De Kracht van Blockchain

De Kracht van Blockchain

Systematiek van de toekomst

Timo Baldwin en Marcel Sanders

ISBN: 9789463672948

Eerste druk, december 2018

Technische redactie: Thomas Kemmere

Coverontwerp: Tjasker Design

Uitgegeven via Mijnmanagementboek.

INHOUD

Voorwoord

De kracht van Blockchain is geschreven voor alle geïnteresseerden in blockchain-technologie die het de tijd ontbreekt om aan dit onderwerp een hele studie te wijden. Dit boek gaat over de mogelijke impact die blockchain kan hebben op jouw sector, organisatie of bedrijf. En hoe ga je hier dan mee om? Blockchain, een vorm van gedistribueerde grootboek-technologie, opent nieuwe wegen voor samenwerking, interactie, verslaglegging en bescherming van gegevens en identiteit. Het is onze overtuiging dat Blockchains vroeg of laat impact hebben op vrijwel elke sector of ieder vakgebied.

Dit boek is geschreven op een toegankelijke wijze en zonder al teveel onnodige technische verdieping. Een bagage aan technische kennis is daarom niet vereist. Het doel is om de lezer in korte tijd een volledig beeld te geven van blockchain-technologie, zodat hij kan meedenken, meepraten en uiteindelijk het besluitvormingsproces op de juiste wijze kan uitvoeren om blockchain optimaal in te zetten voor het bedrijf.

De kracht van Blockchain neemt u mee op reis door de wereld van de blockchains. Dit doen we aan de hand van het uiteenzetten van de karakteristieken van een blockchain. Wat is het, wat doet het en wat kunnen we ermee? We zullen laten zien dat een blockchain voor een groot deel haar bijzondere eigenschappen te danken heeft aan cryptografische toepassingen. In de hoofdstukken 'cryptografie' en 'hashing technieken en transacties' zullen we deze bijzondere eigenschappen uitleggen en de toepassing ervan laten zien. Aan de hand van de twee bekendste blockchains, Bitcoin en Ethereum, laten we zien dat blockchain al een praktische toepassing is en we bespreken met name het fenomeen smart contracts en cryptocurrencies.

De komst van blockchain-technologie heeft impact op veel fronten. Op sociaal maatschappelijk en economisch gebied zullen instanties de voor- en nadelen moeten afwegen en hier adequaat op moeten inspringen. In de laatste hoofdstukken nemen we de mogelijke toepassingen van

blockchain door en spreken we een verwachting uit over de snelheid van doorontwikkeling van deze technologie.

Waarom het belangrijk is om je te oriënteren op deze technologie?
Voor organisaties is het van belang dat ze zich bewust blijven van hun toegevoegde waarde en de beschikbare technologie om deze waarde zo efficiënt en effectief mogelijk in te zetten. Voor veel organisaties zullen de toepassingen van blockchain een aanzienlijke impact hebben op de huidige strategie en/of bedrijfsvoering. De technische aspecten van blockchain zullen breed omarmd worden zowel vanuit defensief als offensief perspectief.

Veel multinationals doen inmiddels pilots of gaan samenwerkingsverbanden aan met blockchain-initiatieven. Door het lezen van dit boek kun je zelf een oordeel vormen over wat de impact van blockchaintechnologie kan zijn op jouw organisatie. Wij denken dat organisaties die stil toekijken de boot gaan missen. Dit hoeft niet te gebeuren als je de tijd neemt om vast te stellen of blockchain voor jouw organisatie kan gaan werken. Uiteindelijk kun je niet om blockchain-technologie heen. Laat dit boek je gids en inspiratiebron zijn. Wij wensen je veel plezier toe met het lezen van dit boek.

Timo Baldwin
Marcel Sanders

Inleiding

Informatie- en communicatietechnologie verandert in een razend tempo. Nooit eerder volgden vernieuwingen in deze technologie elkaar zo snel op. Dit wordt veroorzaakt door de enorme technologische vooruitgang van computertechnologie en de beschikbaarheid van internet alom. Dit maakt het mogelijk om bruikbare en nuttige technologie dicht bij de mens te brengen. Toch is het niet zozeer de technologie zelf die het meest radicaal is maar de snelheid waarmee de vernieuwing en verspreiding plaatsvindt. Kijken we naar de vooruitgang in de afgelopen eeuwen dan is er sprake van een sneeuwbaleffect.

In de tweede helft van de achttiende eeuw, van ongeveer 1760 tot ongeveer 1840 vond de zogenoemde eerste technologische revolutie plaats. Handenarbeid werd gemechaniseerd en werkplaatsen groeiden uit tot fabrieken. De ontwikkeling van de stoommachine vormde een belangrijke oorzaak voor deze revolutie. De technologische revolutie die daarop volgde vond plaats tussen het einde van de negentiende eeuw en het begin van de twintigste eeuw en liep door tot aan de start van de Eerste Wereldoorlog. Het was de periode van doorontwikkeling waarbij olie als brandstof zijn intrede deed als belangrijke accelerator. Het gebruik van elektriciteit en olie zorgde voor de mogelijkheid van massaproductie van goederen.

Vanaf de jaren zestig van de twintigste eeuw deed de digitale (de derde) revolutie zijn intrede. De ontwikkeling van halfgeleiders leidde tot bedrijfsmatig gebruik van computers waarna in de jaren zeventig en tachtig de personal computer zijn intrede deed. Dat brengt ons bij de vierde (technologische) revolutie waarin we momenteel verkeren. Deze revolutie is gestart rond de eeuwwisseling waarbij vrijwel iedereen in de westerse wereld toegang kreeg tot het internet en waarbij de portabiliteit van apparaten toenam. Nagenoeg iedereen kreeg hierdoor permanent toegang tot het internet. We zien in deze revolutie nieuwe sectoren en activiteiten ontstaan waarbij de toepassing via internet centraal staat. Gebruik van social media, de toepassingsmogelijkheden die drones met zich meebrengen en applicaties op smart telefoons zijn hiervan de meest

in het oog springende voorbeelden. Door het beschikbaar komen van dit mobiele internet en alle mogelijkheden die dat met zich meebrengt ontstaat een wereld waarbij we ons frequent en intensief bezig houden met een van onze digitale apparaten.

Veel digitale activiteiten zijn opgezet vanuit het oude denkbeeld en de oude procesgang. Het digitale beheer van gegevens is toe aan een nieuwe visie waarbij meer en meer de vraag opkomt of het bewaken van gegevens in één centrale database nog de beste oplossing is. De eisen aan het beheer van persoonlijke gegevens van derden worden strenger door wetgeving. Nu de mogelijkheden er zijn voor een gedecentraliseerd alternatief zal het centrale paradigma onder de loep genomen worden.

Het is goed mogelijk dat blockchain-technologie als synoniem voor decentralisatie een van de bepalende factoren wordt van deze vierde revolutie. Blockchain-technologie zal haar bijdrage leveren aan het decentraliseren van waarde voor de consument. Tussenpersonen die onvoldoende waarde toevoegen binnen een transactieketen zullen worden gepasseerd. Bescherming van persoonsgegevens wordt steeds moeilijker door toepassing van centrale databases en dit zal worden vervangen door gedecentraliseerde technologie met cryptografische beveiliging. De consument zal meer en meer aan het roer komen te staan van zijn digitale identiteit en zijn activiteiten. Kortom een ware revolutie, de revolutie van de digitale consument.

Een revolutie heeft in veel gevallen ook een schaduwzijde. Een abrupte verandering kan maatschappelijke ontwrichting met zich meebrengen. Wat zijn de sociale gevolgen van deze versnelling? Hoe gaan we om met een steeds verdere automatisering van processen door onder andere blockchain-technologie? Blockchain heeft wellicht daardoor gevolgen voor de werkgelegenheid.

Deze vierde technologische revolutie gaat, in vergelijking met de eerste drie, naar verwachting misschien wel de grootst sociaal maatschappelijke impact hebben. Instanties moeten op de afzonderlijke maatschappelijke vraagstukken antwoorden gaan formuleren. Hoe snel dit gaat en hoe lang deze revolutie duurt is onzeker, maar wij raden iedereen aan om voor

zichzelf een beeld te vormen van de mogelijkheden en bijkomende vraagstukken die blockchain-technologie met zich meebrengt.

Blockchain 1

Het internet is een mondiaal systeem van onderling verbonden computers. Deze computers werken samen via diverse protocollen. Deze protocollen zijn de afspraken over hoe computers onderling met elkaar informatie uitwisselen.

Het internet komt voort uit een wens van het Amerikaanse ministerie van defensie. Computers waren enorm kostbaar en men zocht naar een manier om informatie op computers met elkaar te delen en ze met elkaar te laten communiceren. Vanuit deze gedachtegang werd aan het einde van de jaren zestig het ARPANET opgericht. Het huidige internet is een doorontwikkeling van dit ARPANET. Het is een mondiaal systeem van verbonden computernetwerken die informatie uitwisselen via bepaalde protocollen. Twee van die belangrijke protocollen zijn het Transmission Control Protocol (TCP) en het Internet Protocol (IP).

Met behulp van het TCP/IP-protocol wordt data of informatie opgeknipt in verschillende pakketjes die worden verstuurd naar de ontvanger. Deze ontvangende computer bundelt de pakketjes en voegt deze weer samen tot het originele bericht, zoals deze was voor het versturen. Mocht een pakketje verloren gaan en niet aankomen dan zal het pakketje na een wachttijd opnieuw worden verstuurd. Dit proces gaat door totdat alle pakketjes zijn aangekomen. Als onderweg computers uitvallen dan wordt geprobeerd om de informatie, eventueel via een andere route, alsnog te bezorgen op de eindbestemming.

Gedecentraliseerde systemen

Het internet werkt zodoende als een gedecentraliseerd netwerk. De verschillende communicatieprotocollen zorgen ervoor dat informatie uitgewisseld kan worden tussen verschillende computers of computernetwerken.

Het internet is een van de grootste uitvindingen van de vorige eeuw. De afgelopen dertig jaar is door de komst van het internet een enorme hoeveelheid gratis informatie beschikbaar gekomen. Steeds meer bedrijven hebben businessmodellen ontwikkeld die in grote mate mogelijk gemaakt zijn door de komst van het internet.

Diensten die worden aangeboden op het internet zijn in veel gevallen in handen van private partijen. Deze partijen hebben de zeggenschap en het beheer over deze data die via dit kanaal ter beschikking wordt gesteld. Grote namen als Google, Facebook en Amazon bepalen in grote mate de regels op de digitale snelweg en niet de consument. Daarnaast zien we ook veel partijen die aan de haal gaan met persoonlijke data van internetgebruikers. In dit tijdperk kunnen we stellen dat data het nieuwe goud is. Het is van belang dat mensen zich er bewust van zijn dat informatie veelal in handen is van zakelijke ondernemingen.

In de praktijk zien we dat het internet ervoor kan zorgen dat de consument zich snel kan verenigen. Onvrede over maatschappelijke ontwikkelingen of misbruik van toevertrouwde data resulteren vrijwel direct in tegenreacties bij de consument.

De mogelijkheid van het beheren van eigen decentraal opgeslagen data zet de consument weer aan het stuur. Blockchain-technologie zou hierin kunnen ondersteunen. Blockchain is een gedeeld up-to-date grootboek dat via een peer-to-peer netwerk wordt gedeeld en waarbij mutaties niet kunnen worden aangepast. Peer-to-peer wil zeggen; directe communicatie tussen computers.

Gefaseerde invoering van het internet

Hoewel het internet nog vrij jong is kunnen we al spreken van enkele fases in de ontwikkeling ervan. De eerste fase, die tot ongeveer 2005 duurde, wordt het informatieve web genoemd waarbij voornamelijk informatie tussen partijen werd gedeeld. Via *platte* webpagina's werd informatie beschikbaar gesteld of gepushed naar het domein van de lezer, dit is de 'read'-fase. Van interactie of bewerking was geen sprake en men kon alleen passief informatie bekijken. Transacties waren sowieso niet mogelijk in deze eerste periode.

Dat werd anders in de daaropvolgende fase van het internet waarin 'tussenpersonen' diensten aanboden op het web. Door tussenkomst van deze bemiddelende (tussen)partijen ontstond de mogelijkheid om aangeboden informatie te wijzigen dan wel er iets aan toe te voegen. Deze wijzigingen werden door de tussenpersonen in een gecentraliseerde omgeving verwerkt en opgeslagen. Dit is de 'read/write'-fase via zogenaamde makelaars. In deze fase was meer interactie mogelijk waarbij iedere gebruiker informatie kon up- en downloaden. Met deze fase ontstonden eveneens nieuwe ondernemingen met dienstverlening via apps en verschillende social media platforms. En ondanks dat social media als dienst gratis wordt aangeboden betaal je een hoge prijs door het beschikbaar stellen van privédata. De tussenpersonen, makelaars in private data, zagen in dat data voor veel geld kon worden doorverkocht aan commerciële partijen. De handel in data nam hierdoor enorm toe.

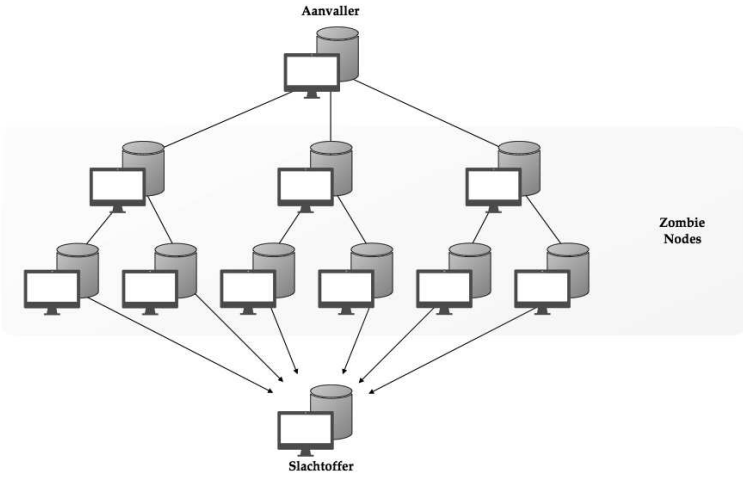
Met de blockchain-technologie kan de derde fase van het internet worden ingezet. Namelijk een internet met een *read én write* functie *zonder* de tussenkomst van *een bemiddelaar*, de tussenpersoon. Met blockchain-technologie kunnen we (peer-to-peer) direct onderling afspraken maken en uitvoeren met onze tegenpartij, zonder dat hier een bemiddelaar bij betrokken is. Dit geldt dan niet alleen voor informatiebewerkingen maar ook voor transacties, vastlegging van (eigendoms-)rechten of het effectueren van contractafspraken en het uitwisselen van waarde. Tussenpersonen die door blockchain-technologie geraakt kunnen worden zijn bijvoorbeeld banken, notarissen of markt-makers.

Netwerksystemen

Zoals je hierboven hebt kunnen lezen is een blockchain een gedecentraliseerd netwerk. Om te beschrijven wat een gedecentraliseerd netwerk is bekijken we ook de overige manieren van systeemnetwerken.
De tegenhanger van een gedecentraliseerd netwerk is een gecentraliseerd netwerk. In een gecentraliseerd netwerk vindt alle sturing en beheer plaats vanuit één punt. Wijzigingen in data, beheer en opslag vindt plaats op één locatie. De zeggenschap en het eigenaarschap zijn eveneens belegd bij één partij.

Een gecentraliseerd netwerk heeft voordelen. Wijzigingen kunnen snel worden doorgevoerd en beheer is eenduidig belegd. Het nadeel van centraal gegevens beheren is de kosten die de bescherming van deze data met zich meebrengen. Een centrale omgeving kent een *single point of failure,* wat wil zeggen dat het binnen dit ene punt ook mis kan gaan. Censuur, controle, uitsluiting, misbruik, (per ongeluk) lekken of verwijderen van gegevens behoren tot de mogelijkheid. Iets wat zonder adequaat controlesysteem misschien niet eens opgemerkt hoeft te worden. Privacygevoelige informatie kan daardoor in verkeerde handen terecht komen of nog erger, gemuteerd worden met alle gevolgen van dien. Een tweede nadeel is de beschikbaarheid van data in een centrale database. Voor vijandige hackers is het eenvoudig om alle pijlen te richten op dit ene punt waarmee het systeem traag wordt en in sommige gevallen helemaal niet meer toegankelijk is voor de buitenwereld. Een veel beproefde methode is een d-dos aanval (distributed denial of service attack) waarmee het netwerk op vijandige wijze tijdelijk wordt platgelegd. In een d-dos aanval wordt gelijktijdig vanuit een veelheid van verschillende locaties informatie opgevraagd bij één centrale omgeving.

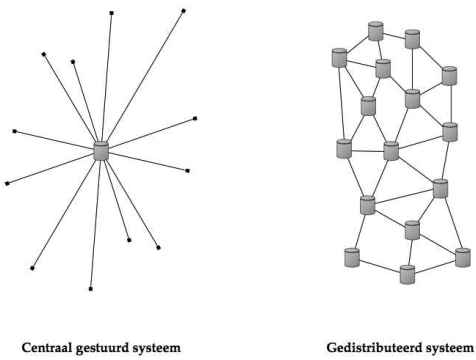
Een gedeeltelijke oplossing hiervoor is om deze ene locatie, deze ene computer/node, te vervangen door meerdere computers/nodes. Dit is het kenmerk van een gedecentraliseerd systeem. Op meerdere plekken wordt het netwerk beheerd en gecontroleerd. Een aanval op één punt zal daarom niet succesvol zijn, andere nodes blijven namelijk hun netwerkfunctie uitoefenen.



Schematische weergave DDOS aanval

Vormen van netwerken

Blockchain-technologie, ook wel *distributed ledger technologie (DLT)* genoemd, voert dit principe helemaal door. Binnen *distributed ledger technologie* is geen centrale autoriteit aanwezig en daarmee geen centrale sturing. Het netwerk is volledig gedecentraliseerd waarbij geen enkele sprake meer is van centralisatie, zelfs niet op gedeeltelijke schaal. Alle deelnemers zijn gelijkwaardig en kennen geen hiërarchie.

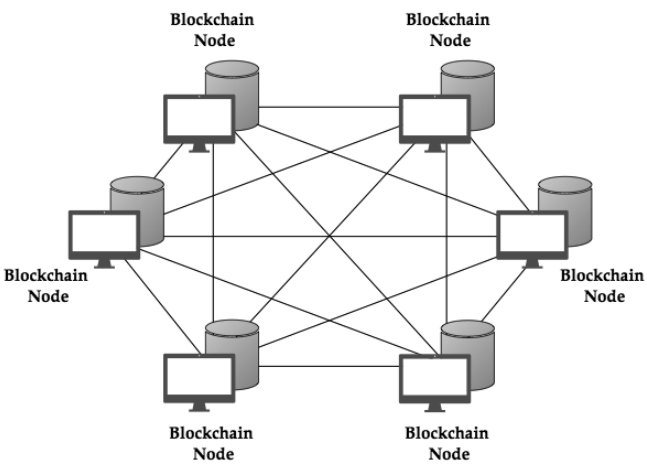


Twee uiterste vormen van netwerksystemen

In een gedecentraliseerd systeem werken de nodes samen om via een gedeeld protocol te komen tot interactie met elkaar. Een gedistribueerd systeem is een volledig doorgevoerde vorm van decentralisatie. De nodes geven over en weer transacties aan elkaar door en werken samen aan overeenstemming, oftewel consensus, in dit grootboek. Deze consensus wordt bereikt over de laatst bekende, actuele status van het grootboek.

Peer-to-peer systemen

Een *peer-to-peer netwerk* is een netwerk van computers, ook wel nodes genoemd, die op gelijkwaardige wijze informatie met elkaar uitwisselen. Het woord 'Peer' komt uit het Engels en staat voor 'gelijke'. De uitwisseling van informatie binnen een peer-to-peer netwerk verloopt volgens een vastgesteld communicatieprotocol. Samen komen ze tot een identieke status van het netwerk, in het geval van blockchain, tot identieke status van het openbaar grootboek.



Peer-to-Peer netwerksysteem