
DE GROENE AMSTERDAMMER

Iedereen

De politiek achter bitcoin

Anarchistische droom of technocratische nachtmerrie?



De uitvinding van crypto currencies zoals bitcoin kwam voort uit activisme. Maar in hoeverre is de droom van een toekomst zonder staatsspionage en neoliberal corporatisme te realiseren?

door Wessel Reijers 03-11-2015

Wie een kijkje wil nemen in de toekomst hoeft niet per se te wachten op Disney's nieuwste *Star Wars*-film, maar kan ook genoeg nemen met de literatuur over Crypto Currencies. In zijn ondertussen legendarische *White Paper* (2008) legt de tot dusver anonieme uitvinder van bitcoin, Satoshi Nakamoto, in zakelijke termen uit hoe het geld van de toekomst kan worden gebruikt zonder te hoeven vertrouwen in derde partijen zoals centrale en commerciële banken. Een revolutionair idee.

Maar Nakamoto was niet de eerste die hiermee kwam; 23 jaar eerder, ver voor de komst van bitcoin, Google en Paypal, schreef de in Amsterdam werkzame wetenschapper David Chaum al over de mogelijkheden van decentrale technologieën als *crypto currencies* in de informatiesamenleving:

De angstaanjagende effecten van toenemende mogelijkheden voor surveillance kunnen leiden tot een afname in de vrijheid van expressie en van deelname aan de maatschappij (...) Vergevoerde online-marketingtechnieken die werken met digitale persoonlijke profielen worden nu ingezet om de publieke opinie en politieke verkiezingen te manipuleren. *Decentrale applicaties bieden niet alleen de mogelijkheid om deze problemen aan te pakken, maar ook om de democratie te versterken.* In deze paar zinnen worden alternatieven aangekondigd voor zowel de online economie als voor ons politieke stelsel. Daarnaast anticipeert Chaum al op de destructieve marketingpraktijken van internetgiganten zoals Google en Facebook.

De activistische insteek van Chaums tekst is nauwelijks te missen en is terug te leiden tot de anarchistische *roots* van crypto currencies in de zogenoemde cypherpunk-beweging: een gekleurd gezelschap van anarchistisch georiënteerde hackers, wetenschappers en activisten.

Crypto currencies komen voort uit een anarchistische droom over een toekomst zonder staatsspionage en neoliberal corporatisme.

De vraag is alleen: heeft deze droom enige kans van slagen?

Bitcoin in de tijd van rekeningrijden en Bill Clinton

De eerder genoemde David Chaum werkte in de jaren negentig aan een belangrijke voorloper van bitcoin voor het Centrum Wiskunde & Informatica (CWI) in Amsterdam. De technologie die hij in zijn tijd bij het CWI ontwikkelde stond centraal binnen het spin-off-bedrijf Digicash dat onder meer samenwerkte met de Nederlandse overheid om een anoniem betalingssysteem te realiseren voor het (herinnert u het zich nog?) controversiële rekeningrijden-project.

Chaums Digicash maakte even een enorme groei door en stond op het punt om grote contracten af te sluiten met overheden, banken en creditcardmaatschappijen. De technologie was zijn tijd echter ver vooruit en uiteindelijk strandde Digicash in een faillissement.

In een *Forbes*-artikel uit 1999 werd de technologie doodverklaard, onder de titel: *Requiem for a Bright Idea*.

De geschiedenis nam een andere wending in 2008. Vlak na het uitbreken van de financiële crisis, en jaren na de oprichting van Digicash, werd de crypto-currencydroom weer tot leven gewekt door de mysterieuze Nakamoto Satoshi, op een mailinglist voor crypto-fanatiekelingen.

Van Amsterdam naar Silicon Valley naar de City

Nadat het project van de crypto currencies zijn eerste kinderstapjes had gezet richting succes in Amsterdam maakte het zijn pubertijd door in Silicon Valley met de komst van bitcoin.

Aanvankelijk kreeg het *White Paper* van Nakamoto Satoshi echter weinig bijval. Het realiseren van een crypto currency was eerder geprobeerd, tot dan toe zonder succes. Dus waarom zou bitcoin wél slagen? Satoshi's idee was echter revolutionair in twee opzichten: zijn ontwerp was gebaseerd op een onaantastbare 'universal ledger' (ook de *blockchain* genoemd), en op een uniek systeem van beloningen om de deelnemers aan het peer-to-peer-netwerk (de 'miners') aan te moedigen om het systeem met transacties te onderhouden.

Dat klinkt nogal ingewikkeld...?

De technische details buiten beschouwing gelaten zou men de blockchain kunnen omschrijven als een publieke boekhouding met daarin alle transacties verwerkt vanaf de eerste bitcointransactie tot nu. Iedere tien minuten valideren alle miners gezamenlijk de meest recente transacties om fraude te voorkomen en voegen ze die in een 'block' toe aan de groeiende digitale keten. Zo wordt de integriteit van bitcoin gegarandeerd door de gebundelde krachten van de miners.

De technologische mogelijkheden van de blockchain zijn niet beperkt tot nieuwe vormen van geld, maar kunnen ook worden benut voor het creëren van allerlei soorten van 'slimme' contracten. Het zou bijvoorbeeld kunnen dat we in de nabije toekomst een blockchainhuwelijk sluiten, een blockchainverzekering afsluiten of de blockchain gebruiken om te stemmen. Vanwege de bijna 'onbegrensde' mogelijkheden van de blockchain is er

een groeiende interesse in de technologie vanuit verschillende hoeken.

Dat bitcoin hierdoor ondertussen ver verwijderd is geraakt van de hobbyprojecten van crypto-anarchisten en wetenschappers blijkt wel uit de grote interesse die nu wordt getoond voor de blockchaintechnologie door overheden en bedrijven. Vandaag de dag investeren in ieder geval tien wereldwijd opererende banken in de blockchaintechnologie en deze zomer is de Britse bank Barclays begonnen met een bitcoinpilot. Tegelijkertijd zijn overheden druk bezig om deze nieuwe technologie te reguleren.

Nu de conventionele machten van de financiële wereld en Silicon Valley de blockchain hebben geadopteerd moeten de anarchisten zich wellicht achter de oren gaan krabben: zal hun crypto-anarchistische droom niet verworden tot een neoliberale nachtmerrie?

De anarchistische droom

Voor buitenstaanders lijkt het aanvankelijk alsof bitcoin en anarchisme weinig met elkaar te maken hebben. Bitcoin: dat gebruiken mensen toch om online te speculeren? Het wordt toch vooral gebruikt door criminelen om drugs te verkopen... en dat minen van bitcoins is toch ongelooflijk slecht voor het milieu?

Wellicht is daar een eerste overeenkomst tussen bitcoin en anarchisme gevonden: ze hebben beide last van een imagoprobleem.

Wie zich echter verder verdiept in de mogelijkheden van de blockchain en de achterliggende ideologie ziet opeens helder in waarom bitcoin en anarchie het goed met elkaar kunnen vinden. En wel om twee redenen:

de blockchain is perfect geschikt voor decentrale organisatie,

en:

de blockchain kan taken op zich nemen die nu bij de overheid horen.

De eerstgenoemde eigenschap zorgt ervoor dat de macht over de technologie gespreid wordt in plaats van dat ze in handen is van een centrale organisatie zoals een staat of een bedrijf. De spreiding van macht is ook een van de belangrijkste idealen van het anarchisme. Niemand kan individueel de blockchain manipuleren of beheersen en dus is de macht in de handen van het netwerk, in de handen van het 'volk'.

Dat dit principe nuttig is bij het tegengaan van centrale macht is gebleken in 2011. In dat jaar blokkeerden de belangrijkste Amerikaanse betalingservices

(creditcardmaatschappijen en Paypal) de betalingen richting WikiLeaks, een van de belangrijkste fronten van de cyber-anarchisten. De filosoof en activist Denis Roio laat zien hoe deze gebeurtenis een averechts gevolg had, omdat het juist een reden bood om te zoeken naar een decentraal alternatief: bitcoin.

De tweede eigenschap van de blockchain is echter misschien nog wel krachtiger, en dat is de mogelijkheid om de technologie in te zetten om enkele kerntaken van de overheid over te nemen. In een online documentaire over de crypto-currencyrevolutie[14] wordt dit idee uitgelegd aan de hand van de huidige vluchtelingencrisis.

We kunnen een vluchtelingenkamp beschouwen als een staat in het klein maar dan zonder een regering. Hoe zouden de mensen die in zo'n kamp wonen gebruik kunnen maken van vitale overheidsdiensten? Het antwoord: als al die mensen een smartphone hebben, en toegang hebben tot een netwerk, kunnen ze hun eigen decentrale applicaties bouwen – *'on the spot'*.

Zo kunnen vluchtelingen zonder tussenkomst van een staat decentraal hun eigen geldsysteem realiseren, hun eigen systeem van eigendomsrechten en hun eigen verzekeringen.

Dat mensen zich 'spontaan' kunnen organiseren zonder tussenkomst van een centrale autoriteit is ook een belangrijk ideaal voor het anarchisme. De blockchaintechnologie lijkt daarom een wereld mogelijk te maken waarin de anarchistische droom eindelijk werkelijkheid kan worden.

De vraag is echter of we niet ook een prijs betalen voor deze verandering. En of dit toekomstbeeld, dat velen van ons als muziek in de oren klinkt, een uitgemaakte zaak is. Kan deze technologische transitie worden gerealiseerd zonder een politieke beweging die ervoor vecht?

Technologisch determinisme en de mogelijke nachtmerrie

Voor sommigen binnen de cypherpunk-beweging zal de laatste vraag met 'ja' worden beantwoord. Zij zullen het idee aanhangen dat technologische veranderingen uiteindelijk de loop van de geschiedenis dicteren. De blockchaintechnologie zal de wereld veranderen – of we het willen of niet, zullen zij zeggen. Nog specifieker: de technologie zal de wereld veranderen op de manier zoals zij het voorzien. Met andere woorden: we stevenen *onherroepelijk* op een wereld af waarin we geen overheid en grote bedrijven meer nodig hebben en ons decentraal organiseren.

Ik ben sceptisch over dit idee, en wel vanwege drie redenen.

Ten eerste wijst de geschiedenis erop dat de idealen van de makers van een technologie lang niet altijd werkelijkheid worden. Het internet (als *the world wide web*) was bijvoorbeeld ontworpen als een neutraal netwerk dat vrije uitwisseling van informatie voor iedereen mogelijk zou maken. Vandaag de dag weten we dat grote bedrijven als Google en Facebook en centrale overheden dit ideaal effectief en succesvol tegenwerken. In plaats van vrije informatie hebben we nu 'gepersonaliseerde' informatie, toegespitst op onze specifieke wensen als consument. Ook kijkt de overheid altijd mee over onze digitale schouders en beheersen grote bedrijven onze persoonlijke identiteiten.

Ten tweede bestaat de cypto-currencybeweging uit ten minste twee fundamenteel verschillende groepen die tot dusver gezamenlijk optrekken. De ene groep, bestaande uit de idealisten van het eerste uur, hangt de originele anarchistische gedachte aan en ziet crypto currencies voornamelijk als een mogelijkheid om de wereld te veranderen, niet als een manier om geld te verdienen. Deze groep keert zich zowel tegen de staat als tegen de macht van het grootkapitaal. De andere groep, die zich voornamelijk schaart onder de ideologie van het Amerikaans libertarisme, bestaat uit ondernemers en investeerders. Deze groep deelt de afkeer tegen de centrale staatsmacht, maar stelt zich veel sympathieker op ten opzichte van globale corporaties in Silicon Valley.

Nicholas Negroponte, de oprichter van het medialab aan het MIT, waarschuwde al voor deze tweedeling. De grootste vergissing die jullie kunnen begaan, vertelt hij de bitcoin-community, is bitcoin te zien als een manier om geld te verdienen. Zijn advies is daarom: organiseer je enkel als non-profit en maak exclusief deel uit van de publieke sfeer.

Ten derde, en dit is wellicht het belangrijkste bezwaar, behelst de blockchaintechnologie een verborgen paradox. Deze paradox wordt door de Canadese onderzoeker Quinn Dupont aan het licht gebracht in zijn paper *The Politics of Cryptography*. Hij beargumenteert dat crypto currencies niet alleen staan voor hun anarchistische idealen van persoonlijke privacy en decentrale organisatie, maar ook voor een 'politiek van orde' in de 'controlemaatschappij'. Het blockchainprotocol, volgens Dupont, komt angstaanjagend dicht in de buurt van het idee dat softwarecode onze wetten kan vervangen.

Wat gebeurt er met onze vrijheid als iedere menselijke handeling kan worden vastgelegd in digitale, contractuele vorm? Voor degenen die zich interesseren voor politieke filosofie: men zou kunnen zeggen dat de blockchaintechnologie kan worden gezien als de realisatie van de leviathan in de werken van Thomas Hobbes, de meest perfecte realisatie van de soevereine macht. Anarchisten moeten zich daarom wellicht gaan afvragen: wat betekent deze sociale controle precies voor ons ideaal van individuele vrijheid?

Het is duidelijk dat de blockchain een krachtige technologie is die het potentiëel heeft om onze maatschappij revolutionair te transformeren. Juist vanwege dit potentiëel is het

belangrijk om het publiek bij deze ontwikkeling te betrekken, en om de politieke implicaties van deze technologie te verkennen. Dit betekent dat de technologie toegankelijk moet worden gemaakt voor mensen die geen technisch expert zijn. We moeten op z'n minst proberen om de implicaties van deze technologie uit te leggen aan ieders vrienden, burens en familie.

Daarnaast moeten we de aanname dat de technologie onherroepelijk zal leiden tot positieve uitkomsten zonder politieke tussenkomst sterk in twijfel trekken. Het idee dat mensen zich los van een centrale autoriteit kunnen organiseren is een krachtige, positieve boodschap, maar ook een boodschap die verdedigd moet worden. Dit betekent dat we vraagtekens moeten zetten bij de investeringen van banken en overheden in de blockchaintechnologie. Ook moeten we vraagtekens zetten bij initiatieven die de blockchain zien als een belangrijke *'business case'*, die uiteindelijk blockchain en het grootkapitaal hand in hand zien gaan.

Als reactie moeten we actief op zoek naar een 'politek' achter de blockchaintechnologie. De anarchistische idealen waar de technologie op rust moeten expliciet worden gemaakt en onderdeel worden van een publiek discours. Ook moeten we ons gaan afvragen wat de effecten zullen zijn van de 'sociale controle' die de blockchain afdwingt en vooral waar we deze wel of juist niet willen inzetten.

Welke menselijke relaties willen we eigenlijk vastleggen door middel van de blockchaintechnologie? En zijn er bepaalde menselijke sferen, bijvoorbeeld de familiesfeer, de zorg, het onderwijs, waarin we de toepassing van de blockchaintechnologie actief moeten tegengaan?

Ik pleit ervoor om deze vragen op korte termijn onderdeel te laten worden van het publieke discours, om de anarchistische droom van crypto currencies niet te laten verworden tot een technocratische nachtmerrie.

Chaum, David. 1985. "Security without Identification: Transaction Systems to Make Big Brother Obsolete." *Communications of the ACM* 28 (10): 1030–44. doi:10.1145/4372.4373.

DuPont, Q. 2014. "The Politics of Cryptography: Bitcoin and The Ordering Machines." *Journal of Peer Production* 1: 1–10.

Naughton, John. 2000. *A Brief History of the Future: The Origins of the Internet*. Vol. 7. London: PHOENIX PAPERBACK. doi:10.1177/1744935912438311.

Roio, Denis Jaromil. 2013. "Bitcoin, the End of the Taboo on Money." *Dyne.org Digital Press*, no. April: 1-17.

Vigna, Paul, and Michael J. Casey. 2015. *The Age of CryptoCurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: St. Martin's Press.

Beeld: het Bitcoin logo. Foto Duncan Rawlinson / Flickr