tekst **RENS LIEMAN**

MONEY ₿ALL

Bitcoins *worden door steeds meer diensten en winkels (thuisbezorgd.nl, Starbucks) geaccepteerd. Maar lukt het bitcoins ook om de wereld te veranderen?*

We gebruiken sterke encryptie om data te beveiligen, we zouden hetzelfde moeten doen met ons geld

'Ik heb aan een nieuw, elektronisch geldnetwerk gewerkt dat volledig *peer-to-peer* is en waar dus geen derde vertrouwenspartij voor nodig is.' Zo begint Satoshi Nakamoto een e-mail die op 1 november 2008 wordt verstuurd naar cryptografen, nerds, wetenschappers en andere abonnees van The Cryptography Mailing List. Onderwerp: 'Bitcoin P2P e-cash paper'. Nakamoto, die tevens linkt naar een online witboek, 'bitcoin.pdf', vat in zijn mail dat nieuwe geldnetwerk samen: 'Het netwerk voorkomt dat iemand zijn geld twee keer kan uitgeven, geen [tussenpersonen], deelnemers aan het betalingssysteem kunnen anoniem blijven, nieuwe munten worden gemaakt door [het netwerk van gebruikers], dat tevens de drijvende kracht is achter het netwerk dat dubbele uitgaven voorkomt.'

Satoshi Nakamoto is op dat moment een onbekende naam in de cryptografiegemeenschap. Mede daarom wordt er aanvankelijk sceptisch gereageerd. In het witboek legt Nakamoto in zakelijke, technische bewoordingen de infrastructuur van Bitcoin uit, alsook de motivatie daarvoor. 'Hij' spreekt over 'we', al is het onduidelijk wie hij daarmee bedoelt. (Het is nog altijd onduidelijk of Nakamoto één persoon is of een groep – zie kader op de volgende pagina. In dit artikel wordt het enkelvoud aangehouden.) 'Wat we nodig hebben, is een elektronisch betaalsysteem dat gebaseerd is op cryptografie in plaats van op vertrouwen.

Zo zijn twee partijen, welke partijen dan ook, in staat direct online met elkaar zaken te doen. Digitale handtekeningen maken dat mogelijk, maar kunnen niet voorkomen dat iemand meer uitgeeft dan zou moeten kunnen. Wij stellen een peer-to-peer-netwerk voor dat dat wel kan.'

Nakamoto heeft een betaalsysteem bedacht waarbij gebruikers elkaar controleren. Vertrouwen in een bank of andere financiële instelling is niet meer nodig, noch is dat wenselijk, redeneert Nakamoto. Hij ziet zich daarin waarschijnlijk gesterkt door de economische crisis die medio 2007 uitbreekt en eind 2008 haar hoogtepunt bereikt. Belangrijke veroorzakers: schimmige hypotheken die mensen onmogelijk kunnen aflossen en een gebrek aan vertrouwen tussen banken onderling, waardoor die elkaar geen geld meer lenen. De belastingbetaler draait grotendeels op voor de gevolgen.

Bitcoin-pioniers zijn miljonair geworden door bitcoins te delven, te sparen of te verkopen

All ver voordat de financiële crisis uitbrak, werkte Nakamoto aan Bitcoin, maar hij presenteerde het anderhalve maand na de val van de Amerikaanse bank Lehman Brothers. Later, in februari 2009, schrijft hij op een peer-to-peer-forum: 'Het probleem met conventionele betaalmiddelen is het vertrouwen dat nodig is om het te laten werken. We moeten de centrale bank vertrouwen dat de valuta niet ineens minder waard wordt. We moeten banken vertrouwen dat ze ons geld veilig bewaren, maar in plaats daarvan leenden ze het uit via zeepbelkredieten en hielden ze weinig in reserve. En we moeten ze vertrouwen met onze privacy. We leven in een tijd waarin we sterke encryptie gebruiken om data te beveiligen. Het wordt tijd dat we hetzelfde doen met ons geld.'

Bitcoin was niet de eerste cryptovaluta. *Wall Street Journal*-journalisten Michael Casey en Paul Vigna schrijven in hun boek *The Age of Cryptocurrency* (Atlas Contact geeft een Nederlandse vertaling uit: *Het tijdperk van cryptovaluta*) over de in 1992 opgerichte cypherpunks-beweging en het daarbij behorende 'cryptoanarchisme'. Daar werd de basis gelegd voor Bitcoin: 'Cypherpunks is een groep van in cryptografie geïnteresseerde nerds die zich allemaal druk maakten over de toenemende aantasting van privacy en het steeds onmondiger worden van individuen in de moderne samenleving. Dit was lang voordat iemand had gehoord van Edward Snowden of zich bezighield met de term "big data". Een van de eerste ideeën van deze groep was een digitale munt.'

Binnen de cypherpunks werd gedacht over, en vaak ook software ontwikkeld om anoniem e-mails te versturen, anoniem informatie te verzamelen en te delen (via BlackNet, een voorloper van WikiLeaks) en te handelen met ontraceerbaar digitaal geld. Niet alles kon het daglicht verdragen, er zou ook nagedacht zijn over een anonieme marktplaats voor huurmoordenaars. 'Het streven van Bitcoin naar anonimiteit en vrijheidsgezinde principes zonder een centrale autoriteit was welhaast een reïncarnatie van de principes van de beweging uit de jaren negentig', schrijven Casey en Vigna. Cypherpunkers bedachten onder meer b-money, hashcash, bit-gold en DigiCash (in Amsterdam bedacht door de Amerikaan David Chaum); allemaal betaalsystemen gestoeld op vergelijkbare principes als dat van Bitcoin. Het verschil zat 'm vooral in hoe gebruikers bijdragen aan het systeem en hoe nieuw geld in het monetaire systeem terechtkomt. Uit die ideeën kwam Bitcoin voort – aan sommige daarvan refereert Nakamoto in het witboek.

Op 8 januari 2009 kondigt Nakamoto versie 0.1 van de Bitcoinsoftware aan. Voor het eerst kan iedereen die het programma downloadt aan bitcoins komen en die naar elkaar overmaken. Uit de *release notes* van Nakamoto: 'Compleet gedecentraliseerd, zonder een server of centrale autoriteit.' Nakamoto legt uit dat er uiteindelijk 21 miljoen bitcoins in omloop zullen zijn. De software is zo ingericht dat munten stapsgewijs in 'blokken' uitgegeven worden. De eerste vier jaar 10,5 miljoen (een blok van vijftig munten iedere tien minuten), de vier jaar daarna de helft van dat eerste bedrag, 5,25 miljoen (25 munten per blok iedere tien minuten), de vier jaar daarna weer de helft daarvan, enzovoorts. Totdat in 2140 de 21 miljoen bereikt is. Zo blijven vraag en aanbod – en dus de waarde van de valuta – in balans.

Gebruikers van de Bitcoinsoftware – beter gezegd: hun computers – zijn verantwoordelijk voor die uitgifte. Zij ontvangen de nieuwe munten ook; wie precies en hoe, daar komen we zo op. Eerst moet je weten dat diezelfde gebruikers ook verantwoordelijk zijn

WIE IS SATOSHI NAKAMOTO

Bitcoin-oprichter Satoshi Nakamoto trok zich medio 2010 terug, anderhalf jaar nadat de eerste versie van het programma gepresenteerd werd. De basis voor het systeem was gelegd, het was nu aan de gemeenschap de toepassingen verder te ontwikkelen – de programmacode van Bitcoin is voor iedereen beschikbaar. Er is nog altijd geen sluitend bewijs over wie Nakamoto is of wie het zijn, ondanks verwoede pogingen van journalisten over heel de wereld en inmiddels meerdere speculaties over de anonieme oprichter. De recentste poging-tot-ontmaskering was in december 2015, toen technologiemagazine Wired en website Gizmodo tegelijkertijd onthulde dat achter Nakamoto de Australische oud-academicus Craig Steven Wright schuil ging. Wright bevestigde dat op zijn blog, deelde wat hij zag als cryptografisch bewijs daarvoor maar stuitte daarbij op een bitcoingemeenschap die het bewijs onvoldoende vond. Wright postte later een cryptisch bericht: 'Ik had me voorbereid om bewijs te overleggen, maar brak. Ik heb de moed niet. Ik kan niet.'


Edward Snowden, hier op 29-jarige leeftijd, in Hong Kong.


Guo-hua controleert de servers in Bitcoins mine site in de Chinese provincie Sichuan.

In The Old Fitzroy Pub in Sydney kun je met bitcoins je bier afrekenen.


Het huis van Craig Wright in Sydney, waar de politie in 2015 een inval deed.

Een bitcoin-automaat (BTM) op een beurs in New York.

Een winkelsticker in Berlijn geeft aan dat hier bitcoins worden geaccepteerd.

De echte Satoshi Nakomoto, die niet de bedenker van bitcoin bleek te zijn.

Opening van de eerste bitcoin-winkel, in Hong Kong, 2014.

Een casino in Las Vegas waar bitcoins als betaalmiddel gelden.

Fotografie GETTY IMAGES

voor het controleren van elke bitcointransactie. Als gebruiker X iets naar Y wil overmaken, controleren de computers van A en B of X dat bedrag daadwerkelijk te besteden heeft. Dat gebeurt door naar de eerdere transacties van X te kijken – alle transacties van alle Bitcoingebruikers worden opgeslagen in een digitaal logboek. Die controle is in feite een wiskundesom, een cryptografische puzzel. De gebruiker wiens computer als eerste de som heeft opgelost, wordt voor zijn inzet (lees: de energie die zijn computer verbruikt) beloond met een nieuw blok bitcoins. Dit verificatieproces en de daarbij behorende beloning van nieuwe munten wordt *mining* genoemd: delven.

De moeilijkheidsgraad van de puzzel wordt automatisch hoger naarmate er meer computers meedoen aan dit proces, zodat de uitgifte van nieuwe munten niet te snel gaat. Daardoor is bitcoins delven een uiterst gespecialiseerde bezigheid geworden. In China en Amerika zijn er heuse 'bitcoinmijnen': fabriekshallen vol superkrachtige computers die uitsluitend hiervoor ingezet worden. Voor het individu is bitcoins delven niet meer mogelijk, wel kan hij zich aansluiten bij een groep, wat hem op een fractie van de eventuele beloning komt te staan.

In het vroege stadium van Bitcoin was dat anders. Satoshi Nakamoto was uiteraard de eerste delver, maar met geen enkele transacties om te controleren was dat een fluitje van een cent. Daar werd Nakamoto overigens toen niet rijk van, bitcoins hadden nog geen waarde. (Nu wel; cryptograaf Sergio Lerner maakte een *educated guess* dat Nakamoto ongeveer een miljoen bitcoins moet hebben die nu 642,4 miljoen euro waard zouden zijn.) Wie er vroeg bij was, kon gewoon met zijn eigen laptop bitcoins delven. Hal Finney was zo iemand, cryptograaf en tevens mede-ontwikkelaar van Pretty Good Privacy (PGP). Direct nadat de eerste versie van de Bitcoinsoftware was te downloaden, deed hij dat. Op Bitcoinforum bitcointalk.org schrijft hij dat hij na een paar dagen al enkele blokken (van dus elk 50 bitcoins) gedolven had. Finney, die met Nakamoto in contact kwam en hem hielp bij het ontwikkelen van de software, zou veel geld verdienen met zijn bitcoins, maar stopte al snel met delven omdat zijn computer te heet werd en te veel lawaai maakte. Zijn kapitaal van omgerekend een geschatte zestigduizend euro heeft hij omgezet naar 'echt geld' voor zijn nabestaanden (Finney overleed aan ALS). Andere Bitcoinpioniers zijn miljonair geworden door bitcoins te delven, te sparen of te verkopen.

Zij die de nieuwe bitcoins ontvingen, konden daar aanvankelijk nog weinig mee, behalve ze overmaken naar andere gebruikers of opslaan op de eigen rekening, een *wallet* in Bitcoin-terminologie. Zo'n digitale portemonnee staat op je computer, smartphone, USB-stick of ergens op een server. Naarmate er meer gebruikers kwamen, werd er meer mee gehandeld. Er kwamen bijvoorbeeld wisselkantoren waar je bitcoins kon kopen of verkopen voor dollars of euro's. Het aantal producten of diensten dat je met bitcoins kunt betalen groeit tegenwoordig dagelijks. In Nederland accepteerde Thuisbezorgd.nl drie jaar geleden als eerste grote dienst bitcoinbetalingen. Inmiddels kun je er bij enkele honderden webshops, cafés, autoverhuurbedrijven, loterijen en andere zaken mee betalen. In Amerika kun je je kop koffie ermee afrekenen bij Starbucks, je vakantie op de site van Expedia en je meubels op webshop Overstock. Met dit soort grote en kleine bedrijven die bitcoins als betaalmiddel accepteren, verliest Bitcoin steeds iets van zijn – in de ogen van de massa – schimmigheid.

Finney stopte met het delven van bitcoins, omdat zijn computer te heet werd en te veel lawaai maakte

De waarde van geld zit 'm niet in het betaalmiddel zelf, niet in de katoenlinnenmix waarvan eurobiljetten worden gemaakt. Het gaat om hoeveel je ermee kunt kopen. Toch voelt een bitcoin voor de meesten vooralsnog minder waardevol dan het equivalent in euro's (op het moment van schrijven: 632 euro), simpelweg omdat het iets digitaals is. Bitcoins zijn een *string*, een reeks cijfers en getallen op je scherm. Euro's zijn tastbaar, en de overheid garandeert dat we er overal mee kunnen betalen.

Daarbij komt dat Bitcoin een imagoprobleem heeft, namelijk dat criminelen er graag mee handelen vanwege het anonieme karakter ervan. Daaraan dankt Bitcoin overigens ook een groot deel van zijn bekendheid: op internetmarktplaats Silk Road, waar veel drugs, wapens en andere illegale waar werd verhandeld, kon uitsluitend met bitcoins worden betaald.

Ander nadeel: de koers fluctueert heftig (december 2013: 950 dollar, december 2014: 350 dollar, december 2015: 450 dollar). En er was een reeks incidenten waarbij hackers miljoenen aan bitcoins stalen. Onze huidige munt is evenmin waterdicht: bankrekeningen en creditcardgegevens kunnen gehackt worden, overheden kunnen een munt desastreus laten inflateren, criminelen kunnen contant geld witwassen. Toch zullen veel mensen meer vertrouwen in de euro hebben dan in de bitcoin. En zonder vertrouwen sneuvelt elk monetair systeem.

Rationeel bekeken liegen de voordelen van Bitcoin er niet om. Met bitcoins ligt de macht niet langer bij een paar banken – de macht over hoeveel een transactie kost en hoe die gevalideerd wordt, maar ook wie er wel en niet een bankrekening mag openen of lening mag afsluiten. Niet langer is iedere betaling terug te herleiden tot de koper, waarmee zijn bewegingen in kaart gebracht kunnen worden als de autoriteiten dat nodig achten. Voor winkeliers zullen transactiekosten omlaag gaan, evenals bancaire kosten voor de consument. Betalingen, of ze nu over de landsgrens plaatsvinden of niet, zijn in enkele minuten in plaats van dagen voltooid. Klein bier, zeg je? Casey en Vigna berekenden de kosten van creditcard- en pintransacties in 2013 die Visa en MasterCard gezamenlijk wereldwijd verwerkten: 250 miljard dollar.

Voor het ware potentieel van cryptovaluta moeten we verder kijken dan betalingen en ons meer richten op dat logboek, de blokkenketen. In theorie kunnen daar ook afspraken over hypotheken, verzekeringen en contracten in staan en gevalideerd worden. In zo'n wereld hoeven we geen vertrouwen meer in instanties en in elkaar te hebben, alleen nog maar in de wiskunde.