# Virtuele valuta

Onder invloed van blockchaintechnologie zijn er de laatste jaren diverse virtuele valuta geïntroduceerd in aanvulling op nationale munteenheden. In hoeverre worden deze munten ook gebruikt voor het dagelijkse betalingsverkeer? En hoe kan voorkomen worden dat deze valuta worden gebruikt voor criminele activiteiten?

ONDERNEMERSCHAP & INNOVATIE

# De betekenis van blockchain

Zoals internet in 1994 de wereld op zijn kop zette, doet blockchain dat de komende jaren. Of blockchaintechnologie daadwerkelijk zo'n impact zal hebben op de samenleving is nog onderwerp van discussie, maar de potentie is er. Hoe werkt het, wat is de kracht ervan en welke toepassingen staan al op de rails?

**MAARTEN EVERTS**
*Onderzoeker bij TNO en universitair docent bij de Universiteit Twente*

Een wonderlijke combinatie van cryptografie, gedecentraliseerde computernetwerken, speltheorie en economische theorie – dat is blockchain. Eenvoudig gezegd gaat het om een gedistribueerd grootboek dat niet op één computer staat, maar op de verschillende deelnemende computers verspreid over de wereld. Dat is meteen de kracht van blockchain. Een deelnemer kan wel proberen voor eigen gewin transacties te manipuleren, maar de andere aangesloten computers nemen deze wijzigingen niet over. Aangespoord door slimme economische prikkels houden die elkaar continu in de gaten en bewaken ze gezamenlijk de correcte toestand en geschiedenis van het gedeelde grootboek.

In de klassieke situatie is een grote transactie alleen mogelijk door tussenkomst van bijvoorbeeld een bank of een notaris. Dat geeft een klein aantal partijen relatief veel macht. Blockchaintechnologie kan ervoor zorgen dat personen en organisaties minder op dergelijke tussenpersonen hoeven te vertrouwen. Doordat blockchain hun dienstverlening geheel of gedeeltelijk overbodig maakt, zijn transacties via blockchain mogelijk efficiënter, goedkoper en sneller.

Elke econoom die adviseert over investeringsbeslissingen, handelsprocessen monitort of de uitwerking van wetgeving analyseert, krijgt vroeg of laat met blockchaintechnologie te maken. Des te belangrijker is het om te leren wat blockchain inhoudt en om de ontwikkelingen te volgen.

## VIER LAGEN

Een blockchain bestaat uit een *peer-to-peer*-netwerk van computers van verschillende eigenaren, die elkaar mogelijk niet allemaal vertrouwen of die verschillende belangen hebben. Maar toch kunnen ze samenwerken om overeenstemming te krijgen over een continu veranderende gedeelde realiteit. Bij de bitcoinblockchain is dat bijvoorbeeld wie op dat moment eigenaar is van welke bitcoin. Om die samenwerking voor elkaar te krijgen, draait op elk van de computers in het netwerk een kopie van blockchainsoftware, waarin is vastgelegd hoe wordt samengewerkt.

Om de technische aspecten van blockchainsoftware in kaart te brengen is een vierlagenmodel erg geschikt. Zo zijn er een netwerk-, een consensus-, een transactie- en een applicatielaag. De netwerklaag zorgt voor het uitwisselen van informatie die wordt gebruikt in de lagen erboven. Zo wordt in de consensuslaag een consensusprotocol uitgevoerd, om het eens te worden over de volgorde van veranderingen in het gedeelde grootboek. In dit proces zouden deelnemende partijen zich kunnen misdragen, om te proberen het consensusprotocol te verstoren of het voor eigen gewin te manipuleren. Maar zolang een meerderheid van de partijen zich aan het protocol houdt, kunnen de deelnemende partijen het eens worden.

Een belangrijk en vernieuwend aspect is, dat het economisch ongunstig is om af te wijken van het protocol, wat een onderdeel is van het speltheoretische element van blockchaintechnologie. Een bijdrage aan het consensusproces die niet voldoet aan de afgesproken

regels is namelijk eenvoudig te detecteren. Deze wordt dan ook niet geaccepteerd door de andere partijen, met als gevolg dat de beloning voor deelname – het controleren en beschikbaar stellen van het gedeelde grootboek – niet wordt uitgekeerd. Als de andere partijen de foutieve bijdrage wel accepteren, lopen ze grote kans om vervolgens zelf hun beloning mis te lopen.

De beloning wordt uitgegeven in de transactielaag. Deze laag controleert of transacties voldoen aan de afgesproken regels, waarbij de transactie een verandering is in het gedeelde grootboek. Zo wordt bijvoorbeeld bij de bitcoinblockchain in deze laag gecontroleerd of een bitcoin nog niet eerder is uitgegeven. De applicatielaag met de daadwerkelijke toepassingen voor de eindgebruiker vormt ten slotte de vierde laag.

## LIBERTAIRE CRYPTO-ANARCHISTISCHE WENS

Blockchaintechnologie heeft haar oorsprong in Bitcoin. Die werd bedacht vanuit de libertaire crypto-anarchistische behoefte aan een globaal digitaal systeem voor waarde-uitwisseling dat niet onder controle staat van centrale, autoritaire entiteiten. Iedereen mag meedoen, zonder eerst toestemming te hoeven vragen. Deze blockchainsystemen worden daarom ook wel *permissionless* genoemd.

Het bedrijfsleven zag vervolgens wel de potentie van blockchaintechnologie, maar maakte met het oog op onder andere schaalbaarheid (capaciteit), vertrouwelijkheid en regulering liever gebruik van een meer gecontroleerde omgeving. Door die wens ontstonden de laatste jaren ook *permissioned* of consortiumblockchains, waarin een kleinere set van geïdentificeerde en geauthenticeerde partijen kan samenwerken en er meer vertrouwd kan worden op de traditionele (ook juridische) handvatten om elkaar in het gareel te houden. De toekomst zal uitwijzen of dergelijke consortiumblockchains slechts een tussenstation zijn totdat de wereld geconvergeerd is naar een kleine set van globale permissionless blockchains, of dat we uiteindelijk in de richting van een veelvoud van onderling verbonden blockchainnetwerken zullen gaan.

## SMART CONTRACT ALS ONVERMURWBARE DERDE PARTIJ

Terwijl bij Bitcoin de focus vooral ligt op waardeoverdracht, richten tweedegeneratieblockchainplatforms als Ethereum zich op het programmeerbaar maken van een blockchain. Ze bieden de mogelijkheid om kleine programmaatjes uit te laten voeren die autonoom en zelfstandig wijzigingen kunnen aanbrengen in het

## Voorbeelden van blockchaintoepassingen

**KADER 1**

### CONTAINERTRANSPORT

In het TKI Dinalog Blockchain Consortium onderzoeken experts van TNO samen met andere partijen de mogelijkheden van blockchain voor containertransport. Van de 40 dagen dat een container onderweg is van Midden-China naar Midden-Europa, is hij ongeveer 24 dagen in beweging en staat hij 16 dagen stil. Dat komt vooral doordat de betrokken partijen niet realtime informatie delen.

Bij het transport zijn zeker 20 tot 25 partijen betrokken: verzender, douane, havenautoriteiten, stuwadoors, vracht- en wegvervoerders, ontvanger, banken, enzovoort. Elk uur dat een schip langer aan de kade ligt, betekent 50.000 tot 100.000 euro extra kosten. De havens delen al informatie via het Port Community System, maar de verwachting is dat met blockchain de efficiëntie kan worden verbeterd en de kosten nog verder omlaag kunnen.

Waar bedrijven aan moeten wennen, is dat ze een specifiek deel van hun data met de andere partijen moeten delen, in plaats van die voor zichzelf te houden. Het consortium helpt de deelnemers met de techniek vertrouwd te raken en in te zien dat blockchain voor iedereen die ermee werkt voordeel oplevert.

*(Bron: TNO Time, 2017a)*

### VOEDSELCERTIFICATEN

In het project Blockchain for Agrifood onderzoeken TNO en Wageningen University & Research in opdracht van het Ministerie van Economische Zaken de impact van blockchain op de agrifoodsector. Met een casus over druiven die uit Zuid-Afrika worden geïmporteerd, wordt uitgezocht of de technologie kan helpen om de naleving van voedselcertificaten te verbeteren.

In agrifoodketens worden momenteel heel weinig data gedeeld, waardoor voedselfraude of andere fouten in het systeem mogelijk zijn. Er bestaan voedselcertificaten, die aangeven of een product fair trade of biologisch is en of de hygiëne in orde is. Maar in de praktijk worden die niet gecheckt en moet de handelaar er maar op vertrouwen dat ze geldig zijn.

De vraag in dit project is of de voedselcertificaten gedurende het hele traject van productie tot supermarkt met blockchaintechnologie beheerd zouden kunnen worden. Ook tracking en tracing van voedsel behoort tot de mogelijkheden. Er bestaat al commerciële interesse, zoals voor de tracking van farmaceutische middelen.

*(Bron: TNO Time, 2017b)*

Meer voorbeelden zijn te vinden op http://blockchain.tno.nl.

gedeelde grootboek. Deze zogenaamde *smart contracts* worden uitgevoerd en gecontroleerd door alle deelnemende computers. Ook worden ze opgeslagen in hetzelfde grootboek en zijn ze daarom niet zomaar aan te passen. Hierdoor kunnen alle deelnemende partijen vertrouwen op de afgesproken uitvoering en kunnen smart contracts de rol van onvermurwbare derde partij op zich nemen.

Een eenvoudig voorbeeld van een smart contract is een digitale portemonnee, waarvoor is vastgelegd dat elke uitgave boven een bepaald bedrag altijd moet zijn voorzien van een digitale handtekening van drie van de tien beheerders. Maar ook een coöperatie van boeren zou, zonder enige tussenpersoon, een fonds kunnen oprichten, ondersteund door een smart contract waarin precies is vastgelegd wat de inleg van elke partij is en onder welke voorwaarden het fonds uitkeert. Zo kan erin staan dat alleen regencompensatie wordt uitgekeerd wanneer een specifieke partij (KNMI) heeft aangeven dat er op een bepaalde plek meer dan twintig millimeter regen is gevallen.

De toekomstvisie voor smart contracts is, dat ze controle krijgen over grote hoeveelheden waarde. Enerzijds past dat bij de trend van toenemende digitalisering en autonomie van systemen. Anderzijds leidt het tot risico's, want een fout in de code kan grote gevolgen hebben. Zo ontdekte een hacker medio 2016 op de Ethereumblockchain een fout in de smart-contractcode van het virtuele investeringsfonds The DAO. Daardoor kreeg de hacker de controle over meer dan 50 van de 150 miljoen dollar in het fonds.

Bij TNO wordt aan technologie en tools gewerkt waarmee eventuele gaten tussen de intentie en de uitvoering van een smart contract verkleind worden, om zo te komen tot veilige en robuuste smart contracts.

## TOEKOMST

Er wordt veel geëxperimenteerd en ge-pilot met blockchaintechnologie, voor een belangrijk deel omdat er nog veel uitdagingen en vragen zijn op gebieden als schaalbaarheid, privacy, businessmodellen en governance. Deze experimenten worden uitgevoerd binnen een verscheidenheid van praktijkcases, van containertransport tot voedselcertificaten (kader 1).

Wat al wel duidelijk is: blockchain doe je nooit alleen. Het is een middel voor samenwerking, en pas wanneer er sprake is van meerdere partijen, kan het nuttig zijn. Het is daarom belangrijk heel kritisch te kijken of blockchaintechnologie wel een oplossing is voor het probleem. Voor veel toepassingen is een blockchain helemaal niet nodig en is een enkele server in een datacentrum of de cloud eigenlijk wel voldoende.

Daarnaast is blockchain vooral een technologie die op de achtergrond zal draaien. De meeste gebruikers zijn zich er net zomin van bewust als dat voor internet de netwerkprotocollen TCP/IP worden gebruikt. Waar het om gaat, is dat nuttige en goedkopere diensten mogelijk worden doordat computers taken van traditionele partijen zoals banken, energiemaatschappijen of pensioenfondsen geheel of gedeeltelijk kunnen overnemen. In hoeverre de hype waargemaakt wordt, is lastig te zeggen. Maar blockchain heeft de potentie om de manier waarop we werken te transformeren en om machtsverhoudingen te verstoren of verplaatsen, met name naar het individu. Weer wat meer *power to the people*.

### LITERATUUR

TNO Time (2017a) *Blockchain zet extra vaart achter containertransport in Rotterdamse haven*, 29 juni. Artikel te vinden op tinyurl.com/tnodinalog.

TNO Time (2017b) *Pilot toont dat blockchain en agrifood een vruchtbare combinatie zijn*, 28 juli. Artikel te vinden op tinyurl.com/tnoagrifood.

### In het kort

- Blockchaintechnologie kan ervoor zorgen dat men minder op tussenpersonen hoeft te vertrouwen.
- Er zijn nog veel uitdagingen en vragen op gebieden als schaalbaarheid, privacy, businessmodellen en governance.
- Voor veel toepassingen is een blockchain helemaal niet nodig en is een enkele server voldoende.