

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

Door Chris Baraniuk, Niall Firth, Ruben Boyd

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.

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.

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 blockchaintechnologie 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 blockchaintechnologie 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 invoerde 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.’

Door Abigail Beall

CRYPTOSTEMMEN

Vloeibare 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

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 getalvervlindende computers. Maar nu blockchains en cryptocurrency's steeds meer gemeengoed worden, blijkt hoe ongelofelijk 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

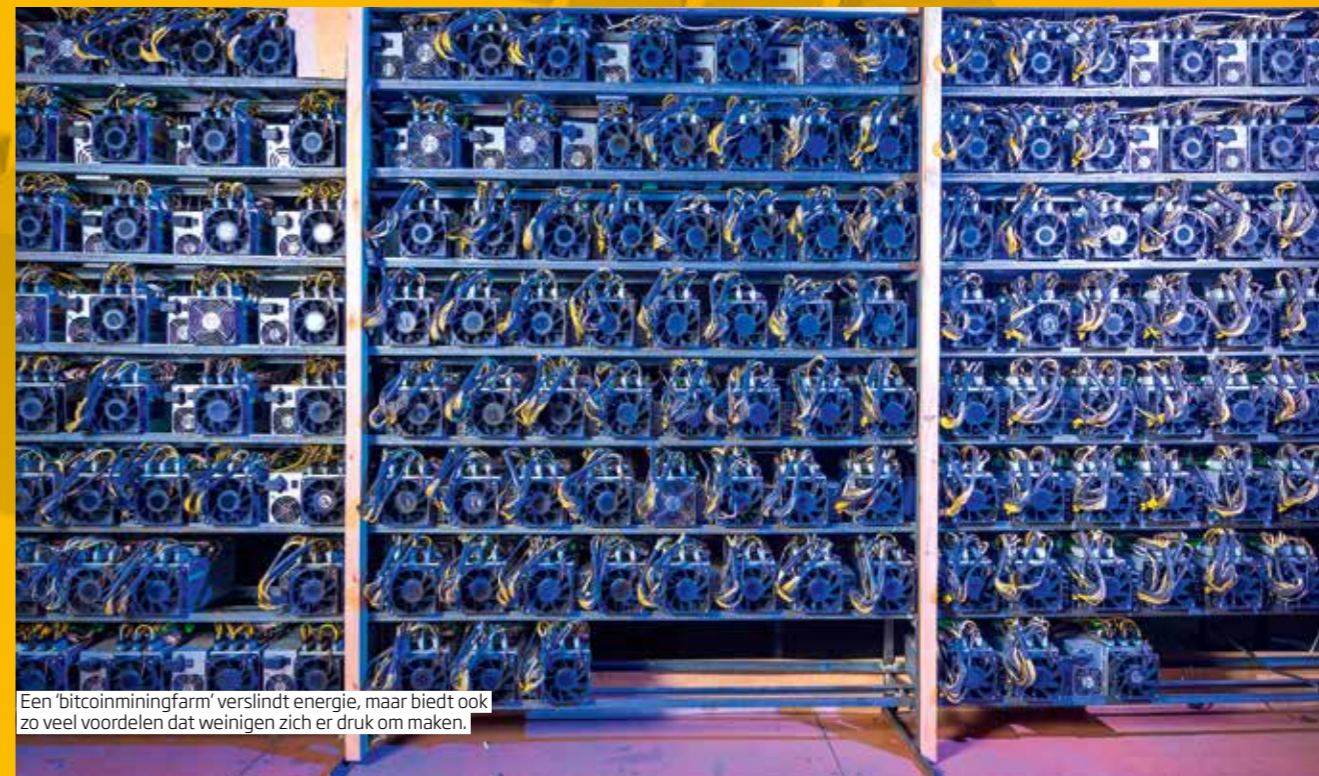
Ontwikkelaars noemen de blockchaintefoon een 'Zwitserse bank in je broekzak'

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. ■



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