

DE KASBOEKREVOLUTIE

Zet blockchain ons leven op losse schroeven, of loopt het zo'n vaart niet? Nieuwe technologie maakt zelden al haar beloften waar, maar blockchain steekt wel al in allerlei domeinen de kop op. Je kunt ermee stemmen, bellen en jezelf identificeren. Nadeel: het slurpt meer energie dan een land als Ecuador. Geen wonder dat er nu al her en der bitcoinvegetariërs zijn gespot.

SUPERSLIM EN HUFTERPROOF 32

INTERVIEW MET BALÁZS BODÓ 35

VERDEEL EN BEHEERS 39

MAG 'T EEN BEETJE ZUINIGER? 40

SUPERSLIM EN HUFTERPROOF

Vergeet de hype en negeer het gespeculeer. De werkelijke waarde van bitcoin schuilt niet in zijn aandelenkoers, maar in de solide onderliggende mechaniek: blockchain. Volgens deskundigen gaat blockchain onze samenleving drastisch veranderen. Wat maakt deze technologie zo veelbelovend?

Laat je huidige bestaan achter je en reis in gedachten terug naar een droge zomerdag in het jaar 2716 voor Christus. Je bevindt je in Uruk, de hoofdstad van Soemer. Hier ben je geboren en hier werk je, als functionaris van de koning. Jouw taak vandaag? Inventariseren hoeveel waardevolle spullen verborgen liggen in de kelder van het paleis. Gelukkig heb je onlangs een Soemerische *lifehack* geleerd. Eenmaal in

de kelder begin je met een priem te krassen in een vochtig kleitablet. Drie strepen: het symbool voor een kruik wijn. Nog twee krassen. Het getal tien. Dit is een verdomd handige truc om voorraden bij te houden, denk je bij jezelf. Jammer dat je die streepjes niet ook kunt gebruiken om het zo lastig te onthouden heldenlied van Gilgamesj op te tekenen, mijmer je. Dan begint het in je hoofd te duizelen.

Bijna vijfduizend jaar later bevinden we ons in eenzelfde soort positie. Zoals voorraadinventarisatie de eerste toepassing was van het schrift, is bitcoin de eerste toepassing van blockchain. Net zoals de Soemeriers destijds, hebben we een instrument in handen waarvan de mogelijkheden verder reiken dan we momenteel kunnen zien. 'Blockchain zal misschien een grotere impact op de wereld hebben dan heel het internet tot nu toe,' zegt de Tilburgse hoogleraar Geert Duijsters.

DIGITALE WAARDE

Maar wat is dat blockchain dan precies? Na bovenstaand relaas klinkt dit haast als een anticlimax, maar een blockchain is... een kasboek. Een online, gedecentraliseerd kasboek, zonder eigenaar of toezichhouder, dat op miljoenen plekken tegelijk kan bestaan. Een kasboek waar duizenden verschillende partijen synchroon transacties in kunnen bijschrijven, maar waar dankzij een slim concept niemand mee kan sjoemelen.

Om de werking en potentie van dit kasboek beter te begrijpen, is het nuttig om te beseffen dat het internet al vanaf zijn geboorte enkele gebreken kent. De digitale snelweg excelleert weliswaar als het gaat om *informatie* uitwisselen – elke rangschikking van symbolen kunnen we eindeloos kopiëren en downloaden – maar daarmee is het internet veel minder geschikt voor het uitwisselen van *waarde*. Want hoeveel waarde kan een digitaal geldbiljet vertegenwoordigen als iedereen met een flinke copy-paste-sessie zijn vermogen kan vermiljardvoudigen?

Het internet mist bovendien een mechanisme om individuele identiteit te verankeren. Online weet je nooit zeker of de gene aan de andere kant werkelijk is wie

die zegt dat die is. Door dit fundamentele gebrek aan online vertrouwen zijn we genooddakt om betrouwbare tussenpartijen, zoals banken, in te schakelen om online waardetransacties te faciliteren.

Maar wat als er een systeem zou bestaan dat digitale data overdraagt maar niet vermenigvuldigt? Een systeem dat kan garanderen dat als ik jou een bepaald stukje digitale waarde stuur, daadwerkelijk dat specifieke stukje (en dus geen kopietje) bij jou arriveert? Dát systeem, dat banken overbodig maakt, is de blockchain.

REKENKRACHT

Om precies te zijn werkt het als volgt. Stel, je wilt drie bitcoin naar je moeder sturen. Dan moet je moeder eerst een virtuele, versleutelde identiteit aanmaken bij de blockchain (dat kan eventjes duren), en daarna kun je bij de blockchain een transactieverzoek indienen. Dit verzoek wordt doorgestuurd naar duizenden *nodes*. Dit zijn de leden van het netwerk die gezamenlijk de blockchain draaiende houden. Hier vindt de eerste betrouwbaarheidscheck plaats. Elke node verifieert, via het kraken van complexe versleutelingen en puzzels, of dit verzoek daadwerkelijk afkomstig is van jou en je moeder, en of jij wel echt drie bitcoin bezit. Eenmaal goedgekeurd voegt elke node de transactie toe aan zijn eigen lijstje met recente transacties. Met vaste intervallen, in het geval van de bitcoin-blockchain elke tien minuten, vindt er een synchronisatie plaats tussen alle nodes. Nu geschiedt de tweede betrouwbaarheidscheck: alleen transacties die door de meerderheid van alle nodes zijn goedgekeurd, worden definitief bijgeschreven in het kasboek. Klaar. De blockchain is weer tot een *blok* gegroeid.

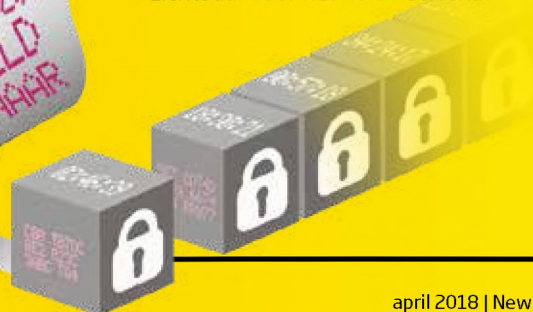
VERTROUWEN IN HET NETWERK

De blockchain is een digitaal kasboek: om de lijst van transacties veilig te beheren, zijn de data versleuteld en verspreid over vele computers.



Nieuwe transacties worden gebundeld in een blok en onderworpen aan een reeks ingewikkelde berekeningen om een unieke code te genereren, een zogeheten *hash*.

Deze code wordt verzonden naar alle computers in het blockchainnetwerk. Wie de transactiedata probeert te veranderen, creëert een nieuwe *hash*, zichtbaar voor het hele netwerk.



Een blockchain is dus vergelijkbaar met een democratie met een sterke grondwet. Consensus is nodig, alleenheerschappij onmogelijk. Eén node hacken is zinloos; individueel gesjoemel wordt tijdens de synchronisatie genegeerd. De rekenkracht die nodig is om 51 procent van alle systemen te hacken is zo bizar groot, dat elke poging bij voorbaat zinloos is. 'Het zegt genoeg dat de blockchain van bitcoin in tien jaar nog nooit is gehackt, terwijl er

zien. In het geval van bitcoin bestaat die beloning uit... vers vrijgespeelde bitcoins. Zo garandeert het systeem zijn eigen functioneren. Sol: 'Voor dit concept verdient de uitvinder, de mysterieuze Satoshi Nakamoto, de Nobelprijs. Mits hij bestaat.'

BITCOINVEGETARIËRS

Blockchains maken online transacties dus kosteloos betrouwbaar. Dure tussenpartijen zoals banken, verzekeraars,

'Het zegt voldoende dat na tien jaar de blockchain van bitcoin nog nooit is gehackt, terwijl er miljarden mee te verdienen zijn'

miljarden mee te verdienen zijn', aldus Duijsters.

Maar is dit systeem, waarbij één transactie duizenden keren wordt geverifieerd door verschillende nodes, niet ontzettend duur? Wie betaalt al die rekenkracht? 'Dat is nu wat blockchain zo geniaal maakt', zegt hoogleraar Egbert-Jan Sol van TNO. 'Blockchains betalen voor zichzelf.' Iedereen die zijn computer beschikbaar stelt als codekrakende node (in de digitale volksmond *miners* genoemd) kan via een centraal algoritme een beloning tegemoet

hypotheekverstrekkers en notarissen zijn daarmee in principe overbodig. 'Ik zie op termijn enorme potentie in marktplaatsen die draaien op blockchain. Stel je Airbnb en Uber en eBay voor, maar dan zonder centrale partij die allerlei commissies int', voorspelt Sol. 'Nog verder in de toekomst kun je denken aan koppelingen met intelligente apparaten. Een zelfrijdende auto krijgt zijn eigen digitale identiteit bij de blockchain, zodat je direct transacties aan kunt gaan met de auto zelf. Die haalt jou op, in ruil voor een

bepaald bedrag, dat uiteindelijk naar zijn eigenaar zal gaan', aldus de hoogleraar. Hij voorziet een wereld die niet gericht zal zijn op bezit, maar op gebruik.

'Toch willen we bij TNO blockchain vooralsnog *dehypen*. Er zitten haken en ogen aan de eerste generatie implementaties. Het groeiende energieverbruik van bitcoin is bijvoorbeeld onhoudbaar', voegt Sol toe. 'We hebben hier bij TNO zelfs een aantal 'bitcoinvegetariërs' die uit milieuoverwegingen weigeren erin te handelen. Maar ook op juridisch gebied moet er nog veel gebeuren. Voordat alles is uitgekristalliseerd, zijn we weer tien jaar verder.' Een relatief lange tijd, in onze snelle wereld. Maar in het licht van de honderden jaren die de Soemeriërs nodig hadden om hun voorraadsymbolen te transformeren tot een instrument geschikt voor poëzie, is dat een oogwenk. ■

'DE INVLOED VAN NIEUWE TECHNOLOGIEËN OP DE MAATSCHAPPIJ VALT VAAK WAT TEGEN'

Telkens wanneer een nieuwe technologie de kop opsteekt, verwachten tech-optimisten een grondige herschikking van de samenleving. Volgens sociaal-wetenschapper Balázs Bodó loopt het meestal niet zo'n vaart. Vormt blockchain een uitzondering?

Blockchainevangelisten hebben dromen die tot aan de hemel reiken. Ze voorspellen een nieuwe financiële lente, sjoemelvrije verkiezingen en een einde aan tussenpersonen zoals bankiers, verzekeraars en notarissen. En inderdaad: de blockchain-technologie is veelbelovend. De techniek legt veilig en onomkeerbaar transacties vast en kan daarmee de pijlers onder onze maatschappij aan het wankelen brengen.

Pas echter op, waarschuwt sociaal-wetenschapper Balázs Bodó: de beloften van nieuwe technologieën worden zelden waargemaakt. Ruim twintig jaar verdiept hij zich al in de maatschappelijke impact van technologische ontwikkelingen. En dus verstrekte de Europese Unie hem afgelopen jaar een gewilde onderzoeksbeurs toen hij voorstelde om de impact van blockchain eens goed in kaart te brengen. Is deze nieuwe technologie de maatschappelijke *game changer* die fans erin zien? Of valt het toch weer tegen? 'Je moet de drijfveren van alle betrokkenen snappen,' zegt Bodó. 'Dan heb je een beter idee welke kant het op gaat.'

Waarom bent u onderzoek gaan doen naar blockchain?

'Ik ben een sociaal-wetenschapper. Ik werk al twintig jaar vooral aan digitale vraagstukken, aan de manier waarop de techniek invloed heeft op onze maatschappij en het bedrijfsleven. En omgekeerd: de manier waarop de maatschappij, economie en politiek invloed hebben op de ontwikkeling van technologie. Wat ik in die periode vooral heb gezien, is dat we altijd hopen dat zo'n nieuwe technologie de wereld ingrijpend gaat veranderen. Dat onze maatschappij de waarden zal overnemen die in zo'n technologie zijn ingebakken.'

'Neem web 2.0, dat ongeveer tien jaar geleden enorm in opkomst was. Daarin ging het vooral om delen. Veel digitale zaken – software, afbeeldingen – kregen een *commons*-licentie, werden gemeenschappelijk bezit. Tegelijk ontwikkelde de praktijk op het internet zich juist in een heel andere richting. We delen tegenwoordig wel dingen met elkaar, maar dan toch vooral op sterk gecentraliseerde, commerciële platformen. Niet via hori-

zontale, op commonslicenties gestoelde samenwerkingsverbanden. De nieuwe technologie bleek helemaal niet profetisch voor de toekomst. Dat was voor veel mensen een tegenvaller.'

'Met blockchain hebben we nu weer zo'n technologie waar mensen veel van verwachten. Het is een technologie met eigenschappen die we nog nooit eerder hebben gezien. Ik wil daarom graag weten hoe mensen die technologie gaan gebruiken of hoe ze zich er juist tegen verzetten. Hoe ze proberen zo'n technologie naar hun hand te zetten.'

Hoe pak je zoiets aan?

'We moeten allereerst de technologie in kaart brengen. Proberen te ontdekken welke vorm van blockchain de meeste potentie heeft. Welke technologie trekt investeerders? Welke heeft de handigste toepassingen? Daarnaast moeten we vooral veel praten, met iedereen die iets met blockchain te maken heeft. Uit interviews kunnen we dan hun visie op deze technologie reconstrueren.'

'We spreken daarom met alle betrokkenen. Met advocaten, met mensen van de belastingdienst, de banken – de vertrouwde tussenpersoon, de mensen die blockchain overbodig willen maken. Hoe denken zij over de toekomst? Maar we spreken natuurlijk ook de 'barbaren aan de poort': de start-ups die al deze dingen bedenken en ontwikkelen. Wat zijn zij van plan? Wat zijn hun dromen en angsten?'

Als vorige technologische noviteiten minder impact hadden dan verwacht, ligt het dan niet voor de hand dat het ditmaal net zo zal gaan?

‘Misschien heeft blockchain inderdaad weinig impact. Dat kan. Misschien is het een bubbel. Maar het kan ook van fundamenteel belang blijken, grote impact hebben op manieren die we ons nu nog niet voor kunnen stellen. Op basis van het huidige bewijs denk ik echter dat deze

lezen. Dat kan soms heel handig zijn, maar diezelfde algoritmen kunnen ook gebruikt worden om mensen, stemmers en zelfs de bevolking van hele landen te manipuleren. Dat is natuurlijk een onwenselijke, onverwachte bijvangst van zo’n nieuwe technologie. Daarom zijn mensen nu hals over kop aan het nadenken hoe we deze algoritmen kunnen reguleren, hoe we ze kunnen laten doen wat wij willen.

dus flexibel zijn. Mijn idee is dat je dan iets van een testomgeving, een *regulatory sandbox*, nodig hebt waarin je kunt experimenteren met verschillende oplossingen in regelgeving of beleid.

‘Op de lange termijn moet je dat alleen wel goed in de gaten blijven houden. Wanneer je een concessie doet op korte termijn, moet je daar meteen een vinkje bij zetten. Zodat je het later weer kunt bijsturen. Zo kun je flexibel zijn zonder dat je jezelf met gehaaste, slechte wetgeving opscheept, of zelfs helemaal geen wetgeving maakt.’

Hoe verschilt dat van wat we nu doen?

‘Wetten maken kost tientallen jaren. Neem een beslissing op EU-niveau, bijvoorbeeld de algemene verordening gegevensbescherming (AVG), waarin de bescherming van consumentengegevens geregeld is. Dat kost vijf jaar debat, vergt vele compromissen. Zodra je dan uiteindelijk een wet uit het vuur gesleept hebt, blijf je er wel een jaar of twintig af. Niemand heeft zin die hele mallemolen nog eens door te lopen.

‘Het vervelende is alleen dat technologie zich in een veel korter tijdsbestek ontwikkelt. Facebook ging in dertien jaar van nul naar twee miljard gebruikers. En dat is dan nog relatief lange termijn. Het is misschien een tikje gechargeerd, maar de meeste technologie leeft korter dan een hamster (*1,5 tot 3 jaar, red.*). Daarom zijn die flexibele testomgevingen, met kortetermijnwetgeving, misschien de beste aanpak.’

Kun je voor zo’n idee de handen op elkaar krijgen?

‘Dat is één van onze onderzoeksvragen. Misschien zitten mensen er wel helemaal niet op te wachten. Veel tech-start-ups vinden het eigenlijk wel lekker als er nog geen regelgeving is. Dat is hoe bedrijven als Airbnb en Uber ook zijn begonnen, door in een gat in de regelgeving te springen. Als maatschappij moeten we ons dan alleen afvragen: willen we dit? En vervolgens een kosten-batenanalyse maken. Wat kost het om niet te reguleren, en wat kost het om dit soort flexibele testomgevingen op te zetten?’

‘Ik zie niet in waarom jij of ik elke transactie die we ooit doen voor de eeuwigheid willen vastleggen’

technologie niet zo veel impact zal hebben op de consumentenmarkt. Tegelijk kan het op andere gebieden juist enorm interessant zijn. Er bestaan bijvoorbeeld al interessante blockchaintoepassingen die het gemakkelijker maken voor machines om met elkaar te communiceren. Een ander voorbeeld zijn de zogeheten *smart contracts*, waarmee we een grote hoeveelheid ‘domme transacties’ – zaken waarbij eigenlijk nooit iets misgaat – kunnen automatiseren, zonder tussenkomst van advocaten en notarissen. Daarnaast blijkt blockchain enorm handig bij flitshandel.’

Is onze maatschappij wel klaar voor dergelijke toepassingen?

‘Ik zal je een voorbeeld geven. In 1999 kwam voor het eerst peer-to-peersoftware op de markt. Ineens waren er toepassingen als Napster en later BitTorrent, waarmee mensen direct dingen van elkaar konden downloaden. Niemand was daar echt op voorbereid. Het had een enorme impact op de wetgeving rond auteursrechten, maar die wet paste zich lethargisch traag aan. Het leverde een enorme worsteling op om dat weer recht te breien.

‘Hetzelfde gebeurde recent met sociale media. Ineens kwamen er algoritmen op de markt die bepalen welk nieuws we

‘Beide gevallen zijn voorbeelden waarbij we de problemen pas ontdekten op het moment dat de technologie al door veel mensen gebruikt werd. We moeten er dus eerder bij zijn. Daarvoor moeten we opkomende technologieën zoals blockchain scherp in de gaten houden en een manier ontwikkelen om bedreigingen zo vroeg mogelijk te herkennen en meteen het hoofd te bieden. Anders zijn we er als maatschappij straks inderdaad niet klaar voor. We moeten echt pro-actiever worden.’

Maar zijn opkomende technologieën niet per definitie heel onvoorspelbaar? Hoe weet je dan wanneer je alarm moet slaan?

‘Aan de ene kant moet je goed kijken naar de huidige wetgeving. Je moet het direct in de smiezen hebben wanneer je ziet dat ergens een technologie ontstaat die op gespannen voet staat met de bestaande regelgeving. Zo is er nu bijvoorbeeld een spanningsveld tussen onze wens om het witwassen van geld aan banden te leggen, en de mogelijkheid tot pseudo-anonieme transacties met bitcoin.

‘Je moet jezelf dan afvragen: wat voor soort regelgeving kan deze juridisch onduidelijke situatie oplossen? Daarvoor heb je snelle antwoorden nodig. Je moet



Zijn die testomgevingen afdoende om dit probleem op te lossen, of is er nog meer nodig?

'Je moet goed in de gaten hebben welke kant een ontwikkeling op gaat. En daarvoor moet je bovenal goed snappen wat de drijfveren zijn van alle betrokkenen. Laten we weer kijken naar een voorbeeld, in dit geval een probleem dat zichtbaar werd rond de verkiezing van Donald Trump. Tijdens die verkiezingen wisten onder andere pro-Trump-groepen op heel fijnmazig niveau stemmers te bereiken. We weten al sinds het begin van het commerciële internet dat microtargeting de toekomst van online adverteren is. Voeg daar allerlei big data over

Terug naar blockchain - wat zijn daar de prikkels? Weten we dat al?

'Wat ik in elk geval níet zie, is een prikkel voor individuele gebruikers om deze technologie te omarmen in het dagelijks leven. Neem nu bijvoorbeeld bitcoin – er is geen enkele reden om dat als geld te gaan gebruiken. Het is voor individuen handig als speculatiemiddel, een ding om in te beleggen. Zodra je dat weet, kun je het als speculatiemiddel behandelen. Je kunt dan vanuit die visie regels gaan ontwikkelen.

'De vraag is natuurlijk wel: komen er nog nieuwe toepassingen bij? Gaan we blockchain gebruiken om muziek te luisteren, nieuws te lezen of om onze

eeuwigheid willen vastleggen in een blockchain. Dat klinkt meer als iets dat handig is voor bijvoorbeeld professioneel voorraadketenbeheer.

'Toch kun je je specialistische toepassingen voorstellen waarbij het wél handig is. Misschien willen we er wel onze belastingbetalingen in vastleggen. Of de dingen die je op je cv hebt staan – diploma's en certificaten en dergelijke. Of, zoals ik net zei, vastleggen hoe we gestemd hebben tijdens verkiezingen, zodat niemand kan sjoemelen met de uitkomsten. Maar het is voorlopig nog wel even afwachten of de blockchaintechnologie die kant op gaat, of daarvoor de juiste prikkels ontstaan.'

Is dat vooral een kwestie van technologie of van de wensen van de maatschappij?

'Beide zijn onlosmakelijk met elkaar verbonden. Neem bijvoorbeeld de enorme hoeveelheid energie die een blockchain vreet. Dat is duidelijk een technologisch vraagstuk. Maar als je een blockchain, bijvoorbeeld die van bitcoin, wilt gaan inzetten bij verkiezingen, dan is die energiekwestie juist een maatschappelijk vraagstuk. En die maatschappelijke afweging kan weer een andere uitkomst krijgen wanneer de technologie verandert.

'Dat samenspel maakt het enorm lastig om de verre toekomst van blockchain te voorspellen. Maar als we de boel scherp in de gaten houden en een flexibelere manier hebben om regelgeving te maken, kunnen we wel zorgen dat we er als maatschappij klaar voor zijn wanneer de grootste veranderingen zich aandienen.' ■

Balázs Bodó (Hongarije, 1975) is afgestudeerd in de economie en in media-onderzoek. Hij onderzocht eerder de maatschappelijke invloed van peer-to-peersoftware en de invloed van Creative-Commonslicenties op de productie van kennis. Sinds 1 januari 2018 is hij het hoofd van het Blockchain & Society Policy Research Lab bij het instituut voor informatierecht aan de Universiteit van Amsterdam.

'Dat samenspel maakt het enorm lastig om de verre toekomst van blockchain te voorspellen'

stemmers en hun voorkeuren aan toe, verzameld via sociale media en bedrijven die bereid zijn om in die data te handelen, en je hebt een compleet andere politieke situatie. Een situatie die we onvoldoende zagen aankomen. Niemand had het inherente gevaar voorzien van manipulatie, propaganda en het demobiliseren van stemmers met dit soort politieke microtargeting.

'Misschien zouden we dus wat meer moeten focussen op de vraag: welke motieven hebben goedaardige of kwaadaardige partijen om een bepaalde technologie te gebruiken of misbruiken, in plaats van dat we ons alleen blindstaren op alle prachtige beloften. Dan zouden we al een stuk eerder een discussie kunnen hebben over de maatschappelijk wenselijke uitkomsten van een bepaalde technologie.'

verkiezingen veiliger te maken? Op dit moment zie ik die ontwikkelingen niet.

'We moeten wel scherp blijven op nieuwe prikkels die onze conclusie kunnen veranderen. Misschien besluit een overheid blockchain te gebruiken voor een nieuw stelsysteem. De technologie zelf is immers transparant en betrouwbaar. Ik geloof in de meerwaarde van blockchain. Maar voorlopig ben ik sceptisch over in hoeverre individuen het gaan gebruiken.'

Wat moet er gebeuren om blockchain wel groter te maken, om ervoor te zorgen dat het breder gebruikt wordt?

'Misschien is dat helemaal niet nodig. Misschien is het bovenal geschikt als een heel gespecialiseerde technologie en past het niet goed bij dagelijks, persoonlijk gebruik. Ik zie niet in waarom jij en ik elke transactie die we ooit doen voor de

VERDEEL EN BEHEERS

Het begon met de handel in cryptovaluta, maar inmiddels duikt blockchain in meerdere domeinen van het leven op. Je kunt er bijvoorbeeld al mee stemmen, bellen en jezelf identificeren.

Bewijs maar eens dat je bent wie je zegt dat je bent. Je kunt je geboorteakte opvragen via internet, maar menigeen doorloopt een nogal ouderwetse procedure. Je neemt contact op met de gemeente waar je bent geboren, ontvangt een kopie van je geboorteakte per post, stopt deze in een nieuwe envelop, stuurt hem op naar degene die dit wil nagaan en hoopt vurig dat de postbode hem niet kwijtraakt. Onzeker en tijdrovend. Met blockchain-technologie hoeft dit maar enkele seconden te duren.

De Amerikaanse staat Illinois experimenteert daarom met een manier om de controle over gevoelige gegevens zoals geboorteakten volledig terug te geven aan de burger. Met behulp van een gedecentraliseerd digitaal grootboek, vergelijkbaar met de technologie van bitcoin, zou dit werkelijkheid moeten worden.

Het idee is om een digitale identificatiemethode te creëren voor inwoners die toegang willen tot bijvoorbeeld hun geboorteakte. Die is via een applicatie alleen toegankelijk voor de persoon zelf

en voor derden aan wie de persoon toestemming heeft verleend. Een centrale autoriteit zoals de gemeente is dan niet meer nodig als tussenpersoon.

EIGEN BAAS

Deze wens bestaat bij veel activistische burgers al langer: meer controle over de eigen gegevens. Door hackers en datalekken lijkt het steeds riskanter dat de overheid als enige dit soort gevoelige gegevens bewaart. Met de blockchain-technologie wordt dat gevaar een stuk kleiner. Alle deelnemers van een netwerk ontvangen hun eigen identieke kopie van de gegevens. Zo kan niemand de cryptografisch verzegelde geboorteaktes bekijken, tenzij dat de bedoeling is.

Nadelen zijn er ook. Fout ingevoerde informatie is niet meer te veranderen. 'Als iemand in het ziekenhuis het gewicht of de naam van je kind verkeerd spelt, is dat de realiteit,' zegt privacy-analist Steve Wilson van Constellation Research, een onderzoeks- en adviesbureau op het gebied van technologie uit Silicon Valley. 'Eens fout, altijd fout.'

Toch zet de blockchaintechnologie mogelijk een stap in de richting van een veiligere en eerlijkere wereld waarin al jouw gegevens ook door jou beheerd worden. De invloed en macht van de overheid zou hierdoor kunnen afnemen.

VLOEIBARE DEMOCRATIE

Dat lijkt ook op een heel ander terrein het geval: de democratie. Bij het illegaal verklaarde referendum voor onafhankelijkheid in Catalonië hebben burgers bijvoorbeeld met blockchaintechnologie toch hun stem uitgebracht. De regering in Madrid stond machteloos.

Democracy Earth, een 'wereldwijde gemeenschap van hackers, denkers en makers,' heeft een applicatie ontworpen die de manier waarop we deelnemen aan een democratie op zijn kop zet. Deze app, genaamd Sovereign, combineert de blockchaintechnologie met het concept van 'vloeibare democratie', waarin individuen meer flexibiliteit krijgen in hoe ze hun stemmen gebruiken.

In een vloeibare democratie kunnen kiezers met hun stemmen rechtstreeks hun wensen uiten over een kwestie, of hun stemmen delegeren aan iemand die volgens hen meer kennis van zaken heeft. Deze afgevaardigden kunnen vervolgens die stemmen op hun beurt hoger in de keten doorgeven. Belangrijk is dat via blockchain iedereen kan inzien hoe zijn afgevaardigde heeft gestemd, en iedereen zijn stem kan terugvragen wanneer die dat wil.

CRYPTOSTEMMEN

Vloebare democratie is een intrigerend concept, maar zeker niet zonder problemen. Een schijnbaar oneindige hoeveelheid stemmen kan de motivatie van de stemmer ondermijnen. Bovendien kunnen een paar 'beroemdheden' op basis van hun populariteit – en niet hun bekwaamheid – een ongezond aantal stemmen verzamelen en veel macht uitoefenen.

De Argentijnse ondernemer Santiago Siri, een van de oprichters van Democracy Earth, denkt dat Sovereign beide problemen kan oplossen. De blockchaintechnologie produceert in plaats van cryptomunten een eindig aantal stemmen. Deze worden via een simpele applicatie aan gebruikers

stem, is zichtbaar voor iedereen – nogal anders dan het naamloze stembiljet. Bij dat probleem kunnen blockchains zoals ZCash, die zich specialiseren in anonieme transacties, mogelijk uitkomst bieden.

EIGEN KLUIS

Anonimiteit van de stem kan ook gegarandeerd worden met de BitVault, de eerste blockchain-telefoon, die zo goed beveiligd is dat de ontwikkelaars hem een 'Zwitserse bank in je broekzak' noemen. Naast vingerafdruk en irisscan genereert de BitVault, eind vorig jaar voor het eerst in Nederland gepresenteerd, zogenoemde dynamische encryptiesleutels waarmee alle data die verzonden

Ontwikkelaars noemen de blockchaintefoon een 'Zwitserse bank in je broekzak'

gegeven die lid zijn van een politieke partij, of inwoner van een gemeente of land. Als een soort universeel basisinkomen worden de stemmen in de portemonnee van de gebruikers geplaatst.

Stemfraude is praktisch onmogelijk omdat het registreren van stemmen op een blockchain zeer complexe wiskunde vereist. 'De blockchain is onveranderlijk. Niemand kan de opslag van de stemmen wijzigen – een voorwaarde voor de democratie,' zegt Siri.

Toch is er een groot probleem: elke blockchaintransactie, en dus

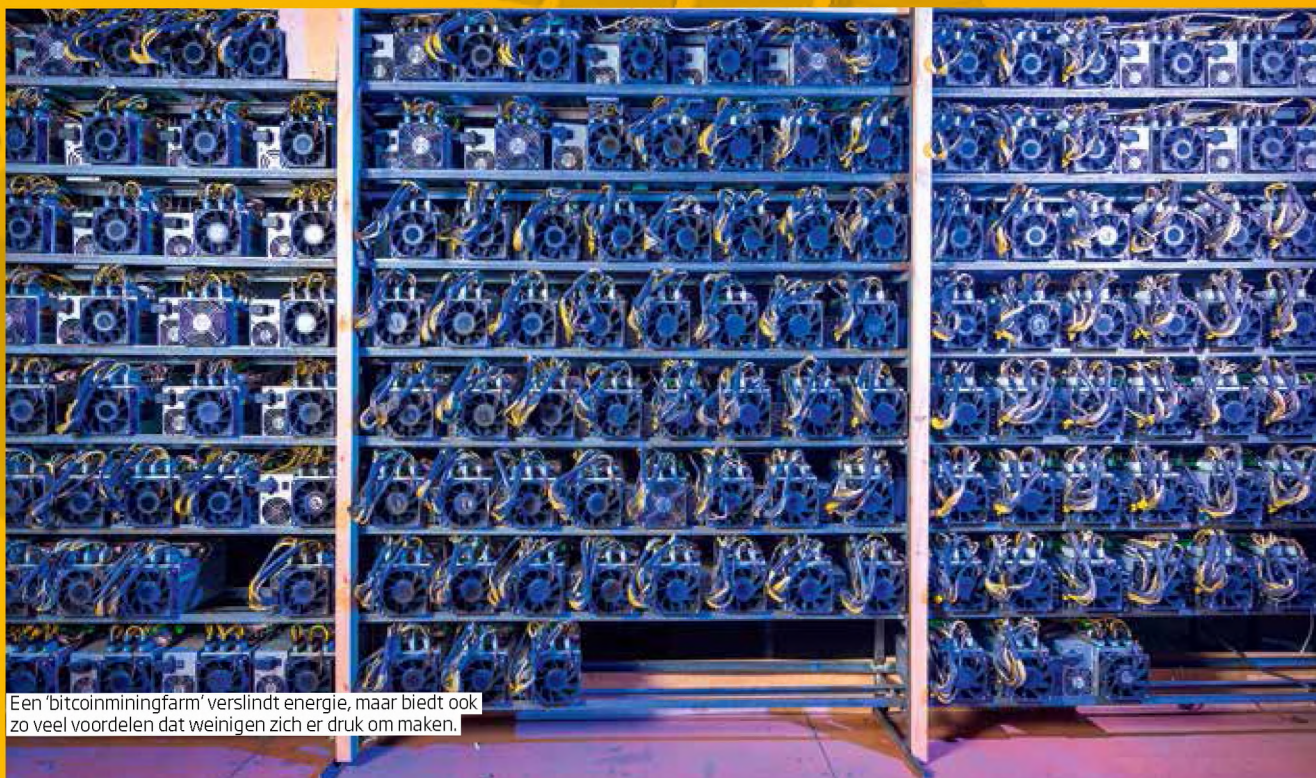
en ontvangen worden op slot gaan. Hoe de encryptie precies werkt, is niet bekendgemaakt. Het grote verschil met diensten zoals WhatsApp is dat BitVault een eigen blockchain gebruikt om alle informatie centraal op te slaan. Zo blijven er geen metadata achter op een centrale server, wat bij WhatsApp wel het geval is. Het toestel kent bovendien vijf bitcoin-portemonnees en een eigen kluis, waarin de cryptovaluta worden opgeslagen. Vele malen veiliger dan bij een webdienst. Aldus de ontwikkelaars. ■

MAG 'T EEN BEETJE ZUINIGER?

Bitcoinmining verbruikt meer energie dan heel Ecuador bij elkaar – maar dat hoeft niet.

De bitcoin heeft een energieprobleem. De cryptocurrency en de blockchaintechnologie die erachter zitten, zijn lang gezien als de lonkende toekomst van transacties, waarin mensen vervangen zijn door een serie getallenverslindende computers. Maar nu blockchains en cryptocurrency's steeds meer gemeengoed worden, blijkt hoe ongelooflijk veel energie deze methode slurpt. Dit besef was aanleiding voor opmerkelijke houtje-touwtje-oplossingen, zoals huizen die verwarmd worden met de blockchain en 'duurzame mining'. Onlangs heeft de geestelijk vader van een van 's werelds grootste cryptocurrency-netwerken echter een ingrijpende verandering aangekondigd die het probleem echt moet oplossen.

Dat bitcoin energie slurpt, weten we al een tijdje. Dat heeft alles te maken met de manier waarop het de blockchain gebruikt. Elke transactie begint met een gebruiker die de details van die transactie stuurt naar een netwerk van verbonden computers. Daar wordt die informatie gekopieerd naar duizenden identieke onvervalsbare grootboeken. 'Een blockchain, en dus ook bitcoin, moet opereren op basis van de aanname dat geen enkele andere computer te vertrouwen is,' zegt Teunis Brosens, analist bij ING. Elke computer



Een 'bitcoinminingfarm' verslindt energie, maar biedt ook zo veel voordelen dat weinigen zich er druk om maken.

controleert daarom op een onafhankelijke manier een deel van de transactie. Dat proces wordt *mining* genoemd.

Dankzij mining kunnen computers geen nep-grootboeken maken. Ze moeten

Een aantal ondernemende bitcoinminers heeft daarom een systeem gemaakt waarmee de opgewekte warmte gebruikt kan worden om een ruimte op een aangename temperatuur te krijgen. De Russische

begon met minen het Green Energy Bitcoin Mining Project. Hierbij draait de mining op wind- en zonne-energie.

Maar is compenseren wel genoeg?

'Duurzame energie is leuk, maar aangezien het aanbod daarvan nog steeds schaars is, kan die energie weer niet gebruikt worden voor toepassingen waar de samenleving als geheel meer aan heeft dan aan bitcoinmining,' zegt Brosens.

Er is ook een radicalere oplossing: de werkwijze van blockchain veranderen. Vitalik Buterin, de bedenker van het cryptocurrencynetwerk Ethereum – iedereen kan hiermee blockchainapplicaties bouwen – kondigde onlangs een andere manier aan om transacties te valideren, namelijk 'proof of stake'.

Buterin meent, net als een groeiend aantal anderen, dat als alternatief voor het 'proof of work' een computer ook zijn betrouwbaarheid kan aantonen door een klein geldbedrag in een fonds te storten, dat teruggestort wordt als de validatie echt blijkt.

Deze benadering heeft volgens Brosens echter zwaarwegende nadelen. Proof of stake zou degenen met meer geld onevenredig kunnen bevoordelen. Maar tot nog toe heeft niemand een beter idee geopperd. ■

De radicalere oplossing: blockchain een andere werkwijze geven

'proof of work' kunnen laten zien: een afmattende cryptografische puzzel die zo veel processorkracht vereist dat valse posten opvoeren ondoenlijk is.

WINDENERGIE

Al dat gereken kost grote hoeveelheden energie. Volgens een recente schatting is het jaarlijkse energieverbruik van bitcoinmining zo'n 23,07 terawattuur, ruwweg de hoeveelheid elektriciteit die een land als Ecuador in een jaar verbruikt. En als de populariteit van bitcoin zou verdubbelen, geen onrealistische schatting, zou het netwerk net zo veel energie verslinden als vijf miljoen Amerikaanse huishoudens bij elkaar.

cryptocurrency-startup Comino hoopt er geld mee te kunnen verdienen.

Afgezien van een paar miners die op koude plekken wonen, hebben tot nu toe echter weinig mensen zich druk gemaakt om het energieverbruik van bitcoin. Maar daar lijkt verandering in te komen. Er duiken steeds meer concurrerende cryptocurrency's op die de strijd aangaan met bitcoin. Een groeiend aantal bedrijven bouwt zijn verdienmodel op de blockchain, onder meer in het vastgoed.

'Ik denk niet dat het genoeg is om de geproduceerde warmte te gebruiken,' zegt een bitcoinminer die zichzelf OgNasty noemt. Om een en ander te compenseren, startte OgNasty toen hij in 2012