0***. Tim O'Reilly (2005) omschreef Web 2.0 als een web voor oprechte interactie tussen gebruikers, omdat mensen zowel informatie kunnen uploaden als downloaden. Waar Web 1.0 vooral HTML gebruikte, werd deze binnen Web 2.0 uitgebreid met nieuwe technologieën die applicaties interactiever maken. De programmeertaal ***JavaScript*** en ***AJAX*** hebben hierin een grote rol gespeeld. Webscripts kunnen op een deel van de pagina worden geladen, zonder dat de gehele pagina hoeft te worden ververst. Hierbinnen verschuiven het web en internet van een wat meer technisch niche netwerk naar een gebruiksvriendelijke manier voor mensen en organisaties om met elkaar te communiceren en samen te werken. Social media, blogging, chats, wiki's, filesharing en e-commerce komen onder andere op. De grootte van het web neemt exponentieel toe nu meer mensen content maken en delen met elkaar. Dit gebeurt op goedkopere en snellere manieren, zodat onderwijsinstellingen, bedrijven en thuisgebruikers het netwerk ook kunnen gebruiken om bijvoorbeeld onderzoek te delen, de bibliotheektitels beschikbaar te stellen en om met stakeholders te communiceren binnen een globaal netwerk. Hiermee worden inhoudsgedreven leveranciers als nieuwsbladen, boekuitgevers, muziekproducenten, videoproducenten,

distributeurs, hotels, taxiservices en andere intermediairs meer vervangen door nieuwe internettoepassingen zoals zoekmachines, Wikipedia, professionele apps om foto's of video's te bewerken, digitale verkoopkanalen van digitale media, Alibaba, Airbnb, Uber en MonsterBoard.

Het gebruik van Web 2.0 verloopt echter vaak via commerciële tussenpartijen, stelt onder andere centrale overheden in staat om te censureren en is gevoelig voor beveiligingslekken die door kwaadwillenden kunnen worden misbruikt. In die zin lijkt het Web aan het oppervlak volledig in handen te zijn van gebruikers die inhoud maken en deelnemen, maar is het onderliggend in handen van centrale partijen die invloed kunnen uitoefenen op wat er mag worden gepubliceerd en wie er mogen deelnemen. (Henley, 2015)

Wat volgt is een opsomming van de belangrijkste ontwikkelingen binnen Web 2.0.

1997 AOL komt met instant messaging.
1999 De eerste blogs zoals Blogger.com worden gelanceerd.
2001 Apple introduceert de iPod, een gebruiksvriendelijke digitale muziekspeler.
2002 De BlackBerry 5810 wordt geïntroduceerd met toepassingen als push e-mail, tekst messaging en een webbrowser.

Afbeelding 107: De BlackBerry 5810 telefoon wordt gezien als de eerste smartphone (Segan, 2013).

2003 Skype wordt geïntroduceerd.
2004 Facebook wordt gecreëerd.
2005 YouTube brengt user-generated videocontent.
2006 Twitter lanceert microblogging.

2007	Apple introduceert de iPhone en Dropbox komt op met diensten voor cloudopslag.
2008	Spotify lanceert een online muziek streamingdienst. AirBnB en Android komen op.
2009	Het eerste Bitoin-blok wordt geproduceerd op 3 januari 2009 en Uber wordt opgericht.
2009	Berners-Lee en Rosemary Leith zetten de ***World Wide Web Foundation*** op met het streven dat deze bijdraagt aan een open web alszijnde een publiek goed en een basisrecht voor mensen.
2010	Oprichting van Pinterest, WhatsApp, Instagram en IBM Watson. IBM Watson is een computersysteem dat in staat is om op basis van grote hoeveelheden data en zelflerende algoritmes analyses uit te voeren. Momenteel wordt het mede ingezet voor analyses van investeringskansen tot het herkennen van kanker metastasen.
2011	Snapchat gelanceerd en Apple Siri uitgerold.
2016	Onder verdere druk van andere overheden wordt de eindverantwoordelijkheid voor het IANA overgedragen van het Amerikaanse Ministerie van Commercie aan ICANN. De perikelen omtrent Amerikaanse surveillance, zoals ook is gebleken uit Edward Snowdens gelekte documenten in 2013, hebben een rol gespeeld in de transitie.

11.2.4 Web 3.0

Blockchain is een belangrijke technologie binnen ***Web 3.0***, omdat het dataopslag decentraliseert en de client-serverrelatie naar een gelijkwaardiger peer-to-peerrelatie brengt. Web 3.0 lijkt hierdoor de belofte die het web in beginsel uitdroeg te kunnen realiseren. Dit wordt later in dit hoofdstuk uitvoeriger besproken. Web 3.0 zal naast blockchain ook gebruikmaken van onder andere een semantisch web, kunstmatige intelligentie, datamijnen, virtual reality en augmented reality. Deze combinatie van verschillende technologieën wordt ook wel de ***digital mesh*** genoemd.

Een aantal voordelen van Web 3.0 ten opzichte van Web 2.0 zijn:

1. Er zullen geen tussenpartijen zijn die jouw persoonlijke gegevens beheren zonder jouw toestemming. Je kunt zelf toestaan welke persoonlijke gegevens je wil laat vastleggen of delen met andere partijen.
2. Er zullen minder datalekken zijn, omdat gegevens gedistribueerd zijn over een gedecentraliseerd netwerk als blockchain.
3. Er zal minder censuur zijn, omdat de gegevens die zijn bewaard op een blockchain haast niet te censureren of te verwijderen valt.
4. Er zal minder uitval zijn van internetdiensten, omdat een gedecentraliseerd systeem haast niet aan te vallen is met bijvoorbeeld een ***DDoS-aanval***. Een dergelijk systeem heeft van nature meerdere back-ups. Gegevens worden hierdoor continu verwerkt.

Zoekmachines zullen de acties die jij op het web neemt, gebruiken om meer te leren over jou en op basis daarvan op een slimme wijze resultaten tonen die passen bij jouw profiel.

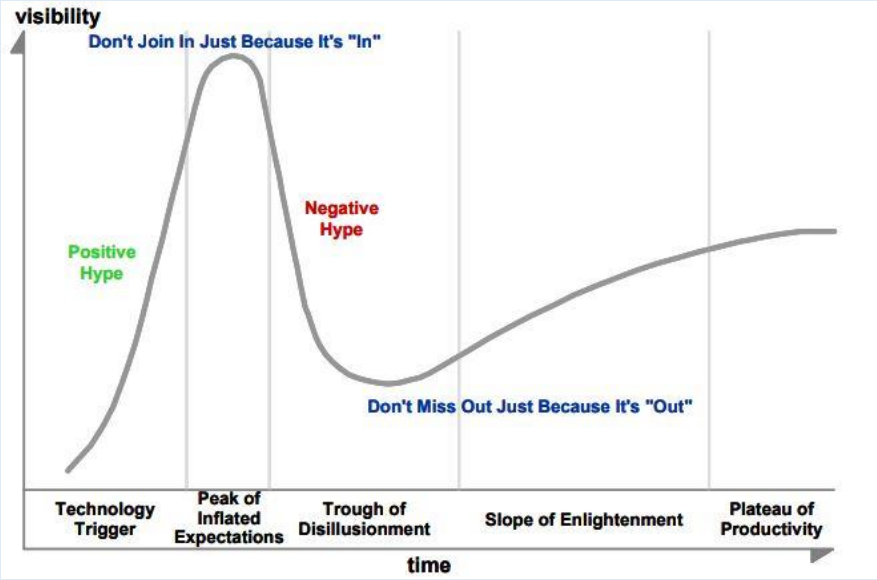
Hieronder vind je een vergelijkingstabel tussen Web 1.0, Web 2.0 en Web 3.0.

Web 1.0	Web 2.0	Web 3.0
Het Web	Het Sociale Web	Het Semantische Web
Informatie delen	Interactie	Immersie
Informatie verbinden	Mensen verbinden	Context, mensen en kennis verbinden
Gebruiker leest content	Gebruiker creëert en deelt content	Content wordt geconsolideerd en gepersonaliseerd
Statische content, interactie is eenrichtingsverkeer	Sociale content, interactie is tweerichtingsverkeer	Visualisatie
Web Forms	Web Applications	Smart Applications
Analogie: Britannica Online	Analogie: Wikipedia	Analogie: Semantisch Web

Tabel 4: Vergelijking tussen Web 1.0, Web 2.0 en Web 3.0.

Intermezzo: Gartner Hype Cycle voor blockchain

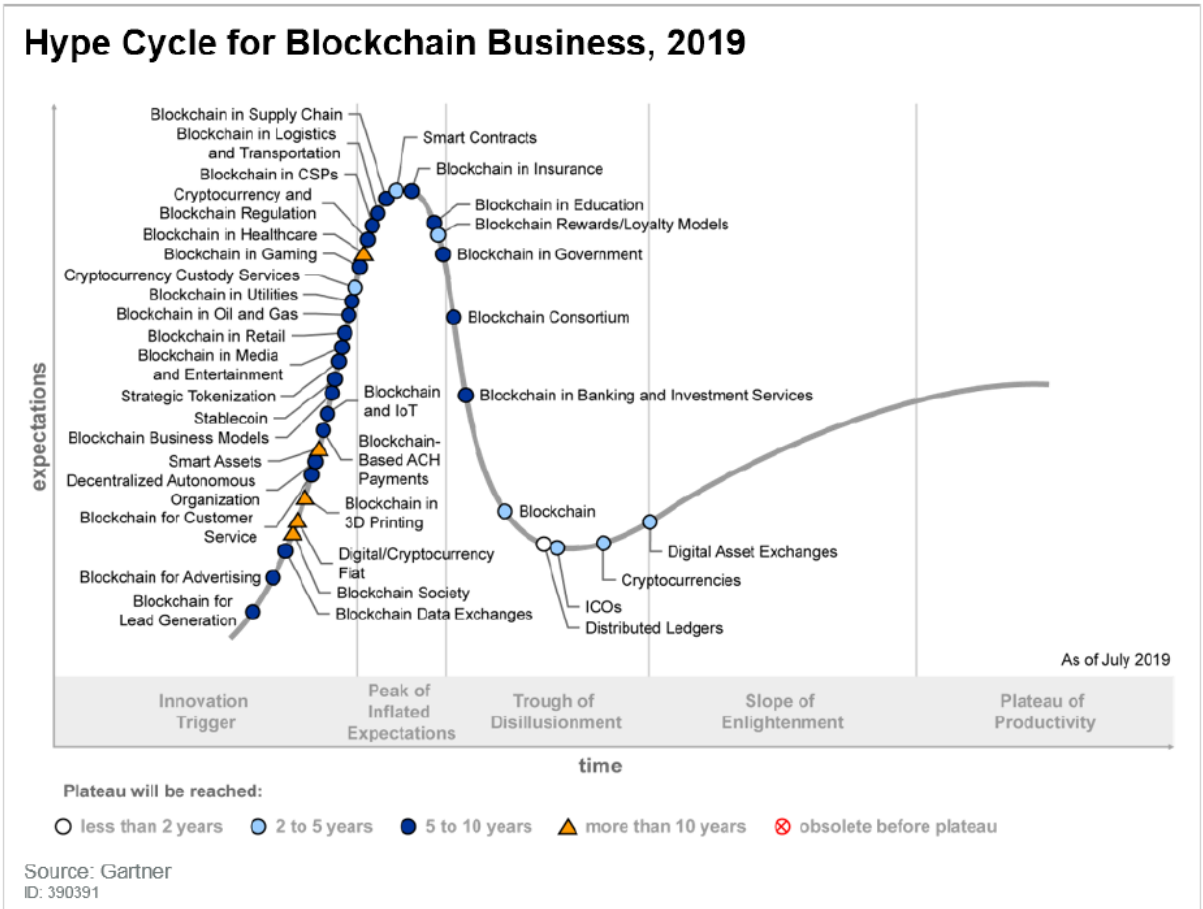
Een bekend model om te kijken hoe een nieuwe, beloftevolle technologie een product in een volwassen markt wordt, is beschreven in het ***Gartner Hype Cycle-***model. Dit model toont dat deze producten de volgende vijf fasen doorlopen.



Afbeelding 108: De Hype Curve (Linden & Fenn, 2003).

1. *Technology Trigger*: de technologie is vooral een technologische doorbraak die nog niet wordt gebruikt in producten. Het krijgt echter wel aandacht van de pers.
2. *Peak of Inflated Expectations*: er zijn grote verwachtingen omtrent de technologie.
3. *Trough of Disillusionment*: de hype deflateert en er vindt eenzelfde overtrokken reactie plaats, maar in negatieve zin. Media is negatief, bedrijven trekken weg, de teleurstelling is groot en er wordt steeds meer getwijfeld of de technologie zal overleven.
4. *Slope of Enlightenment*: investeringen nemen toe en er worden nieuwe producten ontwikkeld op basis van de technologie. Adopties beginnen op grotere schaal plaats te vinden.
5. *Plateau of Productivity*: de voordelen van de technologie zijn duidelijk en de technologie wordt breed toegepast in producten. 20-30% van het publiek adopteert de innovatie.

De Gartner Hype Cycle is een handig model die discussies uitlokt in hoeverre een opkomende technologie een hype is. Het model is echter niet gebaseerd op de wetenschappelijke methode. Steinert en Leifer (2010) bekritiseren dit en stellen aan Gartner voor het model te onderbouwen met een wiskundig model, zodat Gartner de eigen analyses kwantitatief kan onderbouwen.



Afbeelding 109: Volgens Gartner gaat blockchain in 2019 door de fase van Trough of Dilussionment (Gartner, 2019).

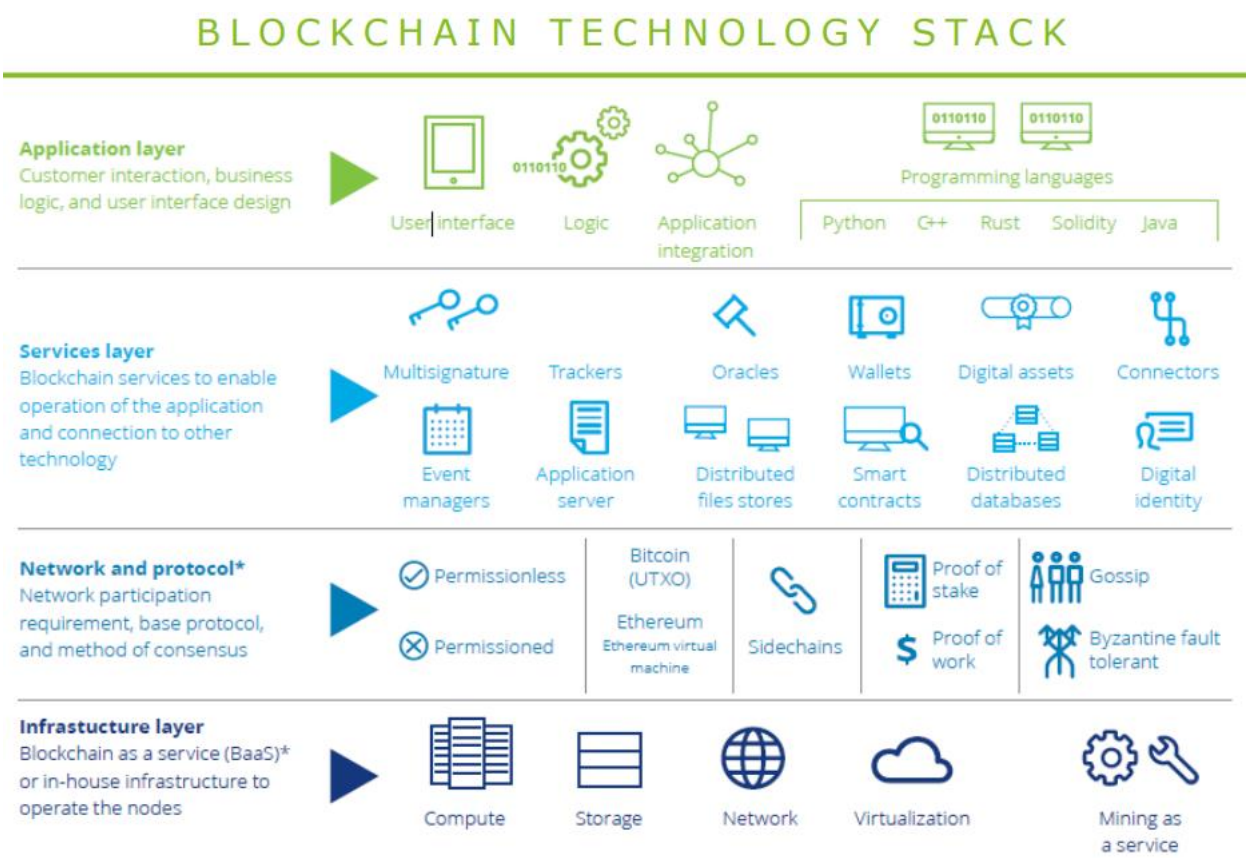
Blockchain gaat volgens Gartner in 2019 door de fase van het Through of Disillusionment, maar zal een transformatieve impact hebben op vele industrieën in 5 tot 10 jaar. De voornaamste industrieën die de grootste impact van blockchain zullen ondervinden, zijn volgens Gartner het bank- en investeringswezen, gaming en retail. Er wordt verwacht dat de ontwikkelingen in de creatie en acceptatie van digitale tokens onder andere door zal zetten en disruptief kan zijn binnen het bank- en investeringswezen. Deze tokens bieden gamers ook meer controle over hun in-game items en zal ze ook transporteerbaar maken van het ene gamingplatform naar het andere. In de retail zal blockchain een grote invloed hebben op het traceability-aspect. Ook zal het wijder verspreid worden toegepast in combinatie met het Internet of Things and Artificial Intelligence om retail businessmodellen radicaal te veranderen. (Gartner, 2019)

De potentie van blockchain en Web 3.0 is zo groot, dat het de verwachting is dat deze tot breed gebruikte toepassingen zullen leiden. Zolang deze toepassingen er niet zijn, bestaat het gevaar van te grote beloften die niet snel genoeg kunnen worden geleverd.

11.3 Blockchain technology stack

Een ***technology stack*** is een combinatie van verschillende technologieën die een applicatie mogelijk maakt. In het geval van blockchaintechnologie, bestaat de technology stack uit vier lagen (Deloitte, 2017). Deze lagen zijn:

1. *Applicatielaag*. In deze laag bevindt zich de user interface, bedrijfslogica en de klanteninteractie. Onderdelen hiervan zijn ook programmeertalen als bijvoorbeeld Solidity, waarmee dApps kunnen worden ontwikkeld.
2. *Services laag*. In deze laag bevinden zich blockchainservices die de operatie van applicaties en connecties met andere technologieën mogelijk maken. Onderdelen hiervan zijn bijvoorbeeld wallets, public en private keys, smart contracs, orakels en digitale identiteiten.
3. *Netwerk- en protocollaag*. In deze laag bevinden zich protocollen en netwerkvereisten om deel te mogen nemen aan de blockchain. Onderdelen hiervan zijn bijvoorbeeld de consensusmechanismen als Proof-of-Work en Proof-of-Stake en de governancestructuur van een blockchain.
4. *Infrastructuurlaag*. In deze laag bevindt zich de onderliggende, vaak fysieke, infrastructuur die benodigd is om een blockchain op te draaien. Onderdelen hiervan zijn bijvoorbeeld servers en mijningapparatuur.



Afbeelding 110: De vier lagen van de blockchain technology stack (Deloitte, 2017).

11.4 De beloften van internet

De beloften van internet, zoals die werden uitgesproken door verscheidene cryptografen en techno-libertariërs, omvatten begrippen als het hebben van:

- één groot netwerk van verbonden individuen
- die direct onderling
- op een veilige manier
- informatie ongecensureerd uitwisselen.

John Perry Barlow, één van de oprichters uit 1990 van de digitalerechtengroep ***Electronic Frontier Foundation***[127], vulde dit in 1996 aan via zijn 'A Declaration of the Independence of Cyberspace'. Dit artikel was mede geschreven naar aanleiding van stringentere wetgeving van het Amerikaanse Congress binnen de 1995 Telecommunications Act. Barlow ziet cyberspace als een grenzeloze omgeving waarin iedereen welkom is en soeverein kan participeren. Deze grenzeloze omgeving is er één waarin de wereld humaner en eerlijker is dan de fysieke wereld die door overheden is gebouwd. Simone Ross noemt dit een techno-utopie waarin individuele vrijheid is verzekerd en sociale, economische en politieke grenzen vervagen. De techno-utopie zoals die is voorzien door Barlow zou idealiter leiden tot een democratisering van alles en een welvarendere, gezondere, rechtvaardigere samenleving waarin ook fysieke en virtuele grenzen vervagen (Ross, 2017).

Internet heeft de belofte kunnen nakomen om mensen in verbinding te brengen met elkaar, zodat ze informatie kunnen uitwisselen. De meerderheid van de mensen heeft nu op een redelijk veilige manier toegang tot internet. De techno-utopie die is beschreven door Barlow is echter geen werkelijkheid geworden.

11.4.1 De beloften die internet niet is nagekomen

Het gebruik van Web 2.0 verloopt vaak via grote commerciële tussenpartijen. Data worden grotendeels opgeslagen op centrale hardware. De data zijn vaak in handen van een kleine groep dominante semi-monopolistische bedrijven, zoals beursgenoteerde Amerikaanse socialmediabedrijven en door de staat gecontroleerde Chinese bedrijven als Alibaba en Tencent. Zij kunnen hierdoor niet alleen de informatie van gebruikers inzien, maar ook aangeven wat gebruikers wel en niet kunnen zien. Ook is het mogelijk dat de informatie die je te zien krijgt is gemanipuleerd. Hieruit kun je afleiden dat de data die je geeft niet altijd geheel

[127] In Nederland kent de Bits of Freedom groep uit 2000 een vergelijkbare missie.

in je eigen bezit zijn. Web 2.0 is daardoor zeer gevoelig voor censuur. Naast het feit dat je een derde partij moet vertrouwen dat deze zorgvuldig omgaat met jouw data, kosten tussenpartijen ook tijd en geld.

De overheid is zelf trouwens ook een tussenpartij. Zo wordt binnen het Chinese Social Credit Rating systeem per bevolkingslid een score bijgehouden aan de hand van het gewenste sociale gedrag dat ze zowel offline als online vertonen. Sommige overheden verbannen bepaalde socialmedia-applicaties of nieuwssites zoals tijdens de Arabische Lente. In andere landen, zoals in de Verenigde Staten, probeert de overheid encryptie te verzwakken. De Amerikaanse overheid heeft dit bijvoorbeeld geprobeerd bij de iPhone.[128] Ook kan een overheid bedrijven dwingen om informatie over hun gebruikers te delen. Daarnaast hebben kwaadwillenden een arsenaal van instrumenten, zoals bijvoorbeeld phishing, DDoS-aanvallen en ***man-in-the-middle-aanvallen***, waarmee ze jouw internetgedrag kunnen verstoren, of jouw persoonlijke data kunnen stelen. Het web is dus vooralsnog niet in staat om goede beveiliging en daarmee ook grote internetvrijheid te bieden aan iedereen. De zeer gecentraliseerde opzet van Web 2.0 is hiervan één van de belangrijkste oorzaken. Binnen het idee van totale vrijheid van meningsuiting past ook het begrip Internet of Information. Het huidige internet is tot op zekere hoogte niet in staat om de belofte van een Internet of Value na te komen. Het is momenteel niet transparant welke partijen zijn betrokken bij een transactie, onder welke voorwaarden ze de gebruikersdata beheren en in hoeverre we erop kunnen vertrouwen dat ze zich houden aan de voorwaarden die gedurende de transactie worden gesteld.

De sleutel tot het terugkrijgen van controle lijkt te liggen in het analyseren en beheersen van de data die dankzij internet worden gecreëerd. De omvang van data op het internet neemt toe door onder andere IoT. Daarmee neemt ook het belang om data te analyseren, te beheersen om er geld mee te verdienen en de veiligheid van ingezetenen te waarborgen toe. Data staan dus centraal en daarmee ook de algoritmes die meer data verzamelen, analyseren en weer tot actie aanzetten. Hiermee wordt ook het vertrouwen in code en algoritme belangrijker. De vraag is echter, is alle code transparant? Is het correct geschreven? Streeft het de doelen na waar we achter staan? Ook hier kun je zeggen dat internet de belofte niet nakomt: het is niet altijd transparant welke partijen betrokken zijn bij je dataverkeer en met welke code zij je met welke motieven ondersteunen in dat dataverkeer. Als je data worden gestolen, hoe weet je dat dan

[128] Na de aanslagen in San Bernardino, waarin 14 mensen overleden, heeft de FBI geprobeerd om Apple zover te krijgen om een backdoor in de iOS-software te implementeren. Apple heeft dit geweigerd, omdat het de beveiliging van de iPhones en de privacy van haar gebruikers op het spel zou zetten. (Kahney, 2019)

tijdig? Zoals eerder gezegd heeft blockchain hier veel potentie, omdat het data niet in gecentraliseerde servers wil plaatsen, maar wil decentraliseren. Ook kan het worden toegepast om de Public Key Infrastructuur te decentraliseren en hiermee de afhankelijkheid van certificerende autoriteiten te verminderen.[129] Het biedt ook mogelijkheden om soevereine digitale identiteiten te creëren en meer controle te krijgen over welke data je met wie deelt. Ook is blockchain in staat om verschillende partijen van verschillende disciplines met elkaar samen te laten werken. Immers, de voorwaarde om elkaar altijd te kennen en te vertrouwen om samen te werken, is vervallen. Dit leidt potentieel tot geheel nieuwe samenwerkingen, zoals de DAO die anders zijn dan traditionele organisatiestructuren. Deze nieuwe samenwerkingen leiden op hun beurt weer tot innovaties die platgetreden paden als business control audits of standard operating procedures teniet kunnen doen of kunnen vervangen.

11.4.2 Belang van privacy

Zoals eerder verteld, is data privacy van cruciaal belang gezien de rol die sommige tussenpartijen momenteel spelen in het beïnvloeden van het individu. Een winstgedreven partij zal eerder op een kruispunt komen waarin het moet beslissen tussen het langs de grens schaven van het vermarkten van persoonlijke individuele data ten gunste van de winst, of ten nadele van privacy. Ook al zijn data binnen de digitale wereld mogelijk een diep persoonlijke reflectie van wie iemand is, het betreffende individu heeft deze reflectie misschien nog niet zelf kunnen maken. Hij wordt echter wel geconfronteerd met een technologie die zijn beslissingen beïnvloedt, terwijl de motieven van de inzet van deze technologieën misschien niet volledig transparant zijn voor hem. Als je als gebruiker niet weet in hoeverre data die je tegenkomt op internet volledig of juist is, vertrouw je er op internet dan op dat mensen zijn wie ze zeggen dat ze zijn? Deze gewaarborgde digitale identiteit is van belang, omdat het je in staat stelt aan te geven dat je bestaat, dat je mening authentiek is, dat digitale data die hieraan zijn gekoppeld bij jou horen en dat het jouw kleur ogen, leeftijd, salaris, partner, huis en paspoort betreffen. Bedenk dat het ook niet mogelijk is dat een product in de fysieke wereld een waterdichte digitale identiteit heeft. Dit bemoeilijkt ook het onomstotelijk aantonen dat je in het bezit bent van het product en recht hebt om de eigendom hierover over te dragen naar een andere persoon.

Blockchain heeft de potentie om met behulp van een gedecentraliseerde database en cryptografie digitale data wel veilig en privaat te maken en te houden. Dit wordt door

[129] Zie ook het intermezzo, 'Public key Infrastructuur (PKI)', in hoofdstuk 5.

sommigen gezien als een Recht van de Mens.[130] In hoofdstuk 12 wordt teruggekomen op de digitale identiteit.

11.4.3 De belofte van internet die blockchain nakomt

Blockchain kan in opzet een decentraal netwerk zonder tussenpartij ondersteunen, om direct onderling en veilig informatie of waarde uit te wisselen. Bepaalde huidige internetstandaarden en -diensten als DNS en ICANN kunnen mogelijk decentraal worden geregeld. Ook kan blockchain de Public Key Infrastructuur decentraliseren, zodat de nood tot centrale derde partijen die nu certificaten uitgeven en public keys authentiseren en distribueren kan worden voorkomen.

Met de hulp van blockchain wordt binnen Web 3.0 ook de data decentraal en versleuteld opgeslagen. De belofte van Web 3.0 is dat het de gebruiker in staat stelt om zelf te bepalen welke persoonlijke data hij laat vastleggen of deelt. De gebruiker heeft dus meer zeggenschap over de mate waarin hij anoniem blijft op het internet. Tussenpartijen worden steeds meer vervangen door directe peer-to-peerhandelingen tussen gebruikers. Dit versterkt weer de decentrale deeleconomie. Gemeenschapsinitiatieven kunnen decentraal worden ingericht, omdat blockchain ze helpt met anonimiteit, sterkere privacy, transparantie en waar nodig een structureel robuuster en veiliger netwerk.

Om een voorbeeld te geven hoe blockchain de initiële belofte van vrijheid van meningsuiting en het delen van informatie ongecensureerd bevordert, kan je denken aan de volgende situatie:

1. Je wil je politieke mening delen op social media.
2. Via een ratingsysteem van nieuwsleveranciers als onderdeel van je social media krijg je meer vertrouwen in de opinie van bloggers en journalisten. Deze leveranciers zijn al dan niet anoniem, maar je kunt wel zien in hoeverre zij zelf weer betrouwbaar worden geacht en door wie.
3. Met deze partijen, die je al dan niet kent, zou je inhoudelijke posts voor een bepaalde mening of partij kunnen organiseren.
4. Tijdens het delen van jouw inhoudelijke posts, bewaar jij je persoonlijke data in een persoonlijke wallet en kun je ervoor kiezen om bepaalde data vrijelijk te delen of niet. Je kunt inbouwen dat berichten onleesbaar zijn voor sommigen, of dat je je data al dan niet verkoopt of beschikbaar stelt voor bijvoorbeeld wetenschappelijk onderzoek.

[130] Hu-manity.co gelooft bijvoorbeeld dat ieder mens het eigendomsrecht heeft over zijn eigen data.

5. Met behulp van smart contracts zou je dan data tussen socialmediaplatforms kunnen delen, zonder dat je te veel data van jezelf weggeeft. Je kan ook instellen dat je post na een bepaalde tijd automatisch ongezien wordt gemaakt.
6. Tot slot is je post niet te censureren, omdat er geen centrale partij is die controle heeft over de opslag van jouw post.

11.5 Technologische ontwikkelingen leidend tot blockchain

De onderstaande ontwikkelingen hebben bijgedragen aan de totstandkoming van blockchaintechnologie.

1970	Filesharing en andere voorlopers van decentrale P2P netwerken worden binnen meerdere initiatieven ontwikkeld.
1975	De Data Encryption Standard (DES), ontwikkeld door IBM en na consult met de National Bureau Standard (NBS) en de National Security Agency (NSA), komt op de markt.
1976	Whitfield Diffie en Martin Hellman publiceren ‘New Directions in Cryptography’. Hierin presenteren zij het concept van public key cryptografie. Kort erop ontwikkelen zij het Diffie-Hellman-sleuteluitwisselingsprotocol waarmee public key cryptografie kon worden toegepast. Daarnaast beschrijven zij het concept van digitale handtekeningen zonder deze te hebben geïmplementeerd in een toepassing.
1978	Ron Rivest, Adi Shamir en Leonard Adleman ontwerpen een eigen public key cryptosysteem, genaamd het RSA. Het doel van het systeem is tweeledig: (a) het waarborgen van privacy in elektronische communicatie en (b) het kunnen plaatsen van digitale handtekeningen. Het systeem werd voor het eerst gepresenteerd in het artikel, ‘A Method for Obtaining Digital Signatures and Public-Key Cryptosystems’.
1979	Ralph Merkle ontwikkelt Merkle trees.
1983	David Chaum publiceert het artikel ‘Blind Signatures for untraceable Payments’ waarin hij uitlegt dat elektronische betalingssystemen een substantiële impact zal hebben op privacy. Chaum presenteert in het artikel hoe blind signatures gebruikt kunnen worden om transacties anoniem te maken.
1989	DigiCash Inc. wordt opgezet door David Chaum op basis van zijn wetenschappelijk artikel uit 1983. Chaum implementeert blind signature technologie in DigiCash om anonieme monetaire transacties mogelijk te maken.
1992	Cynthia Dwork en Moni Naor ontwikkelen het Proof-of-Work concept om spammail te voorkomen. Het concept is gepresenteerd in het artikel ‘Pricing via Processing or Combatting Junk Mail’ (1993). Hierin beschrijven zij een mailsysteem dat de verzender van de e-mail verplicht om eerst een rekenkundige functie op te lossen voordat de e-

	mail mag worden verstuurd. De functie is eenvoudig genoeg dat een computer het binnen korte tijd kan oplossen, maar is ook moeilijk genoeg voor een spamcomputer dat die aanzienlijk veel computerkracht moet verbruiken om grote hoeveelheden e-mails tegelijkertijd uit te sturen. Deze functie noemen zij een prijsfunctie.
1997	Adam Back presenteert Hashcash in het artikel 'Hashcash – A Denial of Service Counter-Measure'. Hashcash is een Proof-of-Work-systeem om e-mail spam en denial-of-service aanvallen te voorkomen. Satoshi Nakamoto zou later de Hashcash Proof-of-Work-functie gebruiken voor Bitcoin.
1997	Nick Szabo introduceert smart contracts in het artikel, 'Formalizing and Securing Relationships on Public Network'.
1998	Wei Dai introduceert B-money, een gedistribueerd geldsysteem dat onder andere gebruik maakt van Proof-of-Work, een collectief grootboek, beloningen voor het onderhouden van dit grootboek en het forceren en uitzenden van contracten op basis van digitale handtekeningen. Satoshi Nakamoto refereert later in zijn Bitcoin white paper naar het artikel van Wei Dai over B-money.
1998	Nick Szabo introduceert Proof-of-Work in een gedecentraliseerd digitale geldmiddel, de Bit Gold, om het double-spending probleem aan te pakken. Bit Gold is echter nooit uitgerold.
1999	Practical Byzantine Fault Tolerance Practical (pBFT) wordt geïntroduceerd door Miguel Castro en Barbara Liskov in het artikel 'Practical Byzantine Fault Tolerance'.
2001	Filesharing programma's, Kazaa en BitTorrent, ontwikkelen gedecentraliseerde peer-to-peersystemen gebaseerd op cryptografie. Dit zijn robuuste systemen waar bestanden op pseudoanonieme wijze efficiënt kunnen worden gedeeld. Deze systemen zijn echter nog gevoelig voor virussen en je kunt er geen smart contracts aan koppelen of applicaties op ontwikkelen.
2001	De National Security Agency introduceert de SHA-2 familie, waaronder Secure Hash Algorithm (SHA)-256.
2004	Hal Finney creëert een Reusable Proof-of-Work systeem.
2008	Op 31 oktober 2008, verschijnt de white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' van Satoshi Nakamoto op een cryptografie mailing lijst.
2009	Op 3 januari 2009, creëert Nakamoto het eerste Bitcoin blok. Hij plaatst de tekst "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" in het blok. Op 12 januari stuurt Nakamoto voor het eerst 10 gecreëerde Bitcoins naar Hal Finney.

Hieruit wordt duidelijk dat blockchaintechnologie vergeleken met internettechnologie nog jong is. Het kan nog wel een decennium duren voordat het een volwassen technologie is die wijd wordt geaccepteerd. Vergelijk blockchain met de vroege jaren van het internet waarbij

initiatieven voornamelijk open source werden gedeeld en waarbij applicaties in de begindagen niet altijd even gebruiksvriendelijk waren.

11.6 Samenvatting, begrippen en bronnen

Samenvatting

In de 3e industriële revolutie organiseert internet mensen op een manier dat voorheen niet mogelijk was. Internet zorgt ervoor dat apparaten direct gegevens uit kunnen wisselen, zonder dat het netwerk eenvoudig uit de lucht te halen is. Voor sommigen, zoals techno-libertariërs, belooft het internet hierbij:

- één groot netwerk van verbonden individuen
- die direct onderling
- op een veilige manier
- informatie ongecensureerd uitwisselen.

Het internet zelf is gebaseerd op vele ontdekkingen die op elkaar voortbouwen. Uit dit internet ontstaat ook Web 1.0 die met een webbrowser en open protocollen voor massa-adoptie van internet zorgen. De ontwikkelingen binnen het web, spelen op hun beurt weer een rol bij de opkomst van blockchain. Blockchain zal weer de 4e industriële revolutie ondersteunen ten bate van technologieën als het Internet of Things, kunstmatige intelligentie, robotisering en biotechnologie.

In Web 2.0 wordt het web dynamischer en interactiever. Gegevensuitwisseling gaat echter nog steeds via tussenpartijen zoals commerciële bedrijven en centrale overheden. Hierbij worden beveiligingslekken in toenemende mate door kwaadwillenden misbruikt.

Web 3.0 reageert hierop door dataopslag te decentraliseren en het belang van de tussenpartij eruit te halen. Hierdoor zal het internet veiliger worden en censuur van tussenpartijen moeilijker. Zodoende wordt mede getracht de belofte van het internet na te komen. Hierbij zijn versleutelingen om data veilig en privaat in de handen van het individu te houden van cruciaal belang.

Opmerkingen die je nu kunt uitleggen

- Blockchain past perfect binnen de digitale revolutie in die zin dat het kruisbestuiving tussen de technologieën bewerkstelligt.
- Blockchain zelf is een voorbeeld van een digital mesh.
- Blockchain kan helpen om het Web veiliger te maken en data betrouwbaarder.
- Blockchainontwikkelingen passen logisch binnen andere technologische ontwikkelingen, zoals die binnen de 4^{e} industriële revolutie.
- Blockchain kan helpen bij de beloften van internet, bijvoorbeeld wat betreft databetrouwbaarheid, directe uitwisseling van informatie en een digitale identiteit voor objecten die in de fysieke werkelijkheid bestaan. Blockchain heeft echter ook nadelen.
- Blockchain kan helpen bij het Internet of Value.

Verklarende begrippenlijst

1e industriële revolutie: Ontwikkeling waarin mens voor het eerst substantiële hoeveelheden energie weet op te wekken en te transporteren, beginnend met de stoommachine. Deze leidde de gang van agrarische samenlevingen naar meer urbane samenlevingen in. Deze revolutie begon rond 1750 in Engeland.

2e industriële revolutie: Ontwikkeling waarin stoomkracht wordt vervangen met elektriciteit wat op een mobielere manier opgewekt en gebruikt kon worden. Daarbovenop leidde de industriële toepassing van massaproductie tot verdere schaalvergroting en goedkopere producten. Deze revolutie duurde ongeveer van 1870 – 1910.

3e industriële revolutie: Ontwikkeling die ook wel de digitale revolutie wordt genoemd. Productie raakt aanzienlijk verder geautomatiseerd en het aandeel van de dienstverlening, en daarmee communicatie, in het bruto nationaal product groeit dankzij de opkomst van elektronica, computers en het internet. Deze revolutie begon ongeveer vanaf 1950.

4e industriële revolutie: Ontwikkeling die wordt gekenmerkt door de invloed van digitale technologie op organische en biologische systemen, nanotechnologie, kunstmatige intelligentie, het Internet of Things, blockchain en andere. Deze revolutie vindt momenteel plaats.

Advanced Research Projects Agency (ARPA): Instituut van het Amerikaanse ministerie van defensie dat verantwoordelijk is voor de ontwikkeling van opkomende technologieën. ARPA heeft het ARPANET, de voorloper van het internet, ontwikkeld. De naam van het instituut veranderde in Defense Advanced Research Projects Agency (DARPA) in 1972.

AJAX: Webtechnologie om data asynchroon te versturen naar en te ontvangen van een server zodat verschillende secties van een webpagina op verschillende tijden kunnen worden ververst. Hiermee worden webpagina's dynamischer.

ARPA: Zie Advanced Research Projects Agency.

ARPANET: De voorloper van het internet die door ARPA is ontwikkeld. Het is een netwerk waarbij datapakketten tussen apparaten worden verstuurd met behulp van internetprotocollen zoals TCP en IP.

CERN: Zie Conseil Européen pour la Recherche Nucléaire.

Conseil Européen pour la Recherche Nucléaire (CERN): Europese Raad van Kernonderzoek.

Defense Advanced Research Projects Agency (DARPA): Zie Advanced Research Projects Agency.

Denial-of-Service aanval (DoS-aanval): Cyberaanval waarbij het doelwit, vaak een webserver, niet meer beschikbaar wordt gemaakt door deze te overspoelen met overtallige verzoeken.

Distributed Denial-of-Service aanval (DDoS-aanval): Hetzelfde als een DoS-aanval, alleen worden de verzoeken vanuit een netwerk van verschillende computers naar het doelwit verstuurd.

Digital mesh: Combinatie van verschillende digitale technologieën zoals blockchain, kunstmatige intelligentie en Internet of Things.

Domain Name System (DNS): Systeem waarmee namen van apparaten en diensten worden onderhouden die aan het internet zijn verbonden. Het systeem vertaalt de namen van computers naar IP-adressen.

Electronic Frontier Foundation (EFF): Amerikaanse stichting die zich bezighoudt met digitale rechten. De stichting strijdt tegen internetcensuur en voor zelfbeschikkingsrechten van internetgebruikers.

Gartner Hype Cycle: Een model dat is ontwikkeld door het IT-bedrijf, Gartner, om te kijken hoe een nieuwe, beloftevolle technologie een product in een volwassen markt wordt.

Hypertext Markup Language (HTML): Standaard opmaaktaal voor webpagina's. Documenten in HTML kunnen worden geopend en gelezen door webbrowsers. De styling van HTML-documenten wordt voornamelijk gedaan met CSS.

Hypertext Transfer Protocol (HTTP): Protocol om data te communiceren tussen een webclient en een webserver. Hierin staat vastgelegd welke verzoeken een client kan indienen bij een server en welke antwoorden de server kan teruggeven.

Hypertext: Klikbare tekst waarmee de gebruiker wordt doorverwezen naar een specifieke tekst of pagina.

Internet Assigned Numbers Authority (IANA): Amerikaanse non-profit organisatie die onder andere IP-adressen distribueert en het Domain Name System beheert. IANA is onderdeel van ICANN.

Internet Corporation for Assigned Names and Numbers (ICANN): Amerikaanse non-profitorganisatie die verschillende internet naamdatabases onderhoudt en coördineert, onder andere met behulp van IANA.

Internet Engineering Task Force (IETF): Organisatie die zich bezighoudt met internetarchitectuur en vrijwillige internetstandaarden ontwikkelt.

Internet Protocol (IP): Netwerkprotocol om data te communiceren binnen een netwerk van apparaten. IP levert datapakketten tussen apparaten op basis van IP-adressen. IP wordt vaak samen met TCP benoemd als TCP/IP.

JavaScript (JS): Programmeertaal waarmee interactieve webpagina's en webtoepassingen worden geschreven. Het is samen met HTML en CSS een van de kerntechnologieën van het WWW.

Man-in-the-middle-aanval (MITM-aanval): Aanval waarbij de aanvaller in het geheim communicatie tussen twee partijen onderschept, bekijkt, aanpast en verlegt waardoor de partijen denken dat ze direct met elkaar communiceren.

Technology stack: Combinatie van verschillende technologieën die een applicatie mogelijk maakt. In het geval van blockchaintechnologie, bestaat de technology stack uit vier lagen: infrastructuurlaag, netwerk- en protocollaag, services laag en de applicatielaag.

Transmission Control Protocol (TCP): Protocol dat gegevensoverdracht over een netwerk mogelijk maakt. Hierbij wordt de garantie geleverd dat gegevens aankomen zoals ze zijn verstuurd.

Uniform Resource Identifier (URI): Identificeert een stuk data met een unieke naam om deze te onderscheiden van andere data.

Uniform Resource Locator (URL): Identificeert de locatie van een stuk data. De URL is een vorm van de URI. Voorbeelden van URL's zijn websiteadressen zoals https://www.saxion.nl/onderzoek/meer-onderzoek/blockchain.

Usenet: Gedecentraliseerd netwerk waarbinnen bestanden en berichten worden uitgewisseld met behulp van nieuwsgroepen. Een nieuwsgroep richt zich meestal op een specifiek onderwerp.

Web 1.0: Een web dat voortkwam uit het gedachtegoed dat elk individu het recht heeft op vrijheid, zelfbeschikking en vrijheid van meningsuiting. Web 1.0 wordt gekenmerkt door statische webpagina's die worden opgemaakt door HTML.

Web 2.0: Waar Web 1.0 vooral HTML gebruikte, werd deze binnen Web 2.0 uitgebreid met nieuwe technologieën die applicaties interactiever maken. De programmeertaal JavaScript en AJAX hebben hierin een grote rol gespeeld. Webscripts kunnen op een deel van de pagina worden geladen, zonder dat de gehele pagina hoeft te worden ververst.

Web 3.0: Derde verschijningsvorm van het WWW waarin internettoepassingen gebruikmaken van onder andere een semantisch web, kunstmatige intelligentie, datamijnen, virtual reality, augmented reality en blockchain. Een aantal voordelen van Web 3.0 zijn: geen tussenpartijen die jouw persoonlijke gegevens beheren zonder jouw toestemming, minder datalekken, minder censuur en minder uitval van internetdiensten.

World Wide Web (WWW): Standaarden waarmee via internet data kan worden gestuurd zoals webpagina's en e-mail. Het wordt ook weleens gezien als de verzameling documenten en toepassingen die op het internet wordt aangeboden.

World Wide Web Consortium (W3C): Internationale organisatie die open standaarden ontwerpt en ondersteunt voor het WWW, zoals HTML, XML, CSS en HTTP.

World Wide Web Foundation: Organisatie die zich inzet voor een open en vrij web voor iedereen, opgezet door onder andere Tim Berners-Lee.

Bronnen

Baran, R. (1962). On distributed communications networks. *The RAND corporation*. Santa Monica. P2626. Doi: 10.7249/RM3420

Barlow, J.P. (1996). A Declaration Of The Independence Of Cyberspace. *Electronic Frontier Foundation*. Geraadpeegd van: https://www.eff.org/cyberspace-independence

Castro, M. & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, 20(4), 398-461. https://doi.org/10.1145/571637.571640

CERN. Servicing the first web server - Tim Berners-Lee's NeXT. Geraadpleegd op 20 december 2019, van CERN website: https://cds.cern.ch/record/1547556

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18

Dai, W. (1998). B-Money. Geraadpleegd op 19 november 2019, van Weidai.com website: http://www.weidai.com/bmoney.txt

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/tit.1976.1055638

Dwork, C., & Naor, M. (1992). Pricing via Processing or Combatting Junk Mail. *Advances in Cryptology — CRYPTO' 92*, 139–147. https://doi.org/10.1007/3-540-48071-4_1

Gartner. (2019, 12 september). Gartner 2019 Hype Cycle for Blockchain Business shows Blockchain will have a transformational impact across Industries in Five to 10 years. Geraadpleegd op 19 november 2019, van Gartner website: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows

Henley, J. (2015, 9 februari). The great internet swindle: ever get the feeling you've been cheated? Geraadpleegd op 19 november 2019, van The Guardian website: https://www.theguardian.com/technology/2015/feb/09/andrew-keen-internet-not-answer-interview.

Johnson, S. (2018, 16 januari). Beyond the Bitcoin Bubble. Geraadpleegd op 19 november 2019, van The New York Times Magazine website: https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

Kahney, L. (2019). *Tim Cook: the genius who took apple to the next level.* Penguin Books.

Linden, A., & Fenn, J. (2003). *Understanding Gartner's Hype Cycles.* Geraadpleegd van https://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/115200/115274/115274.pdf.

O'Reilly, T. (2005, 30 september). What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Geraadpleegd op 19 november 2019, van O'Reilly website: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

Panetta, K. (2017, 15 augustus). Enterprises should explain the business potential of blockchain, artificial intelligence and augmented reality. Geraadpleegd op 15 augustus 2017, van Gartner website: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Ross, S. (2017, 1 maart). Whatever Happened to the Internet's Promise? Geraadpleegd op 19 november 2019, van Techonomy website: https://techonomy.com/2017/03/whatever-happened-to-the-internets-promise/

Steinert M, & Leifer L. (2010, augustus). *Scrutinizing Gartner's hype cycle*. Artikel gepresenteerd bij Portland International Center for Management of Engineering and Technology, Portland. https://www.researchgate.net/publication/224182916_Scrutinizing_Gartner's_hype_cycle_approach

Szabo, N. (1997, 29 december). The Idea of Smart Contracts. Geraadpleegd op 23 december 2019, van Nakamotoinstitute.org website: https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Tully, C. (z.d.). How Can Space Support the Fourth Industrial Revolution?. Geraadpleegd op 19 november 2019, van SpaceNews.com website: https://spacenews.com/sponsored/industrial-revolution/

12. Blockchain en de Self-Sovereign Identity

"Eenieder heeft, waar hij zich ook bevindt, het recht als persoon erkend te worden voor de wet."

- Artikel 6 van de Universele Verklaring van de Rechten van de Mens

"Granting control of digital identity to centralized authorities of the online world suffers from the same problems cause by the state authorities of the physical world: users are locked into a single authority who can deny their identity or even confirm a false identity. Centralization innately gives power to the centralized entities, not to the users."

- Christopher Allen (2018)

12.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat Self-Sovereign Identity (SSI) is.
- Wat het verschil is met een digitale identiteit.
- Wat de scheefgroei is die is ontstaan in Web 2.0 ten aanzien van deze identiteit.
- Waarom deze identiteit binnen een Internet of Value van belang is.
- Hoe je de link tussen een product in de fysieke wereld en de digitale equivalent kunt aantonen.
- Wat de rol van de overheid kan zijn bij een Self-Sovereign Identity (SSI).

Inleiding

Het internet is ontwikkeld zonder een standaard met betrekking tot hoe mensen en organisaties worden geïdentificeerd. Het gevolg is dat websites en online dienstverleners zelf identificatiesystemen hebben ontwikkeld met gebruikersnamen en wachtwoorden die binnen hun databases worden bewaard. Dit heeft het gebruik van applicaties er niet gemakkelijker op gemaakt. Daarnaast trekken databases waarop identiteitsgegevens bewaard worden ook kwaadwillenden aan. Ook heb je niet altijd de volledige beschikking over de data die van je worden bijgehouden en wat er met die data gebeuren.

Overheden willen zeker stellen dat alle burgers een goedgekeurde identiteit hebben, waar de overheid van op de hoogte is. Zodoende kan de Europese Unie bijvoorbeeld de Europese burger ondersteunen om meer beschikking over de eigen data te houden, bijvoorbeeld via de General Data Protection Regulation (GDPR) wetgeving die in Nederland is vertaald naar de Algemene verordening gegevensbescherming (AVG). In dit hoofdstuk wordt naar de huidige situatie gekeken, en naar de rol die blockchain kan vervullen om de individuele digitale identiteit van een burger te versterken met behulp van een Self-Sovereign Identity (SSI).

Hiervoor wordt in paragraaf 12.2 eerst gekeken naar wat een digitale identiteit is. De evolutie van deze digitale identiteit naar een Self-Sovereign Identity (SSI) komt aan bod in paragraaf 12.3. In paragraaf 12.4, bespreken we de rol van blockchain om deze SSI te bewerkstelligen. Hierna wordt in paragraaf 12.5 nog beschreven hoe je praktisch de blockchain kunt gebruiken om de digitale identiteit vast te leggen. Het hoofdstuk wordt afgesloten met een samenvatting en overzicht van de gebruikte begrippen en bronnen in paragraaf 12.6.

12.2 Wat is een digitale identiteit

Identiteit bestaat klassiek uit je naam, geboortedatum en nationaliteit – de informatie die gewoonweg ook op je geboortecertificaat of paspoort staat. Dit is informatie waarbij voornamelijk de nationale overheid een rol speelt en zodoende als toegangspoort fungeert tot andere diensten. Met een valide identiteitskaart heb je toegang tot onderwijs, stemmen, onroerend goed, een bankrekening en andere mogelijkheden die leiden tot volwaardige participatie in de samenleving. Hoe beter de centrale overheid functioneert in de registratie van dergelijke identiteiten, hoe eenvoudiger je toegang kunt krijgen tot diensten.

Een digitale representatie van deze identiteit, ligt hiermee in lijn, maar kan op verschillende begrippen duiden. Zo kan het bijvoorbeeld zowel een legale identiteit zijn, alswel een login voor een socialmediatoegang, waarachter persoonlijke gebruikersdata hangen (Nyst, Pannifer, Whitley, & Makin, 2016).

In het volgende wordt de ***digitale identiteit*** behandeld binnen twee domeinen, enerzijds vanuit commercieel perspectief, anderzijds vanuit het perspectief van de overheid.

12.2.1 Digitale identiteit en de overheid

Traditioneel gezien is de nationale overheid de partij die de identiteit van een persoon bijhoudt. Zo registreert ze bijvoorbeeld registers van geboorte, huwelijk en overlijden. Ook geeft ze

nationale identiteitskaarten en paspoorten af. Een overheid dwingt zodoende af, zeker in goed georganiseerde landen, dat mensen een officiële legale identiteit kunnen overleggen en dat bedrijven alleen handelen met deze mensen. Dit wordt onder andere gedaan om te weten wie hun ingezetenen zijn, maar ook om hun rechten te beschermen en ervoor te zorgen dat ze belasting betalen. Daarnaast kan de overheid dit ook doen om te weten wie zich binnen hun landsgrenzen begeven en waar hun landgenoten zich buiten deze grenzen bevinden.

Met een gewaarborgde digitale identiteit kun je ook een verkiezingsproces verbeteren of ideeën koppelen aan de mensen van wie die ideeën zijn. In lijn hiermee kun je aangeven wat je denkt of stemt en deze stem bijvoorbeeld tijdelijk aan iemand anders verlenen via e-Voting of gebruiken om je eigen idee vast te leggen.

Wat knijpt bij de overheid is dat ze de registratie binnen verschillende instituten bijhouden. Doordat de verschillende instituten niet altijd de informatie delen, zijn veel gegevens vastgelegd in afzonderlijke datasilo's. Soms kunnen de instituten het delen van gegevens nog niet technisch inregelen en soms mag het in verband met privacyregelgeving zoals de AVG niet. Deze AVG is gebaseerd op de GDPR-wet van de Europese Unie. De Europese Unie probeert met deze GDPR ondersteuning te bieden aan zowel een legale identiteit als aan een commerciële identiteit.

Naast de verschillende datasilo's werken overheden nog steeds met papieren processen, terwijl we ons als burger steeds meer in een digitaal domein begeven waar nationale digitale identiteitsgegevens centraal staan. In sommige landen stelt dit overheden in staat om informatie te vergaren met navenante risico's tot misbruik van persoonlijke informatie. Denk bijvoorbeeld aan Aadhaar, een biometrisch ID-systeem van de Indiase overheid, waarbij elke Indiër een identificatienummer krijgt waarmee hij kan aantonen wie hij is en waar hij woont. Anderzijds zijn er ook overheden die niet altijd de middelen of regelgeving hebben om de eigen bevolking te registreren en een identiteitskaart ter beschikking te stellen. Als je officieel niet de documentatie hebt om te bewijzen wie je bent, wordt het lastig internationaal te reizen of toegang te vragen tot uitkeringen of onderwijs. Deze mensen worden soms volledig uitgesloten van het digitale financiële systeem, als ze hierdoor geen bankrekening aan kunnen vragen. Dan kunnen ze ook geen geld digitaal sparen en hebben ze geen kans op krediet bij een bank. Dit gebrek aan online toegang zal de economische groei voor deze individuen en hun landen bemoeilijken.

Vanuit het perspectief van de transformatie van papieren processen naar digitale processen is het ook belangrijk dat de overheid ***e-Signatures*** mogelijk maakt.

12.2.2 Digitale identiteit en andere instellingen

Nyst et al. (2016) zien een digitale identiteit vanuit commercieel perspectief als een middel om vertrouwde relaties te bouwen met klanten die toestaan dat je:

1. De klant beter begrijpt, en hem daardoor kan bedienen met een product of dienst.
2. Dit product of deze dienst veilig kunt aanbieden, zonder al te grote barrières om dit product of deze dienst te gebruiken. Deze veiligheid is niet geholpen door het feit dat internet vanuit de historie is gebouwd om apparaten te identificeren in plaats van mensen (zie hoofdstuk 11). Dit maakt deze digitale identiteit gevoeliger voor hacks en het leidt tot inefficiënties in het bijhouden en beschermen van alle gebruikersnamen en wachtwoorden.

Bepaalde instellingen gebruiken de persoonlijke data dus ten behoeve van hun diensten. Dit zijn naast commerciële bedrijven ook instellingen binnen het medische werkveld of onderwijs. Instellingen binnen deze werkvelden willen bijvoorbeeld weten bij welke apotheek je eerder medicijnen hebt ontvangen, of je gebeld wil worden en welk vervolgtrajectadvies je van je vorige school kreeg.

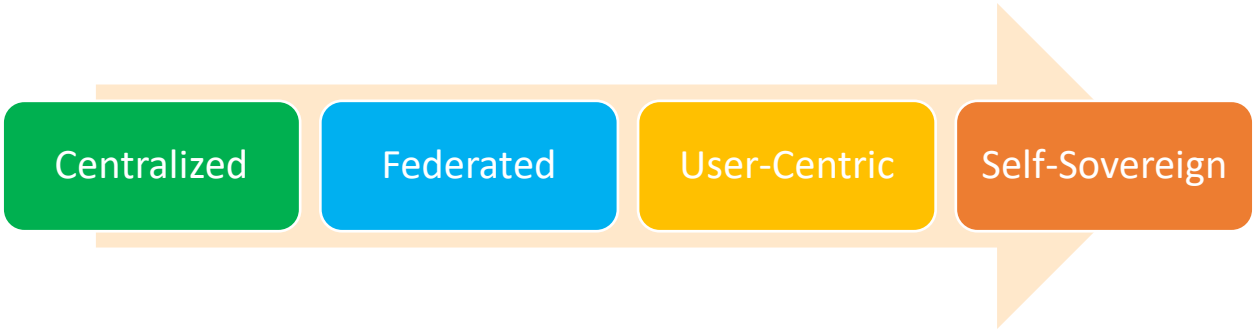
Om deze gegevens betrouwbaar te achten, moeten ze vertrouwen hebben in de online identiteit van een persoon. Als ze de data niet kunnen vertrouwen, is het bijvoorbeeld lastig in te schatten of de mogelijke klant tijdig zal betalen. Dus ook deze bedrijven zoeken naar een technologie die op een laagdrempelige manier vertrouwen en veiligheid biedt. Maar dan wel een technologie die niet al te vertragend of kostenverhogend werkt en die niet de kans heeft op hoge boetes en reputatieverlies. Denk hierbij wederom aan het moeten opvolgen van privacywetgeving als de AVG.

Naast veiligheidsrisico's en privacyvraagstukken, is er ook de vraag van wie de gebruikersdata is. Is informatie over de manier waarop je een app gebruikt bijvoorbeeld jouw bezit of dat van de app-maker? Stel dat er informatie wordt verzameld over hoe je je bankrekening gebruikt, of je auto, of de clicks op je Facebookprofiel. Van wie is dan welke informatie? En waarom staat het je nu als burger niet vrij om waarde uit deze data te halen, behalve dan via het bedrijf dat jouw data in zijn bezit heeft.

12.3 Evolutie van digitale identiteiten

Volgens Christopher Allen (2016) evolueren digitale identiteiten in vier stadia:

1. Centralized Identity.
2. Federated Identity.
3. User-Centric Identity.
4. Self-Sovereign Identity.



Afbeelding 111: De evolutie van online identiteiten (Sovrin, 2017, p. 6).

12.3.1 Centralized Identity: administratieve controle door één autoriteit

Centrale autoriteiten**,** zoals IANA voor IP-adressen en ICANN voor domeinnamen controleren sinds de vroege dagen van internet de digitale identiteit. Vanaf 1995 kwamen ***Certificate Authorities*** (CA) op die commerciële partijen, zoals Service Providers als Bol.com en Facebook hielpen bewijzen wie ze waren. Op hun beurt creëerden deze partijen weer eigen hiërarchieën waarbinnen ze mensen ondersteunden met het beheer van hun digitale identiteit (Allen, 2016).

In een ***centralized identity*** is één organisatie eigenaar van de digitale identiteit. Dit betreft momenteel de meerderheid van alle online identiteiten. Voorbeelden van centralized identity zijn websites, waarvoor je een aparte identifier (gebruikersnaam) en credential (wachtwoord) moet aanmaken per Service Provider. De digitale identiteit is alleen binnen het eigen identiteitsdomein van de Service Provider te gebruiken. Doordat deze gecentraliseerde organisaties je digitale identiteit beheren, kunnen zij deze ook van je afnemen. Dit valt bijvoorbeeld te herleiden uit de voorwaarden wanneer je een account aanmaakt:

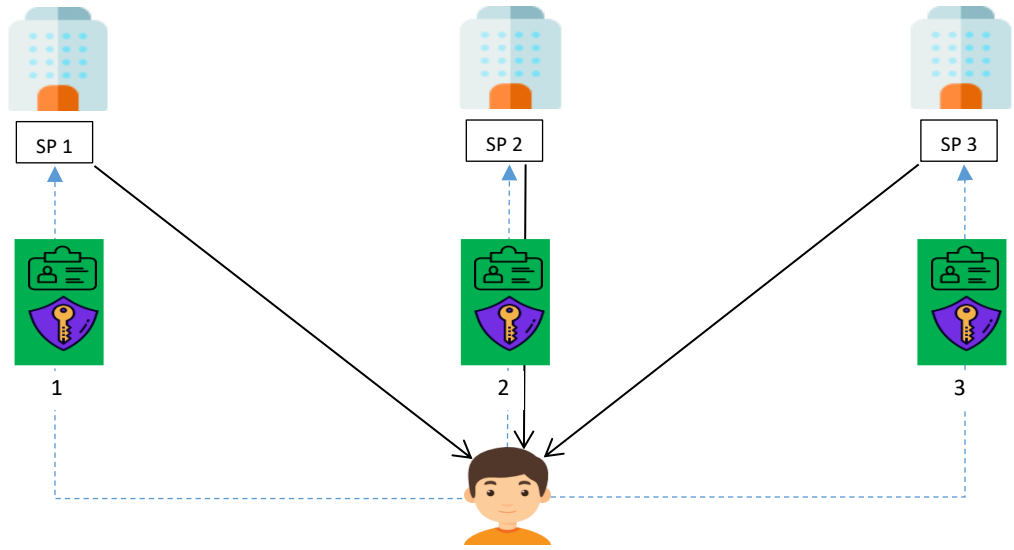
> *"Yahoo may, without telling you, immediately cancel or limit your access to your Yahoo accounts, certain Yahoo Services and any associated email addresses…" [Yahoo]*[131]

[131] De voorwaarden van Yahoo in 2016 (Sovrin, 2017, p. 6).

> *"We reserve the right to modify or terminate the Service or your access to the Service for any reason, without notice, at any time, and without liability to you…" [Instagram][132]*

Hoe meer internet groeide, hoe meer hiërarchieën ontstonden met aparte identiteiten, en hoe meer websites hun gebruikers ertoe dwongen eigen identiteiten te onderhouden met aparte gebruikersnamen en wachtwoorden. Dit alles heeft ertoe geleid dat een selecte groep dominante platformen in staat is zijn geld te verdienen met het vergaren, verkopen en analyseren van gebruikersdata, voornamelijk ten behoeve van adverteerders. Internet is daarmee gecentraliseerd, of in ieder geval is het hiërarchisch opgezet met partijen als CA's, domein registreerders en individuele sites. Dit brengt het risico met zich mee dat ze persoonlijke data delen met andere partijen, vaak zonder dat de gebruiker hiervan bewust is. Je bent hierdoor als gebruiker ook praktisch gedwongen de vele verschillende gebruikersnamen en wachtwoorden bij te houden. Dit verhindert het gebruiksgemak en trekt kwaadwillenden aan die proberen identiteitsgegevens van centrale servers te stelen. Zo zijn ook deze partijen gedwongen deze gegevens op eigen servers te beschermen. De kans op hacks van persoonlijke informatie zoals wachtwoorden, e-mailadressen, maar ook rijbewijsdetails en creditcardgegevens, neemt hierdoor toe. Gebruikers krijgen verder bij centralized identity systemen te maken met verschillende inloggegevens bij verschillende service providers. Het kan weleens lastig zijn om deze inloggegevens goed te managen.

[132] De voorwaarden van Instagram in 2016 (Sovrin, 2017, p. 6).

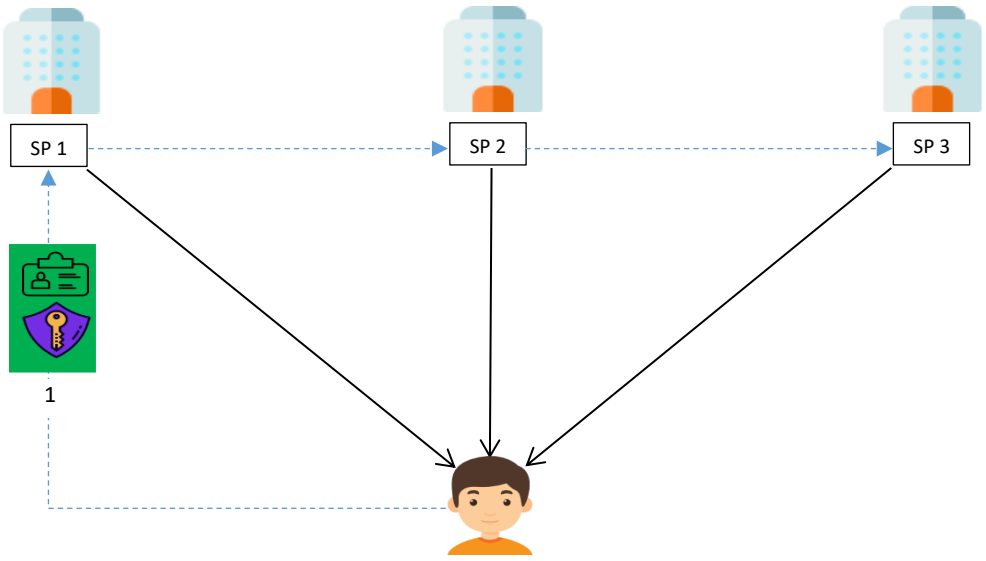


Afbeelding 112: Centralized Identity model. De gebruiker maakt user identifiers en authentication credentials aan bij elk afzonderlijke Service Provider. Nadat de gebruiker toegang heeft verkregen tot het systeem van de Service Provider, verleent de Service Provider zijn diensten aan de gebruiker. (Josang & Pope, 2005, p. 4)

12.3.2 Federated Identity: administratieve controle door een federatie van autoriteiten

In een ***federated identity*** worden één identifier en credential gebruikt om toegang te krijgen tot een Service Provider. De identifier wordt vervolgens verdeeld over een groep van Service Providers die onderling een overeenkomst hebben dat de identifier en bijbehorende credential gebruikt kunnen worden over de verschillende Providers. Dit resulteert in één enkel virtueel identiteitsdomein. Zo kun je met een federated identity met je Saxion-gegevens inloggen bij BlackBoard, e-mail en andere online Microsoft Office diensten – een federatie van Service Providers. Het voordeel van een federated identity ten opzichte van een centralized identity is dat het je een mate van ***draagbaarheid*** verschaft. Met draagbaarheid wordt bedoeld dat de identiteit gemakkelijk mee te nemen is en gebruikt kan worden bij andere Service Providers. In het geval van een draagbare identiteit kunnen één identifier en credential worden gebruikt bij bijvoorbeeld mijn.Saxion, Blackboard en je Saxion e-mail. Zodoende hoef je ook minder gebruikersnamen en wachtwoorden te onthouden.

Hoewel federated identities meer gebruikersgemak bieden dan centralized identities, ligt de identiteit nog steeds in handen van een centrale partij die de identiteit heeft aangeboden. Het gebruik van federated identities maakt hierbij een aantal platformen nog dominanter, en vergroot de privacy- en veiligheidszorgen. Mocht je identiteit worden gestolen vanuit de centrale partij, dan verlies je ook toegang tot andere diensten. De consequenties bij het verliezen van je identiteit is dus groter dan bij een centralized identity. (Sovrin, 2017, p. 7)



Afbeelding 113: Federalized Identity model. De gebruiker maakt één user identifier en authentication credential aan bij een Service Provider. Nadat de gebruiker toegang heeft verkregen tot het systeem van de Service Provider, kan dezelfde identifier en credential worden gebruikt om toegang te krijgen tot het systeem van de andere Service Providers. (Josang & Pope, 2005, p. 5.)

12.3.3 User-Centric Identity: individuele of administratieve controle over verschillende autoriteiten, zonder de nood tot het gebruiken van een federatie van partijen

User-centric Identity zet niet de Service Provider centraal binnen het identiteitsproces, maar de gebruiker. Het draait hierbij voornamelijk om de volgende twee elementen: toestemming en interoperabiliteit. Een gebruiker kan zelf beslissen welke persoonlijke gegevens hij wil delen en met welke Service Provider. (Allen, 2016). De data blijven echter bewaard bij een centrale instantie die in online toegang voorziet. Dat betekent ook dat deze instantie die de registraties verzorgt op elk moment je identiteit kan afnemen.

12.3.4 Self-Sovereign Identity: individuele controle over elke autoriteit

De ***Self-Sovereign Identity*** (SSI) is de laatste stap binnen de identiteitsevolutie. In het geval van een SSI beheer je zelf al je persoonlijke data en registreer je wanneer je wie voor hoelang toegang geeft tot wat. Dit gaat gepaard met volledige controle zonder tussenkomst van een derde partij. Wat centraal staat binnen SSI is autonomie. Om dit mogelijk te maken, dient een SSI draagbaar te zijn, zodat de gebruiker niet afhankelijk is van een centrale partij die zijn identiteit beheert. Ook dient een SSI gebruikers de mogelijkheid te bieden om claims te maken over ***persoonlijke identificeerbare informatie*** (PII). Dit is informatie waarmee een persoon kan worden geïdentificeerd. Denk bijvoorbeeld aan een naam, burgerservicenummer en e-mailadres.

Afbeelding 114: In Self-Sovereign Identity sta jij centraal (Almasi, 2019).

Christopher Allen (2016) heeft tien principes van SSI geïdentificeerd. Deze zijn als volgt:

1. *Bestaan*. Elke SSI moet gekoppeld zijn aan het onafhankelijke bestaan van een gebruiker.
2. *Controle*. De gebruiker heeft autoriteit over zijn identiteit. Hij moet kunnen refereren naar zijn identiteit, deze kunnen uploaden of zelfs kunnen verbergen.
3. *Toegankelijk*. De gebruiker moet toegang hebben tot zijn eigen gegevens, zodat hij ook claims kan maken over zijn persoonlijke identificeerbare informatie. Dit betekent echter niet dat de gebruiker elke informatie die is gelinkt aan zijn identiteit zomaar mag wijzigen.
4. *Transparantie*. De systemen waarmee SSI's worden geadministreerd moeten vrij en open source zijn, zodat het mogelijk is voor iedereen om te zien op welke wijze deze systemen werken.
5. *Volhardend*. De identiteit van een gebruiker moet idealiter voor altijd blijven bestaan of op zijn minst even lang als de gebruiker wil. Het is wel van belang dat deze eigenschap niet tegenstrijdig is met het recht om te worden vergeten. Een gebruiker moet in staat zijn om zich te ontdoen van een identiteit, of zijn identiteit te kunnen actualiseren. Om dit mogelijk te maken dient er onderscheid te zijn tussen identiteit en claims met betrekking tot een identiteit.
6. *Draagbaar*. Identiteitsgegevens moeten draagbaar zijn. Dit houdt in dat deze gegevens niet bewaard mogen worden op slechts één enkele centrale server. Deze servers kunnen de identiteit verwijderen. Draagbaarheid verzekert de gebruiker dat hij in

controle is van zijn identiteit en dat hij deze mee kan nemen om andere diensten te mogen gebruiken.

7. *Interoperabiliteit*. SSI's moeten gebruikt kunnen worden over verschillende platformen en landsgrenzen heen.
8. *Consent*. Gebruikers moeten toestemming geven op het gebruik van hun identiteit door een derde partij.
9. *Minimalisatie*. De openbaarmaking van claims moeten worden geminimaliseerd. Als er identiteitsgegevens nodig zijn, dan zou het mogelijk moeten zijn om selectief de informatie te tonen die relevant is voor dat moment. Dit kan worden ondersteund door cryptografische technologieën, zoals Zero-Knowledge Proofs. Het is ook in lijn met de bescherming van ons recht op privacy.
10. *Bescherming*. De rechten van gebruikers moeten worden beschermd. Als er een conflict is tussen het identiteitsnetwerk en de rechten van een gebruiker, dan moeten ten eerste vrijheid en andere individuele rechten worden beschermd.

Deze tien principes passen binnen de volgende drie essentiële domeinen van een SSI: beveiligd, beheersbaar en draagbaar.

Beveiligd De identiteitsgegevens moeten beveiligd zijn	**Beheersbaar** De gebruiker moet in controle zijn van wie toegang heeft tot zijn gegevens en kan inzien	**Draagbaar** De gebruiker moet in staat zijn om waar dan ook zijn identiteitsgegevens te gebruiken en is niet gebonden aan één enkele dienstverlener
Bescherming	Bestaan	Interoperabiliteit
Volhardend	Volhardend	Transparantie
Minimalisatie	Controle	Toegankelijk
	Consent	

Tabel 5: Principes van Self-Sovereign Identity (Tobin & Reed, 2017, p. 10).

In de eerste plaats dient de SSI de veiligheidsvraagstukken van het huidige Web 2.0 op te lossen. Daarnaast wil je als gebruiker volledige controle over je eigen data en rechten kunnen verlenen aan anderen voor het delen van deze data. Als laatste wil je de identiteit kunnen gebruiken binnen verschillende toepassingen. Het daagt de technische infrastructuur van het huidige Web 2.0 hiermee uit.

Intermezzo: De kosten van KYC en AML

Voor financiële instellingen gelden specifieke regels zoals de ***Know Your Customer*** (KYC) procedure of ***Customer Due Diligence*** (CDD), waarin de instellingen verplichte gegevens over een nieuwe klant moeten verzamelen, voordat ze diensten mogen leveren aan die klant. Deze functie van financiële instellingen wordt ook wel de financiële poortwachtersfunctie genoemd. Daarnaast heb je de anti-witwaswetgeving; de Wet ter voorkoming van *witwassen en financieren van terrorisme* (WWFT). De Engelse term hiervoor is ***Anti Money Laundering*** (AML). De maatregelen voor het bestrijden van terrorismefinanciering zijn gebaseerd op de regels die zijn vastgesteld door het internationale ***Financial Action Task Force*** (FATF). Binnen deze wetten dienen de financiële instellingen actief ongebruikelijke transacties te identificeren en te melden. Zeker bij internationaal zakendoen wil de overheid voorkomen dat partners en klanten van financiële dienstverleningen geld op illegale wijze hebben verkregen. Vaak dien je daarom een due diligenceonderzoek uit te voeren als financiële instelling. Hierbinnen kijkt de instelling bijvoorbeeld of de partner is geplaatst op een lijst van verdachte partijen en stelt het de risico's van deze partij vast aan de hand van zijn eerdere activiteiten.

Er zijn echter wel negatieve consequenties verbonden aan dergelijke regelgevingen zoals:

1. Hogere compliancekosten.
2. Meer klantenfrictie.
3. Meer kans op identiteitsdiefstal.

Volgens Thomson Reuters (2016) spendeert een financiële instelling gemiddeld $60 miljoen per jaar aan AML compliance. Grotere financiële instellingen betalen soms tot wel $500 miljoen per jaar. 10% van 's wereld grootste financiële instellingen spenderen jaarlijks minimaal $100 miljoen. De kosten van KYC is van 2016 naar 2017 met 19% gestegen en van 2017 naar 2018 met 16%. Zulke hoge compliance kosten leiden tot duurdere financiële dienstverlening. (Callahan, 2018)

Het 'Cost of Compliance 2017 Report' van Thomson Reuters heeft een survey gedaan onder internationale financiële instellingen. Hieruit kwam voort dat het proces om klanten te onboarden in 2016 22% langer duurde. In 2017 is het proces verder toegenomen met 18%. Het resultaat is dat het proces bij banken gemiddeld 24 dagen duurt en 12% van de klanten vanwege KYC-issues van banken zijn gewisseld.

De financiële instellingen worden er daarnaast door de overheid toe bewogen proactief persoonlijke data te verzamelen en te analyseren ten bate van die overheid. Deze eis werd tot voor enkele jaren geleden binnen de cryptowereld niet gesteld aan bedrijven die cryptomunten aanbieden. Uit de WWFT vloeit voort dat aanbieders van cryptomunten in Nederland vanaf 10 januari 2020 onder het toezicht van De Nederlandsche Bank vallen. Zodoende dienen ook deze bedrijven actief de wallets en transacties te analyseren. Mensen die bijvoorbeeld Bitcoins willen kopen of verkopen dienen zich te identificeren aan de hand van identiteitsdocumenten en mogelijk krijgen ze ook vragen over inkomen, herkomst van geld en Bitcoins en wat de bestemming is. Er moet van iedere klant een risicoprofiel opgesteld worden en elke transactie zal worden gemonitord en gecontroleerd. Bitonic, één van de eerste Bitcoin-handelsbeurzen in Nederland, ziet dergelijke wetgevingen als een beperking van de financiële vrijheid van burgers:

> "Het recht op privacy wordt door regels van anti-witwas en terrorismefinanciering altijd op de tweede plaats gezet en zo creëer je uiteindelijk een politiestaat. Wij zijn natuurlijk gebonden aan de Nederlandse wet en zullen daaraan gehoor geven, maar wij maken ons zorgen over de verstrekkende effecten op korte en lange termijn. De nieuwe regels en verplichte transactiemonitoring gelden voor álle klanten en álle bedragen en dat beperkt de financiële vrijheid van burgers." (2019)

De KYC-documenten worden momenteel veelal bewaard op gecentraliseerde servers van meerdere partijen. Als je een hypotheek wil afsluiten, dien je bijvoorbeeld je persoonlijke gegevens te overleggen aan je hypotheekadviseur en kunnen ze worden gedeeld met de hypotheekverstrekker en de bank. Dit vergroot het risico op gegevensinbreuken. (Johnson, 2019)

Alle bovenstaande zaken leiden tot langere en duurdere procedures en slechtere dienstverlening voor klanten. Misschien wel de schrijnendste consequentie is dat daardoor minder mensen een bankrekening kunnen openen. Dit betreft vooral de armste mensen in de samenleving, omdat zij vanwege de hoge operationele kosten niet interessant zijn voor financiële instellingen. De mensen zonder bankrekening worden ook wel de ***unbanked*** genoemd. Volgens de World Bank Group (2017) zijn er ongeveer 1,7 miljard volwassenen unbanked. De verwachting is dat cryptowallets op termijn een oplossing zullen bieden voor veel van deze mensen. Je kunt immers gratis bijvoorbeeld Bitcoin wallets creëren.

12.4 Blockchain en Self-Sovereign Identity

Door de decentrale datastructuur hoeven er geen dominante partijen te zijn die het dataverkeer centraal op hun servers zetten en beheersen. Meerdere organisaties kunnen afhankelijk van de rechten die gebruikers geven, de informatie van transacties, eigendom, de identiteit en andere informatie inzien, aanvullen en gebruiken. Dit voorkomt dubbele invoer, fouten, langzame invoer en misbruik van privacygevoelige informatie.

12.4.1 Twee denkrichtingen waarbinnen SSI mogelijk is

Vraag is wie de data erop zet en beheerst. Hiervoor zijn twee denkrichtingen:

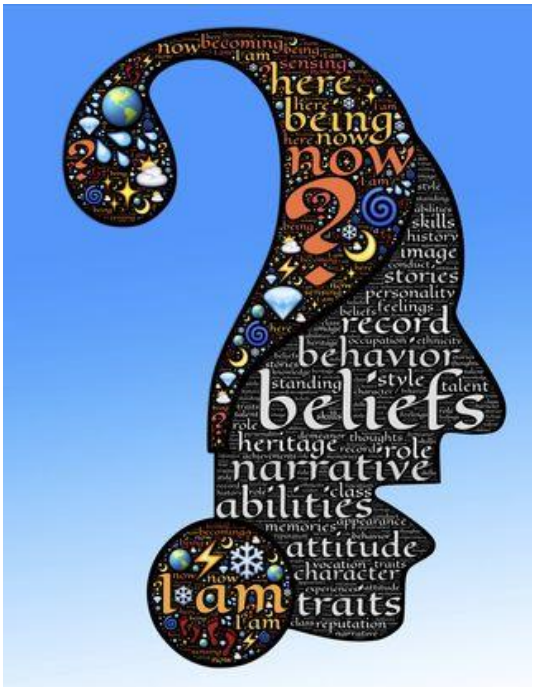
1. Enerzijds kan een gebruiker op de blockchain een account creëren zonder daarvoor enige andere data, zoals een geboortecertificaat, te overleggen. Hier heb je toegang tot al je data via je eigen private key die je bewaart achter bijvoorbeeld je biometrische gegevens en wachtwoorden op je mobiele telefoon. Voorbeelden van bekende applicaties hiertoe zijn Sovrin, ontwikkeld met Hyperledger Indy, en uPort via Ethereum.

   In dit geval verschuift de macht van het bedrijf naar de gebruiker die meer soevereiniteit krijgt en zodoende zelf bepaalt wat er met de eigen identiteitsgegevens gebeurt. Op termijn zou dit de Web 3.0-belofte in kunnen lossen van een decentraler internet met meer privacy. In plaats van in te loggen op Google Gmail om toegang te krijgen tot je e-mail kun je bijvoorbeeld met een persoonlijke cryptografische sleutel inloggen op je browser op je telefoon. Binnen deze browser beheers je zelf je digitale vingerafdruk en koppel je zelf de data die je relevant vindt, zoals scholing, werk en reputatie, of je eigen blockchaintokens ten bate van je dApps die aan elkaar zijn gelinkt. Jij staat hier centraal.
2. Anderzijds wordt een reeds bekende registratie, zoals een paspoort, op een decentrale database gezet door een instelling. Indien iemand nu een service wil verkrijgen dient deze persoon aan te tonen dat hij de juiste gebruiker is, voordat hij bij de digitale diensten kan. Voorbeelden van bekende projecten zijn ID2020, SecureKey en TrueRec van SAP op Ethereum.

   Als je in dit geval bijvoorbeeld een inenting wil hebben, vergelijkt de gezondheidsorganisatie je bewijs op een centrale database en leggen ze je inentingsdata vervolgens vast op de blockchain. Hierdoor ligt de macht in de handen van een centrale instelling die daarmee kan bepalen wat er met deze gegevens gebeurt. Dit ligt in lijn met Web 2.0.

Het ligt in de lijn van de verwachting dat de tweede denkrichting grootschaliger wordt geadopteerd op de korte termijn. Dus de huidige gegevens die verschillende instellingen hebben, zetten ze op de blockchain en als gebruiker dien je daar zelf toegang toe te vragen, zonder er noodzakelijk veranderingen op aan te brengen of rechten aan te ontlenen. Kans is dat de overheid een initiatief neemt om een dergelijke wallet op te zetten. Het risico bestaat dat je identiteit op meerdere blockchains ligt, die niet met elkaar communiceren. Op de lange termijn zal de eerste optie opkomen waarin een gebruiker op de blockchain een account creëert, zonder daarvoor enige andere data, zoals een geboortecertificaat, te overleggen. Waarschijnlijk blijft een hybride systeem zodoende bestaan. Dit kan in de vorm van een all-in-one app voor de klant. Zoeken, entertainment, social media, spelletjes, betalingen en andere activiteiten worden dan geregeld in een oplossing waarin de data van meerdere partijen zijn.

Adoptie van het één of het andere systeem is mede afhankelijk van hoe betrouwbaar de systemen zich tonen en in hoeverre een kritische massa wordt bereikt om het netwerkeffect te creëren.



Afbeelding 115: Aspecten van een zelfsoeverein individu (Allen, 2016).

12.4.2 Andere voor- en nadelen van je identiteit via de blockchain

Een toegankelijke blockchain belooft als voordeel in theorie altijd actuele, goedkopere en vooral veiligere gegevens. Bedenk je de toename van hacks van persoonlijke informatie of het gebruik van je persoonlijke informatie ten behoeve van marketing, waar je je niet altijd even bewust van bent.[133] Ook zijn de gegevens betrouwbaarder, omdat je er samen met een andere partij toezicht op houdt. Op termijn kan dit nog sneller, zonder tussenpartij en kun je je digitale identiteit altijd bij je dragen. Bijvoorbeeld om bij de toegang van een beveiligde site aan te tonen door wie je bent ingehuurd, voor wanneer en waar. In geval van verlies van je data, heb je altijd je eigen biometrische gegevens en een wachtwoord om je private key tot je digitale identiteit terug te krijgen. Of zoals in het geval van uPort, vraag je een quorum van mensen op je contactlijst om een nieuwe private key voor je te maken.

Een SSI vergemakkelijkt het te gelde maken van je economische identiteit die je mogelijk toegang geeft tot bezit of krediet.

Blockchain biedt ook het voordeel van het geven van aangepaste rechten en plichten op de SSI-gegevens via smart contracts. Zo kun je de gegevens geven onder jouw voorwaarden: voor dat project, voor die tijd en met die terugbetaling. Je kunt bijvoorbeeld tijdelijk je stem geven aan een persoon voor een bepaald onderwerp. Voor je net gekochte auto krijg je een digitale sleutel toegestuurd die je weer kunt doorverkopen. En als je te hard rijdt, heb je gelijk je boete te pakken.

Er kan een situatie zijn waarin je geheime informatie zoekt om een beslissing te kunnen nemen. Bijvoorbeeld als je de hoogte van een mogelijke hypotheek wil berekenen voor een nieuwe klant, maar de informatie over het salaris die je nodig hebt, krijg je niet. In dat geval moet je dus de mogelijkheid hebben een geheim te bewijzen, zonder dat het geheim zelf wordt verklapt. Enkele manieren dit te bewijzen zijn ***Multi-party computation*** (MPC)[134], ***attribute-***

[133] Voor een visualisatie van 's werelds grootste datalekken, zie: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[134] Cryptografische techniek waarmee partijen die aan data samenwerken, samen berekeningen kunnen uitvoeren op de blockchain zonder dat ze eigen input onthullen aan elkaar. Een groep partijen kan bijvoorbeeld de gemiddelde salaris tussen hen berekenen zonder dat de partijen elkaars salarissen aan elkaar onthullen.

based credentials[135] en Zero-Knowledge Proofs. Dit mechanisme reduceert de behoefte om een ander te vertrouwen. Of zoals Goossens en Verslype (2019) het verwoorden, in dit geval lag de focus “echter op confidentialiteit, daar waar blockchain net steunt op transparantie” (p. 129).

Zodoende zullen ook bedrijven meer samen kunnen werken, zelfs via publieke blockchains, aangezien ze data willen delen zonder te veel bedrijfsgevoelige details. Het voordeel is dat je alleen die data weggeeft die nodig zijn; via een openbaar gedeeld netwerk waar geen centrale partij tussen zit die je kunt hacken, of die moedwillig informatie aanpast of blokkeert. Op een publiek netwerk staat het je dan vrij naar de transacties te kijken die er plaatsvinden, zonder dat je de details van de transacties kunt achterhalen. Zo kun je bijvoorbeeld real time data inzien over hoeveel hypotheken er binnen een regio plaatsvinden tegen welke rente, zonder te veel persoonlijke details van de transacties te zien. Tegenover deze voordelen van het delen van geheime informatie geldt dat het gebruiksgemak afhankelijk is van in hoeverre overheden en publieke instituten en bedrijven afspraken kunnen maken en naleven.

Los van de digitale identiteit van personen, is het lastig aan te tonen dat SSI van enig fysiek object wel overeenkomt met de werkelijkheid. Dit bewijs van bestaan of ***Proof-of-Existence*** (PoE) wordt verholpen door vertrouwde partijen, zoals auditoren en vertrouwde sensoren die nodig blijven als tussenpartij. Ook is de infrastructuur nog niet klaar om overheden volledig met alle partijen samen te laten werken. Er zijn legale, technische en privacy barrières die onder andere de Europese Unie probeert de slechten.

Een netwerk waarop de identiteit van dingen vastligt, is belangrijk voor het Internet of Things. Een laatste, meer tijdelijk, probleem is dat de wetgeving ten aanzien van blockchain en identiteit nog achterloopt en de publieke blockchain nog niet schaalbaar genoeg is.

Naast mensen zullen ook entiteiten met behulp van smart contracts bepaalde contracten aangaan. Denk aan een huis als legaal bedrijf dat zichzelf bijvoorbeeld verhuurt en partijen inhuurt voor schoonmaak, of een bedrijf dat aan moet tonen dat het bepaalde licenties bezit en de relevante belastingen afdraagt, of aangeeft welke natuurlijke personen het als externe vertegenwoordigers kent. Een onroerend goed koopovereenkomst werkt niet zonder KYC en

[135] Een manier waarop een derde vertrouwde persoon of organisatie alleen benodigde referenties bevestigt zonder andere data weg te geven. Zo kun je voor het kopen van alcohol alleen bevestigen dat je 18 jaar of ouder bent zonder dat je alle andere persoonlijke gegevens laat zien.

overheidscontrole. De entiteit heeft dus een officiële status nodig, inclusief een veilige wallet met een private key en een public key om transacties te ondertekenen. Ditzelfde geldt voor een bedrijf of stichting. Het is duidelijk dat de overheid hierbij een rol heeft om er zeker van te zijn dat de grote sommen geld geen criminele herkomst hebben, dat de wetten worden nageleefd en de belasting wordt betaald. En het is duidelijk dat hierbij een transparant vastgelegde reputatie een grotere rol kan spelen dan voorheen. Zo zou een reputatie gebaseerd kunnen worden op transacties die beoordelaars transparant becommentariëren, waarbij ook de beoordelaars weer transparant kunnen worden bekeken.

Een digitaal eigendom of een entiteit zonder mogelijkheid of nood tot smart contracts daarentegen zou af kunnen met een eenvoudigere versie van een SSI. Een eenvoudigere versie van een SSI is een digitaal certificaat waaraan KYC-data als 'ontstaansdatum' of 'kenmerken' aan hangen. Deze zou kunnen worden gekoppeld aan een token dat weer toevalt aan een eigenaar. Meer over tokens in hoofdstuk 10. Voor nu is het belangrijk te begrijpen dat deze identiteiten een rol zullen spelen in het mogelijk maken van een deeleconomie en het inwisselen van de beloften van het Internet of Things.

12.4.3 Macht naar het individu of bij de instellingen?

Veel van deze blockchain- en internettechnologie verschuift langzaam onder de motorkap. Dus je zult best nog wel een browser hebben en een zoekmachine op je telefoon, maar vooral een telefoon met een paar geïntegreerde super dApps waarbinnen je socialiseert, winkelt, informatie zoekt en muziek luistert.[136] Of een dApp waarmee je met de overheid je identiteitspapieren bijhoudt en je belastingen, salaris, pensioen en schoolpapieren regelt. Je hoeft dan niet meer elke keer in te loggen voor een nieuwe site om in een beveiligde omgeving te komen. Je internettoepassing doet dit vanzelf voor je op het moment dat je je dApp opent. Op deze manier verschuift de macht van de instellingen naar de gebruiker.

12.5 Hoe identiteitsmanagement praktisch op een blockchain werkt

Een identiteitsmanagementoplossing is een gedeeld thema binnen verschillende blockchainapplicaties. Om identiteitsmanagement te bewerkstelligen, is het ***Verifiable Credentials Data Model*** van het World Wide Web consortium belangrijk:

[136] Socialmediabedrijven zoeken constant naar een mogelijkheid om klanten zoveel mogelijk binnen één app te bedienen, om meer data van de klant te verzamelen en te gelde te maken.

1. Iemand of iets maakt een ***identiteitsclaim***, bijvoorbeeld “ik ben een persoon ouder dan 18 jaar”.[137]
2. Er is een ***bewijs*** dat deze claim verifieert, zoals een uittreksel van een geboorteregister inclusief burgerservicenummer van deze persoon, gemaakt en ondertekend door een centrale overheid.
3. Er is een ***verklaring*** van een derde partij die deze claim onderschrijft, zoals een bank die wil weten of een bepaalde persoon ouder is dan 18 jaar.

Om nu de claim, het bewijs en de verklaring voor een persoon op de blockchain vast te leggen en een SSI te bewerkstelligen, wordt het onderstaande proces gebruikt.

Allereerst moeten mensen of partijen een ***agent*** hebben om de claims, bewijzen en verklaringen vast te leggen en te communiceren. Voor mensen is zo’n agent vaak een app op een mobiele telefoon of computer, waarmee een identiteitswallet kan worden benaderd (van Deventer & Joosten, z.d.). Zo gebruikt het Zweeds communicatiebedrijf Telia een ID-app in het Lantmäteriet voorbeeld in hoofdstuk 16, waarmee mensen een identiteitswallet kunnen benaderen op hun telefoon. De Zwitserse gemeente Zug gebruikt hiervoor de uPort app (Zug Stadt, z.d.). Voor een bedrijf kan een agent bijvoorbeeld een webapplicatie zijn.

Een persoon kan nu via een app een identiteitswallet aanmaken waarin verschillende soorten data zijn vastgelegd. In het voorbeeld van Zug dien je binnen de gemeente Zug eerst je telefoon en jezelf te laten registreren door een identiteitsbewijs te overleggen. Als de registratie is verricht, wordt het ID-nummer van de telefoon op Ethereum geknoopt aan een publiek Ethereum-adres. Je identiteitsbewijs wordt alleen op je telefoon opgeslagen. Nu kun je met de digitale identiteit op je app gebruikmaken van diensten waarbij je normaliter fysiek je identiteitsbewijs zou moeten overleggen.

In het voorbeeld van de Telia-app van Lantmäteriet wordt je Zweedse burgerservicenummer vastgelegd op de blockchain. Met deze app kun je nu de koopprocedure starten van land binnen het Zweedse systeem, contracten en dergelijke van de verschillende agenten worden binnen de app bewaard, de deelnemende partijen kunnen elkaar uitnodigen en de benodigde documenten inzien.

[137] Er kunnen bundels van meerdere claims tegelijkertijd worden gemaakt.

In het volgende beschrijven we een methodiek gebaseerd op werk van het World Wide Web Consortium waar in hoofdstuk 11 al over is gesproken.

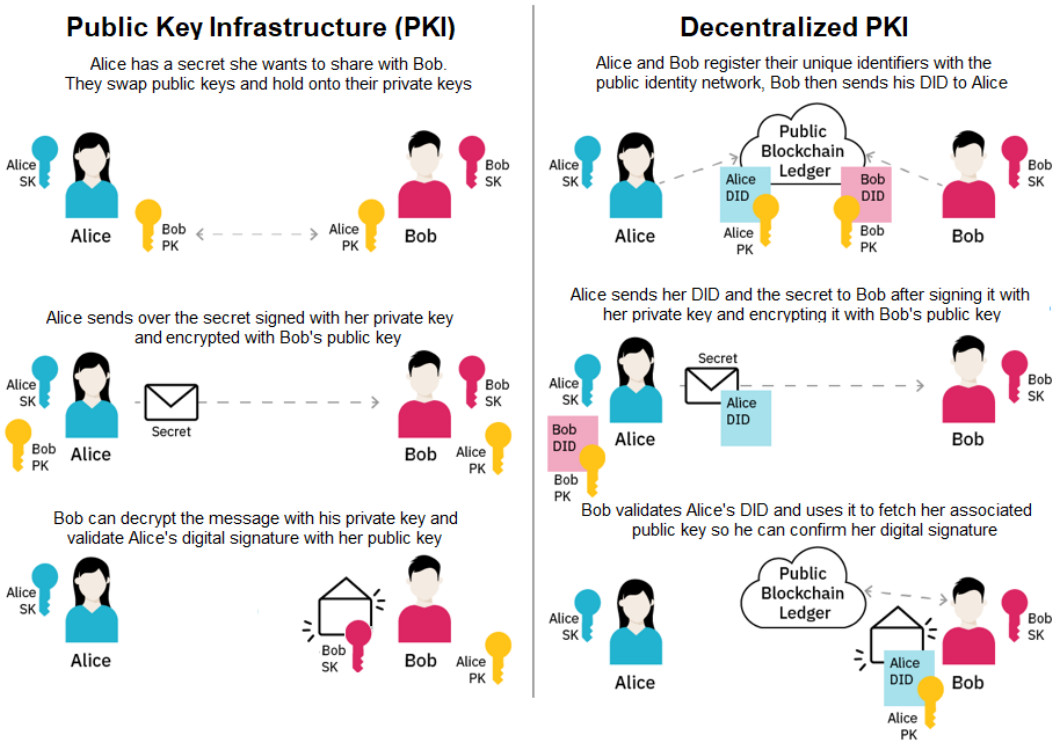
12.5.1 Methode om identiteit op de blockchain vast te leggen

Het idee is dat een identiteitswallet meerdere claims bevat die worden geattesteerd en kunnen worden gestuurd naar diegenen die je verzoeken een dergelijke claim te bewijzen. Bijvoorbeeld de claim dat je ouder bent dan 18 jaar, de claim dat je krulhaar hebt, of de claim dat je digitale paspoort een digitale representant van jou is. Hiervoor maak je per claim een publiek adres met public key en private key aan. Dit adres wordt gezien als een ***decentralized identifier*** (DID). De identiteitswallet beheert de verschillende adressen. Deze DID kun je aanmaken zonder tussenkomst van een centrale autoriteit. Je maakt het adres immers direct aan op de blockchain. De app om zo'n wallet te maken en de data die je hiervoor vastlegt, kan alleen op je eigen computer of mobiele apparaat staan.

Stel dat je de claim dat je ouder bent dan 18 jaar moet bewijzen aan een bank. In dit geval verzoek je de overheid via bijvoorbeeld de Telia-app om een claim op de blockchain te leggen waarin staat dat jij ouder bent dan 18 jaar. Technisch vult de overheid hiervoor je ***DID document*** (DDO) aan. Dit DDO omvat de claim(s) met daarin de publieke sleutels van zowel jezelf als de overheid, het soort agent, de manier waarop de agent wordt gebruikt en identificeert dus eigenlijk de eigenaar van de DID.

De overheid kan in de DDO zien via welke app, telefoon en DID het verzoek wordt gemaakt. De overheid weet bijvoorbeeld dus al dat de gemeente Zug eerder een bepaald identiteitsbewijs heeft geattesteerd om toegang tot de app, en een DID, goed te keuren. De overheid kan op basis hiervan de claim dat je ouder bent dan 18 jaar maken in een apart DDO, of toevoegen aan een DDO met meerdere andere claims.

Stel dat de overheid voor jouw DID een aparte claim maakt. Hiervoor stuurt de overheid de eigen DID plus de claim, tekent het met de eigen private key en encrypt dit alles met de public key van de aanvrager. De aanvrager kan de claim nu openen met behulp van de eigen private key.



Afbeelding 116: De vergelijking tussen Public Key Infrastructure en Decentralized PKI (Gisolfi, 2018).

De aanvrager kan een claim delen met iemand op de blockchain door een DID in een transactie te bundelen, te ondertekenen met de eigen private key en te encrypten met de public key van de andere partij. In dit geval zou de claim dus richting de bank worden gestuurd.

De informatie die nu op de blockchain staat, hoeft niet meer te zijn dan dat de gemaakte claim klopt. De claim zelf kan op de telefoon staan, off-chain, terwijl er een hash van de claim on-chain wordt gedeeld op de blockchain. Ook staat het digitale identiteitsbewijs alleen op de telefoon, off-chain, en is het publiekelijk onduidelijk wie er achter de DID zit. Er hoeft verder dus geen persoonlijke identificeerbare informatie te worden vastgelegd op de blockchain. Als er geen persoonlijke informatie bekendgemaakt is, valt er ook geen persoonlijke informatie te verwijderen. Dit is conform de wensen van de AVG.

De bank kan vervolgens de procedure starten om financiering te onderzoeken voor de koop van land.

Een ***personal identity data management system*** (PIMS) is een instrument om de eigen digitale data te beheren. Via het PIMS op de blockchain is het denkbaar dat een gebruiker op gebruikersvriendelijke wijze de eigen data tot in details beheert. Hierbij zou hij ook mogelijkheid kunnen hebben om data-autorisaties die zijn verleend weer terug te trekken. Dit ondersteunt ook de AVG.

Ook is het binnen het ***eIDAS*** akkoord mogelijk om eSignature te gebruiken om digitale transacties te ondertekenen.[138]

12.5.2 SSI en de kansen voor Internet of Things

Niet alleen mensen halen voordeel uit het delen van een database met anderen. De SSI kan ook worden gebruikt om een identiteit van een apparaat te maken. De sensoren van dat apparaat geven dan informatie over het gebruik ervan en de toestand waaronder het is gebruikt. Ook kan het informatie verschaffen over hoe het was verzekerd, wanneer het is gerepareerd en wie welke reserve-onderdelen hebben vervangen. Dit kan nuttig zijn als je bijvoorbeeld een nieuwe of tweedehandse machine koopt van een leverancier die je niet kent, of als je een slimme koelkast hebt die met behulp van de eigen identiteit als jouw agent optreedt en constant op het internet zoekt naar de beste prijs voor elektriciteit. Op termijn zou het zelfs mogelijk kunnen zijn dat je als individu investeert in een DAO die een eigen SSI heeft waarmee contracten worden aangegaan, winsten worden gegenereerd en vervolgens investeringen kunnen worden gedaan uit naam van de DAO SSI.

Elk apparaat zal met behulp van de eigen identiteit een transactie op de blockchain kunnen vastleggen. Hiermee kan het apparaat onomstotelijk aantonen welke informatie het bijvoorbeeld via sensoren heeft gestuurd. Op deze manier ondersteunt blockchain de groei van een Internet of Things. Ook het Internet of Value wordt hiermee geholpen, omdat blockchain transacties en bezittingen registreren.

[138] Je kunt meer lezen over eIDAS in paragraaf 16.2.

Inermezzo: uPort

De mobiele identiteitswallet uPort is gebaseerd op Ethereum.

Met deze app kun je:

1. Veilig inloggen op applicaties zonder wachtwoorden.
2. Persoonlijke informatie en verificaties controleren.
3. Ethereum-transacties bekijken en digitaal ondertekenen.

Met de wallet sta je in verbinding met het uPort-platform, een netwerk van verschillende dApps voor het decentrale web. uPort zelf communiceert met open protocollen om alle webcommunicatie te bewerkstelligen. Deze communicatie vindt plaats zonder gecentraliseerde servers.

Afbeelding 117: Logo van uPort.

Ter demonstratie kun je op https://uportlandia.uport.me/ zien hoe je in beginsel met gemeentelijke persoonsgegevens een diploma opvraagt die je bij een werkgever kunt gebruiken en weer kunt delen om een verzekering af te sluiten. Het biedt aldus de mogelijkheid om in te loggen op netwerken die jou, anders dan techbedrijven momenteel, de mogelijkheid geven om contracten legaal aan te gaan en zelf te kiezen wanneer je welke data deelt.

Naast uPort zijn ook voorbeelden van Sovrin aangehaald. Beide organisaties zijn, samen met onder andere Microsoft, IBM, Hyperledger, R3, Mastercard, NEO en Blockstack lid van de Decentralized Identity Foundation. De Foundation is te vinden op https://identity.foundation/.

12.6 Samenvatting, begrippen en bronnen

Samenvatting

Het internet is ontwikkeld zonder een standaard met betrekking tot hoe mensen en organisaties online worden geïdentificeerd. Het gevolg is dat websites en online dienstverleners zelf identificatiesystemen hebben ontwikkeld met gebruikersnamen en wachtwoorden die binnen hun databases worden bewaard. Dit leidt tot barrières in het gebruik en de veiligheid van applicaties, en voorkomt dat je volledige beschikking over je digitale data hebt.

De digitale representatie van je identiteit, de digitale identiteit, staat hiermee op het spel als instrument om toegang te krijgen tot zowel overheidsdiensten als tot commerciële en andere diensten.

Om de verschillende barrières te overwinnen, dient het individu directe en volledige controle te krijgen over de verschillende autoriteiten die digitaal bestaan. Deze evolutie van controle verschuift vanuit een centralized identity via een federated en user-centric identity naar een Self-Sovereign Identity. Binnen de Self-Sovereign Identity zijn de identiteitsgegevens veilig, beheerst de gebruiker wie er toegang heeft tot de gegevens en is de gebruiker altijd en overal in staat deze gegevens te gebruiken.

Blockchain kan de evolutie naar een Self-Sovereign Identity ondersteunen door een decentrale te versleutelen datastructuur. Vraag is wie er in de toekomst het account creëert en onderhoudt, de gebruiker of een instelling.

In het hoofdstuk wordt een methode genoemd om identiteit praktisch op de blockchain vast te leggen. Hierbinnen staan een identiteitsclaim, een bewijs dat de claim klopt, en een verklaring die deze claim onderschrijft centraal. De claim wordt als publiek adres zonder centrale autoriteit aangemaakt en op de blockchain gezet. Een andere instantie kan de claim onderschrijven waarop de claim kan worden gedeeld met de partij die deze informatie wil weten.

Opmerkingen die je nu kunt uitleggen

- Zonder SSI geen Internet of Value.
- In potentie verschuift SSI op blockchain de macht naar de gebruiker, maar het is niet gegarandeerd dat dit leidt tot een decentraler internet.
- Elk token heeft minimaal een digitaal certificaat nodig, maar dit is nog geen SSI.
- Elke persoon heeft een SSI nodig, elke entiteit die smart contracts ondertekent zal hetzelfde nodig hebben.
- Zonder SSI wordt het lastig een Web 3.0 als internet of value te ontwikkelen.

Verklarende begrippenlijst

Agent: Iemand of iets om de claims, bewijzen en verklaringen vast te leggen en te communiceren. In het licht van digitale identiteit is dit vaak een app, mobiele telefoon of computer waarmee een identiteitswallet kan worden benaderd.

Algemene verordening gegevensbescherming (AVG): Databescherming en privacywetgeving gebaseerd op de GDPR van de EU. Zie ook GDPR.

Anti-Money Laundering (**AML)**: Richtljnen voor anti-witwaswetgeving, mede opgezet ter bestrijding van terrorismefinanciering. Zie ook Wwft.

Attribute-based credentials: Een authenticatiemechanisme waarbij alleen een specifiek attribuut van een entiteit wordt onthuld. Een derde persoon of organisatie kan bijvoorbeeld alleen de benodigde referenties bevestigen zonder dat andere gegevens worden gedeeld. De gemeente bevestigt bijvoorbeeld dat je 18 jaar of ouder bent, zonder jouw andere persoonlijke gegevens te zien.

Bewijs: Iets dat een claim bewijst. Dit kan bijvoorbeeld een uittreksel zijn dat is ondertekend door een overheid.

Certificate Authorities (CA): Binnen PKI zijn certificate authorities gespecialiseerd in het uitgeven, opslaan en ondertekenen van digitale certificaten die entiteiten helpen bewijzen wie ze zijn.

Customer Due Diligence (CDD): Procedure waarin instellingen verplichte gegevens over een nieuwe klant moeten verzamelen, voordat ze diensten mogen leveren aan die klant. Het gaat hierbij om het verifiëren van de identiteit van de klant en soms ook een evaluatie van het risicoprofiel van de klant. Customer Due Diligence is onderdeel van KYC.

Centralized identity: Digitale identiteit waarbij één organisatie de eigenaar is. Dit betreft momenteel de meerderheid van alle online identiteiten. Voorbeelden van centralized identity zijn websites, waarvoor je een aparte identifier (gebruikersnaam) en credential (wachtwoord) moet aanmaken per Service Provider.

Decentrale identiteit: Een digitale identiteit die is vastgelegd en beheerd op decentrale wijze.

Decentralized identifier (DID): Gegeven dat is geregistreerd op een Distributed Ledger Technology of blockchain waarmee een person kan worden geïdentificeerd. Een decentralized identifier is een URL die de persoon linkt aan een DID document.

Decentralized Identifier Document (DDO): Digitaal document met verifieerbare claims over je identiteit, inclusief de public keys van zowel jezelf als diegene die de claims kunnen onderschrijven.

Digitale identiteit: Identiteit binnen het digitale domein waaraan digitale data van iets of iemand kan zijn gekoppeld.

Draagbaarheid: In het licht van digitale identiteit is dit de mate waarin de identiteit mee te nemen is en gebruikt kan worden bij andere Service Providers. Zo kan één draagbare identiteit met één unieke combinatie van gebruikersnaam en wachtwoord worden gebruikt bij bijvoorbeeld mijn.Saxion, Blackboard en je Saxion e-mail.

eIDAS: Richtlijn van de EU over hoe digitale handtekeningen als legaal bindende handtekeningen kunnen worden gebruikt binnen de EU.

e-Signatures: Digitale handtekeningen met legaal bindende gevolgen.

Federated identity: Digitale identiteit waarbij de administratieve controle bij een federatie van autoriteiten ligt.

Financial Action Task Force (FATF): Intergouvernementele organisatie die is opgericht binnen de G7 voor de bestrijding van witwassen en terrorismefinancering.

General Data Protection Regulation (GDPR): Databescherming en privacywetgeving van de EU uit 2016 die in Nederland is vertaald naar de Algemene verordening gegevensbescherming (AVG).

Identiteitsclaim: Een claim over een identiteit. Bijvoorbeeld, “ik ben ouder dan 18 jaar”.

Know Your Customer (KYC): Procedure waarin de instellingen verplichte gegevens over een nieuwe klant moeten verzamelen, voordat ze diensten mogen leveren aan die klant. CDD valt onder KYC.

Multi-party computation (MPC): Cryptografische techniek waarmee partijen die aan data samenwerken, samen berekeningen kunnen uitvoeren op de blockchain zonder dat ze eigen input onthullen aan elkaar. Een groep partijen kan bijvoorbeeld de gemiddelde salaris tussen hen berekenen zonder dat de partijen elkaars salarissen aan elkaar onthullen.

Personal identity data management system (PIMS): Systeem om de eigen digitale data in detail te beheren.

Persoonlijke Identificeerbare Informatie (PII): Informatie waarmee een persoon kan worden geïdentificeerd. Denk bijvoorbeeld aan een naam, burgerservicenummer en e-mailadres.

Proof-of-Existence (PoE): Bewijs dat een digitale representatie zoals een SSI overeenkomt met de werkelijkheid.

Self-Sovereign Identity (SSI): Een draagbare digitale identiteit waarbij de gebruiker de onderliggende data volledig bezit en onder controle heeft.

Unbanked: Mensen die geen toegang hebben tot de diensten van financiële instellingen.

User-centric identity: Digitale identiteit waarbij de Service Provider niet centraal staat binnen het identiteitsproces, maar de gebruiker. Het draait voornamelijk om de volgende twee elementen: toestemming en interoperabiliteit. Een gebruiker kan zelf beslissen welke persoonlijke gegevens hij wil delen en met welke Service Provider. De data blijven echter bewaard bij een centrale instantie die in online toegang voorziet. Dat betekent ook dat deze instantie die de registraties verzorgt op elk moment de identiteit kan afnemen.

Verifiable Credentials Data Model: Door W3C opgezette standaard om online referenties op een veilige, discrete en verifieerbare wijze te ondersteunen.

Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft): Nederlandse anti-witwaswetgeving die is ingevoerd naar aanleiding van de invoering van de Europese witwasrichtlijn AMLD4 in 2018 en de AMLD5 in 2020. Het AML in deze wetten staat voor de Engelse term van anti-witwaswetgeving, Anti-Money Laundering.

Bronnen

Allen, C. (2016, 26 april). The Path to Self-Sovereign Identity. Geraadpleegd op 20 december 2019, van Lifewithalacrity.com website: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Almasi, P. P. (2019, 7 februari). The Identity Revolution — Self Sovereign Powered by Blockchain. Geraadpleegd op 23 december 2019, van Medium website: https://blog.goodaudience.com/how-blockchain-could-become-the-onramp-towards-self-sovereign-identity-dd234a0ea2a3

Bitonic. (2019, 1 november). *Vanaf 10 januari verplichte identiteitscontrole*. Geraadpleegd 23 december 2019, van Bitonic website: https://bitonic.nl/news/197/vanaf-10-januari-verplichte-identiteitscontrole

Callahan, J. (2018, 10 juli). Know Your Customer (KYC) Will Be A Great Thing When It Works. Forbes. Geraadpleegd op 20 december 2019, van Forbes website: https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/

van Deventer, O. (2019, mei). Self-*Sovereign Identity - the good, the bad and the ugly*. Geraadpleegd op 23 december 2019, van TNO website: https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly/

English, S., & Hammond, S. (2017). *Cost of Compliance 2018*. Geraadpleegd van https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf

Gisolfi, D. (2019, 13 juni). *Self-sovereign identity: Why blockchain*? Geraadpleegd op 19 juli 2019, van IBM website: https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/

Johnson, A. (2019, 3 april). Is Privacy Under Threat From All The Know-Your-Customer Documents Stored With Countless Services? Geraadpleegd op 20 december 2019, van Forbes website: https://www.forbes.com/sites/alastairjohnson/2019/04/03/is-privacy-under-threat-from-all-the-know-your-customer-documents-stored-with-countless-services

Goossens, J., & Verslype, K. (2019). *Blockchain en smart contracts. Het einde van de vertrouwde tussenpersoon?* Brussel, België: Editions Larcier.

Josang, A., & Pope, S. (2005). *User Centric Identity Management*. Artikel gepresenteerd bij *CRC for Enterprise Distributed Systems Technology*. The University of Queensland.

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2016). *Uport: A Platform for Self-Sovereign Identity*. Geraadpleegd van http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

Nyst, C., Pannifer, S., Whitley, E., & Makin, P. (2016). *Digital Identity: Issue Analysis*. Geraadpleegd van https://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

Thomson Reuters. (2016, 9 mei). *Thomson Reuters 2016 Know Your Customer Surveys reveal escalating Costs and Complexity.* Geraadpleegd op 23 december 2019, van Thomson Reuters website: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

Third, A., Quick, K., Bachler, M., & John, P. (2018). *Government services and digital identity*. Geraadpleegd van https://www.eublockchainforum.eu/sites/default/files/research-paper/20180801_government_services_and_digital_identity.pdf

Tobin, A., & Reed, D. (2016). *The Inevitable Rise of Self-Sovereign Identity A white paper from the Sovrin Foundation* [white paper]. Geraadpleegd van https://sovrin.org/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Verenigde Naties. (2017). *Universele Verklaring van de Rechten van de Mens*. Geraadpleegd op 23 december 2019, van Amnesty International website: https://www.amnesty.nl/encyclopedie/universele-verklaring-van-de-rechten-van-de-mens-uvrm-volledige-tekst

W3C. (2019, 26 maart). Verifiable Credentials Data Model 1.0. Geraadpleegd op 23 december 2019, van Github.io website: https://w3c.github.io/vc-data-model/CR/2019-03-26/

W3C. (2019, 9 december). Decentralized Identifiers (DIDs) v1.0. Geraadpleegd 23 december 2019, van W3.org website: https://www.w3.org/TR/did-core/#dfn-service-endpoints

World Bank Group. (2017). *The Global Findex Database 2017*. Geraadpleegd op 20 december 2019, van Worldbank.org website: https://globalfindex.worldbank.org/

Zug Stadt. (z.d.). Digitale ID registrieren. Geraadpleegd op 20 december 2019, van Zug Stadt website: https://www.stadtzug.ch/digitaleid/5295

Iconen

Service provider, Bob en beveiligingsschild gemaakt door Prettycons van www.flaticon.com

DEEL II: DE ACHTERGROND EN HET GEDACHTEGOED VAN WAARUIT BLOCKCHAIN IS ONTSTAAN

Met de voorgaande kennis van blockchain uit deel I, is het tijd inzicht te verschaffen in de grotere gedachten achter blockchain.

In de afgelopen jaren zijn er steeds meer mensen betrokken geraakt bij blockchainprojecten. Hierdoor zijn veel nieuwkomers verwijderd geraakt van de initiële aantrekkingskracht die blockchain had op early adopters. Zeker in de eerste jaren, voordat er een hype ontstond rondom cryptovaluta, werd blockchain gezien als een economisch en politiek instrument dat het individu door middel van cryptografische technologie zou bevrijden van overheidsbemoeienis. In de blockchain community werd blockchain vaak in één adem genoemd met revolutie, financiële vrijheid, privacy, transparantie, enzovoorts.

Een belangrijke economische stroming die veel invloed heeft gehad op de blockchainwereld is de Oostenrijkse School van de Economie. Mensen die deze stroming volgen, zijn voor zo min mogelijk overheidsbemoeienis met de economie en willen overheidsmonopolies op geldproductie opheffen. Zij hangen een politieke ideologie aan die het libertarisme wordt genoemd. Libertariërs willen een zo klein mogelijke overheid. Binnen deze groep bevinden zich ook de cryptoanarchisten en de cypherpunks die technologieën hebben ontwikkeld waar de Bitcoin blockchain gebruik van maakt.

Dit deel bestaat uit twee hoofdstukken. In Hoofdstuk 13 bespreken we Bitcoin en het financiële systeem. Hierbij komen de verschillende economische stromingen en onenigheden van Satoshi Nakamoto met het huidige systeem aan bod. Er wordt ook een verband gelegd tussen de Oostenrijkse School van de Economie en de Bitcoin blockchain.

In Hoofdstuk 14 bespreken we de filosofische achtergrond van waaruit de Bitcoin blockchain is ontstaan. Hiervoor kijken we naar de voornaamste mensen, cryptoanarchisten en cypherpunks, die technologieën hebben ontwikkeld waar de Bitcoin blockchain gebruik van heeft gemaakt. Wij bespreken ook wat de idealen zijn van cryptoanarchisten en cypherpunks om zo een verband te trekken tussen deze idealen en de eigenschappen van de Bitcoin blockchain.

13. Bitcoin en het financiële systeem

"The public at large have learned to understand, and I am afraid a whole generation of economists have been teaching, that government has the power in the short run by increasing the quantity of money rapidly to relieve all kinds of economic evils, especially to reduce unemployment. Unfortunately, this is true so far as the short run is concerned. The fact is, that such expansions of the quantity of money which seems to have a short run beneficial effect, become in the long run the cause of a much greater unemployment. But what politician can possibly care about long run effects if in the short run he buys support?"

- Friedrich Hayek (1977)

"The logical conclusion to be drawn from these facsts would have been to do away with privileged banks altoghter and to subject all banks to the rule of common law and the commercial codes that oblige everybody to perform contracts in full faithfulness to the pledged word. Free banking would have spared the world many crises and catastrophes."

- Ludwig von Mises (1912)

13.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat de belangrijkste economische stromingen zijn op dit moment.
- Dat de Oostenrijkse School van de Economie van zeer grote invloed is geweest op de Bitcoin blockchain.
- Wat de belangrijkste ideeën zijn van de Oostenrijkse School met betrekking tot hun financiële theorieën.
- Wat centraal bankieren en fractioneel reservebankieren zijn.
- Hoe Bitcoin goed aansluit bij het idee van zo min mogelijk overheidsbemoeienis.
- Hoe Bitcoin de monopolie op geldproductie van centrale banken probeert te ontwrichten en het vrij bankieren introduceert.

Inleiding

In dit hoofdstuk bespreken we Satoshi Nakamoto's onenigheden met het financiële systeem. Het is uit deze onenigheden waaruit de behoefte aan Bitcoin is ontstaan.

Dit hoofdstuk begint met een globaal overzicht van de belangrijkste economische stromingen. Vervolgens bespreken we in paragraaf 13.3 de invloed van de Oostenrijke School van de Economie op de Bitcoin blockchain. Daarna behandelen we in paragraaf 13.4 centraal bankieren en fractioneel reservebankieren, twee concepten van het huidige financiële systeem waar Satoshi Nakamoto het niet mee eens was. Vervolgens zetten we in paragraaf 13.5 de ideeën van de Oostenrijkse School af tegen Bitcoin en zien we hoe Bitcoin past bij de Oostenrijkse stroming. Het hoofdstuk wordt in 13.6 afgesloten met een samenvatting en een lijst van belangrijke begrippen en bronnen.

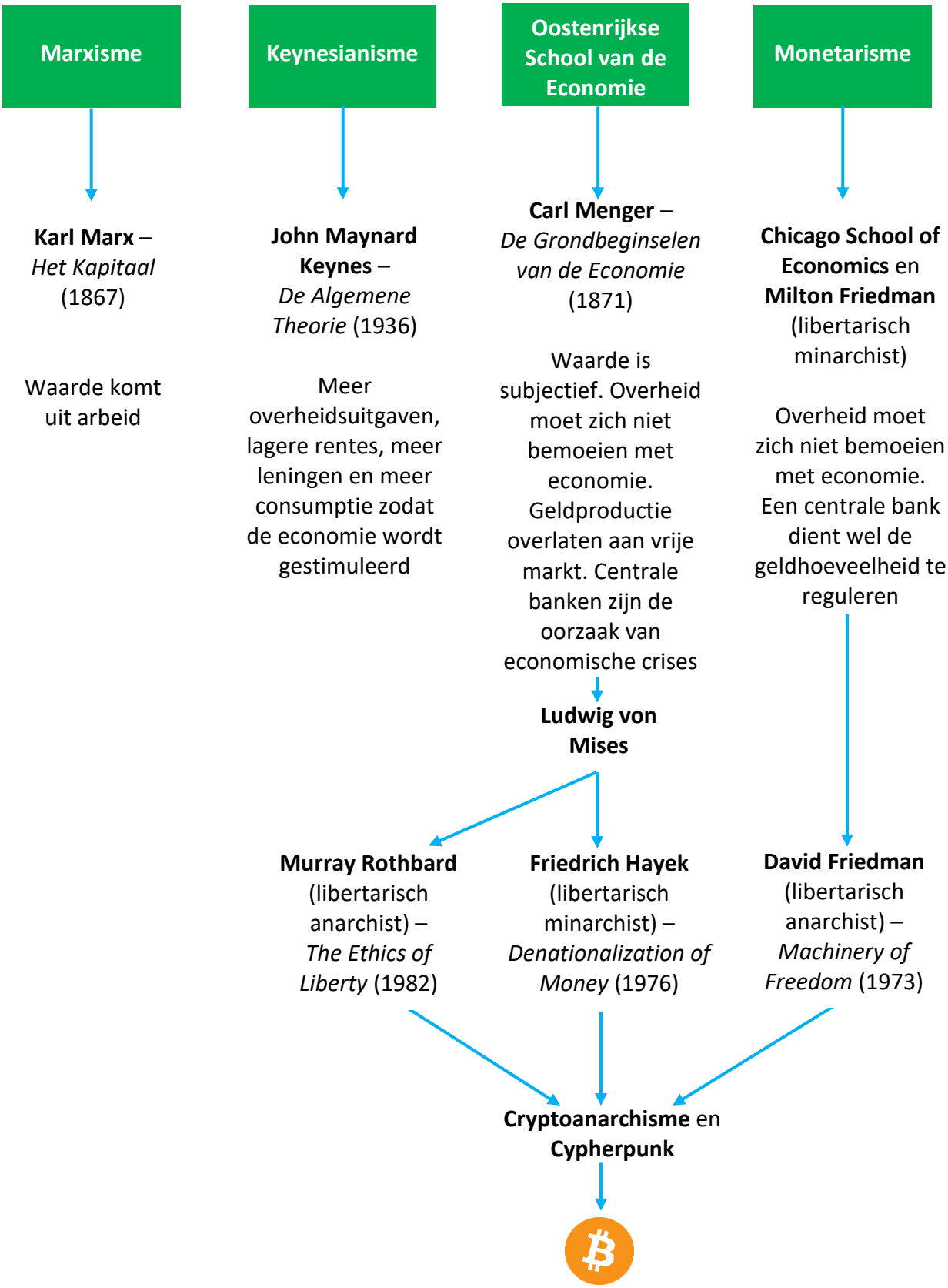
13.2 Globaal overzicht van economische stromingen

De stroming die het invloedrijkst is geweest op het ontstaan van blockchain is de Oostenrijke School van de Economie. Dit wordt ook beaamd door de Europese Centrale Bank in 'Virtual Currency Schemes' (2012). In het artikel zegt de ECB dat de theoretische fundamenten van Bitcoin in de Oostenrijke School van de Economie en diens kritiek op het huidige fiat geldsysteem liggen. (p. 22)

Voordat we Satoshi Nakamoto's onenigheden bespreken met het huidige financiële systeem, geven we eerst een globaal overzicht van de belangrijkste economische richtingen. Vanuit hier kunnen we de intellectuele bewegingen achterhalen die invloed hebben op blockchain. De vier belangrijkste economische richtingen op dit moment zijn:

1. Het Marxisme.
2. Het Keynesianisme.
3. De Oostenrijke School van de Economie.
4. Het Monetarisme.

Voor het historisch perspectief waarin we de Oostenrijkse School van de Economie en diens invloed op de Bitcoin blockchain behandelen, is het handig om het volgende schema in je achterhoofd te houden. Het schema is ook handig voor het volgende hoofdstuk. Daarin behandelen we de filosofische invloeden op de Bitcoin blockchain en komen libertarisme en het cryptoanarchisme aan bod.



Afbeelding 118: Overzicht van de belangrijkste economische stromingen en diens invloeden op de Bitcoin blockchain.

13.3 Oostenrijke School van de Economie

De Oostenrijke School van de Economie is ontstaan met het werk van Carl Menger in 1871, genaamd de *Grondbeginselen van de Economie*. In dit werk zet Menger de ***subjectieve waardeleer*** en de theorie van het ***marginaal nut*** uiteen. Deze twee theorieën gaan in tegen de destijds populaire ***arbeidswaardeleer*** van bijvoorbeeld Adam Smith, David Ricardo en Karl Marx. Marx dacht dat de waarde van een goed afkomstig was van de arbeid die werd gebruikt om het goed te produceren. Menger geloofde daarentegen dat waarde afhing van het nut dat een goed had in het voorzien van de behoeften van een persoon die het goed waardeerde. Met andere woorden, de waarde van een goed is totaal afhankelijk van de waardeoordelen van individuen. De subjectieve waardeleer van Menger staat hiermee niet alleen in contrast met de arbeidswaardeleer, maar ook met intrinsieke waardeleren. Er is volgens Menger dus geen objectief correcte waarde van een goed.[139]

Menger´s theorie van het marginaal nut wordt als volgt uitgelegd. Mensen hebben verschillende behoeften die ze rangschikken in belangrijkheid. De belangrijkste behoeften van mensen zijn normaal gesproken de behoeften waar hun leven van afhangt. Als mensen moeten kiezen welke persoonlijke behoeften zij het eerst willen vervullen, dan willen zij altijd eerder de behoeften vervullen die belangrijker zijn. Als je je in een woestijn bevindt en dorstig bent, zal je de eerste liters water gebruiken om te drinken, zodat je in leven blijft. De overige liters water gebruik je voor behoeften die minder noodzakelijk zijn. Dit is een voorbeeld waarbij het marginaal nut van water afneemt.[140]

[139] Zie ook *The Concise Guide To Economics* (2007) van Jim Cox voor meer uitleg over de arbeidswaardeleer en hoe deze contrasteert met de subjectieve waardeleer. Of een goed intrinsieke waarde kan bevatten of niet, is tot aan vandaag nog steeds een discussie die wordt gevoerd in de blockchainwereld: heeft Bitcoin intrinsieke waarde of niet? Een argument die een beroep doet op de arbeidswaardeleer met betrekking tot de waarde van Bitcoin is dat de waarde afhankelijk is van het werk dat is gestopt in het mijnen van de nieuwe coins.

[140] De theorie van het marginaal nut heeft in de economische theorieën geleid tot de marginale revolutie. Het helpt ons om te verklaren waarom een diamant duurder is dan water, maar wanneer je leven afhangt van het beetje water dat je hebt, je het water waardevoller acht dan de diamant.

Afbeelding 119: Van links naar rechts zijn dit Ludwig von Mises, Friedrich Hayek en Murray Rothbard. Alle drie werkten in de traditie van de Oostenrijke School.

De Oostenrijke School van de Economie heet zo, omdat de vooraanstaandste economen die de theorieën van Menger volgden uit Oostenrijk kwamen. De naam werd ook toegepast om de tegenstelling te duiden met de aan het eind van de 19e eeuw reeds populaire Duitse Historische School.[141] Beroemde economen die werkten in de traditie van Menger waren voornamelijk Oostenrijkers als Eugen Böhm von Bawerk[142], Friedrich von Wieser[143], Ludwig von Mises en Friedrich Hayek. Van de Oostenrijkers in de 20e eeuw, waren Ludwig von Mises en Friedrich Hayek de bekendsten. Ludwig von Mises was de oudere van de twee en had veel invloed gehad op Friedrich Hayek en Murray Rothbard. Hayek won in 1974 de nobelprijs in de economische wetenschappen voor zijn werk in de theorie van geld en conjunctuurgolven. Rothbard is op zijn beurt zeer invloedrijk geweest op de moderne libertarische beweging en wordt gezien als de vader van het libertarisch anarchisme. Wat het libertarisme en het libertarisch anarchisme inhouden, en hoe deze zich verhouden tot de Bitcoin blockchain wordt in het volgende hoofdstuk beschreven.

13.4 De Oostenrijkse kritiek op het financieel systeem

De Oostenrijkse School hield zich onder andere bezig met conjunctuurgolven. Volgens de Oostenrijke theorie zijn conjunctuurgolven het gevolg van monetaire interventies in de markt, waarbij een excessieve expansie van bankkrediet leidt tot een groei in de geldhoeveelheid. Het proces waarbij geld wordt gecreëerd door commerciële banken wordt ***fractioneel reservebankieren*** genoemd. Daarnaast beïnvloeden volgens de Oostenrijkers centrale banken ook conjuncturen door rentestanden kunstmatig laag te houden.

---

[141] De twee scholen raakten in een verhitte intellectuele strijd over de manier waarop economische wetenschappen moest worden bedreven. Op de dag van vandaag speelt de Duitse Historische School geen rol van betekenis meer in de economische theorieën.

[142] Eugen Böhm von Bawerk is onder andere bekend geworden van zijn kritiek op het Marxisme en zijn rol als minister van Financiën in Oostenrijk-Hongarije. Hij bekritiseerde de exploitatietheorie van Marx en beargumenteerde dat kapitalisten hun werknemers niet exploiteren, maar juist helpen door hen een inkomen te bieden, voordat er enige inkomsten voor de kapitalisten worden gegenereerd.

[143] Friedrich von Wieser is onder andere bekend geworden door zijn theorie van alternatieve kosten, ook wel opportuniteitskosten genoemd.

Satoshi Nakamoto (2009) lijkt deze theorie te ondersteunen. Hij schrijft:

> "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."[144]

Volgens Satoshi Nakamoto is het hoofdprobleem van het huidige financiële systeem dat mensen vertrouwen moeten hebben dat centrale banken het geld niet devalueren door lage rentes en dat banken voldoende geld in kas hebben en niet te veel krediet verlenen met slechts een fractie van ons geld als reserve. Als banken te veel krediet creëren op basis van fractioneel reservebankieren, kan dat leiden tot kredietzeepbellen.

Op basis van Satoshi Nakamoto's bovenstaande onenigheden met het financiële systeem, kunnen we het probleem splitsen in de volgende twee deelproblemen die we nader toelichten:

1. Centraal bankieren.
2. Fractioneel reservebankieren.

We lichten beide concepten toe, door te kijken hoe er nieuw geld in omloop komt.

13.4.1 Hoe nieuw geld in omloop komt

In 1928 publiceerde Ludwig von Mises '*Monetary Stabilization and Cyclical Policy*' waarin hij beschrijft hoe overheden en centrale banken door hun monetaire beleid bijdragen aan economische 'booms' en 'busts'. Voor 1914 was het monetaire systeem nog gebaseerd op de goudstandaard. Deze standaard limiteerde de groei in de geldhoeveelheid, omdat een groei in het geld moest corresponderen met de goudreserve die moest worden bewaard. Aangezien goud een schaars goed is en niet zomaar uit het niets gemijnd kan worden, zorgt een goudstandaard ervoor dat er niet te veel geld kan worden gecreëerd. Overheden en centrale banken worden door een goudstandaard dus gelimiteerd in hun monetaire beleid. Sinds we

[144] Het volledige bericht is door Satoshi Nakamoto op 11 februari 2009 geplaatst op het P2P foundation forum. Je kunt het bericht, 'Bitcoin open source implementation of P2P currency', hier vinden: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

volledig zijn afgestapt van de goudstandaard, bestaat er geen limiet meer voor overheden en centrale banken om nieuw geld te creëren.[145]

Centraal bankieren

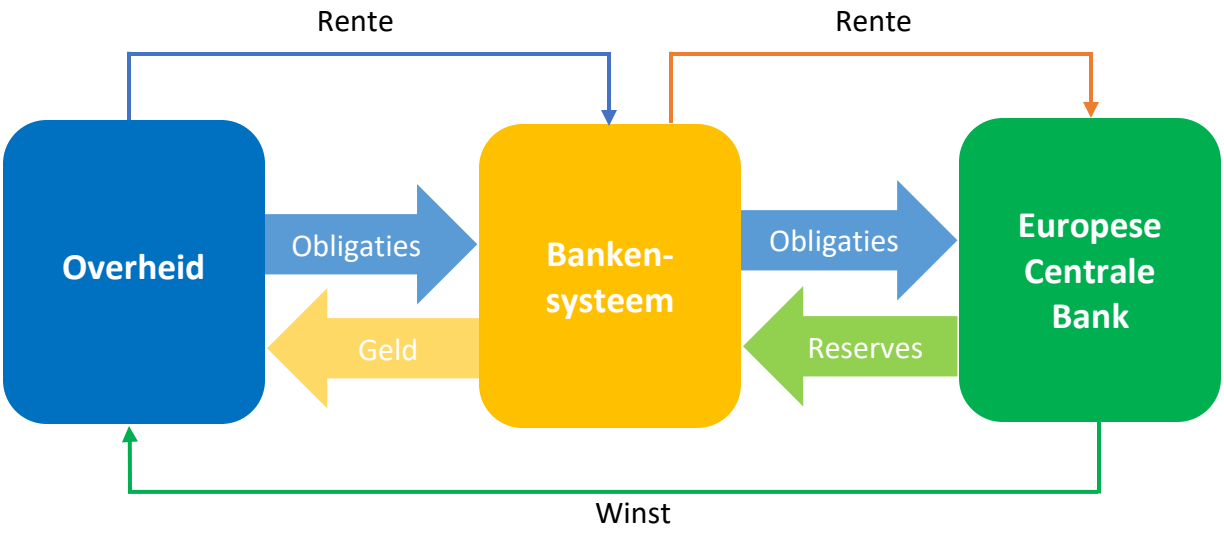
Het hoofddoel van een centrale bank is het handhaven van prijsstabiliteit (ECB, 2019). Daarnaast wordt er ook monetair beleid ingezet om economische recessies en werkeloosheid tegen te gaan. De belangrijkste instrumenten die de centrale bank gebruikt, zijn het reguleren van de rentestanden en het bepalen van minimumreserves voor banken. Banken dienen reserves aan te houden op hun rekeningen bij de Europese Centrale Bank (ECB). De ECB stelt vast hoe hoog deze minimumreserves moeten zijn. Voor elke €100 aan deposito's van een klant, houdt een bank bijvoorbeeld €2 als reserve op kas bij de ECB. De bank leent de overige €98 uit. De ECB kan door de minimale reserves te verhogen of te verlagen het totale krediet uitbreiden of verminderen.

De ECB kan daarnaast rentestanden bepalen door het opkopen van staatsobligaties en andere effecten op de open markt. Dit proces werkt in de Europese Monetaire Unie als volgt. Een overheid verkoopt een ***staatsobligatie*** aan het bankensysteem, waar ze geld voor terugkrijgen. Een staatsobligatie is een staatslening waar rente op staat.[146] Deze rente wordt overgemaakt naar de bank die de obligatie heeft gekocht. De bank kan daaropvolgend de obligatie als onderpand onderbrengen bij de ECB in ruil voor leningen. Hierdoor wordt de bank weer meer liquide. De rente die de bank betaalt op de leningen aan de ECB wordt weer als winst uitgekeerd aan de overheid. De winsten die een overheid boekt op geldproductie wordt ook wel ***seigniorage*** genoemd. In het volgend plaatje vind je een schematische weergave van het proces van ***centraal bankieren***.

---

[145] Veel landen hebben tijdens de Grote Depressie van de jaren 30 in de 20e eeuw de goudstandaarden losgelaten. Aan het eind van de Tweede Wereldoorlog, in 1944, werd er het Bretton Woods-systeem ingesteld. Volgens het systeem werd de US Dollar gekoppeld aan goud en werd er voor andere valuta een vaste wisselkoers met de dollar bepaald. Zo was er indirect een herinvoering van de goudstandaard. John Maynard Keynes is één van de belangrijkste architecten geweest van het Bretton Woods-systeem. Toen aan het begin van de jaren 70 meer landen hun dollarvoorraden begonnen om te zetten in goud, mede doordat de Verenigde Staten de geldpers hadden opgeschroefd om dure overheidsprojecten als de oorlog in Vietnam te financieren, had de Verenigde Staten onder president Nixon in 1973 de koppeling tussen de US Dollar en goud losgelaten.

[146] Halverwege december 2019 is de rente op Nederlandse 10-jarige staatsobligaties ongeveer -0,18%. Zie voor de actuele koers, https://www.iex.nl/Rente-Koers/190118356/Nederland-10-jaar.aspx.



Afbeelding 120: Geldcreatie door het opkopen van staatsobligaties.

Dit wordt ook wel ***kwantitatieve geldverruiming*** genoemd en leidt tot een groei in de totale geldhoeveelheid.[147] De geldhoeveelheid kan daarnaast ook groeien door een proces dat fractioneel reservebankieren heet.

Fractioneel reservebankieren

Bij ***fractioneel reservebankieren*** houden commerciële banken slechts een deel van het aan hun toevertrouwde geld in direct beschikbare vorm aan. Het overgrote deel lenen ze uit. De ECB bepaalt wat het percentage is dat banken als reserve moeten aanhouden. Als we in ons voorbeeld aannemen dat dit percentage 2% is, dan kan de bank van €100 die ze toevertrouwd krijgen €98 uitlenen in krediet. Als de €98 weer in het bankensysteem komt, wordt daarvan weer 2% in reserve bewaard en kan er €96,04 worden uitgeleend. Als dat geld weer in het bankensysteem komt, wordt er weer 2% in reserve bewaard en leent het bankensysteem €94,12 uit. Als dit proces zich blijft herhalen, kan er van €100 in omloop, ongeveer €100 x (100 / 2%) = €5.000 euro in omloop komen. Dit is voornamelijk geld dat als krediet is gecreëerd.

In de volgende tabel vind je een preciezere uitwerking van de berekening.

[147] De manieren waarop centrale banken werken, kunnen verschillen tussen landen. In dit boek geven we als voorbeeld hoe de Europese Centrale Bank werkt.

Stortingsnummer	Bedrag gestort	Uitgeleend	Reserves
1	€100,00	€98.00	€2,00
2	98,00	96,04	1,96
3	96,04	94.12	1,92
4	94,12	92,24	1,88
5	92,24	90,40	1,84
…	…	…	…
291	0,26	0,25	0,01
Totaal:	€4985,93	€4885,93	€99,75

Tabel 6: Berekening van de hoeveelheid geld in omloop wanneer er bij fractioneel reservebankieren een reserve van 2% wordt aangehouden.

Het gevolg van fractioneel reservebankieren is dat de omvang van krediet in relatie tot de reserves aanzienlijk groter is.

Ludwig von Mises schreef in *The Theory of Money and Credit* (1912) over de volgende vier consequenties van fractioneel reservebankieren:

1. Het kan leiden tot hogere ***inflatie***, de stijging van het algemene prijspeil in een economie.[148]
2. Het kan leiden tot een herverdeling van welvaart.[149]
3. Het kan leiden tot paniek in het bankensysteem.
4. Het kan leiden tot conjunctuurcycli.

[148] Inflatie betekent letterlijk opblazen. Monetaire inflatie betekent het opblazen van de geldhoeveelheid.

[149] Wanneer er meer geld in omloop komt, wordt het geld niet gelijkmatig verdeeld over de economie. Hierdoor stijgen prijzen tussen de verschillende goederen onevenredig. Dit wordt ook wel het ***Cantillon-effect*** genoemd, vernoemd naar de 18e-eeuwse Iers-Franse econoom Richard Cantillon. Friedrich Hayek beschrijft het als een proces waarbij je honing in een kopje doet. De honing zal eerst wat klonteren in het midden van het kopje voordat het zich uitspreidt. Volgens de Oostenrijkers leidt dit tot een herverdeling van welvaart, waarbij de mensen die het nieuw geproduceerde geld eerst in handen krijgen, het geld tegen volledige waarde kunnen uitgeven. Door inflatie is het geld al gedevalueerd voordat het in de handen komt van de rest van de samenleving. Inflatie wordt om deze reden ook wel een belasting op de toekomstige koopkracht genoemd. Het herverdeelt namelijk welvaart door de toekomstige koopkracht van mensen die het geld later ontvangen te verschuiven naar mensen die het geld eerder ontvangen. Omdat weinig mensen op de hoogte zijn van deze consequentie van inflatie, wordt inflatie ook wel een geheime belasting genoemd. Aangezien de overheid onder het huidige financiële systeem bij geldcreatie als één van de eersten het geld ontvangt, is inflatie een belangrijk middel voor de overheid om zichzelf, naast belastingheffing, te financieren.

Belangrijke redenen voor kwantitatieve geldverruiming

De belangrijkste effecten van kwantitatieve geldverruiming zijn:

1. Lagere rente, omdat een expansie van de geldhoeveelheid de prijs van kortlopend geld verlaagt. De prijs van financiële middelen als geld is namelijk ook onderhevig aan vraag en aanbod. Een hogere vraag naar geld, terwijl het aanbod gelijk blijft, zou leiden tot een hogere rente. Een gelijke vraag naar geld, terwijl het aanbod stijgt, leidt daarentegen tot een lagere rente. De rente kun je hierbij zien als de kosten om geld te lenen.
2. Meer leningen, omdat de lagere rentetarieven het aantrekkelijker maken voor consumenten en bedrijven om nieuwe leningen aan te gaan.
3. Meer uitgaven, omdat de lagere rentetarieven het minder aantrekkelijk maken om geld op een spaarrekening te laten staan.
4. Minder werkeloosheid, omdat bedrijven door de leningen meer kapitaal krijgen. Daarnaast kunnen ze meer verkopen realiseren door toegenomen consumentenbestedingen. Dit alles stimuleert bedrijven om ook meer werknemers aan te nemen.
5. Meer vertrouwen in de economie, omdat deze wordt aangejaagd door meer investeringen en meer bestedingen.
6. Op langere termijn kan dit leiden tot meer inflatie. Als de Centrale Bank vindt dat de inflatie te laag is, is kwantitatieve geldverruiming een aantrekkelijk middel om de inflatie te verhogen. De Europese Centrale Bank probeert de inflatie op de middellange termijn dicht onder de 2% te houden (ECB, 2019).

John Maynard Keynes was een groot voorstander van kwantitatieve geldverruiming in tijden van economische crises. Daarnaast wilde hij meer overheidsbestedingen en lagere belastingen om een economie uit een recessie te stimuleren.

13.4.2 De Oostenrijkers over centraal bankieren en fractioneel reservebankieren

De Oostenrijkse School is echter fel tegen een centraal gepland geldsysteem en verzet zich daardoor ook hevig tegen het monetaire en fiscale beleid om de economie te beïnvloeden. De Oostenrijkers geloven dat kwantitatieve geldverruiming op de korte termijn inderdaad leidt tot economische voorspoed, maar wijzen erop dat kunstmatig laag gehouden rentestanden ook leiden tot investeringen in projecten die in een vrije markt niet profitabel zouden zijn. De economie wordt volgens de Oostenrijkse School door de lage rentes dus overspoeld door

malinvesteringen en een hogere schuldenberg. Deze situatie kan uiteindelijk uitmonden in een economische zeepbel.[150]

Philipp Bagus stimuleert ons in *The Tragedy of the Euro* (2012) om het volgende voor te stellen. Stel je voor dat je de macht van de ECB hebt dat jij als enige persoon geld kan produceren. Zou je mensen dan niet proberen te overtuigen dat geldproductie belangrijk is voor hun eigen bestwil? Zou je ook niet economen inhuren die jouw corresponderende monetaire theorieën ondersteunen? Zou je ook niet zeggen dat je zo onmisbaar bent dat zonder jou de economie ineenstort? (pp. 73-75) De belangrijke vragen die Bagus hierbij impliciet stelt, zijn of dit systeem niet vanuit eigenbelang wordt onderhouden door een financiële elite en of er geen beter alternatief is.

Vrij bankieren als alternatief voor monopolie op geldproductie

Als alternatief voor het huidige geldsysteem, wilde Friedrich Hayek het monopolie op geldproductie ontwrichten. In 1976 publiceerde Hayek een essay getiteld 'Choice in Currency', waarop hij vrij veel kritiek kreeg. In dit essay pleitte Hayek voor vrijemarktcompetitie in de industrie van geldproductie. Hij schreef dat we het exclusieve recht voor instituten om geld te mogen produceren en het exclusieve recht voor overheden om mensen te dwingen het geld te accepteren, moeten afschaffen.[151] Het idee achter de privatisering van geldproductie is dat er onder de verschillende valuta meer concurrentie plaatsvindt en private geldproducenten daardoor worden gestimuleerd om goed geld te produceren. De wisselkoersen tussen de

[150] De Oostenrijkers geloven dat de financiële crisis van 2007-2008 het gevolg is van de lage rentestanden die de Amerikaanse Centrale Bank, de ***Federal Reserve***, heeft doorgevoerd in 2001. Nadat de dot.com zeepbel was geklapt in 2000-2001, probeerde de Federal Reserve een financiële crisis af te wenden door de rente te verlagen van meer dan 6% in 2001 naar 1% in 2003-2004. Het gevolg, volgens de Oostenrijkers, is dat het goedkoop vrijgekomen geld voornamelijk door mensen werd gebruikt om te investeren in de huizenmarkt. Hierdoor ontstond er een huizenzeepbel die uiteindelijk een financiële crisis inleidde in 2007-2008, toen de zeepbel was geklapt. Voor uitgebreidere informatie over hoe de financiële crisis van 2007-2008 is ontstaan vanuit het perspectief van de Oostenrijkers, zie *Meltdown* (2009) van Thomas Woods.

[151] Friedrich Hayek (1976) schreef het volgende:

> "The best the state can do with respect to money is to provide a framework of legal rules within which the people can develop the monetary institutions that best suit them… if we could prevent governments from meddling with money, we would do more good than any government has ever done in this regard. And private enterprise would probably have done better than the best they have ever done." (p. 22)

verschillende valuta zouden hierbij variabel zijn. Dit is geld waar mensen, uit hun eigen keuzevrijheden, zelf voor kiezen om te gebruiken.

In *The Denationalisation of Money* (1976) veronderstelt Hayek dat competitie leidt tot de adoptie van betaalmiddelen met de grootste stabiliteit in waarde. Volgens Hayek is het waarschijnlijk dat de stabiele betaalmiddelen een koppeling hebben met een mandje van grondstoffen. Een systeem waarbij het bankieren volledig wordt overgelaten aan de vrije markt wordt ook wel ***vrij bankieren*** genoemd. Rentestanden worden onder het systeem van vrij bankieren niet vastgesteld door een centrale bank of overheid, maar door een natuurlijke vraag naar en aanbod van beschikbaar geld.

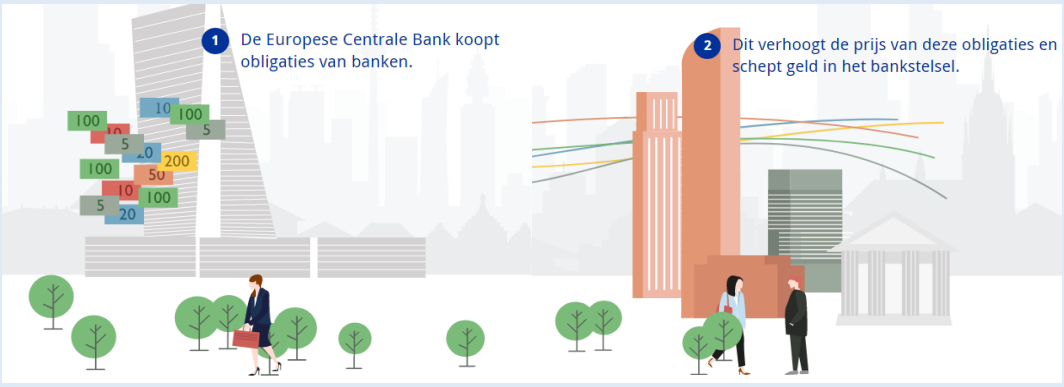
Naast het argument dat vrij bankieren zou leiden tot stabielere valuta, worden ook de volgende argumenten aangedragen door voorstanders:

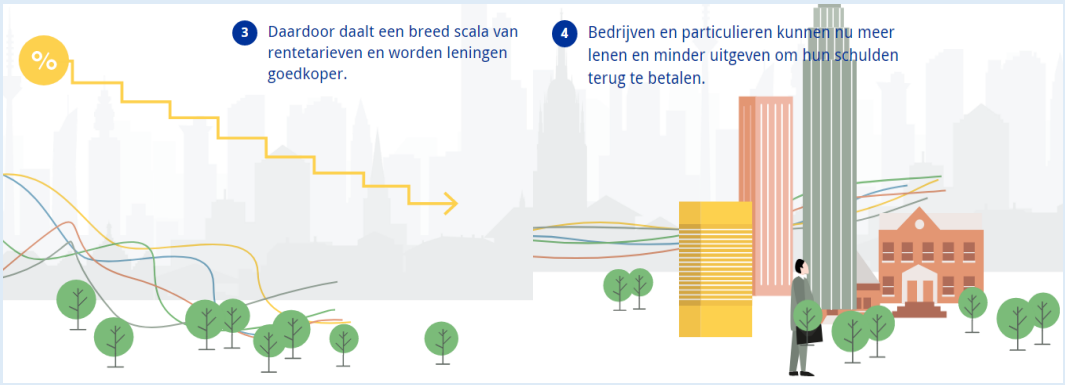
1. Burgers hebben vrijheid in geldkeuze, omdat er geen wettelijk verplichte betaalmiddelen zijn.
2. Burgers hebben vrijheid om financiële instellingen op te richten zonder vergunningen.
3. Burgers hebben vrijheid om financiële diensten aan te bieden.
4. Burgers hebben vrijheid om zelf betaalmiddelen te produceren en van hun eigen merk uit te geven. (RatioVincit.nl, z.d.)

Onder de Oostenrijkers is er geen eensgezindheid of fractioneel reservebankieren moet worden toegestaan onder het vrij bankieren. Oostenrijkers als Friedrich Hayek, George Salin en Michael Rozeff vinden dat het moet worden toegestaan onder vrij bankieren. Anderen, zoals Murray Rothbard, Hans Hermann Hoppe en Walter Block zijn tegenstanders van fractioneel reservebankieren. Zij zien het als een vorm van financiële fraude en zijn een voorstander van ***volle reservebankieren***. Bij volle reservebankieren dient een bank 100% reserve aan te houden.

Intermezzo: Kwantitatieve geldverruiming in 7 plaatjes

De ECB heeft op haar website in 7 plaatjes uitgelegd hoe kwantitatieve geldverruiming werkt. Deze zijn als volgt.





13.5 Bitcoin en de Oostenrijkers

Satoshi Nakamoto's onenigheden met centraal bankieren en fractioneel reservebankieren sluiten goed aan op de kritiek die de Oostenrijkers leveren op het huidige financiële systeem. Hieronder volgt een tabel waarin de ideeën van de Oostenrijkse School met betrekking tot het financiële systeem zijn afgezet tegen de eigenschappen van Bitcoin.

Oostenrijkse School van de Economie	Bitcoin
1. Geld is geen uitvinding van de staat.	Bitcoin is ontstaan in de vrije markt.
2. Mensen moeten vrij zijn om hun eigen betaalmiddelen uit te geven zonder vergunningen.	Naast Bitcoin kunnen mensen eigen cryptovaluta uitgeven. Het decentrale karakter van blockchain zorgt ervoor dat cryptovaluta moeilijk te reguleren zijn.
3. Geldproductie dient ook onderhevig te zijn aan vrijemarktconcurrentie.	Bitcoin doorbreekt het overheidsmonopolie op geldproductie. Bitcoin introduceert weer het vrij bankieren en is een alternatief voor nationale valuta.
4. Centrale bank moet worden opgeheven.	De beste manier om nationale valuta te bestrijden, is door een alternatief te bieden die kan concurreren. Bitcoin heeft de ambitie om het nieuwe geldsysteem te worden.
5. Burgers hebben vrijheid in geldkeuze.	De Bitcoin-community dwingt je niet om Bitcoin te gebruiken. Participeren in Bitcoin is geheel vrijwillig.
6. Lage inflatie is goed en leidt tot meer prijsstabiliteit.	De inflatie bij Bitcoin is voorgeprogrammeerd in het protocol. Om de vier jaar vindt er een halvering van de inflatie plaats. De eerste vier jaar van Bitcoin, ontving een mijner die een geldige blok heeft aangemaakt nog 50 BTC. Vier jaar later werd dat gehalveerd tot 25 BTC. Daarna is het gehalveerd naar 12,5 BTC. In mei 2020 zal de volgende halvering plaatsvinden.

Tabel 7: De monetaire wensen van de Oostenrijkse School van de Economie, afgezet tegen Bitcoin.

13.6 Samenvatting, begrippen en bronnen

Samenvatting

Er zijn over het algemeen vier grote economische stromingen: het Marxisme, het Keynesianisme, de Oostenrijkse School van de Economie en het Monetarisme. Van deze vier stromingen heeft de Oostenrijkse School een aanzienlijk grote invloed gehad op het ontstaan van Bitcoin. De Europese Centrale Bank beaamt ook dat de theoretische fundamenten van Bitcoin liggen in de Oostenrijkse School en diens kritiek op het huidige geldsysteem.

Wat de Oostenrijkse School uniek maakt, ten opzichte van de andere stromingen, is dat zij voor zo weinig mogelijk overheidsbemoeienis is en een scheiding wil van staat en geld. Hierbij hebben centrale banken volgens de Oostenrijkers geen rol van betekenis en mogen overheden geen fiscaal beleid voeren om de economie te stimuleren.

Twee kritieken die Satoshi Nakamoto heeft op het huidige geldsysteem, waar veel van de Oostenrijkers ook mee eens zijn, is dat de centrale bank moet worden vertrouwd om het geld niet te devalueren en dat commerciële banken moeten worden vertrouwd dat zij niet te veel geld uitlenen met slechts een fractie op reserve. De kritiek van Satoshi Nakamoto heeft dus betrekking op centraal bankieren en fractioneel reservebankieren.

Bij centraal bankieren kan een centrale bank geld creëren door activa, zoals bijvoorbeeld staatsobligaties, op te kopen. Hierbij komt er meer geld in omloop. Het gevolg van een groter geldaanbod is dat de rente lager wordt, waarna het goedkoper is om geld te lenen. Dit stimuleert de economie. Het proces van geldcreatie door activa-aankopen heet kwantitatieve geldverruiming.

Bij fractioneel reservebankieren, houden commerciële banken een fractie van het geld dat hun is toevertrouwd op reserve en lenen ze de rest uit. Een reservepercentage van 10%, betekent dat er ongeveer 10 keer meer geld in omloop kan komen, voornamelijk in de vorm van krediet.

De Oostenrijkse School gelooft dat het monetaire beleid van centrale banken en de geldgroei door fractioneel reservebankieren kan leiden tot conjunctuurgolven en kredietzeepbellen. De Oostenrijkers vinden Bitcoin een interessant fenomeen, omdat het het monopolie op geldproductie wegneemt bij overheden en centrale banken en omdat Bitcoin het vrij bankieren introduceert.

Opmerkingen die je nu kunt uitleggen

- De Oostenrijkse School van de Economie heeft een aanzienlijke invloed gehad op Bitcoin.
- De Oostenrijkse School is voor zoveel mogelijk vrije markt en zijn om deze reden tegen activa-opkoopprogramma's van centrale banken.
- Bitcoin introduceert weer het vrij bankieren.
- Er wordt nieuw geld geschept door centraal bankieren en fractioneel reservebankieren.
- De Oostenrijkse School gelooft dat als er meer concurrentie is in geldmiddelen en mensen de keuzevrijheid hebben om zelf te kiezen welke geldmiddelen zij gebruiken, er meer innovatie in de geldindustrie komt.
- Het huidige geldsysteem zorgt volgens de Oostenrijkse School tot meer instabiliteit van het financiële systeem.

Verklarende begrippenlijst

Arbeidswaardeleer: De waardeleer die ervan uitgaat dat de waarde van een goed of dienst bepaald wordt door de arbeid die in het goed of dienst is gestopt.

Cantillon-effect: Wanneer meer geld in omloop komt, wordt het geld niet gelijkmatig verdeeld over de economie. Hierdoor stijgen prijzen van verschillende goederen onevenredig.

Centraal bankieren: De manier waarop centrale banken hun beleid voeren.

Fractioneel reservebankieren: Commerciële banken houden slechts een fractie van het aan hun toevertrouwde geld in direct beschikbare vorm aan. Het overgrote deel lenen ze uit.

Volle reservebankieren: De bank moet 100% reserve aanhouden van het bedrag dat hen is toevertrouwd.

Inflatie: De stijging van het algemene prijspeil in een economie. Veel Oostenrijkers definiëren inflatie als de groei in de geldhoeveelheid wat, ceteris paribus, leidt tot een stijging van het algemene prijspeil.

Kwantitatieve geldverruiming: Vorm van directe geldschepping door centrale banken, waarbij deze activa zoals staatsobligaties opkoopt om meer geld in omloop te brengen. Kwantitatieve geldverruiming wordt toegepast om de economie te stimuleren. De wens van de Europese Centrale Bank is om het inflatieniveau terug te brengen naar onder, maar dicht bij de 2%.

Marginaal nut: Het marginaal nut van een goed of dienst is de verandering in de bevrediging of voordeel dat afkomstig is van een toename in de consumptie van het goed of dienst.

Seigniorage: De winst die een centrale bank boekt op geldproductie.

Staatsobligatie: Een lening die wordt uitgegeven door de overheid.

Subjectieve waardeleer: Waardetheorie die beweert dat de waarde van een goed of dienst afhankelijk is van de subjectiviteit van de mens. Dit staat in contrast met de arbeidswaardeleer.

Vrij bankieren: Een volledig vrije markt van geld en bankieren. Hierbij is er geen centrale bank of overheid meer die het geld reguleert.

Bronnen

Bagus, T. (2012). *The tragedy of the Euro*. Auburn, Al. Von Mises Institute.

Cox, J. (2007). *The concise guide to economics*. Auburn, Ala.: Ludwig Von Mises Institute.

European Central Bank. (2012). *Virtual Currency Schemes*. Geraadpleegd van https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank. (2017, 8 mei). Waarom zijn stabiele prijzen belangrijk? Geraadpleegd op 23 december 2019, van European Central Bank website: https://www.ecb.europa.eu/explainers/tell-me-more/html/stableprices.nl.html

Hayek, F.A. (1974). Choice in Currency: a way to stop inflation. London. The Institute of Economic Affairs.

Hayek, F.A. (1976). *Denationalisation of money: an analysis of the theory and practice of concurrent currencies*. London: Institute Of Economic Affairs.

IEX. (2019). Nederland 10 jaar staatsobligaties. Geraadpleegd op 23 december 2019, van iex.nl website: https://www.iex.nl/Rente-Koers/190118356/Nederland-10-jaar.aspx

von Mises, L. (1912). *The theory of money and credit*. Geraadpleegd van https://mises.org/library/theory-money-and-credit

von Mises, L. (1928). Monetary Stabilization and Cyclical Policy. Geraadpleegd van https://mises.org/library/causes-economic-crisis-and-other-essays-and-after-great-depression/html/c/193

Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency [forum]. Geraadpleegd van http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

RatioVincit, (z.d.). Vrij Bankieren in 25 Vragen en Antwoorden. Geraadpleegd op 23 december 2019, van Ratiovincit.nl website: http://www.ratiovincit.nl/VrijBankieren.html

Woods, T. (2009). *Meltdown*. Washington, DC. Regnery Publishing.

14. Cryptoanarchisme en de cypherpunk-beweging

"Bitcoin is the future. Act like you believe it. Act to prevent corruption of the system. Act to prevent Bitcoin becoming coopted in any way. We must preserve the principles of Satoshi Nakamoto."

- Amir Taaki (2013)

"It's [Bitcoin] very attractive to the libertarian viewpoint if we can explain it properly. I'm better with code than with words though."

- Satoshi Nakamoto (2008)

"Cypherpunks are activists who advocate the mass use of strong cryptography as a way protecting our basic freedoms against this onslaught."

- Julian Assange (2012)

14.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Wat cryptoanarchisme is en hoe dit zich verhoudt tot het libertarisch anarchisme.
- Hoe de cypherpunk-beweging is ontstaan.
- Wat de filosofische achtergrond is van waaruit de Bitcoin blockchain is ontstaan.
- De voornaamste mensen kennen die technologieën hebben ontwikkeld van waaruit blockchain is ontstaan.
- Hoe de filosofische ideeën van het cryptoanarchisme hebben geleid tot bepaalde eigenschappen van de Bitcoin blockchain.

Inleiding

Zoals al is gebleken uit hoofdstuk 11, Blockchain en de Belofte van het Internet, is blockchaintechnologie niet in een vacuüm ontstaan. In dit hoofdstuk herleiden we de filosofische oorsprong van waaruit deze technologie is ontwikkeld. Veel van de bestaande technologieën waar blockchain op gebaseerd is, zijn ontwikkeld door cryptoanarchisten en

cypherpunks. We gaan zien dat het cryptoanarchisme en cypherpunk technologieën hebben ontwikkeld die weer zijn toegepast bij de Bitcoin blockchain. Deze technologieën zijn ontwikkeld om privacy en andere vrijheden te waarborgen.

In paragraaf 14.2 wordt het cryptoanarchisme besproken. Vervolgens komt in 14.3 cypherpunks en hun verlangen om een anoniem geldsysteem te ontwikkelen aan bod. Paragraaf 14.4 trekt de relatie tussen het cryptoanarchisme en het anarchokapitalisme. In 14.5 trekken we een parallel tussen het cryptoanarchisme en de eigenschappen van de Bitcoin blockchain. Het hoofdstuk wordt vervolgens afgesloten met een samenvatting, een lijst van de belangrijkste begrippen en een bronnenlijst.

14.2 Cryptoanarchisme

In de jaren 70 en 80 was een groep cryptografen en computerengineers ongerust over de privacyschendingen van overheden. Daarnaast voorspelden zij dat de samenleving steeds digitaler zou worden, wat uiteindelijk kan leiden tot meer individuele vrijheden, meer economische voorspoed, meer kennisdeling en een drastisch nieuwe manier waarop mensen kunnen socialiseren. Zij vreesden echter ook voor de potentiële grip die overheden op zo'n samenleving zouden kunnen krijgen.

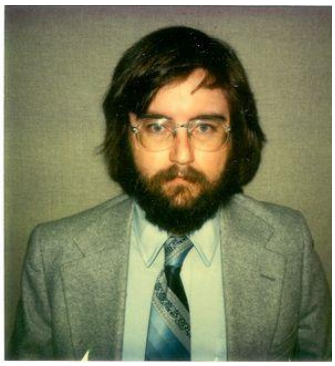
Een dergelijk sentiment werd gedeeld door Paul Armer, vroegere manager en docent aan de Computer Science-afdeling van Stanford University, in 1975. Hij schreef in het artikel 'Computer Technology and Surveillance' (1975), dat een groep van experts in computers, communicatie en surveillance bijeenkwamen om het volgende vraagstuk te onderzoeken:

> "Stel voor dat jullie adviseurs zijn van het hoofd van de KGB, de geheime politie van de Sovjet-Unie. Stel ook voor dat jullie de taak wordt gegeven om een systeem te ontwerpen voor de surveillance van alle burgers en bezoekers binnen de grenzen van de Sovjet-Unie. Het systeem dient niet te indringerig en opzichtig te zijn." (p. 12)

Het systeem dat door de groep experts werd bedacht, was een Electronic Fund Transfer System (EFTS). Het systeem zou alle financiële transacties verwerken en voorzien zijn van de benodigde statistieke analyses die werden overlegd aan de overheid. Met het systeem zouden accounts worden gesloten en transacties worden geblokkeerd. Daarnaast zou de overheid volledig inzicht hebben in welke aankopen je doet, de tijd van de aankopen en ook waar je je bevindt bij

de aankopen. Hierbij vertelt Armer dat hij zich minder zorgen maakt om de bankiers die zijn privacy schenden, maar dat hij banger is dat deze bankiers onder druk van de overheid worden gedwongen om EFTS te gebruiken voor surveillance ten bate van die overheid. Volgens Armer dienen we ons te bekommeren om surveillance, omdat het ons dwingt om te conformeren aan bepaalde gedragingen. Onze creativiteit en onze mogelijkheden om onszelf authentiek uit te drukken, zouden ernstig lijden aan de druk om te conformeren. Het gevolg, volgens Armer, is dat we in zo'n omgeving onze authenticiteit verliezen. (p. 12-13)

Eind jaren 80 ontstond er uit eenzelfde ongerustheid de cryptoanarchistische beweging. Timothy May, een voormalig elektro-engineer bij IBM en mede-oprichter van deze beweging, introduceerde het idee van ***cryptoanarchisme*** op de Crypto '88-conferentie. Hij vond hier gelijkgestemden onder de techno-anarchistische factie die bij de conferentie aanwezig was en deelde zijn zelfgeschreven cryptoanarchistische manifesto met de groep. Hetzelfde manifesto, genaamd 'The Crypto Anarchist Manifesto' (1988), deelde hij op 22 november 1992 ook met de mensen die op de Cypherpunk mailing list stonden.



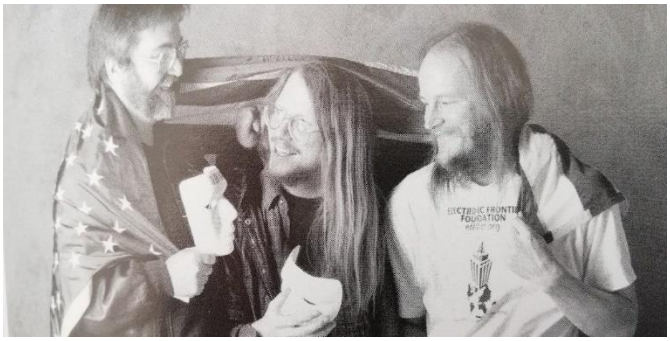
Afbeelding 121: Timothy May.

May beschrijft in het manifesto dat een geest rondwaart in de moderne wereld, de geest van het cryptoanarchisme.[152] Het basisprincipe van het cryptoanarchisme is dat totale anonimiteit, totale vrijheid van meningsuiting en totale vrijheid van handel mogelijk worden gemaakt middels versleutelde communicatie. Volgens May gaat onbreekbare cryptografie zelfs nog verder dan het slechts kunnen faciliteren van anonimiteit en de vrijheden van meningsuiting en handel: het trekt zelfs het concept van natiestaten in twijfel. In 'Crypto Anarchy and Virtual Communities' (1994), schrijft May dat de combinatie van onbreekbare public key cryptografie en virtuele netwerk communities in cyberspace zullen leiden tot grote maatschappelijke veranderingen. Hij omschrijft cryptoanarchie als een realisatie van anarchokapitalisme en dat het ons de mogelijkheden zal bieden om vrijwillige economische interacties met elkaar aan te gaan.[153] We bespreken in een latere paragraaf wat het anarchokapitalisme is.

[152] Met deze openingszin steekt Timothy May de draak met *Het Communist Manifesto* (1850) van Karl Marx dat begint met: "A specter is haunting Europe – the specter of Communism".

[153] Timothy May (1994) schrijft:

14.3 Cypherpunk



Afbeelding 122: De drie oprichters van de cypherpunk-beweging. Van links naar rechts zijn dat Timothy May, Eric Hughes en John Gilmore.

Op 19 november 1992, nodigden Timothy May, Eric Hughes en John Gilmore[154] een groep gelijkgestemden uit om samen te komen in het huis van Eric Hughes. De bijeenkomst ging voornamelijk over hoe crypto-instrumenten dienen te worden gebruikt om de voor hen essentiële vrijheden te kunnen bewaken. Hierbij bespraken zij ook *The Crypto-Anarchist Manifesto* van May. De politieke filosofie die deze mensen bewoog, was sterk libertarisch van aard. Zij vonden dat cryptografie een te belangrijke uitvinding was om het alleen over te laten aan overheden en bedrijven. Dit was het begin van een beweging die later bekend zou staan als de ***cypherpunk***-beweging.[155] (Levy, 2005, pp. 263-265)

Binnen een maand na de eerste bijeenkomst werd een online discussieomgeving opgezet, waarin ze ideeën uitwisselden met betrekking tot cryptosystemen. Enkele weken na de opzet van de omgeving hadden meer dan 100 mensen zich geregistreerd op de mailing list en schreef Hughes het 'Cypherpunk Manifesto' (1992). Julian Assange en Rop Gonggrijp, de medeoprichters van respectievelijk Wikileaks en XS4ALL, zijn overigens twee van de vele noemenswaardige personen die ook lid waren van de Cypherpunk mailing list.

> "The combination of strong, unbreakable public key cryptography and virtual network communities in cyberspace will produce interesting and profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to make the economic arrangements they wish to make consensually."

[154] Naast het belangrijke werk dat John Gilmore deed voor de cypherpunks, was hij in 1990 ook mede-oprichter van de Electronic Frontier Foundation (EFF) met Steve Wozniak, John Perry Barlow en Mitch Kapor. De EFF is een stichting die civiele rechten en vrijheden op het internet promoot.

[155] Cypherpunk is een afgeleide van de woorden "cipher" en "cyberpunk". Een cipher is een algoritme voor de uitvoering van encryptie en decryptie. Cyberpunk is een subgenre binnen sciencefiction, waarin technologische en wetenschappelijke ontwikkelingen een centrale rol spelen.

14.3.1 De essentie van privacy

Het 'Cypherpunk Manifesto' biedt een verdediging voor anonieme transacties door eerst het essentiële verschil tussen 'privacy' en 'geheimhouding' te bespreken. Privacy wordt hierin uitgelegd als de macht om jezelf selectief te onthullen aan de wereld, terwijl geheimhouding een middel is om iets te verbergen wat niemand mag weten. Als je een tijdschrift koopt met contant geld, hoeft de kassière niet te weten wie je bent. Als je een e-mail verstuurt, hoeft de e-mail provider ook niet te weten wat de inhoud is van de berichten die je verstuurt en ontvangt. De taak van de e-mail provider is om te weten hoe hij jouw e-mail kan afleveren bij de juiste bestemming en hoeveel je hem moet betalen voor deze dienstverlening. Een anoniem systeem stelt de gebruiker in staat om alleen de relevante gegevens van zijn identiteit te onthullen, wanneer hij wil en wanneer het benodigd is. Dat is volgens Hughes de essentie van privacy. Cryptografie is de sleuteltechnologie die dit mogelijk maakt en cypherpunks zijn toegewijd aan het bouwen van zulke cryptosystemen.

14.3.2 Anoniem elektronisch geldsysteem

Cypherpunks zijn praktische idealisten die werkende applicaties ontwikkelen om hun idealen te realiseren. Wat opvalt in het 'Cypherpunk Manifesto' is dat naast anonieme e-mailsystemen en digitale handtekeningen ook expliciet anoniem elektronisch geld wordt genoemd. Het technische fundament voor anoniem elektronisch geld werd gelegd door de cryptograaf David Chaum.[156] In 1985 schreef hij 'Security without Identification: Transaction Systems to Make Big Brother Obsolete'. In dit artikel schrijft Chaum dat het mogelijk is om in de nabije toekomst een digitaal geldsysteem te ontwikkelen dat de privacy en beveiliging van individuen en organisaties waarborgt. Hierin spreekt hij zich uit tegen de "dossiersamenleving", een samenleving waarin computersystemen worden ingezet om mensen te monitoren. In deze samenleving, voorspelt Chaum, is data over mensen waardevol en zullen ze worden verkocht zonder dat deze mensen dat weten. In het ernstigste geval worden de data ingezet om publieke opinies en verkiezingen te manipuleren, of is surveillance dermate alom vertegenwoordigd dat mensen niet meer vrij hun mening kunnen of durven te uiten.[157]

---

[156] David Chaum is overigens ook de uitvinder van DigiCash, een anoniem geldsysteem dat gebruikmaakte van blind signatures. De werking van DigiCash is gebaseerd op zijn eerder geschreven artikel, 'Blind Signatures for untraceable Payments' (1983).

[157] Het lijkt erop dat we momenteel al leven in de "dossiersamenleving" waar David Chaum ons voor waakt. Volgens de klokkenluiders, Robert Epstein en Zachary Vorrhies, bemoeit Google zich al actief met verkiezingsresultaten. Dat doet Google met behulp van bijvoorbeeld subjectieve autocomplete suggesties en een

Wei Dai en B-Money

Afbeelding 123: Wei Dai.

Door de jaren heen hebben verscheidene cypherpunks geprobeerd om anonieme geldsystemen te ontwikkelen. Hierbij ontwikkelden zij ook technologieën die later werden toegepast bij Bitcoin. Wei Dai heeft bijvoorbeeld in 1998 het concept van B-Money ontwikkeld, een anoniem geldsysteem dat net als Bitcoin gebruikmaakt van de Hashcash Proof-of-Work-functie.[158] De Hashcash-functie is zelf weer ontwikkeld door een andere cypherpunk, Adam Back.[159]

Wei Dai maakt in zijn essay over B-Money duidelijk dat hij gefascineerd is door het cryptoanarchisme van Timothy May. Hij ziet een cryptoanarchistische community als een omgeving waarin geweld onmogelijk is, omdat de deelnemers niet kunnen worden gelinkt aan hun ware namen en fysieke locaties. Een dergelijke gemeenschap moet werken op basis van vrijwillige samenwerking. Wei Dai gelooft dat het kunnen forceren van contracten en het hebben van een geldsysteem essentieel zijn voor efficiënte samenwerking. B-Money is een geldsysteem waarbij nodes, net als bij Bitcoin, ook geld kunnen creëren als zij een moeilijk wiskundig probleem oplossen. Net als bij Bitcoin wordt hierbij geld overgedragen van persoon A naar persoon B door de transactie uit te zenden naar een netwerk van nodes.[160]

---

partijdig rankingmechanisme van zoekresultaten. Vorrhies heeft als bewijslast meer dan 1.000 interne Google-documenten geüpload naar Project Veritas.

[158] De kleinste eenheid van Ether is vernoemd naar Wei Dai. Deze heet namelijk een “Wei” en is gelijk aan 1/1.000.000.000.000.000.000 Ether.

[159] Adam Back is de CEO van Blockstream, een onderneming die de ontwikkeling van Bitcoin Core helpt financieren. Bitcoin Core is de voornaamste Bitcoin-software.

Hashcash is bedoeld om e-mail spam tegen te gaan door de verzender van een e-mail eerst een cryptografische puzzel te laten oplossen, voordat de e-mail daadwerkelijk wordt verstuurd. Hierbij wordt de metadata van een e-mail (het ‘from’-adres, het ‘to’-adres, de tijd, etc.) geformaliseerd in een protocol. De verzender van de e-mail dient daarnaast ook een nonce toe te voegen, die samen met de metadata wordt gehasht. Alleen wanneer de hash voldoet aan een bepaalde vereiste – bijvoorbeeld dat het moet beginnen met 8 nullen – is de hash geldig en wordt de e-mail verstuurd.

[160] In het essay, ‘B-Money’ (1998), schrijft Wei Dai:

> “I am fascinated by Tim May’s crypto-anarchy. Unlike the communities traditionally associated with the word ‘anarchy’, in a crypto-anarchy the government is not

Wei Dai was overigens de tweede persoon die door Satoshi Nakamoto werd benaderd. Diens essay over B-Money staat ook op de lijst van referenties in de Bitcoin white paper.

Twee andere prominente cypherpunks die we bespreken, zijn Nick Szabo en Hal Finney.

Nick Szabo, Bit Gold en smart contracts

Afbeelding 124: Nick Szabo.

Nick Szabo is duidelijk in zijn doelen als cypherpunk. Hij wil net als de meeste andere cypherpunks een vreedzame cyberspace creëren die losstaat van de staat.[161] Szabo was in de jaren 90 zeer actief in het bekritiseren van de Clipper chip.[162] Hij heeft het concept van smart contracts ontwikkeld en is tevens de uitvinder van Bit Gold, een voorloper van Bitcoin.

Szabo realiseerde zich dat voor het creëren van een staatloze omgeving op het internet, dingen als eigendom en contracten moeten kunnen worden vastgelegd. Dit is hoe hij op het idee van smart contracts kwam.[163] Net als Friedrich Hayek hield hij zich ook bezig met het vrij bankieren: een monetair systeem waarbij private partijen zelf hun eigen geld kunnen uitgeven, dat losstaat van overheden en

---

> temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations."

Wei Dai had het essay verspreid onder de Cypherpunk mailing list.

[161] Nick Szabo schrijft het volgende in zijn e-mail van 17 september 1997 naar de Cypherpunk mailing list:

> "If we step back and look at what many cypherpunks are trying to achieve, a major idealistic theme is a Ghandian cyberspace where violence can only be make-believe, whether in Mortal Kombat or 'flame wars'. … Our 20th century information commerce systems, from publishing to credit cards, have often been very dependent on the threat of violence, usually law enforcement."

Als eerbetoon aan Nick Szabo is een "Szabo" een eenheid in Ether. Deze is gezet op 1/1.000.000 Ether.

[162] De Clipper chip is in paragraaf 5.6.1 uitvoeriger besproken binnen de context van de eerste crypto-oorlog.

[163] Zie 'The Idea of Smart Contracts' (Szabo, 1997) voor meer informatie over het concept van smart contracts. Nick Szabo kwam op het idee van Bit Gold in 1998, maar heeft het pas volledig beschreven in zijn essay 'Bit Gold' (Szabo, 2005).

centrale banken. Szabo had ook gewerkt aan DigiCash van David Chaum, maar zag hierin het risico dat DigiCash een gecentraliseerde onderneming was. Hij zocht naar gedecentraliseerde alternatieven wat uiteindelijk Bit Gold werd. Net als Bitcoin en B-Money, maakt Bit Gold gebruik van een Proof-of-Work-mechanisme dat lijkt op dat van Hashcash.

Hal Finney

Afbeelding 125: Hal Finney.

Hal Finney was een andere cypherpunk die zich al vroeg bezighield met het Bitcoin-netwerk. Het was Hal Finney die de eerste Bitcoin-transactie van Satoshi Nakamoto ontving. In een e-mail naar de Cypherpunk mailing list uit 1992, schrijft Finney over het gevaar van de "dossiersamenleving" en hoe David Chaum laat zien dat cryptografie kan worden gebruikt om mensen te bevrijden en te beschermen, in plaats van te controleren.[164] In 2004 ontwikkelde hij een Reusable Proof-of-Work-systeem en tot aan zijn dood in 2013 werkte hij aan de Bitcoin-software.

Tot dusver hebben we besproken wat cryptoanarchisme en cypherpunk zijn en hebben we enkele noemenswaardige cypherpunks behandeld die van grote invloed zijn geweest op de ontwikkeling van de Bitcoin blockchain. In de volgende paragraaf bespreken we de libertarisch anarchistische filosofie die ten grondslag ligt aan het cryptoanarchisme en de doelen van vele cypherpunks. Tot slot trekken we parallellen tussen het cryptoanarchisme en de eigenschappen van de Bitcoin blockchain.

[164] Hall Finney schrijft:

> "Here we are faced with the problems of loss of privacy, creeping computerization, massive databases, more centralization – and Chaum offers a completely different direction to go in, one which puts power into the hands of individuals rather than governments and corporations. … The work we are doing here, broadly speaking, is dedicated to this goal of making Big Brother obsolete. It's important work. If things work out well, we may be able to look back and see that it was the most important work we have ever done."

Als ode aan Hal Finney, is 1/1.000 Ether vernoemd naar 1 "Finney".

Intermezzo: Internet Freedom Report

Hoe slecht is het eigenlijk gesteld met de internetvrijheden op de wereld? Freedom House (2019) heeft een rapport gepubliceerd, getiteld '*Freedom on the Net 2019*'. Volgens het rapport heeft meer dan 3,8 miljard mensen toegang tot het internet, maar leeft 71% in landen waar individuen worden gearresteerd of gevangengenomen voor het plaatsen van content over politieke, sociale of religieuze issues. 65% woont in landen waar individuen tussen juni 2018 en mei 2019 zijn aangevallen of gedood voor hun online activiteiten. 59% woont in landen waar autoriteiten online commentatoren inzetten om discussies te manipuleren. (p. 2)

Afbeelding 126: Een demonstrant draagt een Guy Fawkes masker terwijl hij protesteert tegen massasurveillance in Manila, de Filippijnen (Freedom House, 2019).

Volgens het verslag zijn 33 van de 65 landen die zijn geëvalueerd achteruitgegaan in hun internetvrijheden. De grootste achteruitgangen vonden plaats in Sudan, Kazakhstan, Brazilië, Bangladesh en Zimbabwe. IJsland en Estland presteerden het best van alle onderzochte landen. China is voor de vierde opeenvolgende keer de grootste misbruiker van internetvrijheden en hoewel de Verenigde Staten vrij goed scoort, is er al drie jaar op rij een achteruitgang. (pp. 4-5)

Overheden hebben nu meer capaciteit voor surveillance dan ooit tevoren, dankzij kunstmatige intelligentie. Freedom House raadt onder andere aan om meer transparantie te creëren in online politieke advertenties en het gebruik van bots in socialmediamanipulatie te adresseren. Daarnaast willen ze een restrictie op de export van geavanceerde instrumenten die dienen ter monitoring van burgers. China is op het gebied van online surveillance het verst. De Chinese overheid werkt samen met bedrijven om individuen online te monitoren. In maart 2019 werd bijvoorbeeld gerapporteerd dat een Oeigoer drie dagen lang was opgesloten en ondervraagd, alleen omdat iemand in zijn contactenlijst op WeChat had ingecheckt vanuit Mekka, Saudi Arabië. (p. 13) Ook de Vietnamese regering zet hoog in op online surveillance (pp. 13-16).

14.4 Cryptoanarchisme als realisatie van anarchokapitalisme

Om te begrijpen wat het doel is van cryptoanarchisme, dienen we het begrip ***anarchokapitalisme*** beter te doorgronden. Een ander woord voor anarchokapitalisme is het ***libertarisch anarchisme*** of ***voluntarisme***. Anarchokapitalisme bestaat uit de volgende twee deelwoorden: “anarchie” en “kapitalisme”. Het woord “anarchie” heeft zijn oorsprong uit het Grieks en is een samenvoeging van *an* en *arkhos* wat letterlijk “zonder heerser” betekent. Tegenwoordig wordt anarchisme regelmatig gedefinieerd als “chaos”, terwijl cryptoanarchisten het woord nog steeds in zijn letterlijke betekenis gebruiken. Cryptoanarchisten zien anarchie dus als een staat zonder heerser, ofwel een staat zonder overheid, en geloven dat een dergelijke samenleving juist zou leiden tot meer sociale harmonie. Een belangrijke eigenschap van deze samenleving is dat het puur kapitalistisch en libertarisch is.

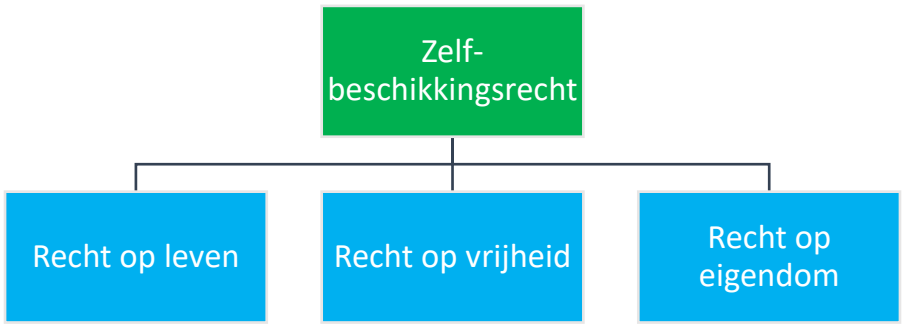
Er zijn op filosofische gronden verschillende argumenten gemaakt ter verdediging van een libertarisch anarchistische samenleving. Murray Rothbard die de term “anarchokapitalisme” had bedacht, volgt de traditie van het ***natuurrecht*** en veronderstelt dat ieder mens van nature bepaalde rechten bezit.[165]

14.4.1 Natuurrechten volgens libertariërs

Rothbard gelooft dat ieder persoon in principe het absolute recht heeft op zijn eigen lichaam. In *For a New Liberty* (1973), schrijft Rothbard dat de mens een specifieke natuur heeft om middels zijn verstand meer te leren over zichzelf en de wereld om zich heen, zodat hij waarden en middelen kan ontdekken waarmee hij zijn doelen kan bereiken. Volgens Rothbard is dit essentieel voor elk persoon, omdat het nodig is voor zijn voortbestaan. Als iemand hem verstoort in zijn natuur om zijn verstand te gebruiken, is dat anti-mens (pp. 32-33). Voor een mens om zijn verstand zelfstandig te kunnen gebruiken, dient hij ook eigendom te hebben over zijn eigen lichaam.

[165] Over het algemeen kun je de argumenten voor een libertarische samenleving onderverdelen in de consequentialistische argumenten en de deontologische argumenten. De consequentialist focust zich op de consequenties van een actie of beleid, terwijl een deontologist zich focust op de moraliteit van de actie of beleid op zich. Een libertarisch consequentialist gelooft bijvoorbeeld dat de overheid zo klein mogelijk dient te zijn, omdat dit leidt tot meer individuele vrijheden en de samenleving er over het algemeen beter van af is. David Friedman, zoon van Milton Friedman, is een voorbeeld van een libertarisch consequentialist. Een libertarisch deontologist gelooft daarentegen bijvoorbeeld dat ieder mens van nature zelfbeschikkingsrecht heeft en dat de overheid hem om die reden zoveel mogelijk vrij moet laten.

Het idee dat mensen zelfbeschikking hebben, is niet nieuw en heeft een aanzienlijke invloed gehad op de Verlichtingsfilosofen in de westerse samenleving.[166] De Britse filosoof, John Locke, schreef bijvoorbeeld al in *The Second Treatise of Government* (1689) dat iedereen een eigendom heeft in zijn eigen persoon, waar niemand recht toe heeft behalve hijzelf.[167] Zowel Locke als Rothbard beargumenteren dat het recht op eigendom en het recht op vrijheid voortvloeien uit dit ***zelfbeschikkingsrecht***.



Afbeelding 127: Volgens de natuurrechttheorie die libertariërs aanhangen, komen de rechten op leven, vrijheid en eigendom voort uit ons zelfbeschikkingsrecht. Je zou kunnen beargumenteren dat je door iemands leven af te nemen een moord pleegt. Iemand van zijn vrijheid beroven, is een vorm van slavernij. Iemand zijn eigendom ontvreemden, is diefstal. Volgens libertariërs overtreden deze drie activiteiten de natuurrechten van de mens.

Door het zelfbeschikkingsrecht kan de mens eigenaarschap nemen over middelen. Het in eigendom nemen van middelen kan hierbij gebeuren door (a) het mengen van je eigen arbeid met iets wat nog niet in beschikking was van een ander en (b) vrijwillige handel.[168] Het idee dat je ergens eigenaar van wordt door je arbeid te mengen met het betreffende middel dat nog niet eigendom is van iemand anders, is vrij intuïtief voor veel mensen. Stel je bijvoorbeeld voor dat je rondloopt in de natuur en je ziet een appel. Door in de boom te klimmen en de appel te plukken, meng je eigenlijk je arbeid met de appel en neem je de beschikking over de appel. De

[166] Een ander woord voor libertarisme is ook wel "klassiek liberalisme".

[167] John Locke beschrijft het als volgt: "… every man has a *property* in his own *person*: this is nobody has any right to but himself" (1689, p. 19)

[168] Het in eigendom nemen van middelen door je arbeid ermee te mixen, wordt ook wel "homesteading" genoemd. John Locke (1689) omschrijft homesteading als volgt:

> "The labour of his body and the work of his hands, we may say, are properly his. Whatsoever, then, he removes out of the state of nature hath provided and left it in, he hath mixed his labour with it, and joined it to something that is his own, and thereby makes it his property." (p. 19)

appel is hierdoor eigendom van jou geworden. Ook vrijwillige handel is voor veel mensen een intuïtieve manier om eigendom te verkrijgen. Als jij op vrijwillige wijze besluit om jouw EURO te verhandelen voor een appel, dan voelt het intuïtief onrechtvaardig als een ander jouw appel ontvreemdt. Door vrijwillig die appel te kopen, voel je intuïtief aan dat die appel van jou is geworden. Rothbard trekt deze zienswijze in extremen door en concludeert hieruit dat de staat onrechtmatig is.

In 'Society Without A State' (1974), definieert Rothbard een anarchistische samenleving als een samenleving zonder legale mogelijkheid om dwangmatige agressie uit te oefenen tegen een eigendom of een individu. De staat is in deze samenleving verboden, omdat de staat agressie uitoefent door private eigendom te ontvreemden in de vorm van belasting.[169]

14.4.2 Hoe de staat volgens libertariërs natuurrechten schendt

Franz Oppenheimer (1908) maakt het onderscheid tussen de ***economische middelen*** en de ***politieke middelen,*** waarmee mensen en instituten zich in stand kunnen houden. Met de economische middelen bedoelt hij het gebruiken en het verhandelen van je eigen arbeid. Onder de politieke middelen verstaat hij het in beslagnemen van de vruchten van andermans arbeid. (p. 25) De economische middelen vereisen vreedzame productie en handel, terwijl de politieke middelen geweld en dwang vereisen.

Libertariërs zien om die reden de staat ook wel als een bende bandieten. Hierbij is het belangrijk om te weten dat er onder libertariërs verschillende opvattingen bestaan over de legitimiteit van hun activiteiten.

14.4.3 Onderscheid in libertarisch minarchisten en libertarisch anarchisten

Het belangrijkste onderscheid dat we in dit boek maken, is het onderscheid in ***libertarisch minarchisten*** en ***libertarisch anarchisten***. Een minarchist is iemand die gelooft dat de overheid inderdaad de bevolking plundert in de vorm van belasting, maar dat deze plundering enigszins legitiem is als het wordt gebruikt om enkele essentiële taken in de samenleving te vervullen. Milton Friedman is een voorbeeld van een libertarisch minarchist. Hij gelooft in een ***nachtwakersstaat***, een staat waarin de overheid zich zo min mogelijk bemoeit met haar burgers.

[169] Rothbard omschrijft de staat in 'The Anatomy of the State' (1974) als een organisatie in de samenleving die de monopolie op het gebruik van geweld en dwang in een bepaald gebied handhaaft. (p. 57)

De overheid heeft volgens Friedman slechts de volgende drie functies:

1. Het verlenen van militaire defensie van een natie.
2. Het forceren van contracten tussen individuen.
3. Het beschermen van burgers tegen misdaden en diefstal.

Rothbard is echter principieel tegen enige vorm van plundering, ongeacht de doelen die ermee worden nagestreefd. Hij gelooft dus dat de staat geen inbreuk mag maken op het zelfbeschikkingsrecht en de daaruit voortvloeiende rechten als het recht op leven, vrijheid en eigendom.[170]

14.4.4 Het non-agressieprincipe

De grondgedachte van het libertarisme leunt op het centrale idee dat geen mens of groep mensen agressie mag uitoefenen op een persoon of op het eigendom van een persoon. Hierbij wordt agressie gedefinieerd als het initiëren van geweld, of de dreiging om fysiek geweld te plegen tegen een persoon of tegen het eigendom van een persoon. Deze grondgedachte wordt ook wel het ***non-agressieprincipe*** genoemd. In plaats van dwang, prefereren libertariërs voor zoveel mogelijk vrijwillige samenwerking, keuzevrijheid en zelfbestuur.

[170] De filosoof, Gerard Casey, verdedigt dit idee in *Libertarian Anarchy* (2012). Hij schrijft:

> "Overheden zijn criminele organisaties. Alle overheden, dus niet alleen de overduidelijk totalitaire of repressieve. … Deze statement is bedoeld om letterlijk te worden opgevat en niet als een vorm van retorische overdrijving. Het argument is simpel. Ontvreemding, diefstal, kidnapping en moord zijn allemaal criminele activiteiten. Zij die betrokken zijn bij zulke activiteiten, namens zichzelf of namens anderen, zijn per definitie criminelen. De overheid is betrokken bij een activiteit die moreel equivalent is aan ontvreemding of diefstal in het innen van belasting; in het opsluiten van sommige mensen in gevangenissen, met name diegenen die veroordeeld zijn van zogenaamde slachtofferloze misdaden, of wanneer het mensen oproept om te participeren in het leger, is de overheid schuldig aan kidnapping of valse opsluiting; in het betrokken zijn met oorlogen die niet uit defensieve belangen voortkomen en zelfs als ze defensief zijn, of wanneer defensieve middelen disproportioneel en willekeurig gebruikt worden, maakt de staat zich schuldig aan doodslag of moord." (p. 1)

14.4.5 Vrijwillige associatie

Libertarisch anarchisten onderschrijven dat de samenleving geen uniforme waarden heeft en dat politieke onenigheden inherent zijn aan een samenleving. Plurale waarden zorgen ervoor dat er conflicten kunnen ontstaan.[171] De vreedzaamste manier om hiermee om te gaan, volgens libertarisch anarchisten, is om iedereen het recht te geven om zichzelf af te scheiden. Vanuit het zelfbeschikkingsrecht, gebaseerd op het non-agressieprincipe en de natuurrechttheorie, hebben mensen ook het recht op ***vrijwillige associatie*** en het recht om hun eigen leiders te kiezen. Als een individu zich niet meer geassocieerd voelt bij de staat waar hij in leeft, heeft het individu het recht om zich aan te sluiten bij een andere associatie en zich af te scheiden als een nieuwe politieke eenheid. Volgens libertarisch anarchisten is er geen limiet aan de afscheiding. Provincies mogen zich afscheiden van een staat, een district van een provincie, een stad van een district, een wijk van een stad, een huishouden van een wijk en een individu van een huishouden.

14.4.6 Het kapitalisme in het libertarisch anarchisme

Volgens libertarisch anarchisten is het kapitalisme niks anders dan een systeem van vrijwillige handel van eigendom en de afwezigheid van overheden om zich te bemoeien met zulke activiteiten. Als je op de markt een appel koopt van een groenteboer, vindt vrijwillige handel plaats: jij geeft jouw geld op in ruil voor een appel. Libertarisch anarchisten geloven dat beide partijen voordelen genieten van deze vrijwillige handel. Als zij er beiden niet beter van zouden worden, uiteraard gebaseerd op hun oordeelsvermogen op dat moment, zouden zij de handel niet zijn aangegaan. In het voorbeeld van de appel waardeer jij de appel meer dan het geld dat jij ervoor hebt opgegeven. Andersom waardeert de verkoper van de appel jouw geld meer dan de appel die hij heeft opgegeven. Zodoende gaan beide partijen erop vooruit bij vrijwillige handel. Hetzelfde geldt ook voor contracten. Je gaat geen vrijwillig contract aan als je er niet beter van wordt. Dit is de reden waarom libertarisch anarchisten voorstanders zijn van het vrijemarktkapitalisme.

[171] De filosoof Bernard Williams, schreef in *In The Beginning Was The Deed* (2005) dat politiek filosofie zich voornamelijk bezighoudt met het idee van politieke onenigheden en dat deze onenigheden voortkomen uit verschillende interpretaties over politieke waarden als bijvoorbeeld vrijheid, gelijkheid en rechtvaardigheid. (p. 77)

14.4.7 Spontane orde

Het idee dat een anarchistische samenleving niet hoeft te vervallen in chaos leunt op het concept van ***spontane orde***. De grondstelling is dat mensen in een samenleving die met rust worden gelaten zelf orde aanbrengen in hun leven en in de samenleving. Dat doen ze door zelf regels te creëren, voor zichzelf en voor de samenleving waar ze in wonen. Om deze regels te bewerkstelligen, is volgens libertarisch anarchisten geen overheid nodig.

Het concept van spontane orde is duizenden jaren oud. Het speelt bijvoorbeeld een grote rol in het daoïstische gedachtegoed.[172] De haast mystieke kracht die ervoor zorgt dat mensen zich vanzelf hervormen, wordt in het Daoïsme de "Dao" genoemd. Deze mystieke kracht, die leidt tot spontane orde, wordt ook weleens vergeleken met "de onzichtbare hand" van Adam Smith. Friedrich Hayek onderschrijft het idee dat orde kan ontstaan zonder een gecentraliseerde partij die de samenleving naar eigen inzichten inricht. Een goed voorbeeld hiervan is taal. Taal heeft zijn eigen regels en grammatica, en verandert continu op natuurlijke wijze. De Bitcoin blockchain is een ander voorbeeld van spontane orde. Hier is er geen centrale partij die de set van regels bepaalt.

---

[172] Lao Tze, de vader van het Daoïsme en volgens Rothbard ook de eerste Libertariër, schreef in hoofdstuk 57 van de *Dao De Qing*:

> "Daarom zegt de Wijze: ik ben Wu Wei
> En dan zal het volk zich vanzelf hervormen.
>
> Ik houd van de rust,
> En dan zal het volk vanzelf recht worden."

Wu Wei is een Chinees begrip dat "handelen door niet te handelen" betekent. In dit geval zegt de Wijze dat hij door niet te handelen toch dingen voor elkaar krijgt. Het volk hervormt zichzelf ten goede.

Intermezzo: Het potlood als metafoor voor spontane orde

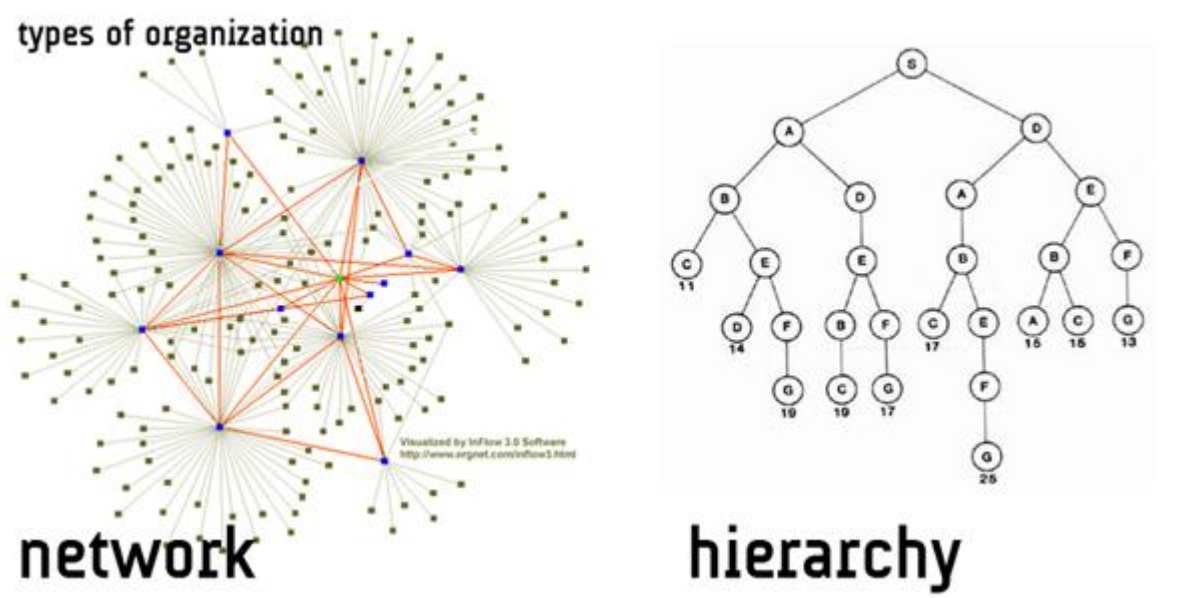
Leonard Read schreef *I, Pencil* (1958) om het concept van spontane orde in de vrije markt aan te duiden. Het is een korte essay over een potlood dat aangeeft hoe complex hij is. Het potlood is, volgens Read, zo complex dat er niet één persoon is op de wereld die hem kan maken. Hij bestaat namelijk uit grafiet, wax, lijm, een stuk metaal om de gum aan het hout te binden, cederhout, etc. Het grafiet is bijvoorbeeld gemijnd in Sri Lanka. Om het te kunnen mijnen, moet je weten hoe je de mijninginstrumenten maakt en weten hoe je het vervoert op schepen. Het grafiet wordt gemixt met klei uit de Mississippi waar ammoniumhydroxide wordt gebruikt voor de raffinering van het grafiet. De gum aan het uiteinde van het potlood wordt verkregen via een raffineringsproces, waarbij rubber uit Indonesië en zwavelchloride wordt gebruikt. De strekking van het verhaal is dat er niemand is die alle vaardigheden bezit om één simpel potlood te produceren. Toch hebben we een potlood.

Het potlood is eigenlijk vervaardigd door miljoenen mensen die, zonder dat ze elkaar kennen, een kleine bijdrage hebben geleverd. De mijner van het grafiet kent de houthakker uit Oregon niet en de producent van het rubber kent de mensen niet die de deelproducten vervoeren op schepen of treinen. Het potlood is een spontaan ontstane configuratie van creatieve mensenarbeid. Ieder persoon ageert uit zijn eigenbelang, waarden en wensen en heeft slechts een klein beetje kennis over het werk dat hij verricht. De les van het verhaal is dat er een productieve orde ontstaat als we mensen vrijlaten. Friedrich Hayek noemt deze spontane orde de ***extended order***, een orde die niet centraal gestuurd is ontstaan. De particuliere kennis die mensen bezitten om tot een product te komen als een potlood, is hierbij gedecentraliseerd. In ons eentje weten we niet hoe we een potlood kunnen maken, maar collectief gezien wel. Friedrich Hayek beschrijft in zijn artikel, 'The Use of Knowledge in Society' (1945), hoe individualisme en gedecentraliseerde kennis in een vrije markt kunnen leiden tot extensieve coöperatie. Volgens Hayek en andere libertariërs moeten we mensen zoveel mogelijk vrijlaten, omdat zij met hun lokale kennis het best weten hoe zij hun eigen leven moeten inrichten. Ludwig von Mises heeft als reactie op de Marxisten van zijn tijd in *Economic Calculation in a Socialist Commonwealth* (1920) in dezelfde trant beschreven waarom centraal geplande samenlevingen leiden tot economische armoede. Economische interventies door de overheid leiden volgens Mises tot distorties in het prijsmechanisme van de vrije markt. Prijzen zijn als een coördinatiemechanisme. Zij signaleren naar mensen waar de samenleving behoefte aan heeft. Als de prijs van graan stijgt, dan weet de boer dat er op dat moment meer behoefte is naar graan. Door prijsdistorties weten producenten niet waar

de samenleving behoefte aan heeft en kunnen zij hun productiecapaciteiten niet richten op de productie van datgene dat de samenleving graag wil hebben.

Het idee dat kennis gedecentraliseerd is en het principe dat we daardoor mensen zoveel mogelijk vrij moeten laten, werd door Jimmy Wales ook toegepast bij de oprichting van Wikipedia. Het achterliggende idee van Wikipedia is om mensen zelf artikelen te laten schrijven op het platform en artikelen zelf te laten redigeren. Hoewel Wikipedia zichzelf niet beschouwt als een betrouwbare bron, is het resultaat wel een online encyclopedie die vrij nauwkeurig is en die veelal wordt gebruikt als startpunt om meer te leren over een onderwerp. Sommige onderzoeken hebben zelfs aangetoond dat Wikipedia niet meer fouten bevat dan traditionelere encyclopedieën als bijvoorbeeld Encarta. (Wiegand, 2007)

Je kunt de inrichting van een spontaan ontstane organisatie ook wel afzetten tegen een hiërarchische organisatie. In de afbeelding hieronder zien we een grafische weergave van beide typen.



Afbeelding 128: Links is een spontaan ontstane organisatie, ook wel een netwerkorganisatie genoemd. Rechts is een hiërarchische organisatie. (Silver84, z.d.)

Het Bitcoin-netwerk is een goed voorbeeld van een netwerkorganisatie, ontstaan uit een spontane orde.

14.5 De relatie tussen het cryptoanarchisme en de Bitcoin blockchain

Hoewel de cryptoanarchisten en cypherpunks al vanaf de jaren 80 technologieën hadden ontwikkeld voor anoniem elektronisch geld, hadden hun toepassingen nog altijd een Single Point of Failure. Een centrale partij was nodig om zeker te stellen dat er geen double-spending kon worden uitgevoerd. Het grote nadeel, naast het feit dat er vertrouwen moet zijn in een centrale partij, is dat een staat zulke geldsystemen kan aanvallen. Het is niet ondenkbaar dat staten geldsystemen die serieuze concurrentie bieden tegen nationale valuta zouden aanvallen.

Gezien zijn bekendheid met de technologieën van de cryptoanarchisten en cypherpunks, is het zeer waarschijnlijk dat Satoshi Nakamoto iemand (of een groep mensen) is geweest die ook actief was op de Cypherpunk mailing list in de jaren 90. Het gebruik van een pseudoniem om Bitcoin te introduceren, past overigens goed bij een cypherpunk.

De relatie tussen het cryptoanarchisme en de Bitcoin blockchain wordt verder toegelicht aan de hand van negen cryptoanarchistische idealen. Deze idealen worden in de volgende tabel afgezet tegen de eigenschappen van de Bitcoin blockchain.

Cryptoanarchistische idealen	Eigenschappen van de Bitcoin blockchain
1. **Voluntarisme:** vrijwillige interacties	Je mag vrijwillig aansluiten bij het netwerk en je wordt niet gedwongen om gebruik te maken van Bitcoin.
2. **Privacy**	Bitcoin wallets zijn pseudoanoniem. Je hoeft geen persoonlijke gegevens op te geven om een wallet aan te maken en je wordt aangemoedigd om bij elke transactie een nieuwe sleutelpaar te creëren.
3. **Eigendomsrechten:** je hebt het recht om de vruchten van je arbeid te behouden	Zolang jij jouw private key weet en deze met niemand deelt, kan niemand beslagleggen op jouw Bitcoins.
4. **Vrije markt:** geen overheidsbemoeienis en overheidsmonopolies	Doorbreekt het monopolie op geldproductie van centrale banken en overheden. Het introduceert weer vrij bankieren en een alternatief voor nationale valuta.
5. **Decentralisatie:** zo weinig mogelijk macht in gecentraliseerde instituten	Er is geen vertrouwde derde partij waardoor het resistent is tegen censuur. Het netwerk is radicaal neutraal. Transacties gebeuren peer-to-peer. Iedereen wordt gelijk behandeld volgens het protocol. Het is open en inclusief voor iedereen.
6. **Transparantie:** verantwoording afdwingen van overheden door middel van transparantie	De blockchain is open source en alle blokken zijn transparant in te zien met bijvoorbeeld block explorers.
7. **Spontane orde:** regels kunnen zonder overheid bottom-up worden gecreëerd. Dit leidt tot meer sociale harmonie	Regels worden bottom-up vastgesteld middels een democratisch proces. Dit maakt het systeem anti-fragiel.
8. **Vrijwillige associatie:** je mag je eigen leider kiezen, jezelf aansluiten bij een associatie en jezelf afscheiden van een associatie	Je kunt zelf kiezen bij welke softwareversie jij je aansluit. Je kunt jezelf ook afscheiden van een chain door middel van een hard fork.

Tabel 8: Cryptoanarchistische idealen, afgezet tegen eigenschappen van de Bitcoin blockchain.

14.5.1 Voluntarisme

Cryptoanarchisten vinden vanuit het libertarische non-agressieprincipe dat je geen geweld mag gebruiken tegen mensen die zelf ook geen geweld hebben gebruikt. Daarnaast mag je ook niemand bedreigen met geweld of hem beroven van zijn bezittingen. Cryptoanarchisten vinden het iedereen is toegestaan om op vrijwillige basis sociale en economische interacties aan te gaan. Dit ideaal zien we ook terug bij de Bitcoin blockchain. Je mag jezelf vrijwillig aansluiten bij

de community en deelnemen aan het netwerk. Je wordt niet gedwongen om Bitcoins te gebruiken. Daarentegen kunnen overheden je wel verplichten om gebruik te maken van hun nationale valuta. Dit doen ze bijvoorbeeld door je belasting te laten afdragen in de nationale valuta. Mocht je een eigen geldsysteem creëren, zoals bijvoorbeeld Bernard von NotHaus heeft gedaan met zijn Liberty Dollar, dan kun je zelfs worden gedwongen door de overheid om het geldsysteem stop te zetten.[173]

14.5.2 Privacy

Cryptoanarchisten maken gebruik van cryptografie om privacy te waarborgen. Satoshi Nakamoto schrijft ook in zijn Bitcoin white paper dat privacy van groot belang is. Banken bereiken privacy door de toegang tot informatie van gebruikers af te schermen. Een systeem als Bitcoin waarbij alle transacties publiekelijk worden geopenbaard kan op twee manieren privacy beschermen.

De eerste manier is om de transacties niet meer herleidbaar te maken naar de gebruikers. Dit wordt mogelijk gemaakt door pseudoanonieme Bitcoin wallets en public keys.

De tweede manier is om voor elke transactie een nieuw sleutelpaar van public en private keys te gebruiken. (Nakamoto, 2008, p. 6) Veel mobiele wallets hebben als standaard de functie dat bij elke transactie een nieuw sleutelpaar wordt aangemaakt. Het is mogelijk dat het Bitcoin-protocol in de toekomst extra privacyfunctionaliteiten krijgt. Enkele forks van Bitcoin, zoals Bitcoin Gold en Bitcoin Private, hebben al Zero-Knowledge Proofs geïmplementeerd.

Daarnaast is ook geen persoonlijke informatie nodig om Bitcoin wallets te creëren. Dit contrasteert met het huidige financiële systeem met de strikte regelgeving omtrent KYC en AML.

[173] De Liberty Dollar werd in 1998 gecreëerd door Bernard von NotHaus en diende om te concurreren met het nationale geld van de Verenigde Staten. Von NotHaus is geïnspireerd door het idee van Friedrich Hayek om het geld te denationaliseren. De Liberty Dollar was zowel in fysieke als in elektronische vorm en werd volledig gedekt door zilver. Het werd dus niet bijgemaakt op basis van krediet. De US Dollar daarentegen is door fractional reserve banking wel gebaseerd op krediet en kan uit het niets worden bijgemaakt door de Federal Reserve. In november 2007 heeft de Amerikaanse overheid $8 miljoen USD aan edelmetalen in beslag genomen waarvan ongeveer $6 miljoen USD werd gebruikt als dekking voor de circulerende Liberty Dollar. Voor meer informatie over de Liberty Dollar van Bernard von NotHaus, zie *A History of Digital Currency in the United States* (Mullan, 2016).

14.5.3 Eigendomsrechten

Cryptoanarchisten geloven dat ieder persoon het recht heeft om de vruchten van zijn arbeid te behouden. Bitcoin speelt op dit ideaal in. Zolang jij jouw private key bewaart en niet deelt met een ander is er niemand die beslag kan leggen op jouw Bitcoins. Met andere woorden, Bitcoin hanteert strikte eigendomsrechten. Banken daarentegen kunnen beslagleggen op het geld dat je bij de bank hebt, je bankrekening bevriezen en zelfs je bankrekening sluiten. Dat is bij Bitcoin onmogelijk.

14.5.4 Vrije markt

Cryptoanarchisten zijn voorstander van een vrijemarkteconomie. Waar mogelijk willen zij overheidsmonopolies doorbreken. In het huidige geldsysteem hebben overheden en centrale banken een monopolie op geldproductie. Bitcoin doorbreekt dit monopolie en blockchaintechnologie heeft de drempel om cryptovaluta te ontwikkelen aanzienlijk verlaagd. Het biedt een alternatief voor het huidige geldsysteem.

14.5.5 Decentralisatie

Cryptoanarchisten zijn zeer sceptisch tegenover gecentraliseerde instituten zoals overheden. Zij pleiten voor zoveel mogelijk decentralisatie van macht en zelfbestuur. De Bitcoin blockchain past goed bij dit gedachtegoed, omdat het een gedecentraliseerd netwerk is waarbij geen enkele partij alle macht heeft over het netwerk. Hierdoor is het netwerk ook resistent tegen censuur. Iedereen is vrij om deel te nemen aan het netwerk en het netwerk te helpen decentraliseren. Het netwerk is hierbij radicaal neutraal. Iedereen wordt gelijk behandeld op het netwerk. Het maakt niet uit hoeveel macht je hebt in de fysieke wereld, je kunt op het Bitcoin-netwerk geen privileges ontvangen. Het netwerk is daarnaast open en inclusief voor iedereen. Het laat zichzelf daardoor moeilijk reguleren.

14.5.6 Transparantie

Cryptoanarchisten willen zoveel mogelijk transparantie van overheden. Julian Assange pleit in *Cypherpunks: Freedom and the Future of the Internet* (2012) voor privacy van de zwakkeren en transparantie van overheden. Transparantie van machtssystemen is hierbij nodig om verantwoordingsplicht af te dwingen. In lijn met dit gedachtegoed, is Bitcoin open source. Dat betekent dat iedereen de broncode van Bitcoin kan inzien en kan bevestigen dat het hele systeem verloopt volgens de regels. Daarnaast is de Bitcoin blockchain ook publiekelijk openbaar en kun je bijvoorbeeld met een block explorer alle transacties op het netwerk inzien. Deze radicale transparantie zorgt ervoor dat meer vertrouwen wordt gewekt in het systeem en

dat mensen niet kunnen sjoemelen met transacties. Daarentegen zijn centrale banken en overheden niet altijd transparant in waar zij het geld aan hebben uitgegeven, waardoor het moeilijker wordt voor de bevolking om ze aansprakelijk te stellen voor hun uitgaven.

14.5.7 Spontane orde

Cryptoanarchisten veronderstellen dat er spontane orde ontstaat als er geen centrale macht is die de samenleving ontwerpt. Bitcoin heeft ook geen centrale partij, maar toch is de gemeenschap in staat om nieuwe regels vast te stellen en updates door te voeren. Dit gebeurt middels een democratisch proces waarbij nodes kunnen stemmen op verbetervoorstellen door hun Bitcoin-software wel of niet te updaten. Veel Bitcoin-ontwikkelaars werken ook vrijwillig of worden betaald met donaties. In die zin is de orde bij Bitcoin op spontane wijze ontstaan.

Als Bitcoin wordt aangevallen, zullen mensen weer werken aan nieuwe verbetervoorstellen om het sterker te maken. Dit zorgt ervoor dat Bitcoin een anti-fragiel systeem is geworden dat lastig uit de lucht te halen is.

14.5.8 Vrijwillige associatie

Cryptoanarchisten geloven dat je je mag afscheiden van een groep. Je mag jezelf aansluiten bij een gemeenschap en je met je gemeenschap afscheiden van een grotere groep. Daarnaast mag je ook je eigen leiders kiezen en zelf regels bepalen voor de nieuwe politieke eenheid. Je mag een ander geen leider opleggen. In de Bitcoin-gemeenschap is veel onenigheid over de richting waar Bitcoin op moet gaan. Onenigheden kunnen worden geslecht door verbetervoorstellen in te dienen en te discussiëren op bijvoorbeeld fora om draagvlak te creëren.

Bij de Bitcoin blockchain is er ook sprake van vrijwillige associatie. Je hebt het recht om mee te stemmen met een update en mocht je je volledig willen afscheiden, dan kun je ook een hard fork uitvoeren. Een hard fork is in principe een afscheiding van de originele chain en is een vreedzame manier om onoverbrugbare geschillen op te lossen.

In de blockchain community is er wel veel onenigheid of een hard fork een gewenste manier is om een update door te voeren. Vitalik Buterin (2017) verdedigt hard forks op basis van libertarische principes. Hij zegt dat soft forks mensen dwingen om of mee te gaan met een update, als er voldoende draagvlak is, of terug te keren naar de originele versie. Daardoor is er bij een soft fork altijd sprake van dwang in het accepteren van of het weigeren van nieuwe protocollen. Een hard fork daarentegen biedt de mogelijkheid om jezelf af te scheiden.

Intermezzo: Bitcoin, de scheiding van staat en geld

Sinds de opkomst van Bitcoin, wordt het geluid om geld en de staat van elkaar te scheiden steeds luider. Shapeshift.io CEO, Erik Voorhees, geeft aan dat dit het belangrijkste aspect is van Bitcoin. Voorhees (2015) vertelt hoe de staat en religie honderd jaar geleden in de westerse beschaving nog sterk met elkaar waren verweven. Weinigen realiseerden zich dat dit immoreel was. Hij denkt dat de meeste mensen zich momenteel ook niet beseffen dat het huidige geldsysteem, waarbij de staat controle heeft over het geld, ook immoreel is. Hij voorspelt dat we de scheiding van staat en geld in de toekomst volkomen moreel gaan vinden en zegt:

> "Money is absolutely as fundamental to our lives as religion, and for many people, it is far more fundamental to their lives as religion. It affects how your life unfolds. The choices that you make about money dictate the ramifications of your life and those around you. And so, to have an institution like money so controlled by a central entity – by a monopoly – is absurd. It is immoral. We should get rid of it."

Veel cryptoanarchisten kunnen zich hierin vinden, omdat zij geloven dat het monetaire systeem is ontworpen op basis van geweld en dwang. Zo kunnen overheden je dwingen om gebruik te maken van een nationale valuta – bijvoorbeeld voor de betaling van belasting – en kunnen zij jouw toekomstige koopkracht ontnemen door middel van inflatie. Andreas Antonopoulos (2017) kan zich hierin vinden en zegt dat het huidige geldsysteem een systeem van controle is geworden. Het is een politiek middel geworden, om te controleren wie wel of geen geld mag ontvangen. Je geld kan daarnaast in beslag worden genomen en je rekeningen kunnen worden bevroren. Mocht je als land niet in de belangen van de Verenigde Staten en het westen ageren, dan kun je worden afgesloten van het SWIFT-netwerk. Dit alles leidt er volgens Antonopoulos toe dat het huidige geld niet langer het beste handelsmiddel is. Daarnaast is het ook geen goed oppotmiddel meer wanneer het in beslag kan worden genomen of bevroren.

Bitcoin wordt door cryptoanarchisten en mensen als Voorhees en Antonopoulos gezien als een nieuw betaalmiddel dat de staatscontrole kan omzeilen. Bitcoin is volgens hen namelijk neutraal, open, grenzeloos en resistent tegen censuur. Het heeft in dat opzicht de scheiding van staat en geld ingeleid.

Intermezzo: De Bitcoin Foundation en diens waarden

De Bitcoin Foundation werd in 2012 opgericht om de reputatie van Bitcoin te promoten. De Foundation heeft het '*Bitcoin Foundation Manifesto*' (2016) gepubliceerd, waarin staat voor welke waarden zij staan:

1. Privacy.
2. Gegarandeerde toegang tot financiële dienstverlening.
3. Decentralisatie.
4. Autonomie.
5. Stabiele geldhoeveelheden.
6. Financiële inclusive.

Zij geloven dat ieder mens financiële rechten heeft, die niet mogen worden beperkt door overheden, financiële instituten of andere mensen. Deze rechten zijn:

1. Het recht op privacy voor transacties die niet schadelijk zijn voor anderen.
2. Het recht om je spaargeld te behouden, of je geld overal op de wereld te spenderen.
3. Het recht op economische participatie met of zonder een bankrekening.
4. Het recht op economische participatie met of zonder een kredietgeschiedenis.
5. Het recht om fiatgeld om te wisselen voor Bitcoin en vice versa.
6. Het recht om Bitcoin als handelsmiddel te gebruiken.
7. Het recht om Bitcoin als oppotmiddel te gebruiken.

Daarnaast gelooft de Bitcoin Foundation dat:

1. Fiatgeld een pover oppotmiddel is, zeker sinds de goudstandaard werd losgelaten.
2. Inflatie consumptie aanmoedigt en sparen ontmoedigt.
3. Traditionele financiële services, in het bijzonder bankieren, niet inclusief zijn voor de 2,1 miljard mensen die in armoede leven (minder dan $3,10 USD/dag).
4. De verwerkingstijd en kosten van elektronische betalingen te hoog zijn, een belangrijke reden waarom 85% van alle globale handel wordt gedaan in kasgeld.
5. De instorting van financiële diensten in 2008 en de opeenvolgende bail-out van het bankensysteem ellende hebben veroorzaakt voor de armsten van de wereldbevolking.
6. Verliezen door kaartfraude $16,3 miljard USD waren in 2014, waarbij meer dan de helft van deze fraude online plaatsvond.
7. Het traditionele systeem van banken en betalingen niet veilig is.
8. Het vertrouwen in traditionele banken en financiële diensten op een dieptepunt is.

14.6 Samenvatting, begrippen en bronnen

Samenvatting

Blockchain is een samenkomst van verschillende ideeën over hoe mensen met elkaar kunnen samenleven. Hierbij passen zowel filosofische, economische, politieke, sociale als technologische stromingen. Door deze gedachtegoeden te begrijpen, krijgen we niet alleen meer inzichten in waarom blockchain is ontstaan, maar krijgen we ook inzichten in wat de vele blockchainpioniers willen bewerkstelligen met de technologie.

Bitcoin is te herleiden uit het cryptoanarchisme en de cypherpunk-beweging. Velen die in de jaren 80 en 90 betrokken waren bij het cryptoanarchisme en de cypherpunk-beweging, hebben een grote rol gespeeld in de ontwikkeling van technologieën waar Bitcoin gebruik van maakt. Enkele van deze mensen die de blockchainwereld hebben geïnspireerd zijn David Chaum, Timothy May, Eric Hughes, John Gilmore, Wei Dai, Adam Back, Hal Finney en Nick Szabo.

Het doel van het cryptoanarchisme is om een libertarisch anarchistische omgeving te creëren op het cybernet. Dit is een samenleving waar de overheid geen enkele rol van betekenis speelt en waar mensen kunnen genieten van het recht op privacy, vrijheid van meningsuiting, vrijwillige sociale en economische associaties en strikte eigendomsrechten. Volgens de cryptoanarchist en oprichter van de cypherpunk-beweging, Timothy May, gaat onbreekbare cryptografie verder dan het kunnen faciliteren van anonimiteit en de vrijheden van meningsuiting en handel. Het zal ook het concept van natiestaten in twijfel trekken.

In dit hoofdstuk hebben we ook dieper gekeken naar de achtergrond van het libertarisch anarchisme. Hierbij hebben we gezien dat Murray Rothbard het libertarisch anarchisme verdedigt op basis van het natuurrecht en dat libertariërs de staat zien als een bende bandieten. In plaats van dwang, prefereren libertariërs voor zoveel mogelijk vrijwillige samenwerking, keuzevrijheid en zelfbestuur. Vanuit het zelfbeschikkingsrecht, gebaseerd op het non-agressieprincipe en de natuurrechttheorie, hebben mensen volgens libertariërs ook het recht op vrijwillige associatie.

Ook hebben we gezien dat er verschillen zijn tussen libertariërs. Een libertarisch minarchist is iemand die gelooft dat de overheid de bevolking plundert in de vorm van belasting, maar dat deze plundering enigszins legitiem is als het wordt gebruikt om enkele essentiële taken in de samenleving te vervullen. Rothbard trekt het non-agressieprincipe van libertariërs naar zijn

uiteinden en concludeert daarmee dat de staat geen recht heeft om te bestaan, omdat het continu de natuurrechten van mensen schaadt.

Het idee dat een anarchistische samenleving niet hoeft te vervallen in chaos leunt op het concept van spontane orde. Een toepassing die is ontstaan uit spontane orde is de Bitcoin blockchain. Er is geen centrale partij die de Bitcoin blockchain reguleert, maar toch zijn er regels en protocollen binnen de blockchain. Beslissingen over de regels en protocollen binnen Bitcoin, worden genomen door de gemeenschap. Daarnaast word je ook niet gedwongen om Bitcoins te gebruiken. Overheden, daarentegen, kunnen je wel verplichten om gebruik te maken van hun nationale valuta. Dit doen ze bijvoorbeeld door je belasting te laten afdragen in hun nationale munt. Zo zijn er veel parallellen te trekken tussen het cryptoanarchisme, cypherpunk en Bitcoin.

Opmerkingen die je nu kunt uitleggen

- Bitcoin is sterk beïnvloed door de cryptoanarchisten en cypherpunks die overheden meer transparant willen maken en het volk meer privacy willen bieden.
- Cypherpunks zijn praktische idealisten.
- Het cryptoanarchisme is gebaseerd op het libertarisch anarchisme.
- Er zijn veel parallellen tussen de cryptoanarchistische idealen en de Bitcoin blockchain.
- Volgens libertariërs hoeft een anarchistische samenleving niet te leiden tot chaos.

Verklarende begrippenlijst

Anarchokapitalisme: De filosofie die een anarchistische samenleving zonder overheid en met volledige vrije markt onderschrijft.

Cryptoanarchisme: De filosofie die de realisering van anarchokapitalisme in cyberspace onderschrijft.

Cypherpunk: Een persoon die cryptografie toepast om maatschappelijke veranderingen teweeg te brengen. Cypherpunks hechten veel waarde aan transparantie van machtssystemen en privacy voor het volk. Ze zijn vaak sterk libertarisch van aard en sommigen, zoals de oprichters van de cypherpunk-beweging, zijn cryptoanarchistisch.

Economische middelen: Productie en handel om eigendom te verkrijgen over goederen en diensten. Franz Oppenheimer gelooft dat dit vreedzame middelen zijn die breeduit worden geaccepteerd in de samenleving.

Extended order: Een extensieve productieve orde die niet centraal is gestuurd. Deze ontstaat spontaan in een vrije markt.

Libertarisch anarchisme: De filosofie die een anarchistische samenleving, gebaseerd op volledige vrije markt en strikte eigendomsrechten, onderschrijft. Zie ook anarchokapitalisme.

Libertarisch anarchist: Iemand die de filosofie van het libertarisch anarchisme aanhangt.

Libertarisch minarchist: Iemand die gelooft dat de overheid nog steeds basisfuncties heeft in de samenleving, maar waar het kan zoveel mogelijk de vrije markt met rust laat.

Nachtwakersstaat: Een staat waarbij de overheid slechts de basistaken als defensie, recht en politie op zich neemt.

Natuurrecht: Recht dat een mens van nature heeft. Volgens libertariërs hebben alle mensen van nature het zelfbeschikkingsrecht.

Non-agressieprincipe: Het principe dat je geen geweld mag gebruiken tegen mensen die zelf ook geen geweld tegen jou gebruiken. Het gaat hierbij om het schaden van de natuurrechten van een ander. Mocht een ander geweld tegen je plegen, dan heb je het recht om jezelf te beschermen. Libertariërs hangen het non-agressieprincipe aan.

Politieke middelen: Volgens Franz Oppenhemier is dit een gewelddadige manier om eigendom te verkrijgen over goederen en diensten. Voorbeelden van politieke middelen zijn inflatie en belastingen.

Spontane orde: Orde die op spontane wijze ontstaat zonder bemoeienis van een autoriteit. Voorbeelden van spontane orde zijn taal en de Bitcoin blockchain.

Voluntarisme: Zie libertarisch anarchist.

Vrijwillige associatie: Het recht om jezelf ergens mee te associëren. Volgens libertarisch anarchisten mag je jezelf associëren met een politieke gemeenschap en vervolgens afscheiden van een staat. Bij een blockchain kan vrijwillige associatie en afscheiding leiden tot een hard fork.

Zelfbeschikkingsrecht: Het recht om over je eigen lichaam te beschikken. Volgens libertariërs volgen uit het zelfbeschikkingsrecht andere rechten, zoals het recht op leven, vrijheid en eigendom.

Bronnen

Antonopoulos, A. (2017, 30 september). Money as a System-of-Control [YouTube]. Geraadpleegd van https://youtu.be/FyK4P7ZdOK8

Armer, P. (1975). Computer Technology and Surveillance. Geraadpleegd van Stanford website: https://stacks.stanford.edu/file/druid:zf198qx6952/zf198qx6952.pdf

Assange, J., Appelbaum, J., & Müller-Maguhn, A. (2012). *Cypherpunks: freedom and the future of the internet*. New York: Or Books.

Bitcoin Foundation. (2016). *Bitcoin Foundation Manifesto*. Bitcoin Foundation.

Buterin, V. (2017, 15 maart). Hard Forks, Soft Forks, Defaults and Coercion. Geraadpleegd op 23 december 2019, van Vitalik.ca website: https://vitalik.ca/general/2017/03/14/forks_and_markets.html

Casey, G. (2012). *Libertarian Anarchy: against the state*. London: Continuum International Publishing Group.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044. https://doi.org/10.1145/4372.4373

Dai, W. (1998). B-Money. Geraadpleegd van Weidai.com website: http://www.weidai.com/bmoney.txt

Finney, H. (1992). Why Remailers I. Geraadpleegd op 23 december 2019, van Fennetic.net website: http://fennetic.net/irc/finney.org/~hal/why_rem1.html

Freedom House. (2019). *Freedom on the Net 2019*. Geraadpleegd van Freedom House website: https://www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

Hayek, F.A. (1945). The Use of Knowledge in Society. Geraadpleegd van https://www.econlib.org/library/Essays/hykKnw.html

Hughes, E. (1993). A Cypherpunk's Manifesto. Geraadpleegd op 23 december 2019, van Activism.net website: https://www.activism.net/cypherpunk/manifesto.html

Levy, S. (2001). *Crypto: how the code rebels beat the government, saving privacy in the digital age*. New York: Viking.

Locke, J. (1689). *Second treatise of government: an essay concerning the true original, extent and end of civil government*. Arlington Heights: Harlan Davidson.

Marx, K., & Engels, F. (1850). *The Communist Manifesto*. London: Vintage Classic.

May, T. (1994). Crypto Anarchy and Virtual Communities. Geraadpleegd op 23 december 2019, van Mit.edu website: http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html

von Mises, L. (1920). *Economic Calculation in the Socialist Commonwealth*. Auburn, Ala., Ludwig von Mises Institute.

Mullan, P.C. (2019). *A History of Digital Currency in the United States: new technology in an unregulated market.* S.L.: Palgrave Macmillan.

Oppenheimer, F. (1908). *The State: its history and development viewed sociologically*. (J.M. Gitterman, Trans.) New York: Vanguard Press.

Project Veritas. (2011). Google Document Dump. Geraadpleegd op 23 december 2019, van Projectveritas.com website: https://www.projectveritas.com/google-document-dump

Read, L. E. (1958). I, Pencil. Geraadpleegd op 23 december 2019, van Fee.org website: https://fee.org/resources/i-pencil/

Rothbard, M. N. (1973). *For A New Liberty.* Blurb.

Rothbard, M.N. (1974). The Anatomy of the State. In M.N. Rothbard *Egalitarianism as a Revolt against Nature and other Essays* (pp. 55-88). Geraadpleegd van http://mises.org

Rothbard, M.N. (1978). Society without a State. *Nomos*, *19*, 191–207.

Silver84. (2019). Ethereum community and its ecosystem: Needs-Based Theories of Motivation approach. Geraadpleegd op 23 december 2019, van kauri.io website: https://kauri.io/ethereum-community-and-its-ecosystem:-structural-analysis/9a486bc098674bb6b70408334947eb93/Venona

Szabo, N. (1997, 29 december). The Idea of Smart Contracts. Geraadpleegd op 23 december 2019, van Nakamotoinstitute.org website: https://nakamotoinstitute.org/the-idea-of-smart-contracts/

Szabo, N. (2005). Bit Gold. Geraadpleegd op 23 december 2019, van Nakamotoinstitute.org website: https://nakamotoinstitute.org/bit-gold/

Szabo, N. (1995, 9 september). VENONA Cypherpunks Archives. Geraadpleegd op 23 december 2019, van Venona.com website: https://cypherpunks.venona.com/date/1995/09/msg01303.html

Williams, B. (2005). *In The Beginning Was The Deed: Realism and Moralism in Political Argument*. New Jersey: Princeton University Press.

Zi, L. (n.d.). *Tao Teh Jing*. Geraadpleegd van https://spiritueleteksten.nl/wp-content/uploads/2014/03/Tao-Teh-Jing-vertaling-door-Henri-Borel-spirituele-teksten-pdf-download.pdf

DEEL III: ENTERPRISE BLOCKCHAIN

Bedrijven handelen met meerdere partijen in een ecosysteem binnen een competitieve en gereguleerde omgeving. Hierbij gebruiken ze tussenpartijen, zoals auditors, banken en notarissen. Ook gebruiken ze grootboeken, zoals een bankrekening, belastingboekhouding, of recepturen om de veranderingen in eigendom en registratie bij te houden. Om fouten en misbruik in deze inefficiënte processen te voorkomen, wordt vaak een inefficiënt intern controlesysteem onderhouden. Mede omdat ze niet alle partijen in hun ecosysteem vertrouwen, missen ze de kans om data te gebruiken of te combineren die in het ecosysteem voorhanden zijn. Sommige bedrijven zien een kans om deze uitdagingen met veilige blockchains te overwinnen. Met blockchain kunnen ze er immers op vertrouwen dat de gegevens die zijn ingevoerd over alle partijen heen actueel en correct zijn. Zo kan elke partij in de blockchain zien wanneer een partij een adres- en bankgegevens bijwerkt, of zien dat een betaling aan een leverancier in voorbereiding is.

Blockchaintoepassingen voor bedrijven worden in dit deel als Enterprise blockchain aangeduid. Dit omvat niet alleen blockchains maar ook Distributed Ledger Technology (DLT).[174] In dit deel beschrijven we de redenen voor en manier waarop een bedrijf Enterprise blockchain invoert.

Hiervoor kijken we in hoofdstuk 15 eerst hoe bedrijven zijn georganiseerd binnen businessmodellen en ecosystemen. Naast een beschrijving van de blockchainbouwstenen kijken we ook naar wat digitale datagedreven modellen en decentrale businessmodellen zijn.

In hoofdstuk 16 schetsen we een raamwerk van hoe blockchaintoepassingen binnen een bedrijf kunnen worden ingevoerd met vier voorbeelden. In deze voorbeelden wegen we publieke en private organisaties tegen elkaar af. We kijken ook naar de mate waarin de organisatie in staat is om blockchain te implementeren.

[174] In een DLT onderhouden verschillende partijen gelijktijdig een grootboek zonder een centraal te vertrouwen entiteit. Een blockchain is een DLT waarbij het grootboek is opgedeeld in cryptografisch versleutelde geordende datablokken. Deze ordening geeft de keten van datablokken een onveranderbaar karakter en zorgt daarmee voor betrouwbaarheid in het systeem. Vaak wordt het ook dermate transparant ingericht, zodat data voor iedereen in te zien zijn. Bedrijven hebben hier echter niet altijd behoefte aan en kunnen kiezen voor een meer gesloten blockchain of een andere DLT dan blockchain.

In hoofdstuk 17 werken we de criteria uit, waar bedrijven naar kunnen kijken om te beslissen of ze blockchain moeten implementeren. Als daaruit voortvloeit dat er een zinvolle blockchaincasus is, is het pas zinvol om te kijken tegen welke voorwaarden een blockchain wordt ingevoerd. We kijken naar verschillende casussen en splitsen de casussen op in concretere toepassingstypen, zodat we per toepassingstype kunnen kijken welke blockchainelementen relevant zijn.

In hoofdstuk 18 leggen we de drie grootste blockchainplatformen en consortia uit en gaan we dieper in op de impact van consortia. We kijken ook naar de uitdagingen waar bedrijven voor staan als ze met andere organisaties gaan samenwerken rondom blockchain.

Zodoende wordt er een logische structuur geschetst waarmee organisaties praktisch blockchain kunnen verkennen. Blockchain is een veelbelovende combinatie van bewezen technologieën, zoals gedecentraliseerde netwerken en cryptografie. De toepassing van deze combinatie bij bedrijven is echter relatief nieuw. Hierdoor is jarenlang wetenschappelijk onderzoek met betrekking tot bedrijfsimplementaties niet voorhanden en hebben we geen volledig zicht op wat blockchaintoepassingen potentieel te bieden hebben.

Deel III beschrijft deze relatief nieuwe blockchainimplementaties zonder de potentie van blockchain uit het oog te verliezen, maar ook zonder te pretenderen te weten wat de exacte impact van deze ontwikkelingen gaat zijn.

15. Businessmodellen

"If you are alone, don't do blockchain, what's the use?"

- Emmanuel Delerm (z.d.)

15.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- De gevolgen van blockchain voor een bedrijf per blockchainbouwsteen te begrijpen.
- Basisconcepten als het business ecosysteem, de omgevingsfactoren via PESTEL-analyse en het Business Model Canvas kennen.
- Het Decentralized Business Canvas Model kennen.

Inleiding

Dit hoofdstuk begint met een introductie van de bouwstenen van blockchain in paragraaf 15.2. Deze bouwstenen zijn de basiselementen waaruit een blockchain bestaat. Deze bouwstenen zijn belangrijk om te begrijpen waar blockchain nut heeft en waar je aan moet denken bij het ontwikkelen van een blockchaintoepassing. Het legt een basis om in hoofdstuk 16 voorbeelden te geven hoe deze bouwstenen in Enterprise blockchaintoepassingen specifiek kunnen worden gebruikt.

Om inzicht te geven in waar bedrijven op welke manier blockchain in kunnen zetten, leggen we ook de basisconcepten van het business ecosysteem (paragraaf 15.3), omgevingsfactoren (paragraaf 15.4) en businessmodel (paragraaf 15.5) uit.

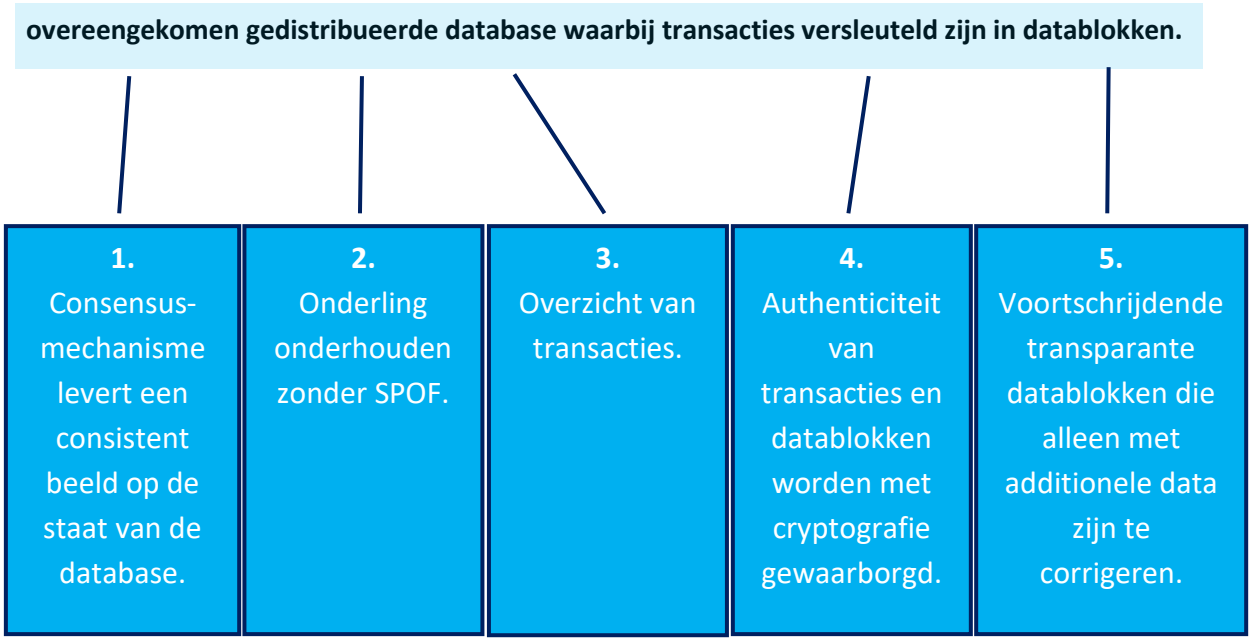
Het is voor een organisatie logischer om strategisch te denken in kansen vanuit het businessmodel en de bedrijfstak, dan vanuit de voor- en nadelen van een onbekend fenomeen als blockchain. Anders gezegd, als je eenmaal weet wat voor type bedrijf je bent, is het makkelijk om te zien in hoeverre de kansen die blockchain biedt aansluiten of niet. Ook is het leggen van nieuwere of sterkere verbanden tussen partners een belangrijke kans die blockchain biedt aan ecosystemen. Dit netwerkdenken wordt versterkt door te kijken naar zowel het businessmodel als het business ecosysteem waarbinnen de organisatie opereert.

Het hoofdstuk gaat daarnaast in paragraaf 15.6 in op digitale businessmodellen en in paragraaf 15.7 op het gedecentraliseerd businessmodel canvas. Al deze modellen worden in hoofdstuk 16 gebruikt om te laten zien hoe blockchaintoepassingen kunnen worden opgezet. Hiermee wordt een basis gelegd waarmee je in kunt schatten wat de gevolgen van blockchain zijn voor een businessmodel of ecosysteem.

We sluiten het hoofdstuk af in 15.8 met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst.

15.2 Bouwstenen

Het nut van een blockchain is afhankelijk van welke bouwstenen je invoert en hoe deze bouwstenen zijn aangepast. De elementaire bouwstenen laten zich zien met een korte definitie van de blockchain. Een blockchain is een:



Afbeelding 129: Elementaire bouwstenen van blockchain.

Deze bouwstenen kunnen, afhankelijk van waar een bedrijf behoefte aan heeft, al dan niet worden aangepast en geheel of in delen ingevoerd worden. Zo kan een bank aan de ene kant cryptografie gebruiken voor het linken van datablokken. Aan de andere kant wil de bank niet alle transactiedata met versleuteling anoniem houden wanneer hij transactiedata moet kunnen overleggen aan zijn toezichthouder, De Nederlandsche Bank.

Deze bouwstenen en hun mogelijke gevolgen worden als volgt in het kort verder uitgelegd.

1. Door een consensusmechanisme levert de blockchain een consistent beeld op van de staat van de blockchain voor alle betrokkenen. Als iemand iets verandert, zien de anderen die het netwerk onderhouden dit en moeten zij de wijziging goedkeuren.

2. De blockchain is gekopieerd, gedistribueerd en onderhouden door een netwerk van verschillende partijen. Er is hierdoor geen Single Point of Failure. Als een node de blockchain verwijdert, is een back-up snel op te halen. Dit maakt het netwerk robuust.

3. De transacties in een blockchain kunnen alle soorten data zijn. Dit kunnen bijvoorbeeld cryptovaluta, rechten, plichten en informatie over een object zijn. De blockchain hoeft dus niet alleen een grootboek te zijn waar alleen financiële transacties in staan.

4. Door het gebruik van cryptografie wordt de authenticiteit van transacties en datablokken gewaarborgd. Dit verhoogt de veiligheid en betrouwbaarheid van de blockchain. Publieke blockchains zoals Bitcoin zijn volledig transparant, met uitzondering van zogenaamde privacy blockchains zoals Zcash en Monero. Deze privacy blockchains gebruiken cryptografie om de privacy voor degenen die betrokken zijn bij de transactie te beschermen.

5. Binnen de voortschrijdende keten van datablokken kunnen er geen data worden aangepast of verwijderd. We spreken hierbij ook wel van een ***append-only datastructuur***. Als je data wil corrigeren, moet je dus nieuwe data toevoegen met een verwijzing naar de vorige te veranderen data. Ook houd je volledig zicht op de datahistorie.

Er is geen tussenpartij meer nodig om de data te vertrouwen. De combinatie van de bouwstenen zorgt er namelijk voor dat de blockchain dit vertrouwen afdwingt. Deze vertrouwde data zijn direct bij alle partijen die deelnemen aanwezig. Dit stimuleert het leggen van relaties tussen partijen. Dit netwerk van samenwerkende partners is een belangrijk element van het business ecosysteem. Ook zijn er waardevolle elementen toegevoegd aan de klassieke blockchain, zoals smart contracts, dApps en tokens. Deze elementen zorgen er onder andere voor dat afspraken automatisch worden afgedwongen, dat eigendom is te digitaliseren en van eigenaar kan veranderen en dat decentrale bestuursmodellen laagdrempeliger kunnen worden geïnitieerd.

15.3 Business ecosysteem

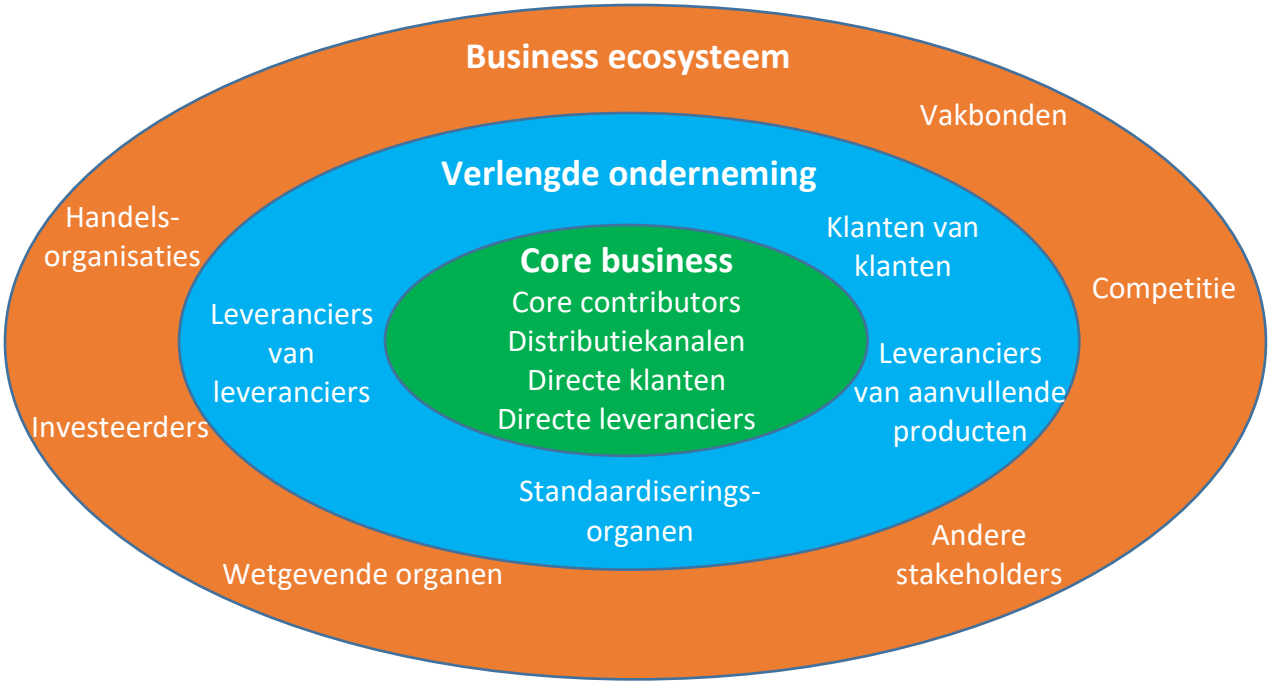
Een ***business ecosysteem*** is een geheel van elkaar beïnvloedende partners die rondom een product of dienst relaties met elkaar hebben.[175] Deze partners kunnen bedrijven, overheden, klanten of andere individuen zijn. In het volgende redeneren we vanuit het perspectief van een bedrijf.

Het bedrijf dat zich het beste aanpast aan de omgeving, creëert voor zichzelf de beste kansen om te overleven. Het aanpassen vertaalt zich in waardecreatie wat een bedrijf doet door gezamenlijk de relaties met andere partijen te versterken. De partijen binnen een business ecosysteem zijn dus tot op zekere hoogte afhankelijk van elkaar. Hierbinnen staat het een bedrijf vrij met een concurrent samen te werken en elkaar te versterken.

Een bedrijf kan onderdeel zijn van meerdere business ecosystemen tegelijk. Airbnb kan bijvoorbeeld samenwerken met het ecosysteem van schoonmaakbedrijven en het ecosysteem van fotografen. Belangrijk in het business ecosysteem is dat bepaalde sleutelpartners bepalend zijn voor de waarde van een product of dienst. Het zijn deze partners waar een bedrijf specifiek naar op zoek gaat als het nieuwe relaties zoekt of de eigen positie wil verstevigen.

Het business ecosysteem kent verschillende lagen van deelnemers. Zie hiervoor de business ecosysteemactoren van Moore (1996).

[175] Je kunt meer lezen over business ecosystemen in *The Death of Competition: Leadership and strategy in the age of business ecosystems* (Moore, 1996).



Afbeelding 130: Het business ecosysteem, gebaseerd op Moore (1996).

De drie lagen zijn:

1. Het kernbedrijf.
2. De verlengde onderneming met klanten en leveranciers van leveranciers.
3. Het business ecosysteem met partners als vakbonden, handelsorganisaties, investeerders, overheden en mogelijk concurrenten die je binnen een bedrijfstak niet snel zou betrekken.

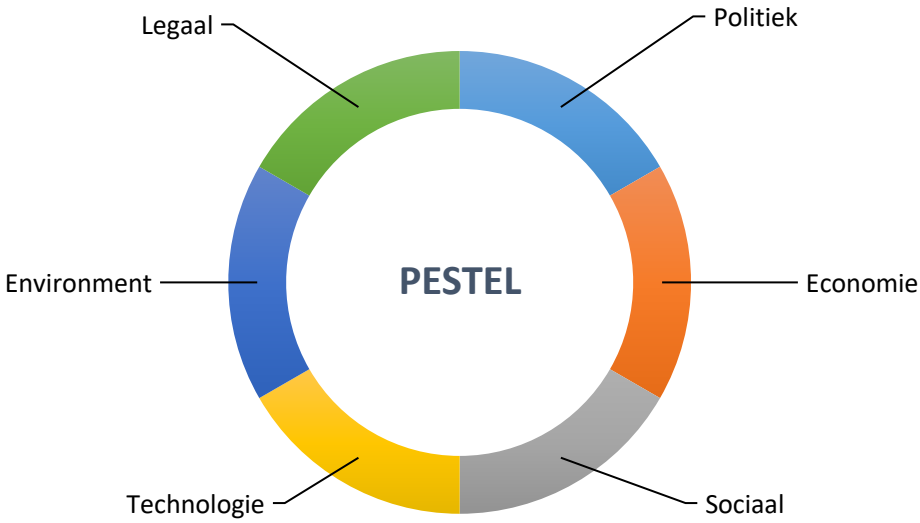
Binnen deze partijen zijn er ook regels en richtlijnen waar bedrijven zich aan moeten houden. Denk hierbij bijvoorbeeld aan arbeidsrecht en winstbelasting. Het verstevigen van samenwerking op alle niveaus is essentieel om zich als netwerk of individueel bedrijf aan te passen aan de omgeving.

Een bedrijfstak is vrij lineair ingericht met leveranciers die in één richting naar de klant of leveranciers kijken, zonder zich met andere partijen in de tak te bemoeien. Daartegenover is een business ecosysteem meer ingericht op wederzijdse afstemming van de deelnemende partijen. Waar je binnen het traditioneel denken van een bedrijfstak van een productiebedrijf bijvoorbeeld geld verhandelt voor goederen, kijk je in een business ecosysteem welke data of waarde je terugkrijgt als je data of waarde levert. Hiermee wordt er waarde gecreëerd voor beide partners.

15.4 PESTEL

Een business ecosysteem functioneert binnen een veranderende omgeving waar de partijen zich aan moeten passen. Een bekend strategisch model om deze omgeving in kaart te brengen is ***PESTEL***.[176] Dit staat voor de volgende omgevingsfactoren:

1. Politiek
2. Economie
3. Sociaal
4. Technologie
5. Environment (omgeving)
6. Legaal



Afbeelding 131: Het PESTEL-model om omgevingsfactoren waarbinnen een organisatie opereert in kaart te brengen.

De elementen van dit model grijpen op elkaar in. Om een beeld te geven van de omgevingsfactoren waar bedrijven mee worden geconfronteerd, met het oog op digitale innovaties zoals blockchain, kun je een PESTEL-analyse als volgt inrichten.

[176] Initieel werd dit het ETPS-model genoemd door Francis J. Aguilar in zijn boek, *Scanning the Business Environment* (1967). Later is dit model op verschillende manieren uitgebreid.

15.4.1 Politiek

In de politiek wordt geprobeerd het concurrentievermogen van het land te verbeteren door te investeren in het digitale vlak. Verder wordt geprobeerd de digitale identiteit van de individuele burger te beschermen, zeker binnen de Europese Unie. Persoonlijke gegevens moeten hierbij worden beschermd en kunnen niet zomaar worden bewaard, geanalyseerd of gedeeld. Op industrieel vlak wordt er flink geïnvesteerd in digitale technologieën om de informatienetwerken van de eigen industrie robuuster te maken. Ook wordt geprobeerd om te voorkomen dat eigen bedrijven worden ontwricht door de dominantie van niet-Europese technologiebedrijven. Denk bijvoorbeeld aan het beschermen van de eigen nationale financiële dienstverleners van de betaalinnovaties die socialmediabedrijven als Google en Facebook en fabrikanten van mobiele telefoons, zoals Apple, introduceren om klanten en hun data te winnen.

15.4.2 Economisch

Digitale innovatie en globalisering zetten aan tot verdere versnelling van handel tussen een steeds groter netwerk van (on)bekende partners en consumenten. Hierbinnen worden thema's als deeleconomie en een dynamischere meer decentraal ingerichte ondernemerscultuur aangehaald. Binnen beide thema's kan blockchain een ondersteunende rol bieden. Blockchain kan op transparante wijze onvervulde capaciteit van investeringsgoederen invullen en burgerinitiatieven ondersteunen. Ook kan het het betalingsverkeer voor de verhuur van je huis versnellen tegen lagere kosten, of burgerinitiatieven als het onderling regelen van een ziektekostenverzekering voor zelfstandigen ondersteunen.

15.4.3 Sociaal

Sociaal gezien is al aangehaald dat de vrijheid van het individu enigszins onder druk is komen te staan met de centrale rol die technologiebedrijven en staten zich hebben aangewend. Blockchain kan een belangrijke rol spelen in het decentraliseren van macht. Het verplaatst hierbij gecentraliseerde controle van overheden en grote technologiebedrijven naar burgers. Blockchain kan dit bewerkstelligen met behulp van bijvoorbeeld een Self-Sovereign Identity, decentralere besluitvorming van de politiek, peer-to-peer vrij onderwijs en vrij verkeer van ideeën.

15.4.4 Technologisch

Technologisch valt blockchain binnen een reeks innovaties die samen de 4^{e} industriële revolutie vormen. Blockchain ondersteunt hierbinnen de opkomst van technologieën als Big Data,

Kunstmatige Intelligentie en het Internet of Things. Ook heeft het de potentie om met een Internet of Value steun te geven aan verdere globalisering en productiviteitsgroei van bedrijven.

15.4.5 Environment (omgeving)

Binnen de environment (omgeving) is het thema circulariteit centraler komen te staan.[177] Transparantie in waar en hoe goederen worden geproduceerd, opgeslagen, aangepast, verbruikt en hergebruikt biedt kansen voor een technologie als blockchain. Blockchain kan hier dienen als een verbindende technologie tussen de verschillende partijen in een waardeketen. Het biedt namelijk de mogelijkheid om aan elk onderdeel van een product een identiteit te koppelen en dit digitaal administratief verhandelbaar te maken. Denk bijvoorbeeld aan het koppelen van een identiteit voor elke spiraal die in een springmatras zit en die weer stuk voor stuk kan worden hergebruikt als het matras teruggaat naar de originele producent.[178]

15.4.6 Legaal

De Europese Unie legt veel nadruk op het beschermen van privacy. Zo heeft de Europese Unie de General Data Protection Regulation (GDPR) ingevoerd, wat in Nederland ook wel bekend staat als de Algemene Verordening Gegevensbescherming (AVG). Net zoals met andere technologische innovaties is de wetgever nog wat afwachtend in het stellen van duidelijke kaders, zo ook voor blockchain. De legale status van cryptovaluta, smart contracts en Decentralized Autonomous Organizations is in veel landen nog niet vastgesteld. Hiernaast zijn overheden actief bezig met het aanpakken van de financiering van criminele en terroristische organisaties. Dit doen ze door onder andere de anti-witwaswetgeving (Wwft)[179], strenger toezicht op cryptovaluta betalingsaanbieders en het verstevigen van de poortwachtersfunctie van financiële instellingen met richtlijnen over Know Your Customer (KYC) en Customer Due Diligence (CDD).

Omgevingsfactoren kunnen op die manier digitale innovaties versnellen. Deze innovaties maken het makkelijker om netwerken op te zetten met partners die je nu nog niet kent,

[177] Binnen circulariteit wordt er veel aandacht geschonken aan People, Planet, Profit.

[178] Nederland Circulair, Sustainable Finance Lab en Circle Economy hebben een white paper gepubliceerd genaamd '*The Circular Service Platform*' (2019) waarin de potentie van blockchain binnen circulariteit is onderzocht. Hierbij kwam blockchain, als een technisch-administratieve infrastructuur, naar voren als een uitstekend instrument om waarde binnen circulaire netwerken te managen.

[179] Naar aanleiding van de invoering van de Europese witwasrichtlijn AMLD4 in 2018 en de AMLD5 in 2020.

inclusief klanten en concurrenten. Blockchain staat toe om decentraal samen te werken, zonder dat een bedrijf zijn autonomie verliest. Blockchain biedt transparantie in goederenstromen die voorheen niet transparant waren. Het kan ook gevoelige informatie afschermen, betalingen tussen onbekende partners afdwingen, informatiesystemen veiliger maken en de Self-Sovereign Identity van het individu ondersteunen, zodat mensen weer controle hebben over hun persoonlijke data. Op sommige vlakken heeft blockchain al de kans gehad zich hierin te bewijzen. Zo hebben cryptovaluta de nodige toepassingen gekend en wordt er volop mee geëxperimenteerd, zoals met de Libra coin. Op andere vlakken zoals smart tokens en DAO's is blockchain vooral nog een experimentele technologie waarvan niet duidelijk is wat de consequenties zijn.

Zoals eerder genoemd zullen juist bedrijven en andere partners waar digitale innovatie binnen het business ecosysteem belangrijk is zich aangetrokken voelen tot het experimenteren met blockchaintoepassingen. Gezien de huidige onbekendheid met de technologie zullen deze bedrijven zich waarschijnlijk richten op minder risicovolle projecten met beperkte impact op het businessmodel.

15.5 Businessmodel

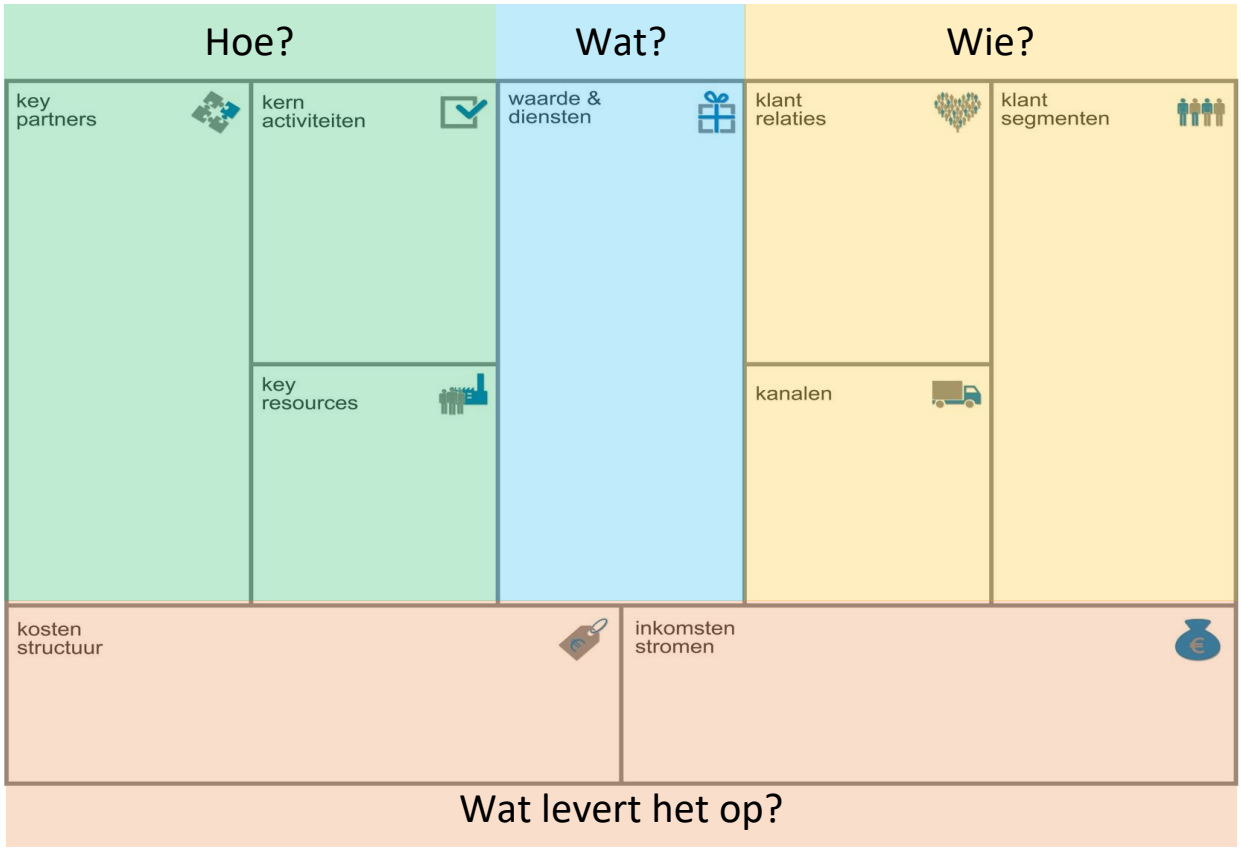
Een ***businessmodel*** beschrijft hoe een organisatie, of netwerk van organisaties, waarde wil creëren voor haar klanten en voor haarzelf. Met andere woorden: hoe verdien ik geld? Met dit businessmodel probeert het zich aan te passen binnen haar business ecosysteem. Naast het businessmodel implementeert een bedrijf daarvoor een strategie van hoe het waarde gaat creëren.

Je ontwikkelt dus een businessmodel als je een idee hebt voor een bedrijf, of als je al een bedrijf hebt, maar dit wilt vernieuwen. Ook kun je een businessmodel ontwikkelen om te analyseren hoe je organisatie waarde creëert, zodat je meer inzichten krijgt of je nog op de goede weg zit.

Om het businessmodel te ontwikkelen, moet je de volgende vier vragen beantwoorden:

1. *Wie?* - klanten en gebruikers, segmenten.
2. *Wat?* - aanbod en waardepropositie.
3. *Hoe?* - activiteiten, hulpmiddelen, partners.
4. *Wat levert het op?* - opbrengsten, kosten, investeringen.

Elementen die bij deze vragen horen werden door Osterwalder en Pigneur bijeengezet in een overzicht om de relevante details van een businessmodel overzichtelijk neer te zetten, zodat je een idee of plan kunt toetsen of bediscussiëren. Het overzicht wordt een ***Business Model Canvas*** (BMC) genoemd.[180]



Afbeelding 132: Business Model Canvas van Strategyzer.com. Het Business Model Canvas is gelicenseerd onder Creative Commons Attribution Share Alike 3.0. Unported License.

Binnen dit canvas is de kern de ***waardepropositie***: het deel van het businessmodel dat beschrijft hoe een organisatie, of netwerk van organisaties, waarde (inkomsten) voor zichzelf genereert. Dit wordt ook wel het ***verdienmodel*** genoemd. Het belang van de waardepropositie is al eerder uitgelegd onder het kopje over business ecosystemen. Door constante waardecreatie te creëren in een veranderende omgeving zorg je ervoor dat je overleeft in dit ecosysteem.

[180] Voor meer informatie, zie 'Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers' (Osterwalder & Pigneur, 2010).

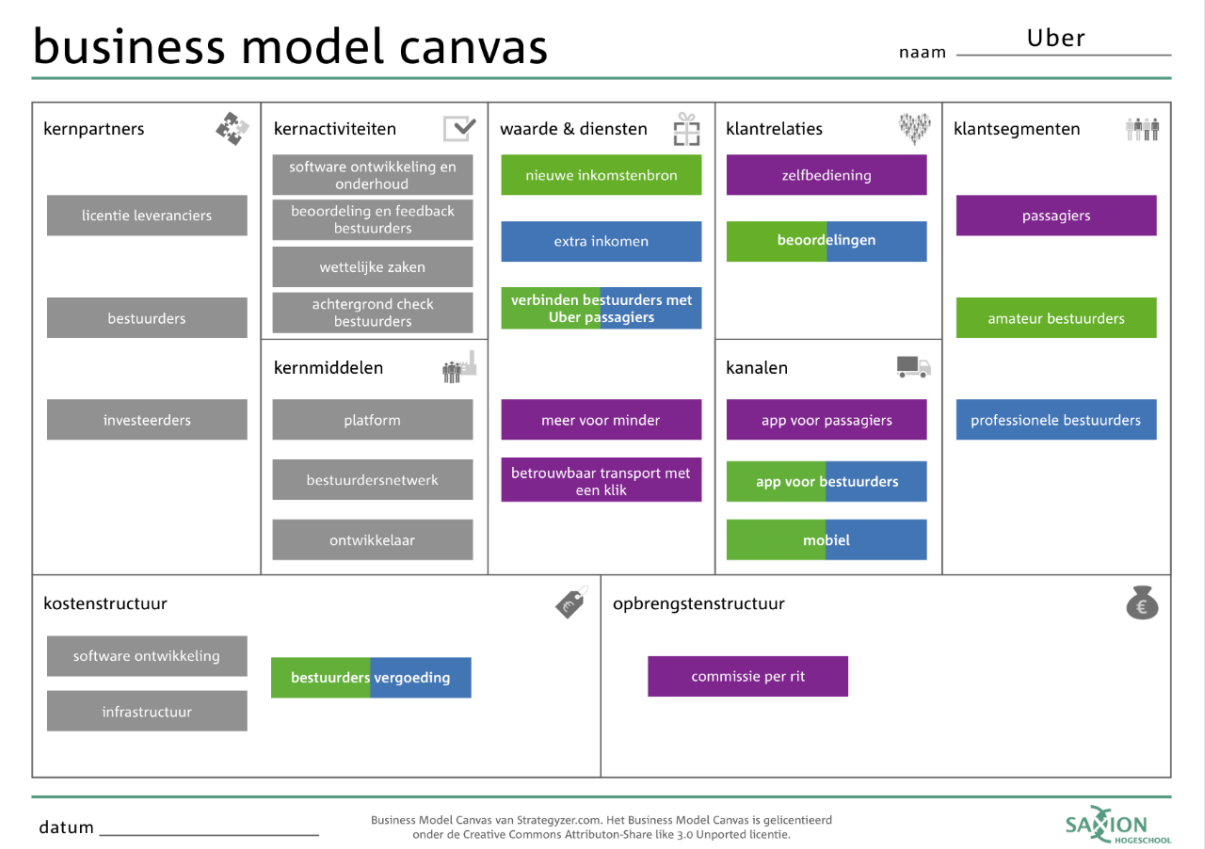
De waardepropositie richt zich rondom de klant en kun je als volgt vinden:

1. Identificeer je klantgroep.
2. Beschrijf doel en de wensen van je klant.
3. Beschrijf je product en de beoogde voordelen.
4. Evalueer de match tussen klant en product.

Hieronder vind je een voorbeeld van een ingevuld businessmodel van Uber.

Ingevuld Business Model Canvas voor Uber

Het volgende voorbeeld is afkomstig van Timber Haaker en Christa Barkel die beiden binnen de minor Digital Business Models & Blockchain werkzaam zijn vanuit de lectoraten Business Models en Blockchain van Saxion Hogeschool.



Afbeelding 133: *Business Model Canvas van Strategyzer.com.*

Managers kunnen dit Business Model Canvas (BMC) gebruiken om een idee te krijgen van de impact van blockchain op hun bestaande businessmodel, of misschien om een nieuw

businessmodel te bouwen. In het volgende wordt een tip van de sluier opgelicht voor de impact van blockchain op een algemeen businessmodel met de vier kernvragen binnen het BMC.[181]

15.5.1 Wie? Klanten en gebruikers

Klantsegmenten betreffen de segmenten waarin je klanten kunt indelen. Blockchain biedt de kans om directere transacties te verrichten met een grote nieuwe groep mensen. Denk bijvoorbeeld aan mensen in opkomende markten die momenteel nog geen financieel profiel hebben, of mogelijke klanten die je nu via de netwerken van andere bedrijven binnen je blockchainsysteem kunt bereiken.

Kanalen worden gebruikt door het bedrijf om te communiceren met de klanten en om de klantsegmenten te bereiken. Hier haalt blockchain in potentie mogelijke tussenpartijen weg, zoals de notaris die tussen de koper en verkoper van een woning in staat. Blockchain kan nieuwe kanalen introduceren. Dit is bijvoorbeeld mogelijk binnen een supply chain waar je als groenteleverancier van een supermarkt ook onder de uiteindelijke afnemers bekend raakt en direct aan deze afnemers levert. Met blockchain kunnen tussenpartijen uit de supply chain worden gehaald, waardoor je een directe relatie met je klant kunt aangaan.

Klantrelaties beschrijven de relaties tussen het bedrijf en de klantsegmenten. Zo kan een bedrijf in een persoonlijk gesprek de relatie met de klant bestendigen door hulp via sociale media of via de telefoon aan te bieden op verzoek van de klant. Een bedrijf kan ook op meer afstand de klant eerst zelf digitale informatie op laten zoeken, zonder verder in contact te treden.

15.5.2 Wat? Aanbod en waardepropositie

Waardeproposities zijn alle activiteiten die waarde creëren voor de klant. Blockchain kan hieraan bijdragen door diensten te bieden die voorheen niet beschikbaar waren. Neem als voorbeeld het Zuid-Afrikaanse Centbee waarmee je binnen je mobiele app op een goedkope eenvoudige manier Bitcoins kunt sturen naar mensen in je contactlijst, onafhankelijk van waar ze zich geografisch bevinden. Complexere eigendomsoverdrachten, zoals die van een huis kunnen ook op eenvoudigere en snellere wijze worden verricht, terwijl er transparant zicht is op de hele keten van financiering, wettelijke eigendomsregistratie en belastingafdracht.

[181] Dit is op basis van 'How blockchain technologies impact your business model' (Morkunas, Paschen, & Boon, 2019).

15.5.3 Hoe? Activiteiten, hulpmiddelen, partners

Key resources zijn processen en middelen die een bedrijf bezit om het businessmodel te laten werken. De middelen kunnen fysiek, intellectueel, financieel of menselijk zijn. Ze verhogen de klantwaarde, bereiken markten, onderhouden relaties met klanten en verzorgen inkomsten. Bij de klanten en medewerkers is het de vraag in hoeverre ze de juiste vaardigheden hebben om met blockchain te werken. Blockchain is een vrij technische oplossing die, omdat mensen hier niet aan gewend zijn, kan leiden tot problemen in de implementatie en uitvoering.

Ook zijn er ***kernactiviteiten***. Dit zijn activiteiten die je nodig hebt om waarde te kunnen leveren. Hoe zorg je er bijvoorbeeld voor dat je de kwaliteit van je product kunt verhogen of de klantrelatie kunt onderhouden? Hier kun je denken aan het verminderen van dubbele invoer van klantgegevens nu anderen binnen je blockchain deze invoer ook verrichten en deze gegevens transparant beschikbaar worden voor jou.

Key partners zijn relaties als leveranciers en partners die je nodig hebt om het businessmodel te laten werken. Blockchain kan ook hier een flinke impact hebben, zoals bij het gebruiken van FinTech -bedrijven in plaats van banken voor het betalingsverkeer, het contacteren van nieuwe leveranciers en andere partijen in een open transparant grensoverschrijdend supply chain of het omzeilen van een tussenpartij als een notaris. Bedenk hierbij welke rollen er nodig zijn om een nieuwe dienst te creëren en te leveren, en welke partijen willen en kunnen samenwerken om deze rollen op zich te nemen. Ook hier is het zaak juist de kritische rollen en partners te onderscheiden van elkaar.

Zoals eerder aangegeven, is het beheren van de relaties met de juiste partners een belangrijke factor voor waardecreatie binnen business ecosystemen. Juist binnen blockchain als datagedreven digitale technologie kan het helpen een ***partnerwaarde-matrix*** op te stellen. Zo'n matrix verduidelijkt de wederzijdse voordelen van een partnerschap of samenwerking. Hiervoor identificeer je de belangrijkste partners, beschrijf je wat een partner zelf inbrengt en wat de partner terugkrijgt uit de relatie.[182]

[182] Meer informatie over de partnerwaarde-matrix is te vinden op https://business modellab.nl/tools/partnerwaarde-matrix of via https://innovalor.nl/.

15.5.4 Wat levert het op? Opbrengsten, kosten, investeringen

Inkomstenstromen betreffen het kasgeld dat door verkopen wordt gegenereerd. Blockchainbedrijven kunnen bijvoorbeeld tokens uitgeven om fondsen te verwerven. Tokens kunnen ook worden uitgegeven om blockchainplatformen te gebruiken, zoals gas wordt toegepast bij Ethereum. Daarnaast kun je ze als geldmiddel gebruiken, zoals het geval is bij Bitcoin. Cryptotokens stellen een bedrijf in staat directe betalingen op een laagdrempelige manier te laten uitvoeren. Door de lage transactiekosten zijn pay-per-usage of betalingen voor advertenties en sponsoring mogelijk.

Uiteindelijk beschrijft de ***kostenstructuur*** alle kosten die een businessmodel heeft. Blockchain kan potentieel kosten verlagen van onder andere transacties, tussenpartijen en de kosten van risico's van onbetrouwbare partners of ingekochte materialen. Zo kun je met blockchain de transactiegeschiedenis en reputatie van leveranciers transparant stellen, zodat je de meest betrouwbare partner kunt kiezen en daarmee op lange termijn kosten van een te late levering of verkeerde hoeveelheden kunt besparen.

Bij kosten is er ook de vraag in hoeverre een nieuw blockchainsysteem aan kan sluiten op de huidige IT-systemen. In hoeverre sluiten de databasestructuren op elkaar aan om directe communicatie tussen de systemen mogelijk te maken?

Gezien de mogelijkheden om samenwerking tussen partners toe te laten nemen, dient ook te worden nagedacht hoe investeringen, kosten en opbrengsten over de partijen worden verdeeld.

Tot zover het klassieke businessmodel. In de volgende paragrafen behandelen we het digitale businessmodel.

15.6 Digitaal businessmodel

Naast meer complete business ecosystemen met een sterke digitale component zijn er specifieke businessmodellen die data-innovatie in de kern van de strategie hebben staan: ***data driven businessmodellen***. Hierin worden data gebruikt om waarde te creëren door bijvoorbeeld big data analyses en kunstmatige intelligentie. Deze data worden samen met relevante partners gemaakt en gedeeld. Logischerwijs biedt dit kansen voor blockchain, omdat het de data binnen een heel ecosysteem op elkaar kan laten afstemmen. Een voorbeeld van een data driven

businessmodel is PatientsLikeMe, een online platform waarin patiënten elkaars ervaringen delen om het resultaat van hun behandelingen te verbeteren.

In lijn met datagedreven modellen zijn er business ecosystemen waarin sterk wordt geleund op data en digitale technologie om waarde te creëren. Juist voor dit soort modellen spelen digitale innovaties als blockchain een belangrijke rol om zich aan de omgeving aan te passen en misschien ook het business ecosysteem te beïnvloeden. Hierbij wordt geïnvesteerd in nieuwe manieren om met partijen data te creëren, aan te passen, op te slaan en te gebruiken. Neem als voorbeeld een ecosysteem rondom financiële services als internationale betalingen. Hierin is Western Union waar de commissies soms wel 8-13% zijn, voorbijgestreefd door de startup TransferWise met 90% lagere kosten. Momenteel probeert de blockchain startup ABRA hetzelfde te doen door eenzelfde dienst aan te bieden die 90% goedkoper is dan TransferWise (Morkunas, Paschen, & Boon, 2019). Deze ontwikkeling werd mogelijk gemaakt door een omgeving waarin digitale innovatie versneld werd geaccepteerd binnen de markt. Daarnaast werd het ook mogelijk doordat er binnen het ecosysteem behoefte is van klanten (core) naar een dergelijke dienst van indirecte leveranciers, zoals die van een internetinfrastructuur (verlengde onderneming) en een overheid die de wetgeving (derde laag) hiervoor heeft opengesteld.

Doordat de dienst of het product binnen deze business ecosystemen digitaal wordt gecreëerd en overgedragen, kan er op laagdrempelige wijze contact worden gelegd met de klant. Mocht een bedrijf besluiten om de digitale component binnen de bedrijfsvoering te verstevigen dan kan digitale transformatie nodig zijn. Hierbij is het misschien handig om je bedrijfsprocessen en businessmodel te herdefiniëren met behulp van digitale technologie. In dit geval staat de vraag centraal hoe je je visie over het bedrijf en de bedrijfsomgeving samenbrengt met de impact van blockchaintechnologie. Je kunt je processen en businessmodel op twee manieren aanvaren. Aan de ene kant kun je stap voor stap innoveren, misschien omdat je organisatie nog niet klaar is voor disruptie, omdat je de negatieve risico's niet wilt lopen, of omdat er nog legale barrières gelden die niet toestaan om in één keer alles te veranderen. Aan de andere kant kun je je gehele businessmodel disruptief veranderen, wat vaak gevolgen heeft voor je ecosysteem.

Eén type van een disruptieve verandering is ***self disrupt***. Hierbij is de aanpassing van je businessmodel dermate disruptief dat je je eigen kernbusinessmodel kannibaliseert. De bedrijfscultuur heeft daarnaast ook invloed op de digitale transformatie. Het is belangrijk dat werknemers een digitale cultuur wordt aangeleerd, waarbij digitale vaardigheden worden

aangescherpt. Mogelijk heeft een dergelijke transformatie ook gevolgen voor het leiderschapsmodel waarin innovatie decentraler wordt geïnitieerd, in plaats van vanuit een centrale leiderschapspositie.

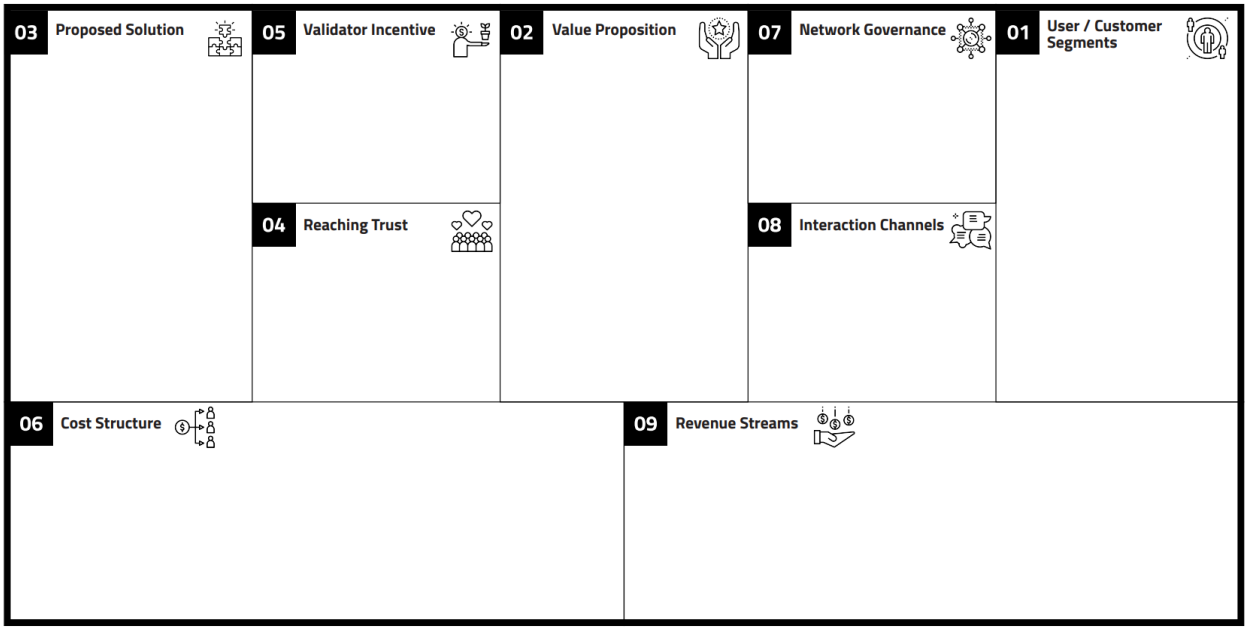
Blockchain is een digitale technologie die veelal draait om het delen en verifiëren van data tussen verschillende partijen. Blockchain kan daardoor een gedecentraliseerd businessmodel versnellen. In de volgende paragraaf wordt ingegaan op dit decentrale businessmodel.

BlockFi
BlockFi is door de bekende blockchain investeerbroers Winklevoss en het aan Ethereum gelieerde software bedrijf Consensys opgezet om cryptovalutaleningen te verstrekken. Het heeft een handelsbedrijf uitgerold op basis van nultarieven. Inkomsten worden in plaats van tarieven verkregen door gebruikersinformatie te verkopen aan grote institutionele cryptobedrijven die BlockFi van meer liquiditeit voorzien, door als market maker te functioneren. Voor meer informatie, zie: https://blockfi.com/.

15.7 Decentralized Business Model Canvas

Businessmodellen zijn in te delen in verschillende typen, zoals die van bijvoorbeeld een fabrikant, een distributeur, een online marktplaats, crowdsourcing en blockchain.

Om de vruchten te plukken van blockchain is het niet altijd noodzakelijk dat het gehele businessmodel op blockchain is geënt. Het kan ook zijn dat sommige uitdagingen die een businessmodel ervaart deels worden opgelost door blockchain. Je kunt het BMC gebruiken om deze uitdagingen en oplossingen een plek te geven. Het BMC is echter te weinig specifiek gericht op blockchain om een juiste analyse uit te voeren. MVPWorkshop heeft om deze reden het Decentralized Business Model Canvas (DBMC) gemaakt, dat specifiek gericht is op blockchain businessmodellen.



Afbeelding 134: Decentralized Business Model Canvas (Bujošević, 2019).

Het grote verschil tussen een gedecentraliseerd en gecentraliseerd businessmodel is dat de eerste in de pure vorm een publiek permissionless systeem is, dat wordt opgezet door verscheidene individuen die elkaar niet hoeven te kennen. Governance is hierbij decentraal opgezet door het publiek, data worden gedecentraliseerd bewaard en de communicatie tussen de verschillende partijen vinden peer-to-peer plaats. Dit is de meest open vorm van een blockchain. Het staat een bedrijf vrij om de bouwstenen van blockchain zelf aan te passen. Bij een gecentraliseerd systeem maakt een centrale organisatie de beslissingen.

Bij een gedecentraliseerd businessmodel wordt de omzet vaak verdeeld onder degenen die het meeste aan het netwerk bijdragen en zijn de kosten om gebruik te mogen maken van het platform bijzonder laag - bijvoorbeeld bij het social blogging blockchainplatform Steemit.

Decentralisatie van het businessmodel kan op verschillende niveaus gebeuren. McKie (2017) beschrijft twee manieren:

1. Decentralized Business Modellen met een lage of geen afhankelijkheid van tussenpartijen.
2. Decentralized Business Modellen met enige afhankelijkheid van tussenpartijen.

In het eerste geval is er een token beschikbaar op een publiek open permissionless netwerk. Dit is een zo gedecentraliseerd mogelijk model, liefst inclusief decentrale governance en de mogelijkheid voor iedereen om deel te nemen aan consensus en tokens te verkrijgen via een

consensusmechanisme als bijvoorbeeld Proof-of-Work. In het tweede geval wordt er eerder gebruikgemaakt van een gesloten privaat netwerk.

Ook voor het DBMC kijken we naar dezelfde vier kernvragen die zijn gesteld voor BMC.

15.7.1 Wie?

Ditmaal komen naast klanten, sleutel partners of gebruikers vooral verschillende soorten stakeholders naar voren (01). Bij blockchain kun je van elke partij of partner die waarde creëert een stakeholder maken door tokens beschikbaar te stellen.[183] Als de cryptoeconomie van een blockchain goed is ingericht, zal een tokenhouder uit eigenbelang betrokken zijn bij de waardecreatie en sneller worden gemotiveerd om gedrag te vertonen dat in lijn is met de strategische richting. Het voordeel hiervan is dat je een betrokken ecosysteem ontwikkelt. De tokenhouder ziet zichzelf immers als mede-eigenaar van het project, ongeacht zijn rol als programmeur, investeerder of klant. Dit is een wezenlijk groot verschil met centrale partijen waar de rollen vaak meer gescheiden zijn, zoals de rollen van een aandeelhouder, een werknemer of een klant. Een decentraal businessmodel zal de relatie met sleutelpartners, onbekende partners en andere stakeholders nog talrijker en dynamischer maken.

Binnen de ‘wie’ kan in de toekomst ook een IoT-apparaat een rol vervullen. Denk bijvoorbeeld aan een zelfrijdende auto die in bezit is van meerdere partijen en autonoom ritten uitvoert voor klanten.

Daarnaast hebben netwerk governance en interactiekanalen ook te maken met de ‘Wie’-vraag, zoals hoe de beslissingen binnen het netwerk worden gemaakt en op welke manier arbitrage plaatsvindt. (07) Wat zijn de beste kanalen om met de sleutelgebruikers en partners te communiceren? (08) Tokenhouders en validators zouden op (pseudo)anonieme wijze kunnen bijdragen aan de beslissingen van het netwerk. Door het peer-to-peerkarakter, biedt het netwerk ook de kans om direct met alle stakeholders te communiceren.

[183] Een token kan worden uitgedrukt in bijvoorbeeld cryptovaluta’s, spaarpunten of aandelen en al dan niet dividend uitkeren.

15.7.2 Wat?

Om de kansen van een waardepropositie (02) te zien, kan er een afweging worden gemaakt tussen centralisatie en decentralisatie. Een analyse van deze afwegingen toont aan waar blockchain de meeste waarde heeft.

Jobs To Be Done	Decentralization Opportunity	Decentralization Downside	Current Intermediary	Centralized Competitors

Afbeelding 135: Decentralized Business Model Canvas (Bujošević, 2019).

Hier is het opnieuw belangrijk om te kijken naar de waarde die wordt gecreëerd door alle betrokken partijen binnen het ecosysteem.

15.7.3 Hoe?

Hoe ziet de voorgestelde oplossing eruit? (03) Hier worden de architecturale technologie en ICT-component meer benadrukt dan bij het BMC, zoals de rollen van de nodes, de wijze waarop informatie wordt bewaard en de cryptografische en consensuscomponenten.

Welke mechanismen gebruiken we om vertrouwen te verkrijgen tussen de stakeholders? (04)

Wat zijn de beloningen voor validators om deel te nemen aan het netwerk en datablokken te helpen valideren? (05) Verschillende stimuleringsmechanismen zijn al genoemd in deel I van het boek.

15.7.4 Wat levert het op?

Wat zijn de kosten? (06) Het gedecentraliseerd businessmodel kan zich via crowdfunding relatief eenvoudig, snel en goedkoop financieren. De kosten om het netwerk te onderhouden, is daarnaast verspreid over een netwerk van verschillende stakeholders.

Daarnaast dient er ook rekening te worden gehouden met de manieren waarop verkopen kunnen worden gegenereerd.[184] (9)

[184] Door MVPWorkshop verrichte cases zijn beschreven in 'Celsius Network: Product Case Study (MVPWorkshop, 2019).

Tot zover de inleiding op businessmodellen en hun elementen. In het volgende hoofdstuk worden deze modellen ingevuld met voorbeelden van blockchaintoepassingen in verschillende sectoren.

15.8 Samenvatting, begrippen en bronnen

Samenvatting

In dit hoofdstuk leer je digitale en datagedreven businessmodellen kennen.

Als je eenmaal weet wat voor type bedrijf je hebt, is het makkelijker om te zien in hoeverre de kansen die blockchain biedt aansluiten of niet. De kansen en uitdagingen van blockchain, en andere externe ontwikkelingen, worden bekeken via een model met omgevingsfactoren. Om een beeld te geven van de omgevingsfactoren waar bedrijven mee worden geconfronteerd, met het oog op digitale innovaties zoals blockchain, kun je een PESTEL-analyse uitvoeren. PESTEL staat hierbij voor:

1. Politiek
2. Economie
3. Sociaal
4. Technologie
5. Environment (omgeving)
6. Legaal

Het businessmodel is te ontwikkelen aan de hand van een Business Model Canvas (BMC), waarbij je de volgende vier vragen moet beantwoorden:

1. *Wie?* - klanten en gebruikers, segmenten.
2. *Wat?* - aanbod en waardepropositie.
3. *Hoe?* - activiteiten, hulpmiddelen, partners.
4. *Wat levert het op?* - opbrengsten, kosten, investeringen.

Hierbij staat de waardepropositie van het bedrijf centraal.

Een belangrijke plaats binnen het BMC wordt ingenomen door netwerken van verbonden partners. Deze ecosystemen bestaan uit een kernbedrijf, de verlengde onderneming en het business ecosysteem met onder andere vakbonden, overheden en concurrenten.

Voor blockchain is het digitale datagedreven businessmodel relevant. Binnen deze modellen wordt data gebruikt om waarde te creëren. Deze data wordt in het ecosysteem samen met partners gemaakt en gedeeld. Blockchain kan hierbij de datastromen beter op elkaar laten afstemmen binnen een ecosysteem van vertrouwde of onvertrouwde partners.

Daarnaast wordt het Decentralized Business Model Canvas (DBMC) geïntroduceerd als adaptatie van het BMC. Een publiek permissionless systeem is het meest relevante voorbeeld voor een blockchain adaptatie. Hierbinnen vindt een onderwerp als de gecombineerde rol van tokenhouders als gebruiker, validator, medewerker en eigenaar een plek. Andere blockchainadaptaties met behulp van dit gedecentraliseerde model zijn mogelijk. Hiervoor kunnen bedrijven de bouwstenen van blockchain al dan aanpassen naar eigen behoeften.

Opmerkingen die je nu kunt uitleggen

- Je dient eerst je business ecosysteem te begrijpen en beheersen, voordat je een blockchain implementeert die binnen het ecosysteem past.
- Blockchain biedt een kans om ecosystemen te digitaliseren.
- Blockchain zorgt voor een toename van datagedreven businessmodellen.
- Daar waar blockchain een dominante invloed heeft, heeft het zin een Decentraal Business Model Canvas te gebruiken.
- Decentraal denken, verandert met de komst van tokenhouders en validators de verhoudingen binnen een ecosysteem en businessmodel.

Verklarende begrippenlijst

Append-only datastructuur: Datastructuur waarbij geen data kan worden aangepast of verwijderd. Als je data wil corrigeren, dien je dus nieuwe data toe te voegen met een verwijzing naar de vorige te veranderen data.

Business ecosysteem: Een ecosysteem van elkaar beïnvloedende partners die rondom een product of dienst relaties met elkaar hebben.

Business Model Canvas (BMC): Een methode om overzichtelijk de relevante details van een businessmodel neer te zetten, zodat je een idee of plan kunt toetsen of bediscussiëren.

Businessmodel: Een businessmodel beschrijft hoe een organisatie, of netwerk van organisaties, waarde wil creëren voor haar klanten en voor haarzelf.
communiceren met de klanten en om klantsegmenten te bereiken.

Data driven businessmodel (datagedreven businessmodel): Businessmodel waarin de data centraal staan om de waarde te creëren. Het businessmodel is bijvoorbeeld gedreven door big data analyses en kunstmatige intelligentie.

Decentralized Business Model Canvas (DBMC): Methode om overzichtelijk de relevante details van een blockchain businessmodel neer te zetten, zodat je een idee of plan kunt toetsen of bediscussiëren.

Inkomstenstromen: Inkomsten die door verkopen wordt gegenereerd.

Kanalen: In een Business Model Canvas betreft het de kanalen voor een bedrijf om

Kernactiviteiten: Activiteiten die je nodig hebt om waarde te kunnen leveren.

Key partners: Relaties als leveranciers en partners die je nodig hebt om het businessmodel te laten werken.

Klantrelaties: Relaties tussen het bedrijf en de klantsegmenten.

Klantsegmenten: Segmenten waarin je klanten kunt indelen.

Kostenstructuur: Structuur van alle kosten die een businessmodel heeft.

Partnerwaarde-matrix: In te vullen model waarin geprobeerd wordt de wederzijdse voordelen van een partnerschap of samenwerking naar voren te brengen.

PESTEL: Model om omgevingsfactoren voor een businessmodel te onderzoeken met de thema's politiek, economisch, sociaal, technologie, environment (omgeving) en legaal.

Self disrupt: Type disruptieve verandering waarin een bedrijf het eigen kernbusinessmodel kannibaliseert.

Verdienmodel: Zie waardepropositie.

Waardepropositie: Het deel van het businessmodel dat beschrijft hoe een organisatie, of netwerk van organisaties, waarde (inkomsten) voor zichzelf genereert. Dit wordt ook wel het verdienmodel genoemd.

Bronnen

Achterberg, E. (2019). *The Circular Service Platform: A technical-administrative infrastructure for managing value in circular networks.* Geraadpleegd van https://circulareconomy.europa.eu/platform/sites/default/files/the_circular_service_platform.pdf

Aguilar, F.J. (1967). *Scanning the business environment*. New York, Macmillan.

Bujošević, V. (2019, 22 juli). Decentralized Business Model Canvas #1. Geraadpleegd op 23 december 2019, van MVPworskhop.co website: https://mvpworkshop.co/blog/decentralized-business-model-canvas-1/

Franch, X. (2015). Business and Software Ecosystems: How to model, analyze, and survive! [PowerPoint slides]. Geraadpleegd van https://www.slideshare.net/xfranch/re-2015-ecosystems-tutorial

Haaker, T., Bouwman, H., Janssen, W., & De Reuver, M. (2017). Business model stress testing: A practical approach to test the robustness of a business model. *Futures*, vol. 89, pp. 14-25, 10.1016/j.futures.2017.04.003.

McKie, S. (2017, 30 september), Investing in Tokens and Decentralized Business Models. Learn the Details behind this impending entrepreneurial Paradigm Shift. Geraadpleegd op 23 december 2019, van Medium website: Bron: https://medium.com/blockchannel/investing-in-tokens-and-decentralized-business-models-e7629efa5d9b.

Moore, J. F. (1996). *The Death of Competition: Leadership and strategy in the age of business ecosystems*. John Wiley & Sons.

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons*, 62(3). https://doi.org/10.1016/j.bushor.2019.01.009

Nederland Circulair, Sustainable Finance Lab, Circle Conomy. (2019). The Circular Service Platform: A technical-administratieve infrastructure for managing value in circular networks. Geraadpleegd van https://circle-economy.com/circular-service-platform

Osterwalder, A., & Pigneur, Y. (2010*). Business model generation: a handbook for visionaries, game changers, and challengers.* John Wiley & Sons.

Strategyzer. (z.d.) Business Model Canvas. Geraadpleegd op 23 december 2019, van Strategyzer.com website: https://www.strategyzer.com/canvas/business-model-canvas

16. Enterprise blockchaintoepassingen

"The economist Hernando de Soto told us that only one third of all people can prove they own their land. Apart from the legal uncertainty, there is $20 trillion in dead capital, as land with unexplained legal titles cannot be sold. So we told him, 'Find us such a country and we bring the land register to the Blockchain for free.' And that was Georgia."

- Marc Taverner (2017)

16.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Het Saxion Blockchain Model kennen om te beoordelen waar kansen voor businessmodellen liggen in het implementeren van blockchain.
- Toepassingen kennen van blockchains in sectoren waar momenteel de meeste ontwikkelingen met betrekking tot blockchain plaatsvinden.
- Toepassingen kennen van disruptieve gedecentraliseerd blockchainmodellen waar nog amper bestaande businessmodellen voor bekend zijn.

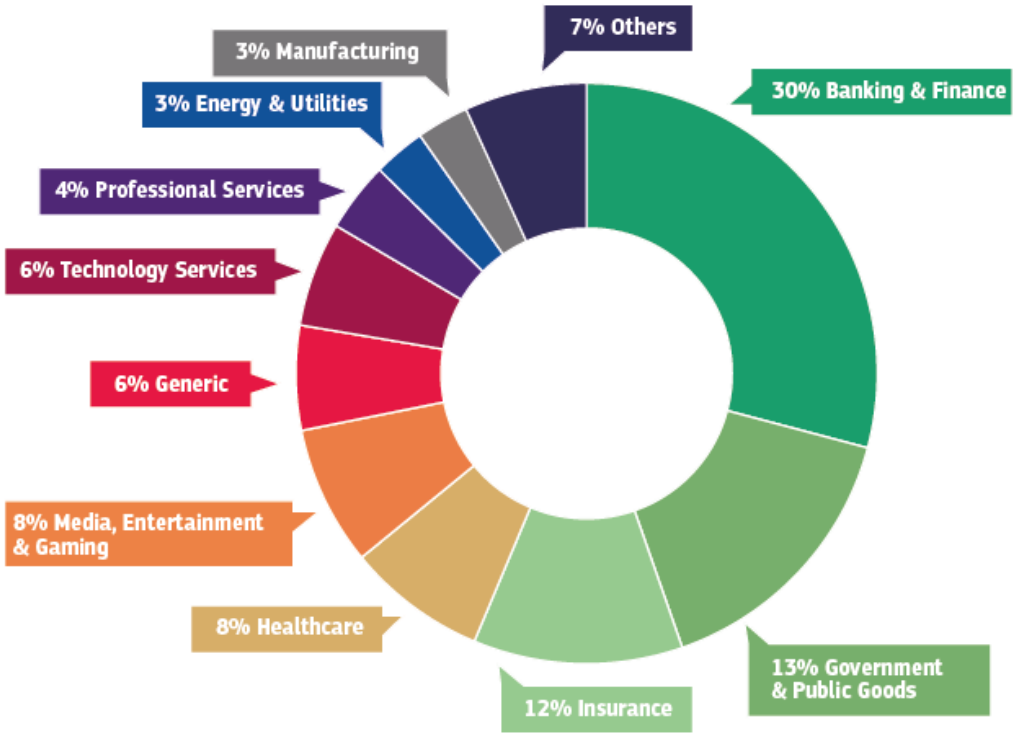
Inleiding

In dit hoofdstuk wordt een model geschetst waarmee kan worden beoordeeld waar de kansen liggen voor businessmodellen die momenteel aan blockchaintoepassingen werken. Redeneren vanuit een daadwerkelijke toepassing biedt ons inzichten in hoe blockchainbouwstenen kunnen worden ingezet. Tijdens de beschrijving van de toepassingen worden basistermen en non-financiële indicatoren gedefinieerd die helpen te evalueren in welke situatie een bedrijf een blockchaintoepassing heeft bedacht, in hoeverre het bedrijf in staat is deze te implementeren en wat de impact van deze toepassing is.

In dit hoofdstuk worden de volgende vier geïmplementeerde toepassingen beschreven:

1. Bankieren en Financieren door ICE Bakkt en BitShares (paragraaf 16.2).
2. Overheid en Publieke Goederen door Lantmäteriet en Land Layby (paragraaf 16.3).
3. Fabricage door BMW en VeChain (paragraaf 16.4).
4. Voorspellingsmarkt door PredictIt en Augur (paragraaf 16.5).

Binnen elk voorbeeld wordt een organisatie met een centraal businessmodel afgezet tegen een organisatie die een radicaal innovatief decentraal model nastreeft. De eerste twee voorbeelden zijn gekozen op basis van een studie van Hileman & Rachs (2017). Zij hebben 132 DLT use cases bekeken en deze gesegmenteerd in sectoren.[185] Uit onderstaande afbeelding, die afkomstig is uit de studie, is te zien dat 30% van de use cases binnen de sectoren vallen van Bankieren en Financieren en 13% in Overheid en Publieke Goederen.



Afbeelding 136: Overzicht van 132 DLT use cases en binnen welke sectoren ze vallen (Hileman & Rauchs, 2017).

De andere twee voorbeelden, Fabricage en Voorspellingsmarkt, zijn om de volgende redenen gekozen:

1. Fabricage om te duiden hoe in een groter ecosysteem verschillende partijen blockchain gebruiken.
2. Voorspellingsmarkt als voorbeeld van een dienst die bestaande businessmodellen volledig kan ontwrichten dankzij de ontwikkeling van blockchaintechnologie.

[185] DLT staat voor Distributed Ledger Technology. DLT's maken gebruik van gedistribueerde grootboektechnologieën, maar deze hoeven niet per se blockchains te zijn. Hashgraph, Holochain, Directed Acyclic Graph zijn geen blockchains, maar zijn wel DLT's. Blockchains zijn dus een subset van DLT's.

De toepassingen worden met behulp van de volgende instrumenten beschreven binnen het Saxion Blockchain Model:

A. **Externe ontwikkelingen** die invloed op het businessmodel hebben in overeenstemming met de PESTEL-methode.
B. **Bedrijfsproces** inclusief de meest relevante karakteristieken van dit proces en het doel dat de blockchainimplementatie zou dienen.
C. **Business ecosysteem**actoren om een beeld te geven welke partners het bedrijf heeft.
D. **Heat map businessmodel**elementen waarin de invloed van de externe ontwikkelingen wordt getoond op het businessmodel. Hiermee kunnen meer inzichten worden vergaard over kansen en uitdagingen voor het bedrijf.
E. Details van de **oplossing** waarin op verschillende vlakken de incrementele oplossing wordt vergeleken met een disruptief model, evenals waar blockchain kansen biedt om binnen het ecosysteem relaties aan te gaan en te verdiepen.
F. **Blockchain Gereedheidsscore** waarmee wordt bekeken in hoeverre de organisatie gereed is om blockchain in te voeren.
G. **Verwachte impact** van blockchain. Dit geeft aan wat het verwachte nut is van blockchain en waar uitdagingen liggen in het invoeren ervan.
H. **Blockchain Innovatiescore** om te duiden in hoeverre het bedrijf een incrementele versus radicale innovatie doormaakt, aan de hand waarvan de kansen op waardecreatie van het businessmodel kunnen worden ingeschat.
I. **Blockchain Implementatie**risico's waarmee naar risico´s wordt gekeken die specifiek met blockchainprojecten samenhangen.
J. **Conclusie**.

Nadat de verschillende blockchainimplementaties zijn behandeld, wordt het hoofdstuk afgesloten met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst.

Er zijn nog geen uitvoerige implementaties van blockchain geweest waarvan de gevolgen op het business ecosysteem uitvoerig zijn onderzocht. Omdat wetenschappelijk onderzoek niet veelvuldig voorhanden is, hebben we het volgende vooral praktisch ingestoken op basis van bestaande casussen.

16.2 Bankieren en Financieren

Bankieren en Financieren is de grootste sector waar blockchain wordt toegepast. Omdat blockchain voor het eerst werd toegepast om waarde snel, goedkoop en zonder tussenkomst van derde partijen over te brengen naar anderen, is het niet zo vreemd waarom blockchain zeer

disruptief is voor deze sector. Satoshi Nakamoto zag immers ook de noodzaak om deze sector te ontwrichten. De casussen die we voor Bankieren en Financieren gaan analyseren zijn ICE Bakkt en BitShares. Bakkt is een platform waarop Bitcoin futures kunnen worden verhandeld en BitShares is een gedecentraliseerde handelsplatform op de blockchain.

A. Externe ontwikkelingen

Uit de eerdergenoemde externe ontwikkelingen van PESTEL, beïnvloeden onderstaande factoren het businessmodel van financiële instellingen het meest. Deze ontwikkelingen worden weergegeven in een heat map die invloeden van de externe ontwikkeling op vier manieren kan duiden:

Rood	Uitdagende ontwikkeling met duidelijke invloed op het businessmodel, actie nodig.
Oranje	Ontwikkeling met mogelijk een invloed op het businessmodel, meer onderzoek nodig.
Groen	Kansrijke ontwikkeling met mogelijk positieve invloed op het businessmodel, actie gewenst.
Grijs	Ontwikkeling heeft geen invloed op het businessmodel.

In de beschrijving van de volgende businessmodellen worden omwille van inzichtelijkheid alleen de belangrijkste uitdagingen en kansen beschreven. Voor Bankieren en Financieren gelden in het algemeen de volgende belangrijke ontwikkelingen.

Politiek

Uitdaging: drang om risico's bij systeembanken te beheersen door het stimuleren van concurrentie aan de ene kant, maar regulering van Big Tech aan de andere kant. Bezie in dit licht ook de discussie over Libra als alternatief voor nationale valuta en als instrument voor Big Tech om financiële relaties met klanten aan te gaan.

Economisch

Uitdaging: nieuwe concurrenten als FinTech en Big Tech dringen de markt binnen met digitale innovaties en financiële diensten en dreigen daarmee de klantrelaties over te nemen. Hierdoor wordt de traditionele waardeketen vervangen door ecosystemen, waarin verschillende partijen die voorheen niet met elkaar samenwerkten aan elkaar worden gekoppeld.

Kans: financiële dienstverleners zien kans in tokenization en fractionalisering van alle soorten bezit. Opkomst van decentrale blockchain businessmodellen. De handel in cryptoactiva neemt flink toe.

Technologie

Kans: blockchain bestaat sinds 2009 en is stabiel genoeg om in specifieke financiële diensten flinke waarde te creëren, gezien het hoge volume van waardeoverdrachten. Hoewel er al verscheidene toepassingen zijn om cryptoactiva op te bewaren en te verhandelen, is de potentiële markt van financiële dienstverlening zo groot dat er hier nog steeds veel kansen zijn. Er is dus ruimte voor nog breder gebruikte toepassingen. Daarnaast bestaat er ook de mogelijkheid dat blockchaintechnologieën de manier waarop sommige huidige financiële diensten worden verleend overbodig zullen maken. Denk hierbij bijvoorbeeld aan het vermijden van Payment Service Providers wanneer betalingen peer-to-peer plaatsvinden.

Uitdaging: de blockchaintechnologie wordt nog niet volledig vertrouwd door grote financiële instellingen die daarbij ook met wettelijk toezicht te maken hebben.

Legaal

Uitdaging: in sommige landen oefent de politiek druk uit om decentrale peer-to-peernetwerken buiten de wet te plaatsen. Zie bijvoorbeeld de Amerikaanse Securities and Exchange Commission (SEC) die publieke blockchaininitiatieven in de financiële dienstverlening zonder KYC/AML niet toestaat.

Uitdaging: de wet legt nadruk op de bescherming van persoonlijke data en de poortwachtersfunctie van financiële dienstverleners. Cryptotokens, blockchains, smart contracts en DAO's hebben verder ook een onduidelijke legale status in veel landen. Daarnaast is er ook het gebrek aan wettelijk toezicht bij ICO's of DAO's. Publieke blockchainsystemen handelen niet in overeenstemming met nationale wetgeving. Sommige toezichthouders staan het direct gebruik van cryptovaluta door grote financiële instellingen niet toe.

Uitdaging: de onveranderbaarheid van transacties wil je door toezicht in sommige landen niet. Ook wil je soms niet dat er geen beslag kan worden gelegd op cryptorekeningen.

Relevante financiële diensten, waar blockchain een grotere invloed heeft, zijn betalingsverkeer, effectenhandel, nationale valuta, cryptovaluta, financiering en crowdfunding.

B. Bedrijfsproces, karakteristieken en doel blockchainhandel in cryptovaluta's en digitaal bezit

Het voorbeeld dat hier wordt beschreven is de handel in effecten, de handel in cryptovaluta en het gebruik van deze cryptovaluta binnen het betalingsverkeer. We beschrijven het huidige bedrijfsproces, het doel van de blockchain en de karakteristieken van de waardeketen voor ICE en BitShares.

Het huidige bedrijfsproces voor effecten is als volgt:

1. Een verkoper heeft een eigendomscertificaat dat bij een custodian fysiek wordt bewaard en geadministreerd.
2. Een koper legt een order in die wordt geplaatst bij zijn broker.
3. De broker probeert op de aandelenbeurs een transactie overeen te komen met verkopende brokers.
4. De brokers van de verkoper en koper bereiken overeenstemming over een transactie en bevestigen dit met de koper en verkoper.
5. Een clearinghouse zorgt er vervolgens voor dat de transactie tussen beide partijen administratief wordt verwerkt.

Bij de handel in cryptovaluta kan er een order worden geplaatst op de blockchain zonder tussenpartijen zoals een broker, custodian en clearinghouse. In deel I is ook het huidige betalingsproces en de mogelijkheid om met verschillende wallets en cryptovaluta te betalen uitgelegd.

Voor het gemak noemen we hieronder alleen de belangrijkste karakteristieken van de handel in effecten binnen de huidige opzet, dus zonder het gebruik van blockchain. De handel in cryptovaluta en het betalingsverkeer dienen als aanvulling:

1. Financieel eigendom wordt in hoge volumes onderling overgedragen tussen professionele partijen.
2. Het eigendom bestaat voornamelijk uit unieke digitale bezittingen met onderliggende papieren documenten, zoals contracten.
3. De overdracht vindt zowel handmatig als digitaal plaats binnen een complex administratief traject waarin wederzijdse afstemming van data een grote rol speelt.
4. Er is veel regulering van de dienstverlening. Partijen kennen elkaar en zijn door de wetten verplicht complexe KYC-processen te ondersteunen.
5. Het snijvlak van hoge winsten, hoge complexiteit van het proces en grote kansen tot automatisering stimuleren nieuwe concurrentie om toe te treden met behulp van innovatieve diensten.

C. Business ecosysteemactoren

In het volgende wordt een bedrijf gebruikt dat binnen deze waardeketen een mogelijkheid zoekt om blockchain toe te passen. Hiervoor kijken we naar het bedrijf Intercontinental Exchange (ICE), het moederbedrijf van onder andere de New York Stock Exchange (NYSE). ICE wil graag gebruikmaken van de kansen die blockchain biedt om de financiële diensten verder uit te breiden met onder andere de handel in Bitcoin futures en andere digitale eigendom.[186]

De belangrijkste actoren binnen het ICE business ecosysteem staan in het volgende tabel.

Core business	Grote financiële instellingen en de eigen exchanges en clearinghouses. Daarnaast custodians en brokers. Aandeelhouders op de publieke markt.
Verlengde onderneming	Klanten van de partijen genoemd onder core business.
Business ecosysteem	Competitie met andere exchanges zoals NASDAQ, maar ook online cryptohandelsplatformen als eToro en Coinbase. ***Securities and Exchange Commission*** (SEC), ***Federal Trade Commission***, ***Commodity Futures Trading Commission*** (CFTC), ***Federal Reserve*** en andere toezichthouders.

Tabel 9: Actoren binnen het ICE business ecosysteem.

D. Heat map businessmodelelementen

Per PESTEL-ontwikkeling wordt gekeken waar nu de grote uitdaging of kans ligt voor het huidige businessmodel van ICE. Normaal gesproken neemt een bedrijf hiervoor 3 tot 4 PESTEL-elementen. Voor ICE nemen we twee ontwikkelingen die we binnen een BMC behandelen: één uitdagende en één kansrijke ontwikkeling.

Aan de ene kant groeien de volumes in de handel in cryptovaluta, terwijl er nog geen grootschalig gebruikte legale toepassingen zijn om cryptoactiva op te bewaren en te verhandelen buiten peer-2-peernetwerken om. Aan de andere kant staat de toezichthouder niet toe dat cryptovaluta daadwerkelijk worden geleverd als afsluiting van cryptovalutaderivaten zoals Bitcoin futures. Vanuit deze ontwikkelingen kan het businessmodel als volgt worden ingevuld.

[186] Bitcoin futurecontracten zijn wettelijke overeenkomsten om Bitcoin te kopen of verkopen tegen een specifieke prijs op een specifiek moment in de toekomst.

	Toenemende handel	Verbod toezichthouder
Wie? klantsegmenten	Mensen die investeren in cryptovaluta, retailers en hun eindklant.	Niet kunnen aanboren van nieuwe klantsegmenten.
Wat? waardepropositie	Bitcoin futures aanbieden via vertrouwde professionele partijen.	Momenteel waardevernietigend. Kans om het verbod te omzeilen opent nieuwe kansen.
Wie? kanalen	Huidige partners, Bitcoin blockchain, massaal gebruikte digitale klanttoepassingen zoals wallets via web en mobiele applicaties en debetkaarten.	
klantrelatie	Integratie van online accounts, wallets en debetkaarten.	
Wat? opbrengsten	Nieuwe diensten en producten.	
Hoe? kernactiviteiten	Handel in cryptovaluta en datadeling.	
mensen & middelen	Innovatieve kennis, informatiesysteem, softwareprotocollen, interne controles en dergelijke.	
sleutelpartners	Publieke blockchain stakeholders, datasystemen, blockchain enthousiastelingen, softwareleveranciers, investeerders en tokenhouders.	Toezichthouders waaronder Securities and Exchange Commission (SEC), Federal Trade Commission, Commodity Futures Trading Commission (CFTC) en de Federal Reserve.
Wat? kosten	Vergt investering in nieuwe kennis en IT-systemen om blockchain te gebruiken.	Risicobeheersing, voornamelijk legale risicobeheersing.

Tabel 10: ICE ingevuld businessmodel.

Uit deze ontwikkelingen vloeit er een kans om een oplossing te verzinnen die voor de toezichthouders aanvaardbaar is, waarmee ICE de financiële diensten uit kan breiden met onder andere de handel in Bitcoin futures en digitale eigendom. Voor dit doel heeft ICE in 2018 Bakkt opgericht.

Bakkt

In 2019 kreeg Bakkt de benodigde toestemming van toezichthouders als de Amerikaanse Commodity Futures Trading Commission (CFTC). De toezichthouders wilden wel dat Bakkt in

staat is om beslag te leggen op cryptofondsen. Bakkt houdt hiervoor de private keys van klanten in bezit. Bakkt zal in overeenstemming met de wet, Bitcoin futures afhandelen door het leveren van Bitcoins waar concurrenten de futures nog afhandelen met kasgeld. Hiervoor maakt Bakkt gebruik van onder andere de Bitcoin blockchain, het Microsoft Azure platform en de custodian BNY Mellon Bank.[187] Op termijn wil Bakkt een toepassing uitrollen waarmee kleinere klanten of eindgebruikers verschillende cryptovaluta en digitaal eigendom direct kunnen inwisselen tegen nationale valuta om er producten en diensten mee te (ver)kopen. Hiervoor bouwt Bakkt met Starbucks en Microsoft en zijn leveranciers aan applicaties waarmee een klant bijvoorbeeld een koffie binnen een Starbuckscafé kan betalen.

In het volgende wordt het traject van ICE verder uitgewerkt. Waar relevant wordt de oplossing vergeleken met een publiek blockchaininitiatief om de vergelijking te laten zien tussen een incrementele innovatie, waarin centraliteit nog een rol speelt en een radicaal innovatief model. Zodoende wordt geprobeerd duidelijk te maken welke gevolgen verdere decentralisatie in de toekomst nog biedt. In dit geval wordt ICE Bakkt vergeleken met BitShares.

BitShares is een DAO handelsplatform waar iedereen zonder KYC een account kan aanmaken, tokens kan creëren en cryptovaluta peer-2-peer kan verhandelen. BitShares wordt ook wel een Decentralized Exchange (DEX) genoemd. Deze tokens hoeven niet alleen maar cryptovaluta te zijn. Ze kunnen ook bijvoorbeeld kunst, onroerend goed, concerttickets en arbeidsuren representeren. Het doel van BitShares is om brede financiële diensten op te zetten voor handel, betalingsverkeer en investeringen. BitShares doet eigenlijk dus al wat Bakkt nastreeft, maar dan op een blockchain.

[187] In dit geval bewaart de custodian zowel het digitale eigendom als de private en public keys.

E. Detail van de oplossing

Hier wordt de oplossing van Bakkt in detail uitgelegd en op de voornaamste punten vergeleken met BitShares.

	Bakkt	bitshares
Dienst	Vooralsnog handel in Bitcoin futures.	Handel in al het digitale bezit en betalingsverkeer.
Governance	Centrale organisatie. Privaat, gesloten, permissioned, eigendom van publiekgenoteerde onderneming. Bakkt behoudt gedetailleerde klanteninformatie over transacties en dergelijke, waardoor informatie-asymmetrie blijft gelden. Akkoord met toezichthouders.	Decentrale organisaties. Publiek open permissionless met centraal committee, witnesses, workers, tokenhouders en ondersteuning van een stichting. Kent als DAO geen legale status.
Technisch oplossing	Bitcoin blockchain, Microsoft Azure en eigen informatiesysteem.	C++ programmeertaal voor de Graphene blockchain.
open source	Nee, wel als Bitcoin tokenhouders.	ja
consensus mechanisme	Nee, wel als Bitcoin tokenhouders.	Delegated Proof-of-Stake.
smart contracts	nee	Ja
dApps	Nee, wel als Bitcoin tokenhouders.	Ja
SSI of digitale identiteit	Digitale identiteit	Digitale identiteit.
blockchain of alternatieve DLT	Nee, wel als Bitcoin tokenhouders.	Blockchain
onveranderbare data	Nee, wel als Bitcoin tokenhouders.	ja
transparante data	Nee, wel als Bitcoin tokenhouders.	ja
Tokens / beloningen		
Validator beloning	Nee, wel als Bitcoin tokenhouders.	ja
Betalings/native token	nee	BitShares
Digitaal eigendom token	In eerste instantie Bitcoin.	Kan worden gecreëerd op het platform.
Fractionalisering	nee	ja

Tabel 11: Oplossing van Bakkt vergeleken met BitShares.

Het ecosysteem van ICE wordt met de komst van Bakkt dynamischer. Het geeft de mogelijkheid data te verkrijgen van de klanten van relaties als Starbucks. Ook geeft het de mogelijkheid om

leveranciers van leveranciers, zoals applicatieontwikkelaars voor het Microsoft Azure platform te betrekken en een mogelijke toekomstige interface met private en publieke blockchains te maken. Ook wordt er gehandeld met Bitcoin tokenhouders, die in de toekomst een nieuw ecosysteem zullen vormen. Ook neemt het aantal concurrenten toe met bedrijven als andere digitale handelsplatformen als eToro, Binance, Circle, Huobi en BitShares. Daarnaast kan het ecosysteem met het uitrollen van nieuwe diensten potentieel nog vele malen dynamischer worden. Dit kan een netwerkeffect in gang zetten.

Het ecosysteem van BitShares bestaat uit een groep van klanten, investeerders en leveranciers die allen ook BitShares tokenhouders kunnen zijn. Dit laatste vergemakkelijkt de governance op het eerste gezicht. Binnen BitShares combineren tokenhouders meerdere rollen, waaronder die van promotor, klant, investeerder en leverancier van bijvoorbeeld software skills. De competitie is niet verschillend van die van Bakkt, hoewel het sneller tegen competitie binnen het blockchaindomein zal oplopen. BitShares heeft samenwerkingsverbanden met professionele private non-blockchainbedrijven, disruptieve technologieondernemingen en andere Graphene-gedreven organisaties en EOS.

In het licht van ecosystemen fungeert Bakkt zelf als tussenpartij tussen de publieke blockchain en private partijen. Ook fungeert Bakkt nog steeds als tussenpartij met rollen als exchange en clearinghouse. BitShares probeert deze rollen weg te nemen en legt de governance in handen van gedelegeerden (delegates) die worden gekozen door tokenhouders.[188]

De businesscase richting zowel traditionele competitie alswel blockchaincompetitie voor Bakkt is al in de bespreking van rode en groene PESTEL-ontwikkelingen duidelijker geworden. Het belangrijke verschil tussen Bakkt en BitShares is dat Bakkt back-up heeft van ICE als een sterke betrouwbare partij met gekende software. Bij Bakkt zijn ook de bestuurders bij naam en reputatie bekend, wat bij BitShares niet hoeft. Uiteindelijk biedt het dus transparantie in en vertrouwen aan een markt die velen nog niet begrijpen. Zodoende worden de voordelen die opkomen door het decentrale karakter van blockchain niet volledig gebruikt – iets wat BitShares wel doet. Verder probeert Bakkt groter gebruikersgemak te creëren door de toepassing te integreren met verschillende massaal geadopteerde systemen van bijvoorbeeld Microsoft.

[188] BitShares maakt, zoals uitgelegd in paragraaf 6.4, gebruik van Delegated Proof-of-Stake. Hierbij worden nieuwe blokken geproduceerd door witnesses en is de governance in handen van delegates.

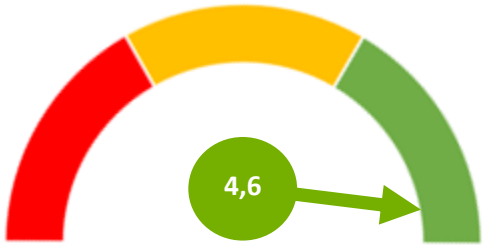
F. Blockchain Gereedheidsscore

De centrale vraag is hier in hoeverre de businesscase voldoet om blockchain als oplossing te verkiezen. Deze vraag wordt beantwoord met een ***Blockchain Gereedheidsscore***. Deze score is verkregen door een score te hangen aan een set van vragen rondom de digitale strategie, de process flow, het ecosysteem en de technische gereedheid. In dit geval voert ICE geen volledige blockchainoplossing door, maar integreert het het gebruik van een bestaand publiek blockchainsysteem. De tabel is ingevuld met de gedachte dat ICE Bakkt Bitcoin futures verhandelt. Een vergelijking met BitShares heeft hier gezien de achtergrond van BitShares als een publiek blockchainsysteem weinig toegevoegde waarde en wordt daarom niet gemaakt.

(1 = absoluut niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Digitale innovatie is onderdeel van de strategie.					5
Verschillende partijen delen gegevens.				4	
Deze gegevens en hun transacties betreffen geldwaarde.					5
De data zijn vertrouwelijk.					5
Verschillende partijen bewerken gegevens.					5
Gegevens moeten worden geverifieerd.					5
Er is een duidelijke Return on Investment te berekenen, en deze voldoet in dit geval.					5
Verificatie is complex, kosten- en of tijdverhogend.					5
De oplossing om voor blockchain te kiezen, is de meest simpele kans om het probleem te overwinnen.					5
De oplossing beïnvloedt de bestaande organisatiestructuur.					5
De oplossing beïnvloedt de bestaande workflow.					5
De oplossing beïnvloedt het bestaande ecosysteem, zo is er geen tussenpartij met een centrale positie.	1				
De technische oplossing ligt dichtbij bestaande systemen en/of het bestaande systeem is van belang.				4	
De oplossing is data-intensief maar schaalbaar: 1k, 10k, 100k, 1 mln. of > 10 mln. transacties per uur.					5
Blockchain Gereedheidsscore Bakkt	**64 / 14 = 4,6**				

Tabel 12: Bakkt Blockchain Gereedheidsscore.

Uit de tabel blijkt ICE een Blockchain Gereedheidsscore te hebben van 4,6. De minimale score is 1 en de maximale score is 5.



ICE lijkt met een score van 4,6 gereed om blockchain in te voeren, wat niet verwonderlijk is omdat Bakkt specifiek als blockchaininitiatief is gestart door ICE. Het heeft in dit geval echter geen volledige blockchainoplossing ingevoerd. Het verhandelt momenteel slechts Bitcoin futures binnen het bestaande businessmodel. Op termijn is de verwachting dat Bakkt verder integreert met andere publieke blockchainsystemen. Misschien zal blockchain uiteindelijk als onderliggende data-infrastructuur worden gebruikt, waarbij tussenpartijen volledig worden ontweken. De volgende stap hiertoe is om een walletapplicatie te ontwikkelen waarmee klanten direct hun digitale eigendom kunnen gebruiken om diensten en producten af te nemen bij retailers binnen het ecosysteem van Bakkt, zoals Starbucks.

G. Verwachte impact blockchain

Op basis van de voorgaande modellen kun je een inschatting maken van de impact die wordt verwacht als blockchain wordt ingevoerd. Omdat de impact van blockchain op ICE inzichtelijker is wanneer we het afzetten tegen BitShares, worden deze twee projecten naast elkaar gezet in het volgende tabel.

	Bakkt	bitshares
Omzetvermeerdering	Nieuwe diensten met mogelijk opschalen van andere diensten, zoals fractionalisering.	Binnendringen nieuwe markt. Betrekken nieuwe klanten.
Datavermeerdering	Potentieel nieuwe data verkrijgen dankzij combinatie met Starbucks.	
Netwerkeffect	Ecosysteem van verschillende nieuwe partners met mogelijkheid tot opschalen van de 'partners van partners'. Dit leidt tot meer data die vallen te combineren en te analyseren, wat weer tot omzetvermeerdering leidt.	Rol van tokenhouders als agenten van het bedrijf zou dit kunnen bewerkstelligen, maar het netwerkeffect moet zich hier nog bewijzen.
Risicovermindering	Verhoogd risico doordat custodian mede public en private keys bewaart en transacties op de Bitcoin blockchain niet kunnen worden teruggedraaid.	
Werkkapitaal	Mogelijk voordeel in het salderen van aan- en verkooporders. Mogelijk nadeel doordat kapitaal vastzit in gekochte Bitcoin.	
Identiteitsmanagement		Anonimiteit en autonomie binnen eigen DAO.
Governance		Tokenhouders met alle sleutelrollen verenigd in DAO.
Disintermediatie		Omzeilen van tussenpartijen, zoals clearing house.
Veiligheid	Gebruik van privaat netwerk ten bate van schaalbaarheid, maar ten koste van beveiliging.	
Wettelijke compliance	Nadeel van een intern controlesysteem optuigen, om met publieke blockchain te kunnen werken.	Dreiging van publieke blockchainsystemen als BitcoinSV en BitcoinCash die applicaties ontwikkelen met Bakkt als juridisch voorbeeld om in overeenstemming met de wet- en regelgeving te werken.
Experimenteren met technologie	ICE Bakkt schaalt gebruik van de technologie langzaam op.	

Tabel 13: Verwachte impact van blockchain op Bakkt en BitShares.

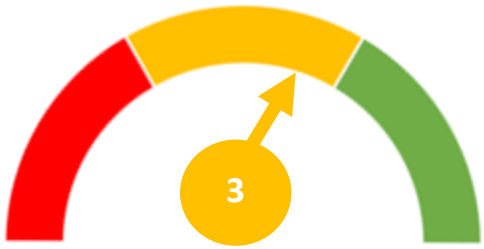
H. Innovatiekracht

De centrale vraag hier is in hoeverre dit een incrementele versus radicale innovatie betreft. Dit is relevant voor de implementatie en de mogelijke opbrengsten en kosten die het model brengt. Deze vraag wordt beantwoord met het volgende tabel. Bij elke deelvraag staat een aantal te behalen punten, die uiteindelijk leiden tot een ***Blockchain Innovatiescore***. De tabel is ditmaal alleen voor Bakkt ingevuld.

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Mate van decentralisatie.	1				
Aanboren nieuwe markt of al bestaande markt.					5
Gebruik van nieuwe processen.				4	
Gebruik van nieuwe stakeholders binnen nieuw ecosysteem.				4	
Omzeilen van tussenpartij.	1				
Technische innovatie: maakt gebruik van SSI, tokenization, smart contracts, nieuw consensusmechanisme, nieuwe technische workflow			3		
Blockchain Innovatiescore Bakkt	**18 / 6 = 3**				

Tabel 14: Bakkt Blockchain Innovatiescore.

De minimale Blockchain Innovatiescore is 1 en de maximale score is 5. In dit geval komt de Blockchain Innovatiescore uit op 3. Het initiatief is dus gemiddeld innovatief.



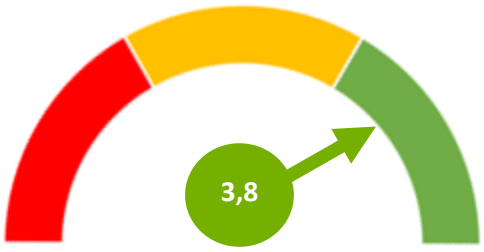
I. Implementatierisico

Een belangrijke vraag is in hoeverre de impact van de innovatie de complexiteit van de implementatie gaat beïnvloeden. Deze vraag wordt beantwoord met de volgende tabel. In de tabel staat een set van elementen die kan worden gescoord van 1 tot 5. Het gemiddelde van het aantal behaalde punten leidt tot een ***Blockchain Implementatiescore***. Een hogere score geeft aan dat de organisatie meer gereed is om succesvol blockchain te implementeren.

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Ecosysteem is eenvoudig, in de zin van dat er geen tussenpartij is, samenwerking geografisch dichtbij huis, wil om samen te werken bij actoren, gelimiteerd aantal actoren te coördineren.			3		
Blockchain Gereedheidsscore					5
Blockchain Innovatiescore			3		
Er ligt intern nadruk op digitale innovatie: data en digitale innovatie staan centraal in strategie, organisatiestructuur heeft bewezen te kunnen innoveren, informatiesystemen en -processen op orde, technische kennis aanwezig.					5
Het initiatief is legaal en in overeenstemming met geldende standaarden en richtlijnen.					5
Het probleem heeft een zekere prioriteit, maar is geen kritisch complex proces dat (grote) organisatorische veranderingen vereist.		2			
Blockchain Implementatiescore Bakkt	**23 / 6 = 3,8**				

Tabel 15: Bakkt Implementatiescore.

De minimale Blockchain Implementatiescore is 1 en de maximale score is 5. In dit geval komt de Blockchain Implementatiescore uit op 3,8. De score is dus ruim boven gemiddeld.



In dit geval lijken de voorwaarden aanwezig voor een succesvolle implementatie. Het ecosysteem zal mee willen werken en de organisatie is intern gereed om blockchain te implementeren.

J. Conclusie

Uit de voorgaande analyses is nu gebleken wat de kansen en uitdagingen zijn voor het businessmodel, de strategie en de implementatie. Hierin komt voornamelijk naar voren dat ICE momenteel niet decentraler gaat werken, maar wel de kans heeft dit in de toekomst te doen. Dit leidt aan de ene kant tot aanpassingen van de processen en aan de andere kant tot een vergroting van de markt. Daarnaast experimenteert ICE samen met nieuwe partners met een nieuwe technologie binnen een ecosysteem dat grote kansen biedt voor het uitbreiden van diensten en producten. De vraag hier is met welke snelheid ICE de nieuwe diensten op weet te schalen en in hoeverre het mede onder druk van decentrale modellen als BitShares zelf stappen neemt richting een decentraal businessmodel.

16.3 Overheid en Publieke Goederen

Overheid en Publieke Goederen is de op één na grootste sector voor blockchain use cases (Hileman & Rauchs, 2017). Er is in deze sector namelijk veel behoefte aan transparantie en efficiëntie van digitaal ontwikkelde overheden en hun e-Governmentprojecten waar blockchain aan kan bijdragen. De casussen die we gaan analyseren zijn het Zweedse Lantmäteriet en het Keniaanse Land Layby die onroerend goed registreren.

A. Externe ontwikkelingen

In de beschrijving van de volgende businessmodellen worden omwille van inzichtelijkheid alleen de belangrijkste uitdagingen en kansen beschreven. Voor Overheid en Publieke Goederen gelden de volgende belangrijke ontwikkelingen.

Politiek

Kans: de behoefte om transparantie en openheid naar de burger te geven over digitalisering en internettoegang via mobiele apparaten.

Economisch

Uitdaging: publieke instellingen gebruiken vaak nog inefficiënte handmatige processen waarin papier van hand wisselt. Dit kan leiden tot fouten, omissies en dubbel werk in de data.

Kans: Zweden is een ontwikkeld digitaal land met een sterke groei in digitale informatie. Hierbinnen neemt het gebruik van informatie via e-Government en e-services toe.

Technologie

Kans: blockchain als technologie biedt de kans om handmatige processen en de overdracht van documenten tussen meerdere partijen op een veilige manier te automatiseren. Hierbinnen kan de Self-Sovereign Identity worden gewaarborgd.

Uitdaging: blockchaintechnologie wordt nog niet volledig vertrouwd door burgers.

Legaal

Uitdaging: Verschillende wetten en regels bemoeilijken de adoptie van digitale technologie. Zo schrijft de EU General Data Protection Regulation (GDPR) voor dat het individu recht heeft op beheer over eigen data, waaronder het kunnen afschermen en verwijderen waar gewenst en mogelijk. Het Zweedse instituut voor standaardisering schrijft ook het gebruik van standaarden voor.[189] Daarnaast is er een ***eIDAS richtlijn*** over hoe digitale handtekeningen als legaal bindende handtekeningen kunnen worden gebruikt binnen de EU. Dit wordt e-Signatures genoemd. In Zweden moet de verhandeling van eigendomsrecht in (on)roerend goed echter nog met geschreven handtekeningen gebeuren sinds 2016. Verder is de status van digitaal ondertekende contracten op basis van blockchain nog onduidelijk – bijvoorbeeld of en hoe contracten op de blockchain bindend zijn.

B. Bedrijfsproces, karakteristieken en doel registratie van onroerend goed in Zweden: Lantmäteriet

Het voorbeeld dat hier wordt beschreven is dat van de registratie van onroerend goed door het Zweedse Lantmäteriet. Lantmäteriet heeft als taken het Zweedse kadastrale systeem te onderhouden, in geodata te voorzien en landregistratie te verrichten.

Het huidige bedrijfsproces voor registratie van land ziet er in de basis als volgt uit:

1. Een landeigenaar en koper vinden elkaar en onderhandelen een prijs.
2. De koopovereenkomst wordt ondertekend door beiden.
3. De koper verricht een aanbetaling.
4. Een makelaar geeft een bewijs van verkoop uit.
5. De bank stuurt het bewijs van verkoop na financiële verificatie door naar Lantmäteriet.

[189] Zoals ISO 15489, TIFF en PDF-A.

De belangrijkste karakteristieken van dit proces zijn:

1. Het betreft overdrachten van hoge waarde.
2. Het zijn veelal papieren processen die in totaal wel 3-6 maanden kan duren. Naast de inefficiënte invoer van gegevens, kan er ook informatie missen en is de informatie fout- en fraudegevoelig.
3. Wederzijdse afstemming van data speelt een grote rol, hoewel data die zijn verkregen niet worden hergebruikt.
4. Gegevens dienen volgens de Zweedse wet 10 jaar te worden bewaard.
5. Er is een hoge mate van regelgeving van de dienstverlening. Partijen kennen elkaar en worden door de wet gereguleerd.
6. De identiteitscheck vindt handmatig plaats.
7. Lantmäteriet wordt pas in de laatste stappen betrokken bij het proces, waardoor het proces dat zich daarvoor afspeelt niet transparant is voor het publiek.

C. Business ecosysteemactoren

Lantmäteriet had in 2015 pakweg 50 kantoren, 2.000 mensen in dienst en een omzet van €165 miljoen (Lantmäteriet, 2016). Als grote publieke organisatie wil het blockchain inzetten ten bate van inzicht in en het coördineren van de aankoop- en registratieproces van onroerend goed.

De belangrijkste actoren binnen het huidige Lantmäteriet business ecosysteem zijn als volgt.

Core business	Kopers, verkopers, advocaten, taxateurs, makelaars en verleners waaronder banken, verzekeraars en pensioenfondsen.
Verlengde onderneming	ICT-bedrijven inclusief ontwikkelaars en datatoeleveringsbedrijven.
Business ecosysteem	Overheidsinstanties, zoals het Zweedse instituut voor standaardisering, het ISO, vergelijkbare bedrijven binnen de Europese Unie.

Tabel 16: Actoren binnen het Lantmäteriet business ecosysteem.

D. Heat map businessmodelelementen

Per PESTEL-ontwikkeling wordt gekeken waar de grote uitdaging of kans ligt voor het huidige businessmodel. Aan de ene kant biedt technologie de kans om handmatige processen te automatiseren om zowel kosten te besparen als transparantie en openheid van het gehele proces te bieden aan de burger. Aan de andere kant stonden in 2016, toen het project begon, wetten en regels zoals GDPR en de Zweedse wetten op publieke informatie de blockchaininnovatie in de weg, zoals de onveranderbaarheid van informatie en digitale handtekeningen voor (on)roerend goed. Verder is de legale status van e-contracten onduidelijk.

Vanuit deze ontwikkelingen is de belangrijkste focus van Lantmäteriet op de volgende factoren binnen het businessmodel.

	Procesverbetering	Verbod toezichthouder
Wie? klantsegmenten		Niet kunnen aanboren van nieuwe klantsegmenten.
Wat? waardepropositie	Met blockchain realtime transparantie in gehele proces aan burger bieden, procesversnelling, kostenbesparing.	Momenteel waarde vernietigend. Kans om het verbod te omzeilen opent nieuwe kansen.
Wie? Kanalen	Online platform met huidige partners.	
klantrelatie	Online platform met gehele transactieketen, inclusief online en persoonlijke ondersteuning.	
Wat? opbrengsten	Meer openheid en transparantie, proces versnellen en fouten verminderen.	
Hoe? kernactiviteiten		Registratie en bewaring van verkoop van landtitels.
mensen en middelen	Innovatieve kennis met partners in online platform en blockchaininformatiesysteem. Reorganisatie door versimpelen van proces.	
sleutelpartners	Nieuw ecosysteem met meerdere partners zoals ChromaWay blockchainleverancier, Telia Zweden, SBAB bank, Landshypotek Bank, Kairos Future consultancy, Evry ICT, andere overheidsinstanties en onroerend goed zoekportaal Svensk Fastighetsförmedling.	Overheidsinstanties om te toetsen in hoeverre e-contracten, e-signatures en GDPR blockchainoplossingen mogelijk zijn.
Wat? kosten	Investering vertaalt zich terug in minder administratieve lasten en onderhoud, resulterend in misschien €100 miljoen besparing per jaar (Kairos Future, 2017).	Legale risicobeheersing en kans op het niet volledig benutten van blockchaintechnologie.

Tabel 17: Lantmäteriet ingevuld businessmodel.

Lantmäteriet heeft in 2019 de verkoop van landtitels via blockchain succesvol getest en werkt sindsdien aan eenzelfde oplossing voor huizen en gebouwen. Ook betrekt Lantmäteriet andere overheidsdiensten, zoals de Zweedse Belastingdienst. Binnen de blockchainoplossing bewaart Lantmäteriet persoonlijke informatie off-chain. Deze informatie kan in overeenstemming met GDPR worden verwijderd als de klant dit wil.

Verder worden contracten handmatig ondertekend en via hashes op de blockchain gezet. De originele contracten staan bij andere partijen op de server. Telia biedt daarbij een mobiele app ID-oplossing aan waarmee mensen zich zonder het Zweedse Burgerlijk Service Nummer te kennen toch kunnen registreren. Deze registraties worden ook via een hash opgeslagen op de blockchain.

In het volgende wordt het traject van incrementele innovatie van Overheid en Publieke Goederen verder uitgewerkt. Waar dat relevant is, wordt de oplossing vergeleken met een publiek blockchaininitiatief dat meer een radicaal innovatief model nastreeft. Hiermee laten we zien wat decentralisatie in de toekomst nog meer te bieden heeft.

In dit geval wordt Lantmäteriet vergeleken met Land Layby. Dit is een Keniaanse holding die transparantie wil brengen in een traag, soms corrupt, administratief landregistratiesysteem in Ghana. De Ghanese overheid heeft meerdere initiatieven gehad om blockchain te integreren met hun landregister, waaronder Bitland, BenBen en in 2018 IBM. Deze samenwerkingen hebben maar niet geleid tot een implementatie van het systeem (Eder, 2019). Om de aan- en verkoop van land voor vooral Ghanese immigranten te vergemakkelijken, wil Land LayBy daarom landtitels bijhouden op de blockchain. Dit land spiegelt de officiële registratie bij de Ghana Land Commissie, maar de informatie over het land wordt op de blockchain bijgehouden door verschillende partijen. Gebruikers kunnen hierbij de Harambee token verdienen. Land LayBy is geen volledig alternatief voor Lantmäteriet. Het biedt 2 jaar lopende callopties op onderliggend land dat potentiële kopers de kans geeft het koopproces officieel af te ronden met behulp van Land LayBy tussenpartijen. De callopties kunnen worden verhandeld.

E. Detail van de oplossing

	LANTMÄTERIET	LAND LAYBY
Dienst	Landregistratie	Verkoop callopties op land.
Governance	Centrale overheidsorganisatie met privaat, gesloten, permissioned blockchainsysteem. Eigendom van overheid, onder toezicht van publieke Zweedse overheidsorganen.	Privaat, ontwikkeld Land LayBy Listing (LLL) dApp op Ethereum dat getuigen, werkers en tokenhouders heeft.
Technisch oplossing	Samenwerking CromaWay's Esplix en eigen informatiesystemen van stakeholders.	Solidity, dApp heeft connectie met Ethereum blockchain.
open source	Ja	ja
consensus mechanisme	Practical Byzantine Fault Tolerance en Proof-of-Work.	Proof-of-Work (ten tijde van het schrijven van dit boek, december 2019, gebruikt Ethereum nog PoW).
smart contracts	Ja, Esplix legt gegevens op blockchain vast.	ja
dApps	Nee, wel apps.	Ja, op Ethereum.
SSI of digitale identiteit	Off- en on-chain, digitale identiteit via mobiele telefoon.	Nee
blockchain of alternatieve DLT	blockchain	blockchain
onveranderbare data	Nee, m.u.v. persoonlijke informatie.	ja
transparante data	Na, m.u.v. persoonlijke informatie.	ja
Tokens / beloningen		
Validator beloning	nee	Ja, ETH. Ook Harambee (HRBE) ERC20-token voor leveren van details over land.
Betalings/native token	nee	Harambee (HRBE) voor dApp.
Digitaal eigendomtoken	Nee, eigendom blijft geregistreerd bij Lantmäteriet informatiesysteem.	nee
Fractionalisering	nee	nee

Tabel 18: Oplossing van Lantmäteriet vergeleken met Land LayBy.

Een verdere uitleg van de oplossing is te vinden in de Annex, aan het eind van dit hoofdstuk.

Het ecosysteem van Lantmäteriet wordt uitgebreid en versterkt met directe data-uitwisseling en onderlinge procesafstemming tussen (ver)kopers, banken, makelaars en andere overheidsinstanties. Daarbij is het systeem publiekelijk toegankelijk geworden ten bate van vertrouwen in het proces en de partijen. Het systeem kan zich nu uitbreiden met partijen als verzekeraars, notarissen en andere lokale publieke autoriteiten.

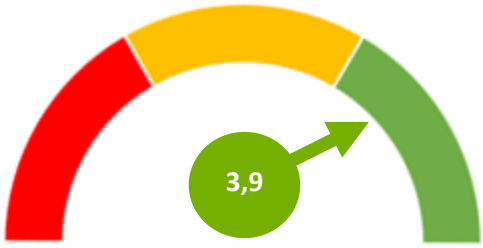
Het ecosysteem van Land LayBy bestaat uit advocaten, ondernemers, klanten en tokenhouders. De governance blijft in de centrale handen van Land Layby. De tokenhouders worden gestimuleerd om als orakels te fungeren door ze te belonen met tokens wanneer ze correcte details aan de dossiers toevoegen. Ze verliezen tokens als de details incorrect blijken. Ook vullen ingehuurde advocaten de rol van orakel in. De wijze waarop advocaten worden gestimuleerd volgens het model, is echter onduidelijk. Als laatste houdt Land LayBy zelf ook bij of officiële documenten aanwezig zijn en overeenkomen met het landregister.

De uitdaging die Land LayBy heeft, is om de trage en soms corrupte processen van landregistratie het hoofd te bieden. Deze uitdaging ontstaat mede door corruptie binnen overheidsinstanties.

Als een klant van Land LayBy land koopt en er een verschil is tussen de gegevens op de Ethereum blockchain en het officiële landregister, dan moet de klant alsnog een lastig traject door met de overheid. Hiermee wordt het probleem dus niet geheel verholpen. Uiteindelijk probeert Land LayBy vertrouwen te verkrijgen door zich als tussenpartij te plaatsen naast een overheid die het vertrouwen niet heeft. Land LayBy heeft een technisch samenwerkingsverband met ICT-bedrijf Winjit. Het register is verder openbaar voor de overheid, rechtbanken, financiële instellingen en (ver)kopers.

F. Blockchain Gereedheidsscore

De centrale vraag is hier in hoeverre de businesscase voldoet om blockchain als oplossing te verkiezen. Deze vraag wordt beantwoord met de Blockchain Gereedheidsscore, waarvan de details in de Annex is te vinden.



De minimale score is 1, de maximale score is 5. De hoge score van 3,9 is niet verwonderlijk, gezien Lantmäteriet al sinds 2016 succesvol blockchainimplementatie test. Ze doen dit bovendien door gebruik te maken van zowel een private als publieke oplossing die ze aan bestaande systemen koppelen. Een vergelijking met Land LayBy laat zien dat Land LayBy geen volledig alternatief vormt, weinig toegevoegde waarde heeft op de bestaande oplossing van Landmäteriet en daarom niet wordt gemaakt.

Op termijn is de verwachting dat Lantmäteriet het dienstenpallet en ecosysteem langzaam verder uitbreidt op de bestaande oplossing.

G. Verwachte impact blockchain

Op basis van de voorgaande modellen kan een inschatting worden gegeven van de impact die kan worden verwacht als blockchain wordt ingevoerd via onderstaande tabel.

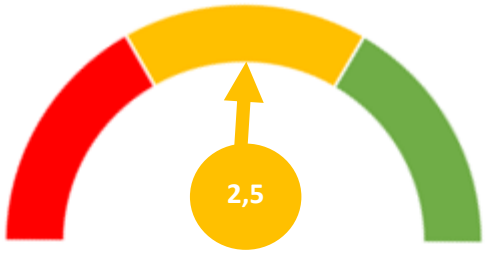
Deze impact is inzichtelijker als we het vergelijken met de impact die Land LayBy heeft.

	LANTMÄTERIET	LAND LAYBY HOLDINGS KENYA LIMITED
Omzet vermeerdering		Meer vertrouwen zou investeringen toe kunnen laten nemen, en daarmee economie verder stimuleren.
Operationele efficiëntie	Tijdsreductie van 4-6 maanden naar paar dagen, €100 miljoen/jaar besparing door minder fouten en onderhoud.	
Werkkapitaal	Tijdsbesparing leidt tot minder geld dat wordt vastgehouden bij banken.	
Datakwaliteit	Verificatie van juiste data, weigering onjuiste data, zekerheid van volledige data.	Verificatie van juiste data, weigering onjuiste data, zekerheid van volledige data.
Risicovermindering	Eén versie van het contract met eenduidige karakteristieken. Minder frauduleuze data. Minder kans dat titel niet wordt verkregen nu proces volgens de wet is opgezet. Minder kans op stelen van bezit.	Eén versie van het contract met eenduidige karakteristieken. Minder frauduleuze data. Minder kans op corrupte handeling door achteraf wijzigen gegevens, hoewel de kans blijft bestaan op originele Ghana landregister. Minder kans op stelen van bezit.
Data-integriteit	Transparantie in waardeketen en bezittingen. Audit trail naar klant, auditor en wetgever. Geen afstemming tussen partijen nodig.	Transparantie in waardeketen en bezittingen. Audit trail naar (ver)koper, bank en overheidsorganen. Reconciliatie met Ghanees landregister.
Data beschikbaarheid	Opheffen informatie-asymmetrie, inzicht in volledige keten t.o.v. eerder systeem.	Online data beschikbaar.
Identiteitsmanagement	Deels oplossing gevonden.	Ethereum ID gelinkt aan eigen oplossing, deels vertrouwd.
Governance	Private blockchain met nadruk op samenwerking tussen vertrouwde tussenpartijen	Meer controle op huidige governance via Ghanees landregister.
Wettelijke compliance	Wordt aan GDPR voldaan, hoewel het onderwerp op de agenda blijft staan i.v.m. transparantie op publieke keten. e-Signaturesoplossing voldoet.	
Gebruiksvriendelijkheid	Automatische bevestiging van ontvangen landtitel.	
Veiligheid	Open source software op gedistribueerd publieke netwerk naast privaat netwerk op 4 nodes. Juiste partijen betrokken bij stappen. Digitale back-ups van relevante informatie.	Gebruik Ethereum en smart contracts, waarvan de oplossing zich technisch nog moet bewijzen.
Experimenteren met technologie	Verkregen kennis wordt gebruikt voor opschaling van diensten en ecosysteem inclusief internationale partijen.	

Tabel 19: Verwachte impact van blockchain op Lantmäteriet en Land LayBy.

H. Innovatiekracht

De centrale vraag in deze paragraaf is te beoordelen in hoeverre dit een incrementele versus radicale innovatie betreft. De Blockchain Innovatiescore van Lantmäteriet is:



De minimale score is 1, de maximale score is 5. De verdere details zijn te vinden in de Annex. In dit geval is de oplossing technisch innovatief, maar is het businessmodel zelf niet innovatief te noemen gezien het dichtbij het ecosysteem, de dienst en het centrale businessmodel blijft.

Het bijzondere hier is dat het bedrijf goed gebruikmaakt van blockchain en daar een positieve impact van krijgt, zonder dat het ambitieus een decentralere rol nastreeft.

I. Implementatierisico

De centrale vraag is hier in hoeverre de impact van de innovatie de complexiteit van de implementatie beïnvloedt. De totale Blockchain Implementatiescore van Lantmäteriet is:

De minimale score is 1, de maximale score is 5. Verdere details zijn te vinden in de Annex. Het probleem dat Landmäteriet oplost heeft een zekere prioriteit gezien de grote financiële en politieke belangen. Verder is de implementatie vrij goed te doen, gezien de bekende partners dichtbij huis en de door de wet gekende processen. De Zweedse overheid heeft hier met andere woorden een goede blockchaincasus gekozen om het laaghangende fruit te plukken.

J. Conclusie

Uit voorgaande zijn de kansen en uitdagingen naar voren gekomen voor het businessmodel, de strategie en de implementatie. Lantmäteriet heeft op bedachtzame wijze een project uitgerold waarmee het een basis creëert om in de toekomst nieuwe diensten als gebouwenverkoop en belastingkoppeling te ondersteunen. De overige partners zullen het project misschien nog een stap verder willen nemen met het versimpelen van hypotheekprocessen en directe betalingen via cryptovaluta.

Lantmäteriet: identiteitsmanagement via de Telia-app

Zoals vermeld in hoofdstuk 12 is Self-Sovereign Identity (SSI) een geschikt identiteitsmanagementsysteem, omdat het een draagbare digitale identiteitsoplossing biedt die op verschillende sectoren kan worden toegepast. Dit verhoogt de controle en privacy, terwijl de identiteit veilig op een vertrouw netwerk wordt bewaard.

De praktische toepassing van SSI en het voorbeeld van de Telia-app, is in hoofdstuk 12 al grotendeels beschreven. Zo wordt binnen de ID-app van Telia een document met een link naar de officiële Zweedse registratie van het burgerservicenummer gebruikt. De keten van berichten die binnen deze app worden gedeeld, is toegankelijk voor alle betrokken partijen binnen het aankoopproces van land en bevat informatie zoals het contract. De originele documenten en de verificaties kunnen worden bewaard door een externe partij, of betrokken partijen.

Digitale handtekeningen zijn binnen eIDAS akkoord. De Zweedse wet lijkt hier ten aanzien van onroerend goed steeds ruimer mee om te gaan. Zo kunnen appartementen al worden verkocht op deze manier. Het legale obstakel van e-signatures dat werd gesignaleerd in 2016 lijkt zichzelf dus grotendeels op te lossen. Het obstakel omtrent GDPR en persoonlijke informatie versus de Zweedse wet van openbaarheid van het onroerendgoedregister is met deze oplossing technisch opgelost.

Als de keten van berichten ertoe leidt dat een contract is afgerond, checkt het Lantmäteriet de informatie en verandert het eigen register. Vervolgens wordt er een hash van de berichten en de verificatie gemaakt en gepubliceerd op de Bitcoin blockchain. Hiermee bewaakt Landmäteriet de integriteit wordt het proces transparant voor het publiek. Digitale persoonlijke informatie kan worden verwijderd als een individu dit wenst en het conform de wet geen publieke informatie behoort te zijn.

16.4 Fabricage

Technische ontwikkelingen zoals bijvoorbeeld blockchain, zijn interessant voor productiebedrijven, omdat hun businessmodellen flink veranderen onder druk van de 4e industriële revolutie. Datadeling binnen de supply chain, productieprocessen, levenscyclus van producten, enzovoorts worden steeds belangrijker. In deze paragraaf gaan we dieper in op de auto-industrie. De casussen die we in de paragraaf onderzoeken zijn BMW en VeChain.

A. Externe ontwikkelingen

Voor autoproductiebedrijven gelden de volgende belangrijke uitdagingen en kansen.

Economisch

Kans: de deeleconomie groeit met relevante succesvolle voorbeelden als Car2Go, SnappCar en Uber.

Sociaal

Uitdaging: een groeiende verwachting van mensen dat zij meer eigenaar worden van hun eigen digitale data.

Technologie

Kans: de 4e industriële revolutie heeft als gevolg dat auto's verbonden worden aan het internet, waarbinnen het belang van data en cybersecurity toeneemt. Ook het belang van Smart Cities en Smart Industries neemt toe. Daarnaast komen de elektrische en autonome auto's op. Blockchain als technologie biedt de kans om data-uitwisseling tussen apparaten veilig te laten plaatsvinden. Hierbinnen kunnen veilige digitale identiteiten worden gewaarborgd.

Environment

Uitdaging: circulariteit en een groene toekomst zijn belangrijke thema's onder jongeren. Het dieselschandaal heeft het imago van autofabrikanten geschaad.[190] Het gebruik van elektrische auto's neemt toe en autofabrikanten voelen de druk om hun processen duurzamer te maken.

[190] Voor meer informatie over het dieselschandaal, zie onder andere 'Dieselschandaal 2.0: Volkswagen installeerde illegale motorupdatse' (Wilman, 2019).

B. Bedrijfsproces, karakteristieken en doel BMW en digitale identiteit

Het voorbeeld dat hier wordt beschreven is het genereren van een digitale identiteit van de gebruiker en de auto. BMW is een Duitse auto- en motorfabrikant die internationaal produceert en verkoopt. 50% van de aandelen zijn publiek genoteerd, de andere helft is in handen van de Quandt familie.

Autofabrikanten beseffen dat het creëren van een digitale identiteit voor auto en automobilist een belangrijke voorwaarde is om de verschillende technologieën van de 4e industriële revolutie te kunnen gebruiken. Dit leidt voor BMW vooralsnog tot drie kansen:

1. Mobiliteit en een gebruiker die een auto koopt of huurt, waar de auto op termijn als autonoom taxibedrijf parkeert, benzine tankt, mensen rondrijdt en dividend en belasting betaalt.
2. Inzicht in de supply chain, grondstoffen, reserveonderdelen, data van het gebruik van de auto-onderdelen en van afval als de auto aan het einde van de levenscyclus is.
3. Klantgerichte producten produceren zoals het direct verkopen van de auto met financiering of directe schadeverzekeringen met de klant afsluiten of de klant de data geven dit zelf te doen.

Voor al deze kansen staat het kennen van de auto of automobilist centraal, en daarmee het verkrijgen van de data via een digitale identiteit.

Het bedrijfsproces omtrent het organiseren van een digitale identiteit van de gebruiker en de auto heeft de volgende belangrijke elementen:

1. Het betreft productoverdrachten van hoge waarde.
2. Het betreft technisch lastig te doorgronden producten. In dit geval wordt voor aankoop van een tweedehands auto vaak vertrouwd op tussenpartijen. Hierbij blijkt in Duitsland bij 33% van de auto's de kilometerstand te zijn teruggedraaid (ADAC, z.d.).
3. Partijen zijn professioneel georganiseerd en kennen elkaar.
4. De trend is naar een auto als app, waarmee de autofabrikant een directe individuele relatie met de automobilist krijgt. Vooralsnog richt BMW zich meer op een ID voor de auto.
5. Het verkrijgen van data van de auto en automobilist biedt kansen voor de gebruiker en de autofabrikant. Producten en diensten kunnen meer gepersonaliseerd worden. Als de data transaparanter wordt, kun je ook fraude voorkomen. Kopers van tweedehandse auto's weten momenteel bijvoorbeeld vaak niet hoe de kilometerstand tot stand komt en of deze ooit handmatig is aangepast.

C. Business ecosysteemactoren

De belangrijkste actoren binnen het BMW business ecosysteem zijn:

Core business	De afnemer die door data over rijgebruik een steeds langere en directere band heeft. Daarnaast de toeleveranciers in de keten zelf.
Verlengde onderneming	ICT-bedrijven en andere leveranciers van technische innovaties zoals IoT- en DLT-bedrijven zoals IOTA of blockchainbedrijven zoals VeChain Thor.
Business ecosysteem	Competitie, overheid, aandeelhouders.

Tabel 20: Actoren binnen het BMW business ecosysteem.

D. Heat map businessmodelelementen

Van de volgende uitdagende en kansrijke ontwikkeling wordt de impact in het businessmodel besproken.

Aan de ene kant ziet BMW de kansen van het integreren van de verschillende opkomende technologieën met daarin een grote rol voor dataverzameling, -bewaring en -analyse. Hoewel BMW zich voorlopig richt op een unieke ID voor de auto, wordt de ontwikkeling bekeken vanuit de kans om op lange termijn ook een ID voor de gebruiker aan te maken en te gebruiken. Aan de andere kant voelt BMW de druk om een rol te spelen in de behoefte aan het beheersen van eigen gebruikersdata.

Vanuit deze ontwikkelingen is de belangrijkste focus van BMW op de volgende factoren binnen het businessmodel.

	Nieuwe technologieën	Beheer van eigen data
Wie? klantsegmenten	Op termijn nieuwe producten en diensten rondom data zoals verzekeringen en auto verhuur.	Mogelijk klantverlies als het niet meegaat in de veranderingen. Kans op klantwinst als het first mover is.
Wat? waardepropositie	Met blockchain verstevigde digitale identiteit voor automobilist en auto als beginstap tot data-analyse voor supply chain en later klantgerichte producten.	Autofabrikant als verantwoord lid van samenleving. Auto en machine als IoT met constante informatie over gebruik, afval, kwaliteit, enzovoorts.
Wie? kanalen	De auto als internet-app om zowel auto als gebruiker te leren kennen.	
klantrelatie	Via 'auto als app' blijvende directe relatie met gebruiker in plaats van via bijvoorbeeld tussenhandel of autofinanciers.	Via 'auto als app' rijgedrag beïnvloeden ten gunste van milieu.
Wat? opbrengsten	Hogere kwaliteit toeleveranties, nieuwe diensten als verzekeringen, verhuur, financiering autokoop, enzovoorts.	Meer openheid en transparantie over herkomst en gebruik van producten. Nieuwe diensten erop instellen om circulariteit te verbeteren.
Hoe? kernactiviteiten	Goederenbeweging binnen keten.	Datacreatie door eigen producten binnen ecosysteem.
mensen en middelen	Kennis en inzet op innovatieplatformen zoals BMW Startup garage.	
sleutelpartners	Door integratie van technologie krijgt de autofabrikant een directe band met de autogebruiker en de auto. De data kunnen worden uitgewisseld met elke relevante partner inclusief spelers als dataverkoopbureaus, auto-investeringsmaatschappijen en verzekeraars.	Nauwe banden met toeleveranciers, klanten, not-for-profitorganisaties. Gebruik de eindklant om feedback, 'gratis advies' en verbeter het eigen imago.
Wat? kosten	Grote investeringen binnen samenwerkingsverbanden in nieuwe technologie. Minder werkkapitaal in supply chain, lagere inkoopkosten, minder afval, lagere onderhoudskosten machines en systemen, enzovoorts.	Verklein risico's van duurdere grondstoffen, productieprocessen en strengere wetgeving op carbon footprint en uitstoot.

Tabel 21: BMW ingevuld businessmodel.

BMW ziet in het verzorgen van een Vehicle Identity (VID) een noodzakelijke stap om een veilig en transparant systeem te ontwikkelen, waarmee je data kan delen en analyseren.

In lijn hiermee heeft het meerdere stappen genomen, zoals toetreding tot het Mobility Open Blockchain Initiative (MOBI), een blockchainconsortium met 100+ partijen. MOBI heeft de VID bovenaan haar agenda gezet om standaarden te bouwen voor bijvoorbeeld communicatie tussen auto's onderling en met verkeersleiders. Dit soort samenwerkingsverbanden zijn in deze bedrijfstak onder druk van innovatie noodzakelijk. Ook zijn er verschillende voorbeelden waarin autofabrikanten samen nieuwe technologieën ontwikkelen.

Afbeelding 137: Mobiliteitsecosysteem en use cases (MOBI, 2019).

BMW experimenteert haar Startup garage in samenwerking met blockchain startups. Hier kwam een nieuwe samenwerking met VeChainThor uit voort, die in 2019 weer resulteerde in

tests met de app VerifyCar. Deze app logt per auto statische informatie zoals type en productiedatum, en dynamische informatie zoals het aantal gereden kilometers op de blockchain. De VerifyCar app kan worden gezien als een eerste blockchainstap richting een VID.

BMW neemt dus kleine stappen richting een disruptieve innovatie op bestaande businessmodellen van zichzelf en deelnemers in haar ecosysteem. Binnen deze innovatie heeft decentralisatie van data een belangrijke plaats ingenomen.[191]

E. Detail van de oplossing

In het volgende wordt de VerifyCar verder uitgewerkt. VerifyCar is één van de apps binnen BMW-mobiliteitsservices. Andere zijn DriveNow voor korte termijn autohuur en ChargeNow voor oplaadservices.

VerifyCar voegt blockchain toe aan de ontwikkeling van een VID voor de auto. Op termijn kunnen ook een VID voor auto-onderdelen, productiemachines, enzovoorts worden aangemaakt. De VerifyCar app biedt BMW op korte termijn vooral de kans om de supply chain efficiënter in te richten. In de toekomst is er misschien ook ruimte om de digitale identiteit van de gebruikers te koppelen aan de auto. De kansen die dit brengt voor mobiliteit en klantgerichte producten bieden grotere, langere termijn, uitdagingen.

[191] Oplossingen die nog radicalere innovaties nastreven binnen dit domein zijn niet aanwezig. De productie van technisch gecompliceerde producten als auto's is vooralsnog voorbehouden aan centrale partijen als BMW. Tevens is VeChain een publieke blockchain. Een beschrijving van een extra publiek decentraal initiatief, zoals gedaan in vorige paragrafen, heeft daarmee geen toegevoegde waarde en wordt hier achterwege gelaten.

	 
Dienst	Autofabricatie en verkoop.
Governance	Centrale private organisatie die een publiekelijk open blockchain, VeChain Thor, gebruikt. VeChain Thor is een DAO met een centraal bestuursorgaan en een levendige gemeenschap van tokenhouders die ieder verschillende rollen vervullen.
Technisch oplossing	Samenwerking eigen informatiesystemen op auto en publieke blockchainoplossing.
open source	ja
consensus mechanisme	Proof-of-Authority (VeChain Thor).
smart contracts	Ja, mede om gegevens op de blockchain vast te leggen.
dApps	Ja, VerifyCar.
SSI of digitale identiteit	Unieke digitale ID op blockchain. Iedere relevante partij vult blockchain aan. Ook worden periodiek data via in de auto gebouwde SIM-kaarten en Machine-to-Machinecommunicatie naar de blockchain verstuurd.
blockchain of alternatieve DLT	blockchain
onveranderbare data	ja
transparante data	ja
Tokens / beloningen	
Validator beloning	ja
Betalings/native token	Ja, VeChain Token VET. Daarnaast is het VeThor VTHO-token nodig om transactiekosten te betalen.
Digitaal eigendom token	nee
Fractionalisering	nee

Tabel 22: Oplossing van BMW.

VeChain Thor gebruikt een VerifyCar app om hashes van de data op een publiek permissioned blockchain vast te leggen en te verifiëren. De hash wordt dus geverifieerd, waarmee je weet dat er data zijn aangevuld. De achterliggende data van de hash worden opgeslagen op een private server, wat een beveiligingsrisico vormt als Single Point of Failure (SPOF). Met de hash kun je bevestigd krijgen dat de data op de server kloppen.

BMW maakt hiermee de keuze dat data niet meer kunnen worden aangepast en dat ze geen controle hebben op de governance of op de code van waar ze de data loggen. De BMW data

staan op de blockchain en kunnen door de eigenaar van die data beschikbaar worden gesteld aan bijvoorbeeld verzekeraars.

Als BMW de app momenteel voornamelijk voor de supply chain in wil zetten, lijkt deze opzet voldoende. Het supply chain ecosysteem zal zodoende opgeschaald kunnen worden om naast machinebouwers, onderdelen leveranciers en banken, ook douaniers, grondstofleveranciers en overheden toe te voegen.

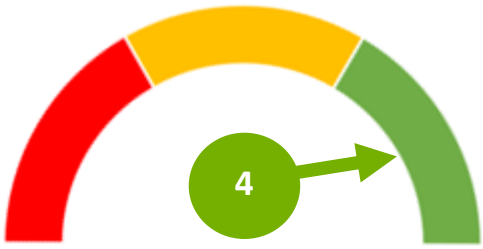
In ecosystemen voor mobiliteit en klantgerichte producten wordt het ecosysteem dynamischer door toevoeging van stedenbouwers, gemeenteraden, kleinere verhuurbedrijven of nieuwe wettelijke toezichthouders door financiële diensten of producten.

BMW deelt al relaties met blockchainconsortia zoals MOBI, Corda R3 en TrustedIoTAlliance. Ook heeft BMW directe relaties met blockchainbedrijven als IOTA en Hyperledger en heeft daarnaast nu misschien ook te maken met tokenhouders, ontwikkelaars en het bestuur van de DAO VeChain Thor.

BMW kent een flinke uitdaging om deze complexe en snelgroeiende ecosystemen te beheersen. Daarnaast heeft BMW de moeilijke opgaaf om de veiligheid en het volledige en verantwoorde gebruik van data uit vele bronnen te verzorgen en zelfs te garanderen.

F. Blockchain Gereedheidsscore

De centrale vraag is hier in hoeverre de businesscase voldoet om blockchain als oplossing te verkiezen. Deze vraag wordt beantwoord met de Blockchain Gereedheidsscore waarvan de details in de Annex zijn te vinden. De minimale score is 1, de maximale score is 5.



Een hoge score van 4 vloeit voort uit de nood van BMW en zijn ecosysteem om de kansen van innovatieve technologieën te grijpen. Blockchain biedt op het gebied van supply chain en datacreatie zeker goede kansen. De blockchainoplossing van BMW levert vrij duidelijke

efficiëntievoordelen. Op termijn moet ook de blockchaingereedheid voor mobiliteit en nieuwe klantengerichte producten verder worden aangescherpt, zoals het nu doet met MOBI, VeChain Thor en IOTA.

G. Verwachte impact blockchain

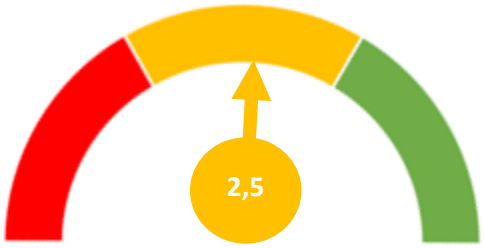
Op basis van de voorgaande modellen kan een inschatting worden gegeven van de impact die kan worden verwacht als blockchain wordt ingevoerd voor supply chain. Met een eerste project kan een basis worden gelegd om op langere termijn blockchainelementen als cryptovaluta en digitale identiteit van de gebruiker in te voeren. Dit kan op zijn beurt weer leiden tot gebruikers die tezamen investeringen doen in een DAO-auto, gebruikers die aanbiedingen voor een huurauto inclusief een verzekering krijgen, gebruikers die hun eigen informatie kunnen verkopen, enzovoorts.

	 
Omzetvermeerdering	Nieuwe producten en diensten rondom data zoals verzekeringen en autoverhuur.
Operationele efficiëntie	Supply Chain leidt tot lagere administratiekosten, hogere kwaliteit leveranties en daardoor lagere kosten. Lagere transactiekosten en overhead fees.
Werkkapitaal	Snellere supply chain leidt tot lager benodigd werkkapitaal.
Datakwaliteit	Verificatie van juiste data, weigering onjuiste data, zekerheid van volledige data.
Risicovermindering	Voorkomen kilometerfraude. Voorkomen namaak auto-onderdelen.
Data-integriteit	Transparantie in waardeketen en bezittingen. Audit trail naar klant, auditor en wetgever. Geen wederzijdse afstemming tussen leveranciers nodig.
Data beschikbaarheid	Opheffen informatie-asymmetrie, inzicht in volledige keten t.o.v. eerder systeem, waaronder actuele informatie over status en locatie product voor alle partijen. Documenten zijn leesbaar voor mens en machine.
Identiteitsmanagement	Eerste stap naar Vehicle ID (VID)
Governance	Open source software, samenwerking met DAO met redelijk transparant bestuur.
Netwerk effect	Grote opschaling van ecosysteem, toegang tot VeChain Thor-tokenhouders via publieke blockchain. Dit leidt tot meer data die vallen te combineren en te analyseren, wat weer tot omzetvermeerdering leidt.
Gebruiksvriendelijkheid	VerifyCar als app om gebruiker inzicht te geven in autodetails op de blockchain.
Veiligheid	dApp op open source publiek netwerk. Auto die veilig kan communiceren op netwerk, gewapend tegen cyberaanvallen. Op termijn veilige transacties gelogd op blockchain.
Experimenteren met technologie	Verkregen kennis wordt gebruikt voor opschaling van verschillende ecosystemen voor supply chain, mobiliteit en klantspecifieke producten.

Tabel 23: Verwachte impact van blockchain op BMW.

H. Innovatiekracht

De centrale vraag in deze paragraaf is te beoordelen in hoeverre dit een incrementele versus radicale innovatie betreft. De Blockchain Innovatiescore van BMW´s VerifyCar app is 2,5. De minimale score is 1, de maximale score is 5. Meer details zijn te vinden in de Annex.

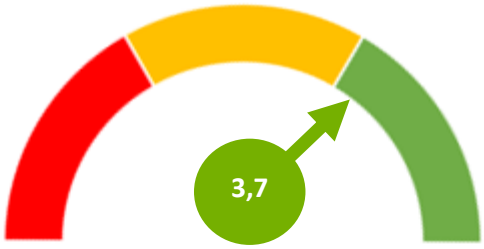


De VerifyCar app is redelijk innovatief als eerste stap om blockchain in te voeren inclusief VID. De volgende stap om een supply chain ecosysteem rondom blockchain te maken, is nog innovatiever. Op langere termijn kan BMW de gebruikers-ID op blockchain zetten en nieuwe businessmodellen ontwikkelen omtrent mobiliteit en klantgerichte producten.

Het bijzondere hier is dat BMW goed gebruikmaakt van blockchain en daar een grote positieve impact geniet, zonder dat het ambitieus een decentralere rol nastreeft.

I. Implementatierisico

De centrale vraag is hier in hoeverre de impact van de innovatie de complexiteit van de implementatie beïnvloedt. De totale Blockchain Implementatiescore van BMW is 3,7.



De minimale score is 1, de maximale score is 5. Meer details zijn te vinden in de Annex.

Het probleem dat BMW probeert op te lossen heeft een grote prioriteit, gezien de belangen voor de gehele industrie om een nieuwe reeks innovaties op elkaar af te stemmen. Het ecosysteem van de auto-industrie zelf is al goed op elkaar afgestemd.

J. Conclusie

BMW neemt met de VerifyCar app een eerste stap met blockchain binnen een grotere strategie, waar op lange termijn voor een decentrale data-infrastructuur een grote rol is weggelegd. Denk hierbij aan het zelf beheren van data die je creëert zoals je rijgedrag dat wordt bijgehouden.[192] BMW kan ook een directe band ontwikkelen met individuele autogebruikers via blockchain, waarmee de weg openstaat voor onderlinge waarde-uitwisseling, zoals verzekeringen en fractioneel investeren in autonome auto's.

BMW's blockchainstrategie geeft vooral een goed beeld op de nood tot samenwerking binnen een ecosysteem.

16.5 Voorspellingsmarkt Augur

Hier wordt een voorbeeld besproken van een dienst die bestaande businessmodellen volledig kan ontwrichten dankzij de ontwikkeling van blockchaintechnologie.

Het betreft het Decentralized Business Model Canvas van de publieke blockchain Augur. Omdat het een disruptieve innovatie betreft die wordt bekeken vanuit de kant van een blockchain startup, wordt afgeweken van de indeling die in vorige paragrafen is gebruikt:

A. Inleiding voorspellingsmarkt.
B. Decentralized Business Model Canvas.
C. Controverse Augur.
D. Conclusie.

A. Inleiding voorspellingsmarkt

Vanuit verschillende organisaties en individuen is er behoefte aan het bevragen van een massa van mensen over hun voorspelling van een toekomstige gebeurtenis. De achterliggende gedachte is dat van hoe meer individuen je voorspellingen verzamelt, hoe groter de kans is dat deze voorspellingen ook uitkomen. Het geaggregeerde antwoord van de menigte wordt ook wel ***wisdom of the crowd*** genoemd. De economische theorie hierachter gaat onder andere terug naar de in deel II beschreven theorieën van Friedrich Hayek en Ludwig von Mises.[193]

[192] Het is onduidelijk in hoeverre welke partij hier recht heeft op de informatie.

[193] Deze economische theorieën zijn onder andere terug te vinden in 'The Use of Knowledge in Society' (1945) van Friedrich Hayek en 'Economic Calculation in the Socialist Commonwealth' (1920) van Ludwig von Mises.

Een voorbeeld van een voorspellingsmarkt is een inschatting van een verkiezingsuitslag of de kans dat een te introduceren product een bepaalde hoeveelheid verkopen haalt. Dit verschilt van een opiniepeiling, omdat er een inschatting van een resultaat wordt gevraagd en geen inhoudelijke mening. Je kunt deze inschatting kracht bijzetten door mensen te vragen geld in te zetten en dit afhankelijk van het uiteindelijke resultaat uit te keren of in te houden. Zo kun je bijvoorbeeld €1 inzetten op de kans dat het morgen daadwerkelijk gaat regenen om 12.00 uur en verlies je dit geld als dit achteraf niet zo blijkt te zijn. Dit geeft ook de mogelijkheid om jezelf financieel in te dekken tegen een ongewenst resultaat door er geld op in te zetten.

In het verleden zijn er zijn verscheidene organisaties gesloten die voorspellingsmarkten aanboden. Dit had onder andere als reden dat deze bedrijven, bijvoorbeeld InTrade, volgens lokale wetten werden gezien als commodity traders of gokbedrijven en niet de juiste vergunningen bezaten. Momenteel zijn er twee bedrijven die beide door de Amerikaanse Commodity Futures Trading Commission (CFTC[194]) worden toegestaan echt geld in te zetten op een voorspellingsmarktplatform. Dit zijn PredictIt en Iowa Electronic Markets.[195] PredictIt wordt alleen gebruikt voor politieke markten en noemt zich ook wel de aandelenbeurs voor politiek. Iowa Electronic Markets voegt daar economische markten aan toe. Beide zijn in het leven geroepen voor onderzoek en onderwijsdoeleinden. Daarbovenop schuiven online gokbedrijven met voorspellingselementen zoals Betfair, pollingbedrijven en crowdsourcingbedrijven tegen hetzelfde voorspellingsmarkt businessmodel aan.

De voorspellingsmarkt komt dus niet echt van de grond. Met de komst van blockchain zijn voorspellingsmarkten nieuw leven ingeblazen. Hierbij zijn Gnosis, Stox en Augur bekende voorbeelden van voorspellingsmarkten op de blockchain. Het disruptieve element zit aan de ene kant in het transparante open peer-to-peer platform waar smart contracts binnen blockchain de plek van een tussenpartij overnemen. Aan de andere kant zit het disruptieve element in het negeren van lokale wetten en regels en de mogelijkheid om voorspellingsmarkten globaal via het internet te verspreiden.

Wat volgt is een vergelijking tussen het gecentraliseerde PredictIt en het gedecentraliseerde Augur.[196] Het proces bij PredictIt is als volgt:

[194] Amerikaanse toezichthouder op derivatenhandel.

[195] Deze initiatieven zijn respectievelijk eigendom van de Victoria University of Wellington en de University of Iowa.

[196] Augur heeft in de laatste week van december 2019 44 unieke gebruikers in één week tijd (DappRadar.com, z.d.). PredictIt geeft zelf aan een experimentele site te zijn die niet mainstream is gegaan (PreditIt, 2019).

1. Een gebeurtenis wordt door PredictIt gecreëerd als markt op de website.
2. Gebruikers zetten geld in op de markt met onderliggend een contract.
3. Een gebeurtenis vindt plaats.[197]
4. PredictIt rapporteert het resultaat op de website.[198]
5. De geldbedragen worden door PredictIt over en weer gestuurd.

De uitdaging is dat PredictIt als centrale partij toegang heeft tot het maken van een markt, de contracten, het geld, de rapportage van de resultaten en het administratieve afrondingsproces. De ontwikkeling van blockchaintechnologie biedt de kans om deze tussenpartijen weg te halen door vertrouwen in een set van open source smart contracts te plaatsen. Augur maakt hier gebruik van. Het is sinds 2015 in ontwikkeling geweest en in 2018 is de applicatie uitgerold en wordt het gebruikt.

Om enige schijn van mogelijke inmenging te vermijden, zet Augur tokens in op het Ethereum-netwerk. Augur trekt zich hierdoor terug als tussenpartij uit elke stap van het bedrijfsproces. Dit proces is als volgt:

1. Ieder persoon kan zich pseudoanoniem aanmelden op Augur en zelf een markt creëren over van alles, terwijl PredictIt alleen de politieke markt bedient.
2. Iedere gebruiker kan peer-to-peer een transactie aangaan op basis van Ether (ETH) of de DAI stable coin. De (ver)kooptransactie wordt geregeld op basis van smart contracts.
3. Een gebeurtenis vindt plaats.
4. Houders van het reputation token, REP, verifiëren het resultaat en worden beloond als ze dit correct signaleren naar de blockchain. Als ze het verkeerde resultaat steunen, verliezen ze hun REP-token.
5. De geldbedragen worden automatisch door de smart contracts over en weer gestuurd.

[197] De bron die het resultaat van een gebeurtenis registreert in een decentrale markt wordt ook wel een orakel genoemd. In het voorbeeld van PredictIt is er een gecentraliseerde markt, dus wordt er geen orakel gebruikt.

[198] Dit wordt ook wel als arbitrage aangeduid.

B. Decentralized Business Model Canvas (DBMC)

Hier wordt het Decentralized Business Model Canvas ingevuld voor de kansen die blockchaintechnologie biedt aan een voorspellingsmarkt als Augur. Details van de oplossing zoals technische aspecten en governance zijn geïntegreerd in dit model. In eerdergenoemde BMC-voorbeelden waren ze dit niet.

	
Wie? Klantsegmenten	Een gebruiker hoeft geen tokenhouder te zijn. Tokenhouders zijn wel nodig om als orakel te dienen of markten te maken. Tokenhouders zijn officieel geen investeerders of softwareontwikkelaars. Klanten zijn voornamelijk mensen die zich willen indekken tegen een gebeurtenis of erop willen speculeren.
Wat? Waardepropositie	Het gedecentraliseerd aanbieden van een transparante en goed beveiligde voorspellingsmarkt.
Hoe? Oplossing	dApp van smart contracts gebouwd op de Ethereum blockchain. Augur is een DAO en kent als decentrale oplossing geen centrale wettelijke toezichthouder.
Consensus	Ethereum is een permissionless Proof-of-Work blockchain.[199] Er is geen KYC of AML. Vertrouwen ligt in de gedecentraliseerde natuur van het systeem en er is geen tussenpartij met uitzondering van de Forecast Foundation.
Validatorbeloning	Een REP-tokenhouder zet tokens in om als orakel te dienen. Hiermee ontvangt hij een deel van de transactiefees en stimuleert hij het gebruik van het netwerk, waardoor er meer vraag komt naar de token. Ook ontvangt hij een grotere weging van zijn deel van de totale REP-tokenpool. 100% van de REP-tokens is namelijk al verdeeld en wordt na elke transactie alleen herverdeeld onder de actieve houders. Inactieve houders krijgen dus minder belang. Een rapporteur verliest REP-tokens als hij incorrect resultaten rapporteert.
Wat? Kosten	ICO in 2015 waarbij 80% van de REP-tokens is gedistribueerd aan participanten, 16% aan oprichters en 4% aan de Forecast Foundation.
Wie? Netwerk governance	De Forecast Foundation zette de 4% REP-tokens om in 5 miljoen USD kasgeld, waarmee het sinds 2015 de salarissen van Augur softwareontwikkelaars betaalt. Hun enige bezigheid is het ontwikkelen en onderhouden van het open Augur-protocol. Niemand bezit het Augur-platform, noch REP-tokenhouders noch de Forecast Foundation. Beslissingen over de richting van Augur worden alleen door de Forecast Foundation genomen via technische updates van de software.
Interactiekanalen	Directe communicatie tussen tokenhouders en met de Forecast Foundation over onder andere wekelijkse updates vinden plaats via Github, Discord, Twitter, Facebook, Medium en de Augur.net website. Actueel nieuws wordt niet automatisch door alle kanalen tegelijkertijd gegeven.
Wat? Opbrengsten	Alle verkregen fees worden verdeeld onder het netwerk van REP-houders en marktinitiatoren. Er wordt geen winst gemaakt. De Forecast Foundation ontvangt geen geld van Augur. Als er meer gebruikers komen die fees genereren, ontvangen de REP-houders ook meer inkomsten in de vorm van fees.

Tabel 24: Augur ingevuld businessmodel.

[199] Ten tijde van schrijven is Ethereum nog niet overgegaan op Proof-of-Stake.

Op basis hiervan kunnen de volgende aanvullende opmerkingen worden gemaakt over het Augur-ecosysteem.

Core business	Augur is een DAO in de zin dat REP-tokenhouders ervoor zorgen dat Augur als applicatie in gebruik blijft. Tokenhouders zijn echter geen eigenaren. Het aantal gebruikers van Augur is bescheiden gezien de geroemde potentiële disruptie van de markt en de €108 miljoen in marktkapitalisatie.
Verlengde onderneming	Bedrijven die toepassingen bouwen op basis van Augur, zoals Guesser en Blitzpredict, en bedrijven die toepassingen binnen de huidige regelgeving gaan ontwikkelen.
Business ecosysteem	Gnosis, Stox, PredictIt, online gokbedrijven, pollingbedrijven en crowdsourcinginitiatieven.

Tabel 25: Actoren binnen het Augur business ecosysteem.

De gedecentraliseerde blockchainmodellen van bijvoorbeeld Augur en Gnosis hebben nog niet geleid tot een wijdverbreide adoptie van de voorspellingsmarkt. Een volledig decentrale publieke blockchaintoepassing lijkt de meeste kans van slagen te hebben, omdat het een laagdrempelig platform biedt om vele individuen te laten participeren. Daarmee kun je ook huidige regelgevingen proberen te vermijden. Momenteel worden Augur-gebruikers gewaarschuwd dat ze op eigen risico het platform betreden. Het mobiliseren van gebruikers heeft echter tijd nodig.

De voorspellingsmarkt zelf is relatief onbekend. In het ecosysteem liggen er ook kansen bij relevante varianten van polling, crowdsourcing en online gokken. Om deze reikwijdte van het ecosysteem te benutten, moet de publieke blockchain meer gebruikers en toepassingen hebben.

C. Augur controverse

Augur heeft als blockchain startup uit 2015 de nodige controverse gekend, die kenmerkend is voor andere blockchain startups uit dezelfde periode. In Amerika en andere landen is er eerst de vraag of de REP-token een security is. De CFTC oordeelt hierover. Dit is de reden geweest voor Augur om de REP-token achteraf specifiek los te noemen van eigendomsrecht op Augur. De CFTC is binnen Amerika ook verantwoordelijk voor het geven van een vergunning voor voorspellingsmarkten. Daarnaast heeft Augur mede door de plotselinge en hoge waardering van de tijd te kampen met een legale strijd voor compensatie tussen de oorspronkelijke

eigenaren. Dit alles heeft invloed gehad op de legale positie van de Forecast Foundation. Er zijn meerdere Forecast Foundations geweest, waaronder één die nog steeds in Estland is geregistreerd door de oorspronkelijke oprichters (Augur, 2018). Verder waren een Forecast Foundation in Oregon en een Dyffy-holding betrokken bij de originele verkopen van Augur. Geen van deze bedrijven heeft een vergunning van de CFTC. (Leising, 2018) De Forecast Foundation heeft statuten vastgelegd door de oprichters. REP-tokenhouders hebben daar geen invloed op. De bestuurders onder wie ook de originele Augur-oprichters hebben dit wel. Legale risico´s zijn een belangrijke determinant van de toekomst van veel van dit soort startups. In lijn hiermee zijn de gebruikers zelf verantwoordelijk voor het creëren van al dan niet (a)morele illegale markten. Zo is direct nadat Augur in 2018 live ging een dodenlijst van bekende personen gelanceerd als markt (Orcutt, 2018). De Forecast Foundation reageerde hierop door te verwijzen naar een verklaring, waarin staat dat ze geen invloed hebben op hoe het platform inhoudelijk wordt gebruikt (Oberhaus, 2018).

Als laatste heeft ook Augur te kampen met technische mankementen die het moet overwinnen. Binance beweerde in april 2019 bijvoorbeed dat Augur niet voldoende veilig is bij een laag gebruikersaantal (Baker, 2019). Bestaande gebruikers zouden namelijk meerdere accounts aan kunnen maken, die ze tegen een zelfgeplaatste hoogstwaarschijnlijke voorspelling in laten zetten om onwetende voorspellers ook geld in te laten zetten. De voorspelling is zo opgezet dat deze kleine gebreken vertoont die onduidelijk zijn voor de onwetende voorspellers. Door deze gebreken kan het contract niet worden uitgevoerd en wordt de totale pot gelijk verdeeld onder alle participanten. Omdat de hoogstwaarschijnlijke voorspelling een buitenkans lijkt, zetten de onwetende voorspellers in de praktijk meer in dan de andere accounts. Doordat de pot gelijk wordt verdeeld onder alle participanten, verliezen de onwetende voorspellers meer geld dan ze terugkrijgen.

D. Conclusie

Publieke blockchains kunnen disruptief zijn en verschillen onderling stevig van elkaar. Zo keren bedrijven als BitShares en Augur al hun fees uit aan tokenhouders of aan actieve participanten, kun je als tokenhouder bij BitShares de koers van de DAO bepalen en heeft VeChain een centraal managementteam dat commercieel succes nastreeft door samenwerking met grote internationale bedrijven.

Uiteindelijk leveren de projecten hun grote beloften nog niet in, mede door onervarenheid met governance, het gelimiteerd engageren van een gemeenschap, tegendruk van de wet en meer

geloof in technische vooruitgang dan focus op de praktische toepassing van deze techniek. Desalniettemin heeft blockchain veel potentie. Het maakt het mogelijk om de samenleving verder op het decentrale pad te brengen. Ook is het lastig als centraal bedrijf te concurreren met een gemeenschap die onderling geëngageerd samen kan werken, maar geen winst nastreeft. Daar ligt de belofte van de publieke blockchains en DAO's.

16.5 Samenvatting, begrippen en bronnen

Samenvatting

In dit hoofdstuk wordt een stappenplan gegeven waarmee kan worden beoordeeld waar de kansen liggen voor bedrijven die blockchaintoepassingen overwegen. Het stappenplan wordt uitgelegd aan de hand van vier casussen van grote organisaties en DAO's. Zodoende wordt elke casus van een centraal businessmodel afgezet tegen een organisatie die een radicaal innovatief decentraal model nastreeft. Deze casussen worden met de volgende instrumenten beschreven binnen het Saxion Blockchain Model:

A. Externe ontwikkelingen die invloed op het businessmodel hebben in overeenstemming met de PESTEL-methode.
B. Bedrijfsproces inclusief de meest relevante karakteristieken van dit proces en het doel dat de blockchain implementatie zou dienen.
C. Business ecosysteemactoren om een beeld te geven welke partners het bedrijf heeft.
D. Heat map businessmodelelementen waarin de invloed van de externe ontwikkelingen wordt getoond op het businessmodel. Hiermee kunnen meer inzichten worden vergaard over kansen en uitdagingen voor het bedrijf.
E. Details van de oplossing waarin op verschillende vlakken de incrementele oplossing wordt vergeleken met een disruptief model, evenals waar blockchain kansen biedt om binnen het ecosysteem relaties aan te gaan en te verdiepen.
F. Blockchain Gereedheidsscore waarmee wordt bekeken in hoeverre de organisatie gereed is om blockchain in te voeren.
G. Verwachte impact van blockchain. Dit geeft aan wat het verwachte nut is van blockchain en waar uitdagingen liggen in het invoeren ervan.
H. Blockchain Innovatiescore om te duiden in hoeverre het bedrijf een incrementele versus radicale innovatie doormaakt, aan de hand waarvan de kansen op waardecreatie van het businessmodel kunnen worden ingeschat.
I. Blockchain Implementatierisico's waarmee naar risico´s wordt gekeken die specifiek met blockchainprojecten samenhangen.
J. Conclusie.

Een conclusie hieruit is dat succesvolle blockchaintoepassingen behapbare wel omschreven blockchain casussen zijn die als onderdeel van een groter plan worden uitgevoerd.

Opmerkingen die je nu uit kunt leggen

- Een gestructureerde aanpak voor een blockchain toepassing vergt niet meer dan een eenvoudig stappenplan, gebaseerd op gedecentraliseerde datagedreven businessmodellen en een gereedheidsscore van de organisatie.
- Afhankelijk van het type uitdaging waarmee een bedrijf wordt geconfronteerd, heeft een blockchain op alle vlakken van het businessmodel impact.
- De huidige succesvolle blockchaintoepassingen waren voorzichtige eerste stappen in een incrementeel veranderingsproces.
- dApps op de publieke blockchains kunnen een disruptieve verandering teweegbrengen, maar worden nog gehinderd door onder andere onervarenheid van de teamleden, huidige regelgeving en praktische toepassing van de techniek.

Verklarende begrippenlijst

Blockchain Gereedheidsscore: In hoeverre de organisatie gereed is om blockchain in te voeren.

Blockchain Implementatierisico: Risico met betrekking tot het implementeren van blockchainprojecten.

Blockchain Implementatiescore: Geeft aan in hoeverre de impact van de innovatie de complexiteit van de implementatie gaat beïnvloeden.

Blockchain Innovatiescore: Duidt aan in hoeverre het bedrijf een incrementele versus radicale innovatie doormaakt. Aan de hand hiervan kunnen de kansen op waardecreatie van het businessmodel worden ingeschat.

Commodity Futures Trading Commission (CFTC): Amerikaanse toezichthouder op derivatenhandel.

Federal Reserve: Amerikaanse centrale bank.

Federal Trade Commission (FTC): Amerikaans overheidsorgaan dat klanten beschermt tegen onder andere frauduleuse en misleidende bedrijfshandelingen.

Securities and Exchange Commission (SEC): Onafhankelijk Amerikaans overheidsorgaan dat zich richt op de bescherming van investeerders en toezicht houdt op het functioneren van de Amerikaanse financiële markten.

Wisdom of the crowd: Collectieve mening van de groep. Dit wordt afgezet tegen de individuele mening van één persoon of expert.

Bronnen

Augur. (z.d.). Overview. Geraadpleegd op 23 december 2019, van Augur.net website: https://docs.augur.net/#overview

Augur. (2018, 9 juli). Forecast Foundation OU Privacy Policy. Geraadpleegd op 23 december 2019, van Augur.net website: https://www.augur.net/privacy-policy/

Baker, P. (2019, 1 april). Binance Research: Design Flaws Make Augur Vulnerable To Attack. Geraadpleegd op 23 december 2019, van Crypto Briefing website: https://cryptobriefing.com/binance-augur-flaw/

Bakkt. (z.d.) Bakkt. Geraadpleegd op 23 december 2019, van Bakkt.com website: https://www.bakkt.com/

BitShares. (z.d.) BitShares. Geraadpleegd op 9 september 2019, van Bitshares.org website: https://bitshares.org/

Carfax. (2019). How to detect mileage rollback? Geraadpleegd op 23 december 2019, van Carfax.eu website: https://www.carfax.eu/article/mileage-rollback

ChromaWay. (z.d.). ChromaWay. Geraadpleegd op 23 december 2019, van ChromaWay website: htps://chromaway.com/landregistry/.

Eder, G. (2019). *Digital Transformation: Blockchain and Land Titles.* Geraadpleegd van http://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf

Garrick, D., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study.* Geraadpleegd van https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

Hayek, F.A. (1945). The Use of Knowledge in Society. Geraadpleegd van https://www.econlib.org/library/Essays/hykKnw.html

Kaoris Future. (2017) *The Land Registry in the blockchain – testbed*. Geraadpleegd van https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Land LayBy. (2019). *Land Layby Listing (LLL) Platform* [White Paper]. Edition 3. Geraadpleegd van https://hrbe.io/images/whitepaper.pdf

Land LayBy. (z.d.). Land Layby Holding Limited. Geraadpleegd op 23 december 2019, van landlayby.com website: http://kenya.landlayby.com/

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *The Land Registry in the blockchain.* Geraadpleegd van http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Leising, M. (2018, 26 juli). As Crypto Meets Prediction Markets, Regulators Take Notice. Geraadpleegd op 23 december 2019, van Bloomberg.com website: https://www.bloomberg.com/news/articles/2018-07-26/as-crypto-meets-prediction-markets-u-s-regulators-take-notice

McKie, S. (2017, 30 september). Investing in Tokens and Decentralized Business Models. Geraadpleegd op 23 december 2019, van Medium website: https://medium.com/blockchannel/investing-in-tokens-and-decentralized-business-models-e7629efa5d9b

von Mises, L. (1920). *Economic Calculation in the Socialist Commonwealth*. Auburn, Ala., Ludwig von Mises Institute.

MOBI. (2019). *DLT-based Vehicle Identity Business Review.* Geraadpleegd van https://dlt.mobi/wp-content/uploads/2019/07/DLT-based-VID-Business-Review.pdf

MOBI. (2019). *Vehicle Identity Standard*. Geraadpleegd van https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Mulligan, C., Zhu Scott, J., Warren, S., & Rangaswami, J. P. (2018). *Blockchain Beyond the Hype A Practical Framework for Business Leaders.* Geraadpleegd van http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf

Mwanza, K. (2018, 16 februari). *African startups bet on blockchain to tackle land fraud.* Geraadpleegd op 23 december 2019, van Reuters website: https://www.reuters.com/article/us-africa-landrights-blockchain/african-startups-bet-on-blockchain-to-tackle-land-fraud-idUSKCN1G00YK

Nimfuehr, M. (2017, 3 december). Blockchain application land register: Georgia and Sweden leading. Geraadpleegd op 23 december 2019, van Medium website: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c

Oberhaus, D. (2018, 25 juli). Assassination Markets for Jeff Bezos, Betty White, and Donald Trump Are On the Blockchain. Geraadpleegd op 23 december 2019, van Vice website: https://www.vice.com/en_us/article/gy35mx/ethereum-assassination-market-augur?utm_source=mbtwitter

Orcutt, M. (2018, 2 augustus). *This new blockchain-based betting platform could cause Napster-size legal headaches*. Geraadpleegd op 23 december 2019, van MIT Technology Review website: https://www.technologyreview.com/s/611757/this-new-ethereum-based-assassination-market-platform-could-cause-napster-size-legal/

Peterson, J., Krug, J., Zoltu, M., Williams, A., & Alexander, S. (2019). *Augur: a Decentralized Oracle and Prediction Market Platform (v2.0).* Geraadpleegd van https://www.augur.net/whitepaper.pdf

PredictIt. (2019). A Predictable Newsletter - 11.1.19*.* Geraadpleegd op 23 december 2019, van PredictIt Political Analysis website: https://analysis.predictit.org/post/188747880043/a-predictable-newsletter-11119#mobile

Annex

Land LayBy: verdere uitleg van de oplossing

Land LayBy ontwikkelt een dApp die via de mobiele telefoon informatie verzamelt die vervolgens via smart contracts wordt geregistreerd op een Land LayBy Listing (LLL) op het Ethereum-platform. Hiervoor ontvangt het technische ondersteuning van ICT-bedrijf Winjit. De Harambee token geeft toegang tot het register. Tokens kunnen worden verdiend door correcte veranderingen te maken in de LLL en tokens worden weggehaald als verkeerde veranderingen worden gemaakt.

Land LayBy verricht verder zelf due diligence op de details, onder meer door ter plekke te kijken en een kopie van het landregister van Ghana te gebruiken. Hiervoor voeren zij zelf ook gegevens in op Ethereum. Land wordt pas geregistreerd op de blockchain als de geschiedenis volledig inzichtelijk gecontroleerd kan worden en alle officiële documenten in orde zijn. Vervolgens deelt Land Layby ook een Land LayBy Listed-certificaat uit, dat het vertrouwen in de informatie naar het publiek toe moet vergroten.

Door de aan- en verkopen van het land ook vast te leggen op de blockchain kan het als een schaduwboekhouding dienen voor de gebruikers.

Blockchain Gereedheidsscore Lantmäteriet

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Digitale innovatie is onderdeel van de strategie.				4	
Verschillende partijen delen gegevens.					5
Deze gegevens en hun transacties betreffen geldwaarde.					5
De data zijn vertrouwelijk.			3		
Verschillende partijen bewerken gegevens.					5
Gegevens moeten worden geverifieerd.					5
Er is een duidelijke Return on Investment te berekenen, en deze voldoet in dit geval.					5
Verificatie is complex, kosten- en of tijdverhogend.					5
De oplossing om voor blockchain te kiezen, is de meest simpele kans om het probleem te overwinnen.				4	
De oplossing beïnvloedt de bestaande organisatiestructuur.	1				
De oplossing beïnvloedt de bestaande workflow.			3		
De oplossing beïnvloedt het bestaande ecosysteem, zo is er geen tussenpartij met een centrale positie.		2			
De technische oplossing ligt dichtbij bestaande systemen en/of het bestaande systeem is van belang.				4	
De oplossing is data-intensief, maar schaalbaar: 1k, 10k, 100k, 1 mln. of > 10 mln. transacties per uur.			3		
Blockchain Gereedheidsscore Lantmäteriet	**54 / 14 = 3,9**				

Tabel 26: Landmäteriet Blockchain Gereedheidsscore.

Blockchain Innovatiescore Lantmäteriet

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Mate van decentralisatie.		2			
Aanboren nieuwe markt of al bestaande markt.		2			
Gebruik van nieuwe processen.			3		
Gebruik van nieuwe stakeholders binnen een nieuw ecosysteem.			3		
Omzeilen van tussenpartij.	1				
Technische innovatie: maakt gebruik van SSI, tokenization, smart contracts, nieuw consensusmechanisme, nieuwe technische workflow.				4	
Blockchain Innovatiescore Lantmäteriet	**15 / 6 = 2,5**				

Tabel 27: Lantmäteriet Blockchain Innovatiescore.

Blockchain Implementatiescore Lantmäteriet

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Ecosysteem is eenvoudig in de zin van dat er geen tussenpartij is, samenwerking geografisch dichtbij huis ligt, wil om samen te werken bij actoren, gelimiteerd aantal actoren te coördineren.				4	
Blockchain Gereedheidsscore.				4	
Blockchain Innovatiescore.			3		
Er ligt intern nadruk op digitale innovatie: data en digitale innovatie staan centraal in strategie, organisatiestructuur heeft bewezen te kunnen innoveren, informatiesystemen en -processen op orde, technische kennis aanwezig.				4	
Het initiatief is legaal en in overeenstemming met geldende standaarden/richtlijnen.					5
Het probleem heeft een zekere prioriteit, maar is geen kritisch complex proces dat (grote) organisatorische veranderingen vereist.				4	
Blockchain Implementatiescore Lantmäteriet	**24 / 6 = 4**				

Tabel 28: Lantmäteriet Blockchain Implementatiescore.

Blockchain Gereedheidsscore BMW

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Digitale innovatie is onderdeel van de strategie.				4	
Verschillende partijen delen gegevens.					5
Deze gegevens en hun transacties betreffen geldwaarde.			3		
De data zijn vertrouwelijk.				4	
Verschillende partijen bewerken gegevens.				4	
Gegevens moeten worden geverifieerd.					5
Er is een duidelijke Return on Investment te berekenen, en deze voldoet in dit geval.				4	
Verificatie is complex, kosten- en of tijdverhogend.					5
De oplossing om voor blockchain te kiezen, is de meest simpele kans om het probleem te overwinnen.				4	
De oplossing beïnvloedt de bestaande organisatiestructuur.			3		
De oplossing beïnvloedt de bestaande workflow.				4	
De oplossing beïnvloedt het bestaande ecosysteem, zo is er geen tussenpartij met een centrale positie.			3		
De technische oplossing ligt dichtbij bestaande systemen en/of het bestaande systeem is van belang.				4	
De oplossing is data-intensief maar schaalbaar: 1k, 10k, 100k, 1 mln. of > 10 mln. transacties per uur.				4	
Blockchain Gereedheidsscore BMW	**56 / 14 = 4**				

Tabel 29: BMW Blockchain Gereedheidsscore.

Blockchain Innovatiescore BMW

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Mate van decentralisatie.		2			
Aanboren nieuwe markt of al bestaande markt.			3		
Gebruik van nieuwe processen.			3		
Gebruik van nieuwe stakeholders binnen een nieuw ecosysteem.			3		
Omzeilen van tussenpartij.	1				
Technische innovatie: maakt gebruik van SSI, tokenization, smart contracts, nieuw consensusmechanisme, nieuwe technische workflow.			3		
Blockchain Innovatiescore BMW	**15 / 6 = 2,5**				

Tabel 30: BMW Blockchain Innovatiescore.

Blockchain Implementatiescore BMW

(1 = totaal niet, 5 = absoluut wel)	**1**	**2**	**3**	**4**	**5**
Ecosysteem is eenvoudig in de zin van dat er geen tussenpartij is, samenwerking geografisch dichtbij huis ligt, wil om samen te werken bij actoren, gelimiteerd aantal actoren te coördineren.		2			
Blockchain Gereedheidsscore.				4	
Blockchain Innovatiescore.			3		
Er ligt intern nadruk op digitale innovatie: data en digitale innovatie staan centraal in strategie, organisatiestructuur heeft bewezen te kunnen innoveren, informatiesystemen en -processen op orde, technische kennis aanwezig.				4	
Het initiatief is legaal en in overeenstemming met geldende standaarden/richtlijnen.				4	
Het probleem heeft een zekere prioriteit maar is geen kritisch complex proces dat (grote) organisationele veranderingen vereist.					5
Blockchain Implementatiescore BMW	**22 / 6 = 3,8**				

Tabel 31: BMW Blockchain Implementatiescore.

17. Criteria en toepassingstypen

"You can replace the term 'distributed ledgers' with 'shared Excel sheets' in about 90 percent of talk about blockchain and finance."

- Tracy Alloway (2019)

17.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Welke criteria relevant zijn om in te schatten in hoeverre blockchain nut heeft voor een bedrijf.
- Hoe de blockchainbouwstenen kunnen worden ingedeeld in soorten blockchaintoepassingen.
- Hoe je de soorten blockchaintoepassingen in kunt zetten om een blockchainapplicatie te bedenken.
- Welke typische vragen er zijn om vast te stellen of je een specifieke blockchain use case hebt.

Inleiding

Uit het vorige hoofdstuk blijkt dat blockchain niet altijd zinvol is. Er dient te worden voldaan aan bepaalde criteria die voornamelijk worden uitgedrukt in de Blockchain Gereedheidsscore en de Blockchain Implementatiescore. In dit hoofdstuk wordt in paragraaf 17.2 een verdieping gegeven op deze Blockchain Gereedheidsscore aan de hand van criteria om blockchain in te voeren. Als daaruit voortvloeit dat er een zinvolle blockchaincasus is, heeft het pas nut te kijken naar de voorwaarden waaronder implementatie plaatsvindt. Change management en implementatiestrategieën voor digitale strategieën zijn vrij generiek en hebben daarom vooralsnog minder nut om in dit boek te behandelen.

De casussen die zijn genoemd in hoofdstuk 16 voldoen grotendeels aan de blockchainimplementatiecriteria. Deze casussen kunnen worden opgesplitst in concretere toepassingstypen. In paragraaf 17.3 categoriseren we de meest voorkomende toepassingstypen en tonen we met voorbeelden aan welke blockchainelementen belangrijk zijn om de toepassingstypen te ontwikkelen. Het hoofdstuk wordt afgesloten met een samenvatting, een lijst van belangrijke begrippen en een bronnenlijst in paragraaf 17.4.

17.2 Criteria om blockchain in te voeren

Hoewel blockchain veelbelovend is, is het momenteel slechts in specifieke gevallen de beste oplossing. Er zijn legio mislukte en gepauzeerde blockchainprojecten. In deze paragraaf geven we aan de hand van 3 uitgewerkte criteria, aanwijzingen hoe je kunt beoordelen in hoeverre een project kans van slagen heeft.

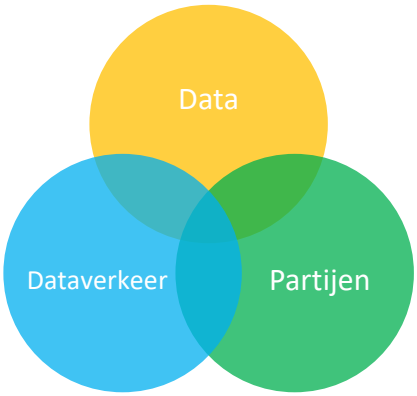
Voordat we langs de criteria gaan, is het aan te bevelen om in lijn met het vorige hoofdstuk het bedrijfsproces vast te leggen. Probeer daarom eerst de volgende vragen te beantwoorden:

1. Welke data zijn er?
2. Welke partij gebruikt, bewaart en bewerkt deze data met welk nut?
3. Hoe worden de data onderling verdeeld?
4. Wie zijn de gebruikers van de data?
5. Welke data zou je niet willen delen of sturen?

Aanwijzingen wanneer een blockchainproject kans van slagen heeft, zijn onder meer te vinden in de definitie van een blockchain alszijnde een “overeengekomen gedistribueerde database waarbij transacties versleuteld zijn in datablokken”.

Er worden dus in het algemeen data gedeeld tussen bepaalde partijen. De specifieke oplossing van blockchain is dat het op een eigen manier fricties opheft, of juist kansen creëert bij het delen van data tussen bepaalde partijen. Deze mogelijkheden zijn in de volgende blokken op te delen:

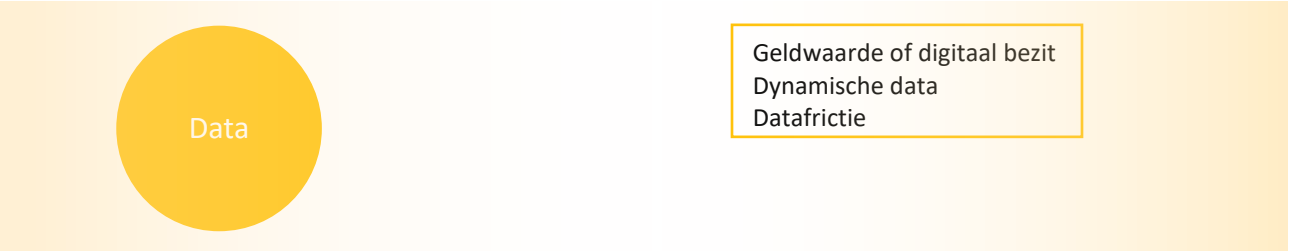
1. Data.
2. Partijen.
3. Dataverkeer.



Afbeelding 138: Kernblokken blockchaincriteria.

In het volgende worden deze criteria verder uitgewerkt aan de hand van aandachtspunten en vragen die je jezelf dient te stellen. Deze criteria zijn opgesteld op basis van Hereijer, Waughray, & Warren (2018) en Castellon, Cozijnsen, & van Goor (2018).

17.2.1 Data



Afbeelding 139: Kernblok data.

a. In hoeverre betreft het data met geldwaarde of digitaal bezit?

Hoe digitaler het product en hoe hoger de geldwaarden, hoe relevanter blockchain is om de waardetransacties vertrouwd tussen partijen onderling te ondersteunen. Andere relevante vragen zijn:

- *In hoeverre is er een datadossier rondom dit product met veranderbare gegevens?*
- *In hoeverre heb je binnen dit dossier de nood tot een digitale identiteit van product, eigen bedrijf, klant, andere stakeholders?*

b. In hoeverre wordt gebruikgemaakt van dynamische data?

Blockchain is gebouwd rond datatransacties. Deze veranderingen in data, zoals sensoren die constant updates doorsturen, worden bij blockchain op een veilige manier opgeslagen en transparant gemaakt om ze tussen partijen te delen. Statische data, zoals persoonsgegevens, kunnen worden opgeslagen op de blockchain, maar alternatieve systemen zijn hier vooralsnog geschikter voor.

c. Waar wordt datafrictie ervaren?

Denk hierbij aan problemen die ontstaan als data:

- *Foutief of incompleet zijn.*
- *Gecorrumpeerd zijn.*
- *Vertrouwelijk of persoonlijk zijn.*
- *Onduidelijk zijn.*
- *Gecensureerd worden.*
- *Ongemerkt zijn aangepast.*
- *Niet beschikbaar zijn, of niet op hetzelfde moment beschikbaar zijn.*

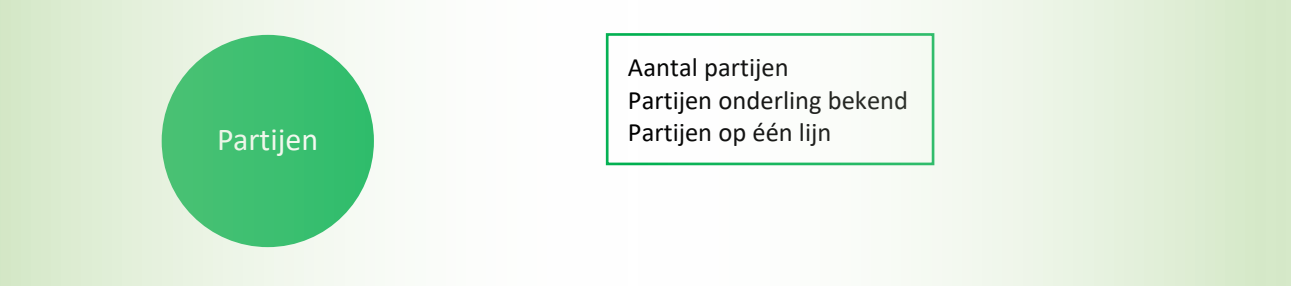
d. Wat levert het op als je deze frictie opheft?

De frictie kun je opheffen door onder andere logs of een complete audit trail te hebben van wat er is veranderd, door data te laten verifiëren door verschillende partijen of door de data en processen te standaardiseren. Hierbinnen is een visie op een verplatting van de organisatie door het decentraal uitvoeren en automatiseren van werk en controles, een belangrijke strategische overweging voor het businessmodel.

e. Waar liggen kansen op het gebruik van nieuwe data?

Welke data liggen er bij partijen die nu niet wordt gedeeld en je zou kunnen gebruiken? Welke potentiële nieuwe gebruikers zou je kunnen vinden voor je eigen data? Vervolgens dien je te kijken hoe bestaande of nieuwe data kunnen worden gecombineerd en geanalyseerd om waarde te creëren binnen het netwerk.

17.2.2 Partijen



Afbeelding 140: Kernblok partijen.

a. Betreft het hier twee of juist meerdere partijen?

Hoe meer partijen samenwerken, hoe waardevoller blockchain is om onderlinge transparantie en vertrouwen te vergroten.

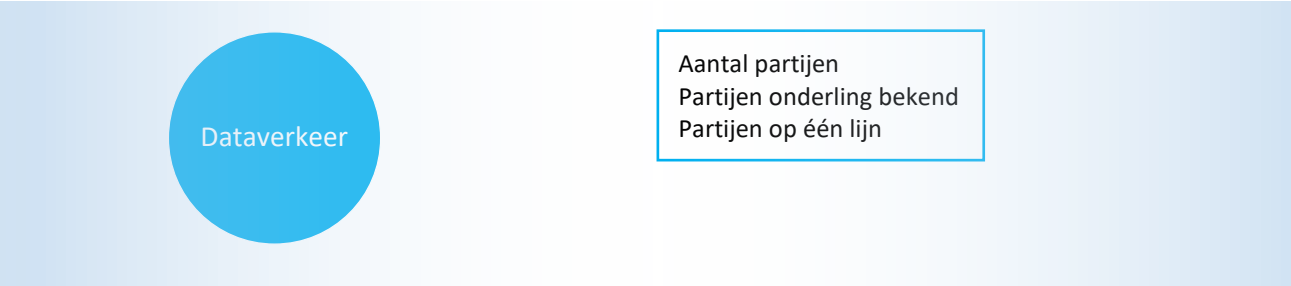
b. Kennen de partijen elkaar?

Bij blockchain ligt het vertrouwen in het systeem zelf en niet zozeer tussen de partijen onderling. Bij Enterprise Blockchain zijn de eerste projecten vooral gericht op bekende partijen om incrementeel het ecosysteem uit te bouwen. In consortia richten bedrijven zich ook duidelijk op samenwerking met concurrenten. Hier kennen de bedrijven elkaar, maar wordt vertrouwen afgedwongen met aanvullende afspraken. Zie hiervoor ook hoofdstuk 18. Hierbij is er nadrukkelijk de kans om de klant te betrekken in het netwerk en deze direct individueel via het blockchainsysteem te kunnen benaderen. In hoeverre kan een netwerkeffect worden gecreëerd?

c. In hoeverre staan de partners op één lijn ten aanzien van het gebruik van blockchain?

Wat hierbij ondersteunt, is als er een dominante partij is die datastandaarden en samenwerking af kan dwingen. Onderzoek de mogelijkheden om elkaars doelen in lijn te brengen. Denk bijvoorbeeld na hoe je samen de loyaliteit van eenzelfde eindklant kunt verhogen, het vertrouwen in de kwaliteit van het product of proces kunt verbeteren, of hoe je jezelf direct kunt presenteren aan de eindgebruiker of hiermee in dialoog kunt treden.

17.2.3 Dataverkeer



Afbeelding 141: Kernblok dataverkeer.

a. Waar wordt frictie ervaren met het dataverkeer?

Zie ook de opmerkingen onder 'datafrictie' bij het kopje Data (17.2.1). Bij dataverkeer ligt de nadruk op suboptimale samenwerking door:

- *Tijdsintensieve projecten zoals de afstemming van gegevens.*
- *Fout- en fraudegevoelige processen.*
- *Processen waarin de ene partij op een ondoorzichtige handeling van een ander partij wacht om verder te kunnen gaan met het proces.*
- *Een tussenpartij die als extra schakel geldt, al dan niet door de wet vastgelegd. De verwachting is dat op langere termijn de overheid onder druk van technologische ontwikkelingen zoals blockchain de rollen van toezichthouders, poortwachters en andere wettelijke tussenpartijen verandert.*

b. Waar liggen kansen binnen het dataverkeer?

In hoeverre is de klant via blockchain direct individueel te benaderen? In hoeverre kan een netwerkeffect worden gecreëerd? Hoe helpt het proces om data anoniem of niet anoniem te delen?

c. Hoe robuust en veilig is het netwerk?

Hierbij is niet alleen de vraag of het netwerk gevoelig is voor cyberaanvallen, maar ook in hoeverre de data op een aparte fysieke plek moeten zitten, of het cryptografisch beschermd is, hoe bedrijfshardware wordt beschermd en wat de minimale data zijn die je af wilt schermen. Robuustheid en veiligheid omvatten ook de rollen en bevoegdheden die verschillende partijen nemen binnen een blockchainsysteem, zoals het actueel houden van gegevens of het onderhouden van de hardware.

d. In hoeverre werkt het netwerk samen met bestaande software?

In hoeverre kan het systeem netwerkdata communiceren naar of zelfs integreren met bestaande CRM en ERP-pakketten? In hoeverre is dit mogelijk met andere publieke of private blockchainsystemen, al dan niet on- of off-chain?

Hieruit vloeien drie hoofdredenen om blockchain in te voeren:

1. Vastleggen van bezit en data.
2. Efficiëntie vergroten.
3. Disintermediatie.

Andere voor de hand liggende redenen zijn toegang tot meer data en een veiliger netwerk.

Vuistregel om een blockchain toe te passen

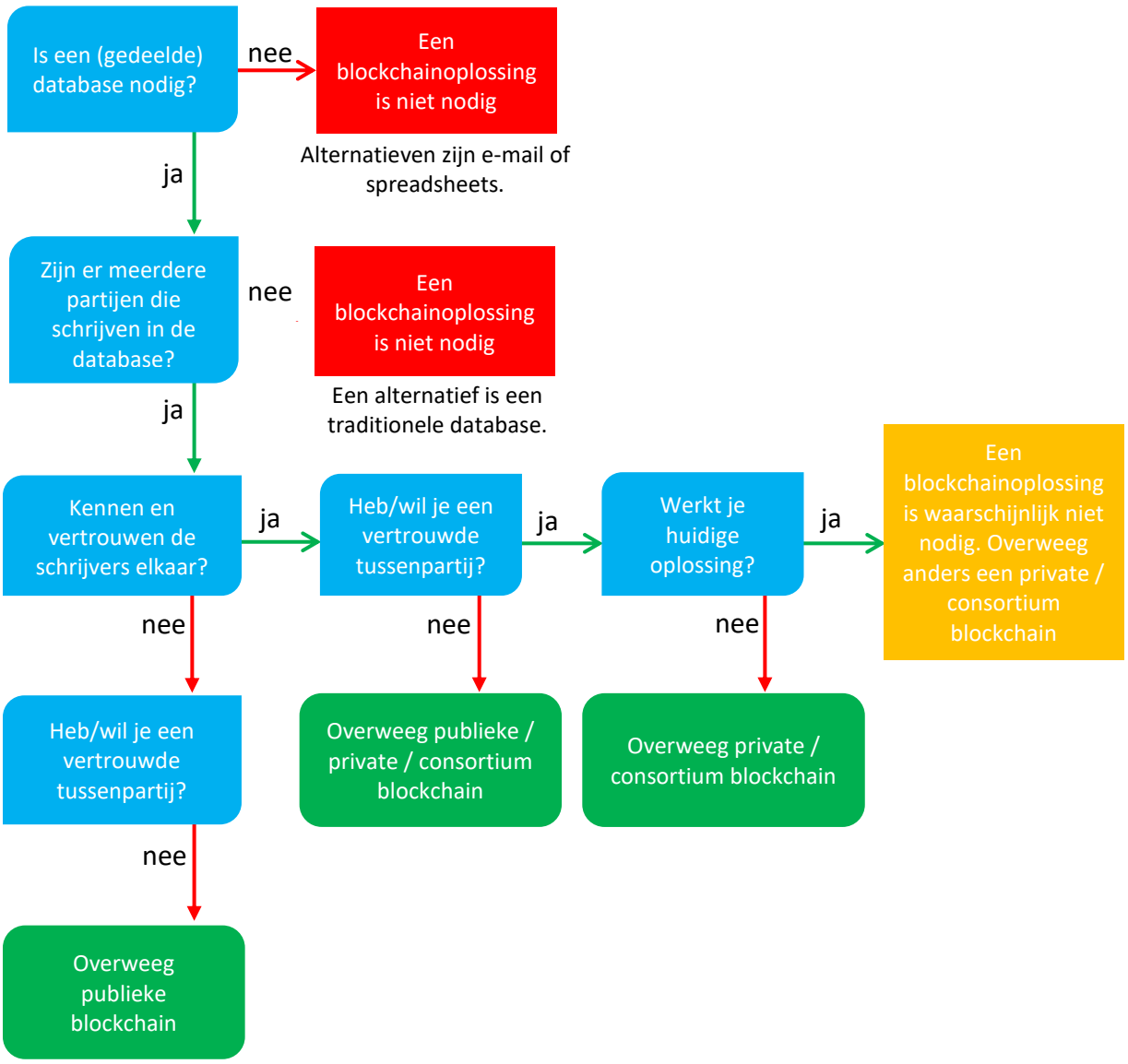
Blockchain heeft nut als er aan de volgende criteria wordt voldaan:

1. Digitale innovatie onderdeel is van de strategie.
2. Verschillende partijen gegevens delen.
3. Deze gegevens en hun transacties geldwaarde betreffen.
4. De data vertrouwelijk zijn.
5. Verschillende partijen gegevens bewerken.
6. Gegevens moeten worden geverifieerd.
7. Er een duidelijke Return on Investment te berekenen is, en deze voldoet in dit geval.
8. Verificatie complex, kosten- en of tijdverhogend is.
9. De oplossing om voor blockchain te kiezen de meest simpele kans is om het probleem te overwinnen.
10. De oplossing de bestaande organisatiestructuur beïnvloedt.
11. De oplossing de bestaande workflow beïnvloedt.
12. De oplossing het bestaande ecosysteem beïnvloedt. Zo is er geen tussenpartij met een centrale positie.
13. De technische oplossing dichtbij bestaande systemen ligt of ermee te integreren valt.
14. De oplossing data-intensief maar schaalbaar is. Denk in verschillen van 1k, 10k, 100k, 1 mln. of > 10 mln. transacties per uur.

Naast het beantwoorden van de eerder genoemde vragen, kun je de volgende vuistregel hanteren.

Wij hebben deze vuistregel ook toegepast om de ***Blockchain Gereedheidsscore*** te maken als een eerste beoordeling in hoeverre een blockchainoplossing de juiste keuze is voor een bedrijf.

Uit de eerdergenoemde criteria en vuistregel valt de volgende eenvoudige beslisboom te maken.



Afbeelding 142: Vereenvoudigde beslisboom of je wel of geen blockchain moet gebruiken.

Hierop volgt de vraag wat voor soort blockchain je wil. Je kunt kiezen uit een publieke, private en consortium blockchain. Daarnaast kan een blockchain ook permissionless of permissioned zijn. Een permissioned blockchain kies je als je de functionaliteit en toegangsrechten wil controleren. Veel bedrijven kiezen ook voor een permissioned blockchain als ze de transacties niet transparant willen laten zien, hoewel je door middel van cryptografische technieken als Zero-Knowledge Proofs ook meer privacy kunt inbedden in permissionless blockchains.[200]

[200] Zie onder andere 'Total cost of ownership for blockchain solutions' van Ernst & Young (2019). Volgens hun onderzoek zullen de transactiekosten van Zero-Knowledge Proofs bij publieke blockchains op korte termijn

Iets anders waar je ook rekening mee moet houden is het onderhoud van de blockchain. Een permissionless blockchain is vaak publiekelijk beschikbaar en open source. Deze blockchains worden door de community onderhouden, terwijl een permissioned blockchain die door jou of in een consortium is opgezet meer onderhoud behoeft. Als updates en nieuwe innovatieve functies automatisch worden toegevoegd aan een permissionless blockchain, hoef je je ook minder bezig te houden met blockchaininnovaties. Je hebt echter minder controle op de richting waar een permissionless blockchain naartoe gaat.

Permissioned blockchains zijn door het geringe aantal nodes die het netwerk onderhouden vaak ook sneller en kunnen meer mutaties per seconde verwerken. Voor sommige bedrijven is een het aantal transacties per seconde die permissionless blockchains kunnen verwerken te laag en is de verwerkingstijd van transacties te lang.

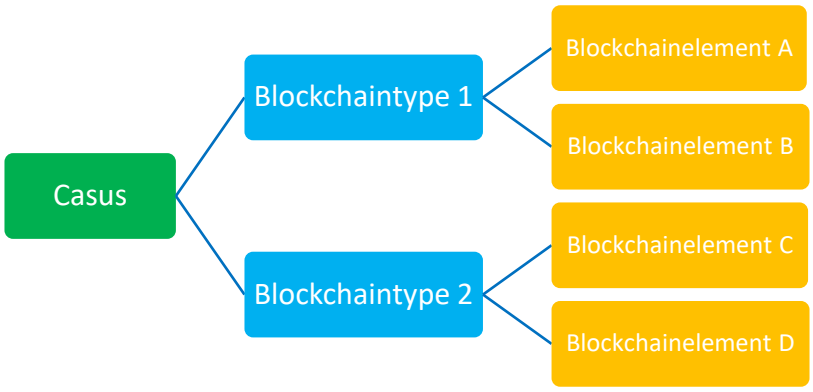
Verder moet je, als je gaat voor een permissionless blockchain, ook afvragen hoe gedecentraliseerd je de blockchain wil hebben. Sterk gedecentraliseerde blockchains zijn vaak veiliger, maar kunnen weer inleveren op schaalbaarheid. Denk hierbij aan het blockchaintrilemma dat in paragraaf 7.2 is besproken.

Tot slot zijn er op permissionless blockchains vaak ook hogere transactiekosten dan bij een permissioned blockchain. Dit zijn allemaal overwegingen die je mee moet nemen in je besluit wat voor type blockchain je wil.

17.3 Typen blockchaintoepassingen

De blockchaincasussen die zijn genoemd in hoofdstuk 16 voldoen grotendeels aan de criteria om blockchain toe te passen. Deze casussen kunnen meerdere concretere ***toepassingstypen*** bevatten. De typen zijn gebaseerd op een praktische grondslag van toepassingsgebieden die al bestaan. Zo is BitShares een blockchainproject met als toepassingstypen een handelsbeurs, clearing en settlement, betalingsverkeer, enzovoorts. Deze typen kunnen we gebruiken om inzicht te krijgen welke essentiële ***blockchainelementen*** belangrijk zijn om de typen mogelijk te maken. Als je een blockchaincasus hebt en weet welke toepassingstypen je binnen de casus wil hebben, weet je ook welke blockchainelementen je moet gebruiken.

goedkoper worden dan privacy transacties op een private blockchain. (p. 14) De verwachting is dat dit ervoor gaat zorgen dat meer bedrijven die privacy willen inregelen voor permissionless open blockchains zullen kiezen.



Afbeelding 143: Schematische weergave van hoe we een blockchaincasus benaderen. De casus wordt onderverdeeld in verschillende blockchaintypen waaraan bijbehorende blockchainelementen worden gekoppeld.

Een blockchainelement is een basale bouwsteen die samen met andere bouwstenen wordt gebruikt om een toepassingstype mogelijk te maken. De blockchainbouwstenen bepalen ook de karakteristieke eigenschappen van een blockchain die je wil gebruiken. Zo heeft het blockchainelement 'betalingstoken' bijvoorbeeld impact op het gemak, de snelheid en transparantie van het betalingsverkeer. Voorbeelden van blockchainelementen zijn wallets, smart contracts, dApps, DAO's, orakels, enzovoorts.

Toepassingstypen bundelen dus blockchainelementen die zelf weer een bepaald gebruikersnut van de blockchain representeren. Het gebruikersnut hangt samen met hoe je deze elementen bundelt en/of aanpast voor je eigen toepassingstypen.

In de volgende tabel staan de casussen uit hoofdstuk 16 weergegeven met bijbehorende toepassingstypen en blockchainelementen. Om de tabel enigszins overzichtelijk te houden, worden binnen de casussen alleen toepassingstypen genoemd die nog niet eerder zijn genoemd. Bij de casus van de Telia-app is digitaal eigendom bijvoorbeeld ook een toepassingstype, maar is deze niet in de tabel opgenomen omdat deze al is genoemd bij de BitSharescasus.

Casus	Blockchainelement / Toepassingstype	Blockchain 1.0 elementen	Wallet & digitale handtekening	Smart contract	dApp	DAO	Orakel	Netwerk-token	Betalings-token	Asset token	Decentrale identiteit	Opmerking
BitShares	Exchange / marktplaats: organisatie van gehele exchange	⊗	⊗	⊗	⊗	⊗	⊗	⊗		⊗		Netwerktoken wordt mede gebruikt voor betalingen.
	Clearing en settlement	⊗	⊗	⊗	⊗	⊗		⊗		⊗		Automatisch verwerken van koop/verkoop/ wisseling eigendom.
	Betalingsverkeer	⊗	⊗	⊗	⊗	⊗		⊗		⊗		Om betalingen te verrichten.
	Tokeneconomics	⊗	⊗	⊗	⊗	⊗	⊗	⊗				Gedrag stimuleren van tokenhouder als klant, investeerder en participant.
	Disintermediatie	⊗	⊗									
	Digitaal eigendom	⊗	⊗	⊗	⊗	⊗		⊗	⊗	⊗		Aanmaken, houden en verhandelen excl. digitale identiteit.
	Stemmen	⊗	⊗	⊗	⊗	⊗		⊗				
	Directe communicatie tussen tokenhouders	⊗	⊗	⊗	⊗	⊗		⊗				
Lantmäteriet	Registratie van dossiers: land	⊗	⊗	⊗				⊗			⊗	Hashregistratie via Ethereum.
	Certificatie van eigenaarschap	⊗	⊗	⊗				⊗			⊗	Gebruik van privaat netwerk voor vastlegging gegevens.
Telia app	Self-Sovereign Identity	⊗	⊗	⊗	⊗		⊗				⊗	
Land Layby	Certificatie van kwaliteit	⊗	⊗	⊗			⊗	⊗	⊗	⊗	⊗	Onduidelijk, mogelijk binnen dApp data van bezit tokens onderhouden.
BWM	Ketensamenwerking	⊗	⊗		⊗		⊗					
	Volgen van goederenbeweging	⊗	⊗	⊗			⊗				⊗	

Tabel 32: Model van blockchaincasussen, gebruikte blockchaintoepassingstypen en blockchainelementen.

Een verdere uitleg van de blockchainelementen is als volgt:

- ***Blockchain 1.0 elementen*:** basiselementen van blockchain zoals consensusmechanisme dat onderling onderhouden wordt, onveranderbaarheid van data (bij open permissionless blockchains), overzicht van transacties, keten van datablokken en toepassingen van cryptografie om authenticiteit van data te waarborgen. Inherent hieraan is een robuuster en veiliger netwerk. De belangrijkste toepassing hierbinnen is cryptovaluta, maar andere toepassingen als registraties van stemmen en eigendom zijn ook mogelijk.
- ***Wallet & digitale handtekening*:** het hebben van een wallet om transacties te verrichten en tokens te bezitten, dus niet direct in overeenstemming met de e-Signatures binnen de eIDAS richtlijn. Hierbinnen valt het aan kunnen tonen van eigenaarschap van een bepaald bezit op enig moment.
- ***Smart contract***: een contract met bepaalde condities en voorwaarden die zijn vastgelegd in code. Het contract is zelfuitvoerend, omdat het zelf de juiste corresponderende acties uitvoert wanneer er aan de condities en voorwaarden wordt voldaan. Mogelijke toepassingstypen zijn digitale rechten, gokken en geld als borg vastleggen.
- ***dApp*:** een applicatie die gebruikmaakt van de gedecentraliseerde dataopslag van een blockchain.
- ***Decentralized Autonomous Organisation***: een autonome entiteit, die ook afhankelijk is van het inhuren van individuen. Deze individuen kunnen bepaalde noodzakelijke taken vervullen die de entiteit niet kan. De DAO heeft hiervoor intern kapitaal tot zijn beschikking, waarmee bepaalde activiteiten van deze individuen kunnen worden beloond. Bitcoin is de eerste DAO.
- ***Orakel***: een bron buiten de blockchain die een smart contract voedt met relevante externe informatie, zodat het smart contract arbitraire condities kan checken.
- ***Netwerktoken*:** token met als doel deelnemers te belonen voor het werk dat ze verrichten om het netwerk te helpen onderhouden.
- ***Betalingstoken*:** token met als doel betalingen te verrichten binnen het blockchainnetwerk. Mogelijke toepassingen zijn e-commerce, peer-to-peer lending en microfinanciering.
- ***Asset token*:** token met een onderliggende waarde in de werkelijke wereld. Mogelijke toepassingen zijn leningen, crowdfunding en private markten.
- ***Decentrale identiteit*:** Een digitale identiteit die is vastgelegd en beheerd op decentrale wijze.

Dit model biedt slechts een overzicht van blockchainelementen die veel voorkomen. Andere elementen die in het boek zijn besproken en kunnen worden toegevoegd, zijn fractionalisering, smart asset, smart token, smart property en Zero-Knowledge Proofs.

Je zou daarnaast nog de volgende toepassingstypen die we eerder in het boek hebben besproken, kunnen toevoegen aan het model:

- ***Crowdfunding*:** het verwerven van fondsen om een initiatief te financieren.
- ***KYC/AML***: op basis van data binnen het gehele ecosysteem aantonen dat een partij is wie hij zegt dat hij is en inzien wat de partij in het verleden deed. Hierbij kan een zogenaamde compliant check box worden gedeeld tussen financiële dienstverleners en klanten.
- ***Notarisatie***: aangeven wat de staat van iets was op een bepaald tijdstip.
- ***Triple entry accounting***: gelijktijdig voor meerdere partijen aantonen dat de transactie heeft plaatsgevonden.
- ***Upfront compliancy***: van tevoren inregelen dat transacties volgens wet- en regelgeving plaatsvinden.

Alternatieve datamanagementsystemen

Het is niet altijd nodig om een blockchain te gebruiken. Er zijn alternatieve datamanagementsystemen die misschien beter, goedkoper en makkelijker zijn. Je zou de volgende alternatieven kunnen overwegen, al dan niet in combinatie met elkaar:

1. Een gedeelde database met toegangsrechten.
2. Een met wachtwoord beschermde spreadsheet op een gedeelde server.
3. Een versleutelde database.
4. Een aanbieder van cloudoplossingen.
5. Een autorisatiemodel voor het accorderen van transacties.
6. Andere Distributed Ledger technologieën.

Veel organisaties hebben al ervaring met deze oplossingen. Het is raadzaam om de ICT-professional binnen de organisatie erbij te betrekken om te zien of dergelijke datamanagementsystemen een beter alternatief zijn dan blockchain. Je kunt ook de use case voorleggen aan verschillend samengestelde teams om te zien in hoeverre ze deze anders zouden aanpakken.

Denk erom dat je de meerwaarde van blockchain over andere alternatieven duidelijk moet kunnen benoemen.

Het model is nu als volgt te gebruiken om een blockchain te conceptualiseren. Stel dat je een financiële dienstverlener bent die voornamelijk leningen en financieringen verstrekt. Binnen dit businessmodel spelen toepassingstypen als KYC/AML, Self-Sovereign Identity, crowdfunding en betalingsverkeer een rol. Deze vertalen zich weer in het analyseren hoe elementen als blockchain 1.0, wallet en digitale handtekening, smart contracts, betaling- of asset tokens en decentrale identiteit worden ingevuld en op elkaar ingrijpen.

Een ander voorbeeld is verzekeringen, de andere sector waar één van de meeste DLT use cases volgens Hileman & Rauchs (2017) zich bevinden. Stel dat je een aanbieder bent van autoschadeverzekeringen. In dat geval zullen je uitdagingen dicht liggen bij de uitdagingen die financiële dienstverleners en autobedrijven ook kennen. Zodoende zul je daarmee ook dezelfde toepassingstypen als die van BitShares en BMW willen gebruiken. Zij bevinden zich immers in deze sectoren. Eerder genoemde voordelen hiervan zijn veilig en goedkoop transacties bewerkstelligen die leiden tot snellere en adequatere afhandeling van het proces.

Zorg is volgens Hileman & Rauchs de sector met de drie na meeste DLT use cases. Binnen deze sector moeten medische gegevens op veilige transparante wijze worden samengesteld en gedeeld tussen verschillende partijen, zoals ziekenhuizen, artsen, apotheken, verzekeraars en de patiënt. Hier staan registratie van gegevens, een robuust netwerk, Self-Sovereign Identity en misschien betalingsverkeer om via een smart contract een verzekeraar te betrekken bij factuurverwerking, centraal. Blockchain kan meer veiligheid en vertrouwen geven in de medische gegevens, waardoor er sneller zorg kan worden verleend.

17.4 Samenvatting, begrippen en bronnen

Samenvatting

Er zijn een aantal criteria waar je naar kunt kijken om te beslissen of blockchain interessant is voor je bedrijf. We hebben criteria opgesteld die vallen binnen de volgende drie blokken:

1. Data.
2. Partijen.
3. Dataverkeer.

Blockchain is immers een instrument om fricties met data of dataverkeer op te heffen, of juist kansen te creëren met data en dataverkeer. Het is als vuistregel handig om minimaal de volgende criteria te gebruiken:

1. Digitale innovatie onderdeel is van de strategie.
2. Verschillende partijen gegevens delen.
3. Deze gegevens en hun transacties geldwaarde betreffen.
4. De data vertrouwelijk zijn.
5. Verschillende partijen gegevens bewerken.
6. Gegevens moeten worden geverifieerd.
7. Er een duidelijke Return on Investment te berekenen is, en deze voldoet in dit geval.
8. Verificatie complex, kosten- en of tijdverhogend is.
9. De oplossing om voor blockchain te kiezen de meest simpele kans is om het probleem te overwinnen.
10. De oplossing de bestaande organisatiestructuur beïnvloedt.
11. De oplossing de bestaande workflow beïnvloedt.
12. De oplossing het bestaande ecosysteem beïnvloedt. Zo is er geen tussenpartij met een centrale positie.
13. De technische oplossing dichtbij bestaande systemen ligt of ermee te integreren valt.
14. De oplossing data-intensief maar schaalbaar is. Denk in verschillen van 1k, 10k, 100k, 1 mln. of > 10 mln. transacties per uur.

Als je een blockchaincasus hebt, dien je de casus op te splitsen in toepassingstypen. Aan de hand van je toepassingstypen, kun je blockchainelementen selecteren. Een blockchainelement is een basale bouwsteen die samen met andere bouwstenen wordt gebruikt om een toepassingstype mogelijk te maken. De blockchainbouwstenen bepalen ook de karakteristieke eigenschappen van een blockchain die je wil gebruiken. Zo heeft het blockchainelement ‘betalingstoken’ bijvoorbeeld impact op het gemak, de snelheid en transparantie van het

betalingsverkeer. Voorbeelden van blockchainelementen zijn wallets, smart contracts, dApps, DAO's, orakels, enzovoorts.

Toepassingstypen bundelen dus blockchainelementen die zelf weer een bepaald gebruikersnut van de blockchain representeren. Het gebruikersnut hangt samen met hoe je deze elementen bundelt en/of aanpast voor je eigen toepassingstypen.

Opmerkingen die je nu kunt uitleggen

- Blockchain geeft bedrijven vooral de kans dataverkeer tussen samenwerkende partijen, binnen het bedrijf en het ecosysteem, te bewerkstelligen.
- Momenteel richt de impact van blockchain bij bedrijven zich vooral op efficiëntie, disintermediatie en registratie.
- De impact van blockchain is groot waar samenwerkende partijen nieuwe data vrijspelen en creëren.
- Na businessmodellen zullen ecosystemen decentraler moeten worden ingericht om de volledige voordelen van blockchain te benutten.
- Een eenvoudige beslisboom kan helpen om snel in te schatten in hoeverre een blockchainproject nut heeft.
- De mogelijkheden om blockchain toe te passen hangen samen met de toepassingstypen en de blockchainelementen.
- De bouwstenen van blockchain zijn vrij te bundelen en aan te passen om van een bepaald gebruikersnut van de blockchain te genieten.
- Een succesvol blockchainproject heeft een te onderbouwen positieve ROI nodig.

Verklarende begrippenlijst

Asset token: Token met een onderliggende waarde in de werkelijke wereld. Mogelijke toepassingen zijn leningen, crowdfunding en private markten.

Betalingstoken: Token met als doel betalingen te verrichten binnen het blockchainnetwerk. Mogelijke toepassingen zijn e-commerce, peer-to-peer lending en microfinanciering.

Blockchain 1.0 elementen: basiselementen van blockchain zoals consensusmechanisme dat onderling onderhouden wordt, onveranderbaarheid van data (bij open permissionless blockchains), overzicht van transacties, keten van datablokken en toepassingen van cryptografie om authenticiteit van data te waarborgen. Inherent hieraan is een robuuster en veiliger netwerk. De belangrijkste toepassing hierbinnen is cryptovaluta, maar andere toepassingen als registraties van stemmen en eigendom zijn ook mogelijk.

Blockchainelement: Een basale blockchainbouwsteen die samen met andere bouwstenen wordt gebruikt om een toepassingstype mogelijk te maken. De bouwstenen bepalen ook de karakteristieke eigenschappen van een blockchain die je wil gebruiken. Zo heeft het blockchainelement 'betalingstoken' bijvoorbeeld impact op het betalingsverkeer.

Crowdfunding: Het verwerven van fondsen om een initiatief te financieren.

dApp: Een applicatie die gebruikmaakt van de gedecentraliseerde dataopslag van een blockchain.

Decentrale identiteit: Een digitale identiteit die is vastgelegd en beheerd op decentrale wijze.

Decentralized Autonomous Organisation: Een autonome entiteit, die ook afhankelijk is van het inhuren van individuen. Deze individuen kunnen bepaalde noodzakelijke taken vervullen die de entiteit niet kan. De DAO heeft hiervoor intern kapitaal tot zijn beschikking, waarmee bepaalde activiteiten van deze individuen kunnen worden beloond. Bitcoin is de eerste DAO.

KYC/AML: Op basis van data binnen het gehele ecosysteem aantonen dat een partij is wie hij zegt dat hij is en inzien wat de partij in het verleden deed. Hierbij kan een zogenaamde compliant check box worden gedeeld tussen financiële dienstverleners en klanten.

Netwerktoken: Token met als doel deelnemers te belonen voor het werk dat ze verrichten om het netwerk te helpen onderhouden.

Notarisatie: Aangeven wat de staat van iets was op een bepaald tijdstip.

Orakel: Een bron buiten de blockchain die een smart contract voedt met relevante externe informatie, zodat het smart contract arbitraire condities kan checken.

Smart contract: Een contract met bepaalde condities en voorwaarden die zijn vastgelegd in code. Het contract is zelfuitvoerend, omdat het zelf de juiste corresponderende acties uitvoert wanneer er aan de condities en voorwaarden wordt voldaan. Mogelijke toepassingstypen zijn digitale rechten, gokken en geld als borg vastleggen.

Toepassingstype: Toepassingstypen bundelen blockchainelementen die zelf weer een bepaald gebruikersnut van de blockchain representeren. Zo heeft BitShares als toepassingstypen onder andere een handelsbeurs, clearing en settlement en betalingsverkeer.

Triple entry accounting: Gelijktijdig voor meerdere partijen aantonen dat de transactie heeft plaatsgevonden.

Upfront compliancy: Van tevoren inregelen dat transacties volgens wet- en regelgeving plaatsvinden.

Wallet & digitale handtekening: Een digitale portemonnee waarmee je transacties kunt verrichten en tokens kunt bezitten. Het verrichten van een transactie gebeurt met het zetten van een digitale handtekening, waarbij een private key betrokken is. Hierbinnen valt het aan kunnen tonen van eigenaarschap van een bepaald bezit op enig moment.

Bronnen

Alloway, T. (2017, 19 januari). An experiment. Bron: http://www.tracy-alloway.com/?p=577.

Castellon, N., Cozijnsen, P. & Van Goor, T. (2018). *Blockchain Security: A Framework for Trust and Adoption*. Geraadpleegd van: https://dutchblockchaincoalition.org/nieuws/cyber-security-framework-helpt-organisaties-met-veilig-toepassen-blockchains.

EU Blockchain Observatory & Forum (2019). Feeling good: Healthcare data and the blockchain. Geraadpleegd van https://www.eublockchainforum.eu/news/feeling-good-healthcare-data-and-blockchain

Herweijer, C., Waughray, D., & Warren, S. (2018). *Building Block(chain)s for a Better Planet*. Geraadpleegd van http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf

Hileman G., & Rauchs M. (2017). *Global Blockchain benchmarking study*. Geraadpleegd van https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

Millar, J. (2018, 10 januari). 6 Questions to Ask When Considering Blockchain Solutions for Enterprise. Geraadpleegd op 23 december 2019, van Consensys website: https://media.consensys.net/6-questions-to-ask-when-considering-blockchain-solutions-for-enterprise-10616a0c63c4

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview.* https://doi.org/10.6028/nist.ir.8202

18. Platformen en consortia

"No matter who the financial advisor of the future becomes, they will be running a Blockchain based operating system for commerce and finance."
- Lex Sokolin (2019)

"The mix of blue chip technology companies, international organizations, logistics and manufacturing players and academia that have joined us from point around the world show the widespread interest and investment in open source enterprise blockchain technologies. This broad-based involvement is what drives our expanding portfolio of open source projects, which are fully conceived, developed and advanced by the ever-growing Hyperledger community."
- Brian Behlendorf (2019)

18.1 Inleiding en leerdoelen

In dit hoofdstuk leer je

- Welke overwegingen bedrijven nemen om blockchain toe te passen.
- De voor- en nadelen van Enterprise blockchainplatformen zoals Ethereum, Hyperledger en Corda.
- De voor- en nadelen van blockchainconsortia zoals Ethereum Enterprise Alliance, Hyperledger en R3.
- De uitdagingen waarmee een blockchainconsortium te maken heeft.
- BaaS als alternatieve wijze om laagdrempelig met blockchainsoftware aan de slag te gaan.

Inleiding

Vele bedrijven die Enterpriseblockchain invoeren, gebruiken hiervoor blockchainplatformen. Deze platformen zorgen ervoor dat je applicaties kunt schrijven met behulp van bepaalde technologieën. Rondom deze platformen hebben zich verschillende samenwerkingsverbanden georganiseerd, zogenaamde consortia.

In dit hoofdstuk worden zowel bekende Enterprise blockchainplatformen, in paragraaf 18.2, als consortia beschreven in paragraaf 18.3. De impact die een consortium kan hebben op bedrijven wordt genoemd in paragraaf 18.4. Het hoofdstuk wordt afgesloten met een samenvatting en gebruikte begrippen en bronnen in paragraaf 18.5.

18.2 Enterprise blockchainplatformen

Verschillende stakeholders hebben zich onder andere in ***consortia*** georganiseerd om gezamenlijk blockchaintoepassingen te ontwikkelen. Hierbinnen zoeken ze samenwerking met al bestaande (publieke) blockchainsystemen en/of creëren ze een eigen blockchainsysteem op basis van een ***blockchainplatform***. Deze platformen zorgen ervoor dat je applicaties kunt schrijven met behulp van bepaalde technologieën. Zodoende kan je applicatie bijvoorbeeld samenwerken met andere dApps, in een eigen of gedeelde programmeertaal, worden documenten bewaard of gedeeld, een technische infrastructuur ontwikkeld of toegang verkregen tot een bepaald netwerk. Platformen richten zich voor blockchain specifiek op communicatieprotocollen, dApps, smart contracts en cryptografie.

In het volgende bespreken we drie vooraanstaande blockchainplatformen waar verschillende consortia gebruik van maken:

1. ***Ethereum*** heeft de meeste ontwikkelaars en ook de hoogste marktkapitalisatie van de blockchain 2.0 publieke blockchainsystemen.[201] De ***Ethereum Enterprise Alliance*** (EEA) heeft ook de meeste deelnemers aan een georganiseerde groep weten te mobiliseren.
2. ***Hyperledger*** is in december 2015 gestart door de Linux Foundation en heeft een groot aantal ontwikkelaars rondom het professioneel georganiseerde open source initiatief. IBM is één van de aanjagers van Hyperledger Fabric, een permissioned blockchaininfrastructuur, om professionele blockchainapplicaties te verrichten.
3. ***Corda*** is een professioneel georganiseerde open source blockchain die sinds 2015 bestaat. Corda is ontwikkeld door R3 en richt zich voornamelijk op de financiële dienstverlening.

Belangrijke verschillen van deze drie platformen zijn hieronder samengevat als leidraad voor de verdere bespreking van deze platformen.

[201] Ethereum heeft van de publieke blockchains momenteel het grootste ontwikkelaarsecosysteem. Groter dan EOS, Cardano en Tron. (Electric Capital, 2019). Het heeft tevens de meeste dApps, hoewel de activiteit van vele dApps nog vrij gering is.

	Ethereum	Hyperledger	R3 Corda
Soort platform	Generiek	Modulair	Financieel
Governance	Ethereum Enterprise Alliance (EEA)	Linux Foundation	R3 consortium
Blockchaintype	Permissionless en permissioned	Permissionless en permissioned	Permissioned
Cryptovaluta	Ether (ETH)	Geen/wel mogelijkheid	Geen/in toekomst mogelijk
Consensusmechanisme	PoW	Pluggable	Pluggable
Smart contracts	Ja	Ja	Ja

Tabel 33: Een vergelijkingstabel tussen Ethereum, Hyperledger en R3 Corda. De tabel is gebaseerd op het onderzoek van HfS research (2018).

Ethereum en Hyperledger worden gebruikt door verscheidene industrieën, terwijl R3 voornamelijk is gespecialiseerd binnen de financiële industrie. Hyperledger lijkt de laatste jaren dankzij toenemende stabiele technologie meer te worden gebruikt, terwijl Ethereum als first mover de potentie van een publiek netwerk voor nieuwe startups biedt.[202]

Hierna gaan we dieper in op de drie platformen.

18.2.1 Ethereum

Ethereum is één van de eerste blockchains geweest die smart contracts gebruikte. Het platform wordt momenteel gezien als de belangrijkste representant van blockchain 2.0. Het biedt de mogelijkheid om verschillende dApps te ontwikkelen op het platform.

Ethereum is van de drie platformen het enige dat in de basis een publieke blockchain is. Rondom dit platform is de Ethereum Enterprise Alliance (EEA) opgezet. EEA is een ledenorganisatie die met behulp van afspraken en standaarden Enterprise-software definiëren.[203] Op basis van deze software kunnen ze toepassingen maken en integraties leggen met hun oude databasesystemen. Hiervoor worden, naast code en smart contracts, de ***Ethereum Virtual Machine***

ENTERPRISE ETHEREUM ALLIANCE

[202] Welke platformen dominant gaan worden, is onduidelijk. Platformen die in beginsel een groot marktaandeel hebben, kunnen door de grote concurrentie forst in marktaandeel inleveren. Dit is in het verleden zo gebleken bij mobiele, e-commerce en socialmediatechnologische veranderingen. Denk bijvoorbeeld aan Nokia, eBay, Yahoo en MySpace. Volgens del Castillo (2019) gebruiken van de 50 grootste blockchainprojecten, 50% Hyperledger en 40% Ethereum.

[203] Onder de EEA-leden bevinden zich bedrijven als Samsung, Microsoft, Accenture, ING en HP Enterprise.

(EVM) gebruikt. De EVM is verantwoordelijk voor de computaties op het netwerk en het behandelen van de interne staat op het netwerk.[204]

Interoperabiliteit
Met interoperabiliteit wordt gewezen op de mogelijkheid om tussen verschillende blockchains informatie te delen. Denk hierbij aan een token dat je op de ene blockchain koopt en op een andere blockchain wilt gebruiken. Een andere mogelijkheid, in lijn met interoperabiliteit, is om veel data off-chain te plaatsen als aparte side chain en deze te koppelen aan de root chain.

Gezien het belang van interoperabiliteit zijn er meerdere bedrijven die zich op dit onderwerp storten.

Ethereum kent nog wel schaalbaarheidsproblemen. Om dit te overwinnen werkt Ethereum onder andere aan een overgang van een Proof-of-Work- naar een Proof-of-Stake-consensusmechanisme via de ***Casper*** updates. Casper wordt ook wel gezien als de nieuwe evolutie van Ethereum, ook wel aangeduid als Ethereum 2.0. Het doel is om naast schaalbaarheid, het netwerk ook veiliger en milieuvriendelijker te maken.

Een andere manier om schaalbaarbaarheid te vergroten, is door ***sharding***. Met sharding wordt een blockchain in verschillende stukken (shards) gesplitst, die een individuele node kan downloaden, bewaren en verifiëren, zodat het netwerk in stukken kan worden onderhouden, in plaats van in zijn geheel.

Als laatste is er het ***Plasma-initiatief***, waarin de blockchaininfrastructuur bestaat uit een root chain dat gekoppeld is aan verschillende side chains. De side chains kunnen worden gezien als blockchains die apart worden onderhouden. In dit licht is het afstemmen van ***interoperabiliteits***protocollen tussen de EEA-leden belangrijk voor zowel de schaalbaarheid, alsook om dApps op elkaar af te stemmen en elkaars data te gebruiken. Of, je kunt informatie en transacties uitwisselen met niet-vertrouwde partijen, zonder dat je je eigen applicatie hoeft te verlaten. Het is mogelijk dat de side chain op het plasmanetwerk een private blockchain is die om de zoveel tijd de staat van de blockchain stuurt naar de root chain. Hierbij helpt de rootchain om de staat van private side chain te verifiëren. Dit leidt tot betere beveiliging van de private side chain. Hierbij staat Ethereum dus toe dat bedrijfsdata binnen private systemen blijven,

[204] Een EVM is een gedecentraliseerde virtuele machine die scripts kan uitvoeren. EVM's zorgen voor de computaties op het Ethereum-netwerk. Smart contracts die worden geschreven in de programmeertaal Solidity worden gecompileerd in 'bytecode' die kan worden gelezen en uitgevoerd door de EVM. Elke node op het netwerk bevat een EVM en compileert en voert smart contracts uit.

terwijl de resultante staat van alle data wordt verwerkt en onderhouden binnen het Ethereum-netwerk. Voor meer informatie over het schaalbaarheidsprobleem van blockchains en hoe het kan worden opgelost met sharding en plasma, zie paragraaf 6.9.

Ethereum is een breed ingezette technologie en wordt door verschillende externe partijen voor onder andere ***Blockchain-as-a-Service*** (BaaS) aangeboden om de ontwikkeling van een eigen blockchainsysteem laagdrempelig te houden. In het publieke systeem is er een Ethereum cryptovaluta (Ether) die wordt gebruikt om ***gas*** te betalen voor het schrijven van een transactie en het uitvoeren van diens computaties.

Verder is Ethereum zoals genoemd een publiek netwerk. Dit geeft de EEA-leden de kans om binnen de stakeholdersgroep een bestaand publiek netwerk van duizenden gebruikers en ontwikkelaars aan te laten sluiten bij de toepassing die het bedrijf ontwikkelt.

Ook is Ethereum open source en kent het al standaarden voor tokens, gedecentraliseerde opslag, berichten en leesvriendelijke adresnamen. Daarnaast staat Ethereum als platform toe om daar waar nodig de toegang en functionaliteit van gebruikers te beheersen en transacties al dan niet verborgen te houden.

Ook kun je een private blockchain ontwikkelen op basis van Ethereum. Zo kun je bijvoorbeeld een private Ethereum blockchain maken met een permissioned consensusmechanisme als Proof-of-Authority of Practical Byzantine Fault Tolerance. Deze permissioned opzet is voor leden van EEA belangrijk, omdat ze hiermee zelf kunnen bepalen wie toegangsrechten heeft tot hun eigen opgezette blockchain. Ook kunnen ze de private chain zo inrichten dat er geen cryptotoken wordt gebruikt en er ook geen gas hoeft te worden betaald. Zo hoeven ze alleen samen te werken met partijen die ze kennen en ook vertrouwen. Ethereum kan zodoende als Enterprise-software worden gebruikt.

Enterprise Ethereum biedt door de eerdergenoemde mogelijkheden een oplossing voor problemen die bedrijven ervaren met publieke modellen zoals:

1. Dat je voldoende invloed houdt op de beslissingen binnen een DAO.
2. Dat je niet weet hoe te reageren als er een hard of soft fork komt.
3. Dat het onduidelijk is in welke mate open source-ontwikkelingen worden gedeeld met concurrenten.

4. Dat er participanten zijn die een rol binnen het netwerk hebben, zonder dat duidelijk is welke doelen ze dienen.
5. In hoeverre wet- en regelgeving wordt opgevolgd.

18.2.2 Hyperledger

De EEA werkt samen met het ***Hyperledger Project***, het tweede platform. Hyperledger wordt ondersteund binnen de ***Linux Foundation***. Deelnemers van Hyperledger zijn onder andere Airbus, Ant Financial, Huawei, SAP, TNO, Bank of England, Smart Dubai, ABN Amro, Rabobank, en R3.[205]

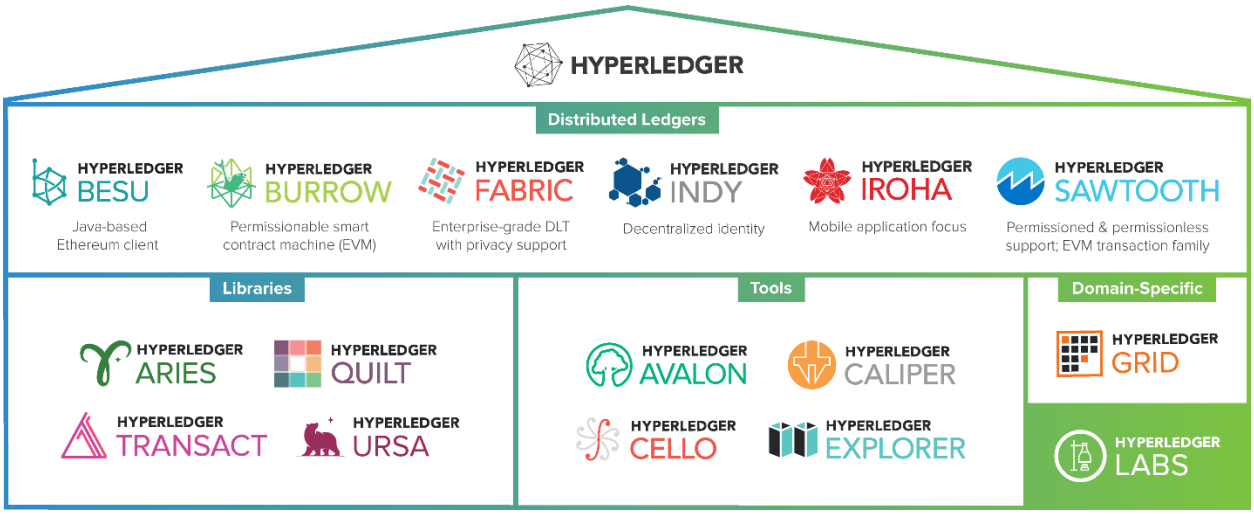
Hyperledger is ontstaan doordat verschillende bedrijven de behoefte hadden samen te werken aan een blockchain die niet direct rond cryptovaluta was gebouwd, maar toch toestond rondom smart contracts samen te werken.[206] Hiervoor brachten deze bedrijven hun blockchainsystemen samen op het open Linux-platform. Zodoende stonden verschillende open source templates en modules tot hun beschikking, die bedrijven laagdrempelig konden invoeren. De templates en modules worden ook wel ***pluggable*** genoemd, omdat je zelf kunt kiezen welke van deze je wil implementeren of aanpassen en welke niet.

De leden van Linux werken, net als EEA, samen rondom de modules om af te spreken hoe ze Enterprise-software kunnen bouwen met smart contracts, client libraries, grafische interfaces en toepassingen. Hierbinnen wordt ook gesproken over hoe deze systemen onderling kunnen samenwerken om interoperabel te zijn. Daarnaast zijn er templates voor verschillende bedrijfstoepassingen waarbij de opslagmodellen, contracten, rollen en dergelijke kunnen worden aangepast. Uit de verschillende initiatieven binnen Hyperledger zijn er een zestal blockchainraamwerken ontstaan binnen Hyperledger.

In de volgende afbeelding vind je een overzicht van de verschillende raamwerken en de libraries en tools die worden gebruikt bij Hyperledger.

[205] Sommige bedrijven zoals Samsung en JP Morgan zijn lid van zowel EEA als Linux, of zelfs ook van R3.

[206] Dit is verklaarbaar gezien Hyperledger als privaat initiatief geen cryptotokens nodig heeft om deelnemers te belonen om op goede wijze consensus te bewerkstelligen.



Afbeelding 144: Overzicht van Hyperledger en de verschillende raamwerken (Hyperledger.org, 2019).

Zo is er het veelgebruikte ***Hyperledger Fabric***, mede opgezet door IBM, waarmee je identiteiten en verantwoordelijkheden kunt splitsen per rol. Het is bedoeld als basis voor het ontwikkelen van applicaties of modulaire architectuuroplossingen. Hierbij wordt vaak opgemerkt dat doordat IBM een grote rol speelt binnen Hyperledger Fabric, het lastiger wordt om een andere leverancier dan IBM te gebruiken. Dit wordt ook wel ***vendor lock-in*** genoemd.

Andere blockchainraamwerken binnen Hyperledger zijn Sawtooth (Intel), Burrow (Monax), Indy en Iroha. Deze ondersteunen de Ethereum Virtual Machine (EVM) ten bate van smart contracts en een cryptografisch beloningssysteem. Hyperledger Fabric en Hyperledger Sawtooth kunnen weer worden aangepast om ook permissionless netwerken toe te staan. Sawtooth is na Fabric het meest populaire raamwerk van Hyperledger. Het staat dApps toe en gebruikt het Proof-of-Elapsed Time (PoET) consensusmechanisme. Het mechanisme voorkomt hoge energieconsumptie voor het onderhoud van de blockchain. Hyperledger Indy is speciaal ontwikkeld voor gedecentraliseerde identiteit. Sovrin, het initiatief om Self-Sovereign Identities op uit te rollen, is gebaseerd op Indy.

Hyperledger is niet gebonden aan een bepaalde blockchaintechnologie en is in die zin een open platform waar andere platformen zoals Ethereum en Corda worden gebruikt. Zo kunnen er binnen Hyperledger verschillende consensusmechanismen en smart contracts worden ontwikkeld en gehanteerd. Hiervoor wordt onder andere ***chaincode***, een smart contractslaag, gebruikt. Ook kunnen tokens worden ingebouwd, hoewel ze niet standaard zijn voorzien binnen Hyperledger. Dit werkt cryptoeconomics in de hand om de samenwerking tussen (cross) industriële partners te stimuleren.

De data van de verschillende entiteiten die Hyperledger blockchains gebruiken, kunnen worden gecombineerd om een pool te vormen waar iedereen uit kan vissen. Dit voorkomt onder andere dubbele input en fouten en biedt potentieel meer informatie daar waar de participanten in eerdere instanties geen toegang of alleen toegang toe hadden na omslachtige aanvragen bij anderen. Met Zero-Knowledge Proofs wordt dit makkelijker toegankelijk. Ook kun je nog steeds een eigen chain openen met een eigen grootboek. De data uit je eigen chain worden vervolgens met niemand anders gedeeld mits je dat wilt.

Hyperledger is als verband van private netwerken in tegenstelling tot het publieke Ethereum minder robuust. De verwachting is dat deze private blockchains en R3 Corda op termijn connectiviteit met publieke blockchains krijgen en hun robuustheid vergroten.

Hyperledger heeft zich door stabiele technologie met een redelijke schaalbaarheid en een ingebouwde manier om data privé te houden de laatste jaren goed kunnen profileren richting Ethereum. Hyperledger wordt net als Ethereum gebruikt voor verschillende Blockchain-as-a-Service-oplossingen (BaaS).

Blockchain-as-a-Service (BaaS)
Soms hebben bedrijven niet de hardware, kennis of connectiviteit om een blockchaintoepassing op te draaien. Hiervoor gebruiken ze dan cloud providers als IBM, Microsoft, Amazon Web Services, Huawei, Alibaba, Oracle en Tencent. Deze verhuren hardware-omgevingen met cloudverbindingen, back-upmogelijkheden en netwerksoftware, waarop je je eigen blockchainsysteem of reeds geprogrammeerde templates kunt draaien. Additioneel verzorgen BaaS-leveranciers ook de integratie met de huidige databases en servers van deze bedrijven, evenals auditinginstrumenten.

Een Enterprise Ethereum-, Hyperledger- of Corda-applicatie kan daarmee dus efficiënt worden ontwikkeld en onderhouden, waarmee BaaS een belangrijke rol kan vervullen voor bedrijven die blockchain willen ontwikkelen, maar niet alle instrumenten tot hun beschikking hebben. Een interessante ontwikkeling hierbij is dat Enterprise Resource Planning-leveranciers als SAP ook BaaS-diensten aanbieden, zoals Hyperledger. Voor deelnemende bedrijven is dit een kans om hun data met behulp van API’s snel te actualiseren op een vertrouwde manier, terwijl ze de data toch privé kunnen houden.

18.2.3 R3

Het derde platform, R3, is een consortium van financiële instellingen dat de Corda-blockchain heeft ontwikkeld. Het is specifiek bedoeld voor financiële transacties, zoals voor financiering, handel, verzekeringen, gezondheidszorg en digitaal eigendom.

R3 heeft zelf financiering ontvangen van de deelnemers om een team van ontwikkelaars op te zetten. Onder de initiële deelnemers bevonden zich Barclays, JP Morgan, Credit Suisse, UBS, SWIFT, HSBC, Deutsche Bank, ABN AMRO, ING en Rabobank. Inmiddels is B3i, een verzekeringsconsortium, ook lid van R3. Naast B3i maakt het trade finance-consortium, Marco Polo[207], en MOBI ook gebruik van Corda. Zie voor dit laatste ook de BMW casus in paragraaf 16.4. R3 is op zijn beurt weer lid van Hyperledger.

De toename van leden en het toegenomen gebruik van Corda komt ook doordat het een toepassing biedt die je makkelijk kunt kopiëren en naar eigen wensen kan wijzigen. In dit geval biedt Corda een toepassing die je, als je dat wilt, als organisatie kunt kopiëren van een template en waar je op hoofdlijnen aanpassingen kunt laten maken door het Corda team. Je hoeft dan niet vanaf het begin de gehele toepassing te programmeren.

Bij Corda worden berichten van ***punt-naar-punt*** verstuurd in plaats van globaal uitgezonden naar alle nodes op het netwerk. Elk bericht wordt geadresseerd aan de partij voor wie het bedoeld is. Dit waarborgt dat transacties alleen worden gedeeld tussen partijen die bij deze transactie betrokken zijn en anoniem worden gehouden voor anderen. Dit betekent ook dat een transactie niet in een datablok wordt geplaatst in een gedeelde database. Consensus wordt dus mede verkregen op transactieniveau, of zelfs op slechts delen van transacties in plaats van de gehele transactie. Om de verwerkingssnelheid te vergroten, kunnen verschillende transacties naast elkaar worden verwerkt.

Ook is bij Corda elke transactie - overdracht van geld tussen partijen - onderdeel van een overeenkomst die wordt uitgevoerd via smart contracts met legale consequenties. Een ander kenmerk dat laat zien dat Corda moet voldoen aan de specifieke wet- en regelgeving van de flink gereguleerde financiële dienstverlening is dat transacties kunnen worden teruggedraaid en de

[207] Zo verrichtte Daimler, eigenaar van Mercedes-Benz, een eerste transactie waarin een order werd geleverd voor een balanceersysteem met ingenieursbedrijf Dürr.

database weer naar een andere historische staat terugbrengt. Deze ***roll-backfunctie*** zorgt er daarmee voor dat een verkeerde transactie dus teniet kan worden gedaan. Corda is dan ook een Distributed Ledger Technology en geen pure blockchain waarin de datablokken aan elkaar worden geketend. Daarbij heeft Corda een doorzoekbare en afgescheiden database in SQL-format. Dit maakt het makkelijker voor toezichthouders om hun werkzaamheden uit te voeren.

Net als bij Hyperledger zijn tokens niet inherent aan Corda. Deze zullen in de toekomst wel mogelijk zijn. Een nadeel van Corda is dat je al snel vastzit aan ontwikkelingen vanuit de R3 Corda-organisatie. Dit komt omdat concurrenten die binnen Corda samenwerken elkaar niet toestaan om binnen het eigen bedrijf aan Corda te werken. Dit zou er namelijk toe kunnen leiden dat dit bedrijf hiervoor gevoelige informatie zou moeten gebruiken die zijn concurrenten aan Corda beschikbaar hebben gesteld.

18.2.4 Noemenswaardige verschillen en overeenkomsten tussen de drie consortia

Binnen de drie eerdergenoemde consortia spelen ook noemenswaardige verschillen. Zo ervaart EEA minder de noodzaak om alle participanten van het Ethereum-platform te kennen, omdat Ethereum in beginsel permissionless is. De leden van EEA zelf overleggen met elkaar en met de Ethereum Foundation.

Hyperledger heeft meer een ledenstructuur en centralere governance, waardoor individuele leden sneller overgaan tot het maken van samenwerkingscontracten mochten ze een deel van de software willen laten implementeren door leveranciers zoals IBM. Dit in tegenstelling tot Corda, waar bijvoorbeeld B3i zelf een bedrijf heeft opgezet met aandeelhouders waar Corda voor verzekeringen wordt ontwikkeld. Corda zal door de specialisatie van financiële dienstverlening in de governance weer meer wet- en regelgevende instanties bij het netwerk betrekken.

Er zijn ook overeenkomsten, zoals dat in alle drie de consortia de leden beslissen en ze alle drie werken met technische stuurcommissies, die de technische richting van de gemeenschap bepalen, technische bijdragen beoordelen en keuren en de werkgroepen overzien.

Tot zover de drie voornaamste platformen.

Uitvindersdilemma
Tot op zekere hoogte werken bedrijven samen in de wetenschap dat ze gelijktijdig hun concurrerende krachten verbeteren. Door samen te werken, verdeel je het risico van het ***uitvindersdilemma***. Namelijk dat je investeert in een disruptieve technologie die enerzijds je klanten helpt met verbeterde dienstverlening, maar aan de andere kant kan leiden tot het kannibaliseren van je verdienmodel.

18.2.5 Andere relevante platformen

Naast deze platformen worden de volgende relevante platformen in het kort beschreven: Quorum, EOS, Ripple en Stellar.

In de eerste plaats is er ***Quorum ledger,*** gemaakt door JP Morgan en gebaseerd op Ethereum. Het gebruikt dus Ethereum-code, maar heeft dit naar de hand gezet om te voldoen aan de eisen van de eigen industrie. In dit geval voor financiële transacties. Zo zijn er bij Quorum bijvoorbeeld geen gaskosten en kan het updates die worden doorgevoerd bij het Ethereum-netwerk makkelijk doorvoeren naar het eigen systeem. Quorum heeft door samenwerking met Zcash zijn eigen vorm van Zero-Knowledge Prooftechnologie geïntegreerd om privétransacties tot stand te brengen. Externe toezichthouders hebben ook rollen gekregen binnen het Quorum-netwerk.

In de tweede plaats is er ***EOS*** dat in 2017 is geïntroduceerd. Deze goed gefinancierde publieke blockchain is net als Ethereum een blockchainplatform waarop applicaties worden ontwikkeld. Het is vrij schaalbaar door het Delegated Proof-of-Stake-consensusmechanisme. Vanuit publiek oogpunt is EOS opgericht door een commerciële partij, Block.one, en is er een beperkt aantal van 21 blokproducenten (witnesses), wat door sommigen als te gelimiteerd wordt gezien. Zeker voor consortia kan dit een argument zijn om zich niet te verbinden aan EOS. Het is daarentegen wel één van de schaalbaarste publieke blockchains.[208] Ook heeft het een eigen cryptovaluta genaamd EOS.

Een derde platform is ***Ripple,*** dat zich met de cryptovaluta XRP[209] richt op intervaluta en betalingsverkeer. Ripple is geen DAO maar onderdeel van de private onderneming, Ripple Labs. Ripple Labs werft financiële dienstverleners door een sneller en goedkoper globaal

[208] Zie ook paragraaf 6.4 voor meer informatie over Delegated Proof-of-Stake.

[209] XRP is de cryptovaluta van het Ripple-platform. De X staat hier voor het land van uitgifte van deze valuta. Omdat XRP geen land van uitgifte kent, wordt de X gebruikt. Zoals ook voor Bitcoin soms XBT gangbaar is.

blockchainalternatief op te werpen voor internationaal betalingsverkeer. Hiermee vormt het een bedreiging voor onder andere het bestaande SWIFT-systeem.

Ripple werd in 2012 onder andere opgericht door Jed McCaleb die in 2014 ***Stellar*** oprichtte binnen de Stellar Development Foundation. Stellar biedt net als Ripple betalingsinfrastructuur, maar richt zich ook op digitaal eigendom. Het Stellar-platform is een publieke blockchain en een DAO. Het werkt onder andere samen met Hyperledger Fabric om buitenlands betalingsverkeer te verzorgen met behulp van Stellar's token, XLM. SWIFT is hier, naast R3, mede bij betrokken.

18.3 Consortium

De drie eerdergenoemde grote platformen zijn opgezet door verschillende verbanden van samenwerkende partijen zoals Ethereum Enterprise Alliance, Linux/Hyperledger en R3. De partijen die hierbinnen samenwerken kunnen variëren van overheidsorganen, belangenorganisaties en onbekenden, tot aan toeleveranciers, klanten en directe concurrenten. Deze verbanden worden consortia genoemd als het een samenwerkingsvorm van blockchains betreft waarin de toetreders bekend zijn en specifieke rollen krijgen toebedeeld.[210]

Een stap verder is er de ***hybride blockchain***, een blockchain die verschillende elementen van een private blockchain combineert met elementen van een publieke blockchain. Binnen EEA wordt er bijvoorbeeld gebruikgemaakt van verschillende versies van Ethereum. Sommige zijn vrij open en decentraal, maar bevatten wel het permissioned element. Voor nu worden de termen consortium en hybride systemen geschaard onder de terminologie consortium, omdat de uitdagingen en aandachtspunten gericht op de Enterprise blockchain in grote lijnen overeenkomen.

18.3.1 Blockchainuitdagingen waarvoor bedrijven samenwerking als oplossing zien

De grote consortia richten zich op het ontwikkelen van toepassingen, standaarden en infrastructuur rondom een Enterprise blockchain om specifieke uitdagingen aan te kunnen. Een aantal van de uitdagingen waar bedrijven ten aanzien van blockchain mee worden geconfronteerd die door samenwerking het hoofd kunnen worden geboden, zijn als volgt.

[210] De andere relevante platformen die zijn genoemd zijn niet opgezet door consortia maar door private partijen, zoals JP Morgan, block.one, Ripple Labs en de Stellar Development Foundation.

In de eerste plaats is de wet- en regelgeving niet altijd duidelijk door de afwachtende houding van toezichthouders. Consortia delen hier kennis over en onderhouden via consortia actief contact met toezichthouders. Binnen internationale consortia spelen verschillen in nationale wetgevingen en de meer globale opzet van blockchains een rol. Zeker binnen Europa leidt dit tot complicaties, omdat je tot op zekere hoogte bovenop het overbruggen van geografische en culturele grenzen ook wettelijke begrenzingen binnen één platform coördineert. Hierbij zullen toezichthouders de vinger willen leggen op hoe consortia ervoor zorgen om binnen een multinationaal systeem voornamelijk de GDPR-wetgeving na te komen en data-uitwisseling te beperken.

Ten tweede is de technologie in ontwikkeling, waardoor er te weinig middelen kunnen zijn of te hoge risico's om blockchain alleen te implementeren. Samenwerking helpt om ontwikkelaarstalent te delen. Afspraken over interoperabiliteit, datastructuren, programmeertalen en dergelijke helpen de risico's te verkleinen van een te generiek of juist te complex systeem voor het specifieke bedrijf. Een bedrijf zal de eigen hard- en software voor zichzelf willen blijven afschermen, hoewel ook daar wellicht samenwerking mogelijk is.

Ten derde is een bedrijf niet zeker of het de kritische massa kan bereiken die nodig is voor adoptie en een stabiel presterend systeem. Deze kritische massa is door samenwerking met anderen wel te bereiken. Adoptie geldt zowel voor de klantenkring, als voor de eigen medewerkers binnen het bedrijf, gezien de impact die blockchain op de organisatie zelf heeft.

In lijn hiermee is een vierde aspect te benoemen. Blockchain kan het ecosysteem veranderen waarin zowel bekende als onbekende partijen samenwerken.[211] Blockchain geeft een kans op nieuwe businessmodellen die voordien niet voor de hand lagen. Deze businessmodellen maken al dan niet gebruik van de kans om data, die voorheen niet aanwezig of bruikbaar waren, te delen tussen en te vermarkten door de verschillende partijen. Dit hoeft niet alleen een bedrijf te zijn die de waarde van nieuwe data gebruikt, maar het kan bijvoorbeeld ook de klant zijn die de eigen gebruikersdata verkoopt. In dit licht kunnen sommige blockchainimplementaties ook worden gezien als een digitaliseringslag van een ecosysteem of waardeketen die informatiesystemen van bedrijven en organisaties op elkaar afstemt.

[211] In beginsel werken in een consortium partijen samen die elkaar kennen. In specifieke gevallen kan dit verband onder andere door de koppeling met publieke systemen uitgebreid worden tot een samenwerking met onbekende partijen.

Mogelijk wordt binnen het ecosysteem ook voorkomen dat een dominante speler ontstaat die, zoals in Web 2.0 gebeurfde, het blockchainsysteem naar de hand zet. Hiervoor is een open source netwerk, het liefst in combinatie met een publiek systeem, voor de eindgebruiker zelf een belangrijke voorwaarde.

18.3.2 Voorbeelden van consortia

Een voorbeeld waar verschillende uitdagingen door samenwerking worden aangegaan, is het Industrial Value Chain Initiative.[212] Deze Japanse groep van IoT-fabrikanten deelt informatie over de blockchain. Dit helpt zowel kleine als grote fabrikanten om productontwikkeldata, gebruik van productiemiddelen en kwaliteitsdata veilig en betrouwbaar te delen. Kleinere fabrikanten hoeven minder grote investeringen te doen in het verkrijgen van data. Zowel het verminderen van datalekken als het goedkoper delen van informatie worden beoogd. Zo hoef je geen data-integratiesysteem te bouwen om toch snel betrouwbare informatie te delen. Je kunt eenvoudig toetreden, terwijl je data wel veilig staan en je zelf bepaalt met wie je wat deelt. Alle partijen die meewerken, zetten transparant hun data neer, wat verkeerde data voorkomt. Degene die de data en de software onderhoudt, kan worden betaald via een cryptovaluta.

Andere voorbeelden van consortia zijn verbanden voor:

1. Verzekeringen (Blockchain Insurance Industry Initiative, B3i).
2. Energiehandel (VAKT, lid van EEA).
3. Transport (Blockchain in Transport Alliance, BiTA).
4. Internet of Things (TrustedIoTAlliance).
5. Trade finance (we.trade).
6. Mobiliteit (Mobility Open Blockchain Initiative, MOBI).

Zoals B3i en SWIFT laten zien, gebruiken dezelfde consortia of bedrijven meerdere platformen om blockchainsystemen te ontwikkelen en werken de grote drie platformen, EEA, Hyperledger en Corda, samen. Dit is omdat de platformen aan de ene kant qua ontwikkeling als stabiele technologie naar elkaar toegroeien, terwijl er aan de andere kant ook specialisatie ontstaat. Zo koos B3i voor de herverzekeringen initieel voor het gebruik van Hyperledger, omdat dit de meeste ontwikkelde technologie was. Toen Corda echter de achterstand inhaalde, maakte B3i alsnog de overstap naar Corda.

[212] Voor meer informatie, zie ‘100 Japanese manufacturers harness blockchain to share data’ (Matsui, 2019).

18.3.3 Uitdagingen waarmee een bedrijf binnen een blockchainconsortium wordt geconfronteerd

Naast de uitdagingen van blockchain, zijn er andere uitdagingen waar een blockchainconsortium rekening mee moet houden. Binnen blockchain staat samenwerking met andere partijen centraal. Voor deze samenwerking binnen een consortium is echter wel vertrouwen tussen de partijen noodzakelijk. Dit lijkt in tegenspraak met hoe blockchain initieel was opgezet door Satoshi Nakamoto, die vertrouwen in het systeem biedt in plaats van vertrouwen tussen de partijen. Een blockchainconsortium vertoont sterke gelijkenissen met andere samenwerkingsvormen, zoals bijvoorbeeld joint ventures.

In consortia kiezen partijen in beginsel voor samenwerking met een gelimiteerd aantal partijen van buiten de eigen organisatie, en dan het liefst partijen waar ze al mee samenwerken en die ze al vertrouwen. Hierbij vindt meer samenwerking plaats tussen concurrenten. De concurrenten waarmee je samenwerkt worden ook wel ***concullega's*** genoemd. In specifieke gevallen, of op langere termijn, wordt de samenwerking uitgebreid met onbekende partijen om van de voordelen van blockchain als netwerktechnologie te genieten. Om deze samenwerking te reguleren, zijn legale samenwerkingsovereenkomsten een belangrijk onderdeel van de beheersmaatregelen van een consortium. Hierbinnen worden onderwerpen aangesneden die zowel blockchain als niet-blockchain gerelateerd zijn, zoals:

1. Het onderling verdelen van de middelen en investeringen zoals ingebrachte kennis en intellectual property. Hierbij schuift de ontwikkeling van programma's door van bedrijven naar de consortia.
2. Het verzorgen van besluitvorming binnen een consortium. In hoeverre moet er een nieuw bedrijf worden opgericht waarin aandeelhouders vertegenwoordigd zijn? Hoe wordt de financiering geregeld en wat wordt de taakverdeling tussen het centrale orgaan en deelnemende bedrijven?
3. Het omgaan met fouten die worden gemaakt. Hoe moeten fouten worden gecorrigeerd? Welke sancties worden er gesteld als een partij nalatig is?
4. Het afschermen van bedrijfsgevoelige informatie, zoals die over klanten en processen. Hierbij dient te worden vermeld dat het zowel een voor- als nadeel is dat concurrenten bij elkaar in de keuken kijken, en mede inzicht geven in elkaars strategische prioriteiten, manier van denken en bedrijfsprocessen.[213]

[213] Dit is onderdeel van het zogenaamde ***coöptatiedilemma***, waarin samenwerkende concurrenten die op basis van onderkende voor- als nadelen van deze samenwerking constant afwegen in hoeverre samenwerking nut blijft hebben.

5. Het onderling delen van data en de waarde die deze data opbrengen. Denk bijvoorbeeld aan de waarde van persoonlijke data waarmee de partijen die samenwerken aan Corda gepersonaliseerde verzekeringspremies kunnen aanbieden.

Een blockchainconsortium is voor veel bedrijven een eerste stap om in een bredere context het verdienmodel en daarmee het businessmodel van een organisatie en zijn ecosysteem breder op te zetten en voortdurend aan te passen. In die zin moeten organisaties zichzelf aan kunnen passen aan het efficiënt samenwerken met gedistribueerde netwerken rondom onderlinge datadeling en toegang tot efficiënte marktplaatsen waarbinnen waarde wordt gedeeld.
Dit gaat verder dan het invoeren van een technologie of een update hiervan.

Als afsluitende uitdaging ondervinden samenwerkende bedrijven dat je niet makkelijk gedeelde bezittingen kunt waarderen en dat het lastig is om contracten te maken die de gecompliceerde interactie binnen een consortium volledig afdekken.

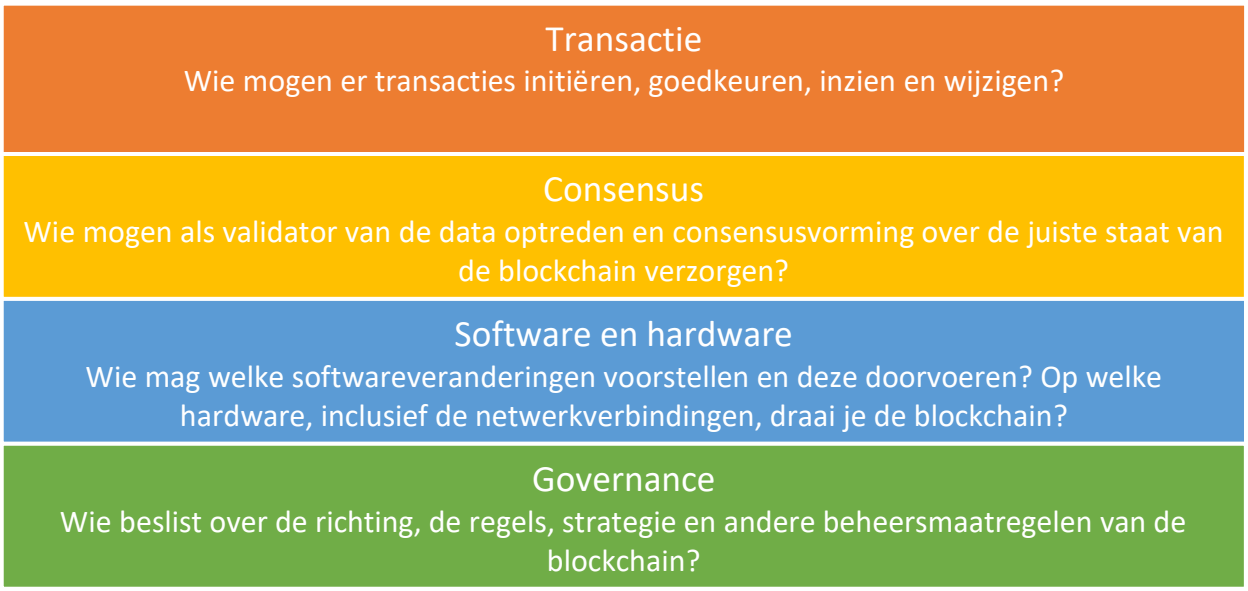
18.3.4 Rollen binnen een consortium

Een bedrijf heeft als individuele winstgeoriënteerde entiteit binnen een competitief en gereguleerd landschap een andere behoefte aan samenwerking dan een gemeenschap van gelijken. Een bedrijf heeft bijvoorbeeld specifieke behoeften aan veiligheid, prestatie, compliance en betrouwbaarheid.

Uit deze behoefte van bedrijven komt een meer centrale besturingsvorm voort. Hierbinnen neem je mensen aan, coördineer je het werk tussen de groepen mensen, controleer je het werk van de groepen en stimuleer je om de doelen van de totale groep na te streven. Zo bepaalt binnen een schildersbedrijf de eigenaar wie er tegen welke commerciële voorwaarden wordt aangenomen. De eigenaar bepaalt ook hoe hij de medewerkers motiveert tot betere prestaties, bijvoorbeeld door successen te vieren of variabele beloningen in te stellen.

Een bedrijf heeft dus de neiging om volledige controle te houden. Als ze mensen aannemen en werk coördineren, dan geven ze de voorkeur aan mensen die ze beter kennen om werk met hogere verantwoordelijkheid uit te voeren. Dit leidt ertoe dat een bedrijf veelal voor een permissioned private blockchain kiest. Binnen zo'n blockchain kan een bedrijf de toetreders en rollen vaststellen, wat de governance aanzienlijk vergemakkelijkt. Hierbij krijgt het bedrijf ook de kans om gegevens als klantnamen of bepaalde transacties van anderen afgeschermd te houden.

In paragraaf 9.3 werden de rollen binnen een blockchain als volgt ingedeeld:



Afbeelding 145: De vier aspecten waaraan je kunt deelnemen binnen een blockchain.

Deze rollen kunnen worden gecombineerd in profielen. Hierbij staat identiteitsmanagement centraal, in lijn met het organigram en partijen in het ecosysteem. Het ene profiel zal bijvoorbeeld zijn om de hardware te beheersen om een volledige geschiedenis van de blockchain bij te houden. In een ander profiel is een wallet met private en public keys nodig om transacties te verrichten.

Een indeling van de nodige profielen voor een bedrijfsnetwerk dat functioneert volgens wet- en regelgeving ziet er als volgt uit binnen het eigen netwerk:

1. Beslissers over beheersmaatregelen zoals een IT-manager, interne controleur, bedrijfseigenaar en algemeen directeur.
2. Systeembeheerder van de al bestaande informatiesystemen om de interactie met andere informatiesystemen te verzorgen.
3. Blockchainnetwerk operator die het netwerk beheert.
4. Blockchainontwikkelaar die aan de blockchainapplicatie werkt en daarmee werkt aan bijvoorbeeld het veiligheidsprotocol, het consensusmechanisme en de cryptografie.
5. Certificaatsautoriteit die de digitale certificaten uitgeeft, waarmee onder andere eigendom van een public key wordt aangetoond.
6. Validator die betrokken is bij consensusvorming.
7. Eindgebruiker die de transacties goedkeurt, initieert, inziet of wijzigt.
8. Regelgevende en instanties die toezicht houden binnen het land of een sector. (Hok, Fuentes, & Riviera, 2016)

Het coördineren van al deze verschillende rollen kan complex worden als de verantwoordelijkheden over een netwerk van bedrijven worden verdeeld. De rollen verschillen dan per node, per persoon, per bedrijf en per samenwerkingsvorm.

Ten aanzien van de regelgevende en toezichthoudende instantie is er al eerder gesproken over het verzorgen van besluitvorming binnen een consortium. Hierbij zijn verschillende vormen mogelijk, zoals het oprichten van een nieuw bedrijf, een joint venture, een stichting, enzovoorts.

18.4 Samenvatting, begrippen en bronnen

Samenvatting

Veel bedrijven die Enterprise blockchain invoeren, gebruiken hiervoor blockchainplatformen. Deze platformen zorgen ervoor dat je applicaties kunt schrijven met behulp van bepaalde technologieën. Zodoende kan je applicatie bijvoorbeeld samenwerken met andere applicaties, in een eigen of gedeelde programmeertaal, worden documenten bewaard of gedeeld en wordt toegang verkregen tot een bepaald netwerk. De drie meest vooraanstaande platformen zijn Ethereum, Hyperledger en Corda.

Elk platform heeft zijn eigen unieke eigenschappen. Zo is Ethereum in beginsel een publieke blockchain, biedt Hyperledger plug-and-play modules met behulp van verschillende technologieën en is Corda als DLT meer gespecialiseerd op financiële dienstverlening. De leden die zich hebben aangesloten bij een samenwerkingsverband rondom het ene platform zijn veelal ook lid van samenwerkingsverbanden rondom de andere platformen. De platformen zelf zijn open source.

De samenwerkingsverbanden worden consortia genoemd als het een samenwerkingsvorm van blockchains betreft waarin de toetreders bekend zijn en specifieke rollen krijgen toebedeeld. De samenwerkende partijen kunnen variëren van overheidsorganen, belangenorganisaties en onbekenden, tot aan toeleveranciers, klanten en directe concurrenten.

Consortia kunnen partijen helpen om vier uitdagingen te overwinnen. Ten eerste delen consortia kennis over en onderhouden ze actief contact met toezichthouders. Dit om onder andere de wet- en regelgeving duidelijk te krijgen. Ten tweede spreiden ze de risico’s door samen de middelen te delen om blockchainsystemen te ontwikkelen. Ten derde zorgen ze door samenwerking voor kritische massa om een stabiel presterend systeem geadopteerd te krijgen. En ten vierde nemen ze de kans om nieuwe decentrale samenwerkingsverbanden op te zetten

met vertrouwde en onvertrouwde partijen, zonder al te veel autonomie die blockchain biedt te verliezen. Denk hierbij specifiek aan concurrenten die met elkaar data gaan creëren en uitwisselen, of aan samenwerkingen met elkaars klanten en leveranciers.

Hiertegenover staat dat de partijen vooral in elkaar moeten vertrouwen om samen te werken. Meestal wordt dit vertrouwen afgedwongen door overeenkomsten te maken over middelen, besluitvorming, sancties, bedrijfsgevoelige informatie en onderlinge datadeling.

Opmerkingen die je nu kunt uitleggen

- Gezien de nood tot standaardisatie en de voordelen van datadeling, zullen blockchain consortia een steeds grotere rol gaan spelen binnen ecosystemen van bedrijven.
- Het is voor bedrijven lastig om in een consortium te stappen, om er blijvend mee samen te werken en om een consortium te verlaten. Toch hebben bedrijven grote voordelen bij deelname aan een consortium.
- Bedrijfsconsortia wegen schaalbaarheid, veiligheid en decentralisatie af in het zoeken naar waardecreatie via blockchain en Distributed Ledger Technologie.
- Verschillende consortia blijven waarschijnlijk naast elkaar bestaan. Interoperabiliteit binnen en tussen consortia speelt hierbij een belangrijke rol.
- BaaS is voor bedrijven zonder grote middelen een alternatief om laagdrempelig met blockchainsoftware aan de slag te gaan.
- Het is nog te vroeg om te zien wat de gevolgen zijn als massaal geadopteerde publieke en private systemen bij elkaar aansluiting vinden.

Verklarende begrippenlijst

Blockchain-as-a-Service (BaaS): Diensten van een derde partij om bedrijven te helpen hun blockchainoplossingen via de cloud te bouwen en uit te rollen.

Blockchainplatform: Technisch platform waarop je smart contracts en applicaties kunt schrijven met behulp van bepaalde technologieën. Bekende platformen zijn Ethereum, Hyperledger en Corda.

Casper: Set van updates om Ethereum de overgang te laten maken van een Proof-of-Work naar een Proof-of-Stake consensusmechanisme. Het doel is om naast schaalbaarheid, het netwerk ook veiliger en milieuvriendelijker te maken.

Chaincode: Smart contractslaag dat door Hyperledger wordt gebruikt.

Concullega: Concurrent waar je mee samenwerkt alsof het een collega is.

Consortium: Geheel van samenwerkende bedrijven rondom een blockchain dat veelal permissioned netwerken gebruikt.

Coöptatiedilemma: Het dilemma waarbij concurrenten die op basis van onderkende voor- en nadelen van een samenwerking constant afwegen in hoeverre de samenwerking nut blijft hebben en of ze uit de samenwerking moeten stappen of niet.

Corda: DLT-platform voor financiële dienstverleners, ontwikkeld door R3.

Cordapp: dApp op Corda.

EOS: EOS is een goed gefinancierde publieke blockchain en is net als Ethereum een blockchainplatform waarop applicaties worden ontwikkeld. Het is schaalbaar door het Delegated Proof-of-Stake-consensusmechanisme.

Ethereum Enterprise Alliance (EEA): Groep van samenwerkende bedrijven om Ethereum te gebruiken voor Enterprise blockchain.

Ethereum Virtual Machine (EVM): Een gedecentraliseerde virtuele machine die scripts kan uitvoeren. EVM's zorgen voor de computaties op het Ethereum-netwerk. Smart contracts die worden geschreven in Solidity worden gecompileerd in 'bytecode' die kan worden gelezen en uitgevoerd door de EVM. Elke node op het netwerk bevat een EVM en compileert en voert smart contracts uit.

Gas: Transactiekosten die je betaalt om een transactie op de Ethereum blockchain uit te voeren.

Hybride blockchain: Blockchain die verschillende elementen van een private blockchain combineert met elementen van een publieke blockchain. Binnen EEA wordt er bijvoorbeeld gebruikgemaakt van verschillende versies van Ethereum. Sommige zijn vrij open en decentraal, maar bevatten wel het permissioned element.

Hyperledger: Open source samenwerkingsverband, geleid door Linux, rondom het ecosysteem van Hyperledgerraamwerken. Het doel van Hyperledger is om blockchaintoepassingen te ontwikkelen die kunnen worden gebruikt door bedrijven.

Interoperabiliteit: De mogelijkheid om blockchains met elkaar te laten communiceren en informatie te delen.

Linux Foundation: Non-profit technologieconsortium dat open standaarden ontwikkelt voor het Linux besturingssysteem. Het ondersteunt tevens open source softwareprojecten waaronder Hyperledger.

Plasma-initiatief: Een schalingsoplossing waarbij er side chains (child chains of plasmachains) worden gemaakt die gekoppeld worden aan de hoofdchain (root chain). Je kunt side chains zien als nieuwe blockchains die regelmatig hun staat naar de hoofdchain sturen. Plasma is dus een netwerk van blockchains die gelinkt zijn aan de hoofdchain.

Quorum ledger: Een blockchain gebaseerd op Ethereum en ontwikkeld door JP Morgan.

R3: Organisatie die Corda ontwikkelt.

Ripple: Een privaat blockchainalternatief dat zich richt op intervaluta en betalingsverkeer.

Roll-backfunctie: Functie om verrichte registraties op een blockchain terug te draaien tot aan een bepaalde originele staat van de blockchain.

Sharding: Een schalingsoplossing waarbij de blockchain wordt opgesplitst in partities, ook wel “shards” genoemd. Elke shard krijgt dan een eigen transactiegeschiedenis, zodat de nodes die een shard onderhouden alleen de transacties hoeven te verwerken die relevant zijn voor de shard. Het is wel van belang dat er voldoende nodes binnen de subset transacties verifiëren, zodat het systeem veilig is.

Stellar: Stellar biedt net als Ripple betalingsinfrastructuur, maar richt zich ook op digitaal eigendom. Het Stellar-platform is een publieke blockchain en een DAO.

Uitvindersdilemma: Er kan sprake zijn van een uitvindersdilemma binnen samenwerkingsverbanden. Aan de ene kant investeer je in een disruptieve technologie die je klanten helpt met verbeterde dienstverlening, maar aan de andere kant kan het leiden tot het kannibaliseren van je verdienmodel als je de concurrerende krachten van andere bedrijven verbetert.

Punt-naar-punt: Bij punt-naar-puntcommunicatie wordt elk bericht geadresseerd aan de partij voor wie het bedoeld is. Dit waarborgt dat transacties alleen worden gedeeld tussen partijen die bij deze transactie betrokken zijn en anoniem worden gehouden voor anderen. Dit betekent ook dat een transactie niet in een datablok wordt geplaatst in een gedeelde database. Consensus kan hiermee worden verkregen op transactieniveau.

Vendor lock-in: Een leverancier maakt een klant afhankelijk voor zijn producen en diensten, omdat de klant niet in staat is om van leverancier te veranderen zonder substantiële omschakelingskosten of andere ongemakken. Hierbij wordt vaak opgemerkt dat doordat IBM een grote rol speelt binnen Hyperledger Fabric, het lastiger wordt om een andere leverancier dan IBM te gebruiken.

Bronnen

Del Castillo, M. (2019, 10 december). Blockchain 50: Billion Dollar Babies. Geraadpleegd op 23 december 2019, van Forbes website: https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/

Fersht, P. (2018, 16 maart). The top 5 enterprise blockchain platforms you need to know about. Geraadpleegd op 23 december 2019, van Horses for Sources website: https://www.horsesforsources.com/top-5-blockchain-platforms_031618

Hok, D., Fuentes, B., & Riviera, J. U. G. (2017, 6 maart*). IBM Bluemix Nice Meetup #4-20170302 6 Meetup @INRIA - BlockChain*. Geraadpleegd op 23 december 2019, van Slideshare.net website: https://www.slideshare.net/IBMFranceLab/ibm-bluemix-nice-meetup-420170302-6-meetup-inria-blockchain

Hyperledger. (2019) Business Blockchain Frameworks & Tools Hosted by Hyperledger. Geraadpleegd op 23 december 2019, van Hyperledger website: https://www.hyperledger.org/

Matsui, M. (2019, 16 juni). 100 Japanese manufacturers harness blockchain to share data. Geraadpleegd op 23 december 2019, van Nikkei Asian Review website: https://asia.nikkei.com/Business/Business-trends/100-Japanese-manufacturers-harness-blockchain-to-share-data

Shen, M. (2019). *Developer Report. January - June 2019.* Geraadpleegd van Electriccapital.com website: https://www.electriccapital.com/developer_report_H1_2019_pdf

Nawoord

Blockchain-technologie staat gezien de adoptietijd van voorgaande technologieën nog steeds in de kinderschoenen. De parallellen van blockchain met internet technologie zijn al genoemd. In die zin is e-mail net geïntroduceerd en wachten we totdat blockchain en dApps grootschalig worden gebruikt. Belangrijk hierbij is dat standaarden worden afgesproken tussen samenwerkende organisaties. Op globaal niveau willen we alle blockchains uiteindelijk aan elkaar knopen om iedereen de kans te geven van het Internet of Value gebruik te maken. Hiervoor zullen de verschillende blockchains die blijven bestaan met publieke blockchains worden verbonden, leidend tot een groot netwerk zoals internet ooit bestond uit kleinere individuele netwerken.

Ook wij verwachten dat we aan de vooravond staan van mainstream adoptie. Gartner voorspelt dat grote bedrijven steeds meer blockchain gaan toepassen en de technologie in 2025 zover is dat het convergeert met andere complementaire technologieën als het Internet of Things, kunstmatige intelligentie en gedecentraliseerde Self-Sovereign Identities. Blockchain zal volgens Gartner tegen 2030 $3,1 biljoen USD aan nieuwe business waarde creëren.

Hoe dan ook zorgen de ontwikkelingen ervoor dat mensen vertrouwd raken met het decentrale denken. Mensen zullen door de decentrale mindset eerder decentrale alternatieven bedenken voor centrale systemen die ze nu bijvoorbeeld al kennen binnen het onderwijs, politiek, geldproductie, pensioenregelingen en businessmodellen. Dit past in een trend waarin er meer wordt vertrouwd op peer-to-peer communicatie. Daarnaast zorgen platform businessmodellen als Airbnb en Uber ervoor dat de samenleving al meer bekend raakt met decentralisatie. Iedereen kan op Airbnb immers een woonruimte aanbieden en iedereen kan op Uber een autorit aanbieden. Blockchain belooft echter nog verder te gaan door gebruikers in staat te stellen direct peer-to-peer diensten te verlenen en met elkaar samen te laten werken. Hierbij zullen we een verdere verplatting van de organisatie zien.

Blockchain is een veelbelovend onderdeel van opkomende technologieën die ieder op de schouders staat van het werk en inzicht van veel individuen. Het is een combinatie van eerdere technologieën zoals het internet, cryptografie en gedistribueerde computersystemen die zichzelf hebben bewezen. Blockchain is een originele gedachte die nieuwe ideeën voorbrengt, sociologische verbeeldingskracht stimuleert en de kans biedt om welbedoelde ideologieën van decentralisatie ten uitvoer te brengen.

Graag willen we gezamenlijk de volgende personen danken voor de ondersteuning die we kregen tijdens het maken van het boek.

Sander Reinderink, Tekla van Marle, Jurgen Scheffer en Bert Velt voor de prachtkans een boek te mogen maken, voor het organiseren van het Blockchain Lectoraat op Saxion en het constante enthousiasme. Bedankt!

Jan Veuger, Christa Barkel en Joris Heuven voor de steun vanuit ons Blockchain Lectoraat; zowel organisatorisch, inhoudelijk als moreel. Bedankt!

Misha de Boer, Michael Damen en Remko van Yperen voor hun vele feedback op ons werk. Bedankt!

Kjell Heinenbernd, Niek Horstman, Tom Kleine, Lesly ter Heerdt, Mart Swensson, Tom Bruggink, Pim van Kaam, Michel Koop, Iris Diender, Jochem Schmaloer en Erik Horsthuis voor hun opmerkingen en feedback op het boek. Bedankt!

En natuurlijk onze dank aan Satoshi Nakamoto en alle anderen op wiens schouders we staan, de vele grote denkers, de vele grote doeners, alles grijpt op elkaar in, open source werkt. Bedankt!

Dankwoord Chhay Lin

Mijn dankwoord gaat uit naar alle cryptoanarchisten, cypherpunks en andere blockchainpioniers die de wereld een zodanig disruptieve technologie hebben geboden dat de wereld radicaal in betere zin zal gaan veranderen. Verder bedank ik mijn familie: Im, Lok, Lang, Chhay Lem en Chaneng. Ook wil ik mijn steun en toeverlaat, Nicole, bedanken.

Dankwoord Arthur

Mijn dochters, voor het gedartel rond mijn hoofd en mijn voeten op de momenten dat ik er niet om vroeg, maar het wel nodig had.
Voor mijn vrouw, mijn lieve lieve vrouw die mijn werk las en die links en rechts de ballen opving die vielen toen ik er weer niet was, fysiek of mentaal.
En natuurlijk mijn moeder. Het verbaasde me altijd enigszins dat Oscar winnaars vaker de moeders bedankten dan de vaders. Maar het verbaast ook weer niet als je de paar regels hierboven nogmaals leest. Als ik terugkijk naar de gelukkige uitgangspositie om de mooie kansen die het leven schonk te nemen, dan kijk ik terug naar één vrouw die me in die positie stelde. Bedankt mam, bedankt Mer, bedankt Fem en Lente!