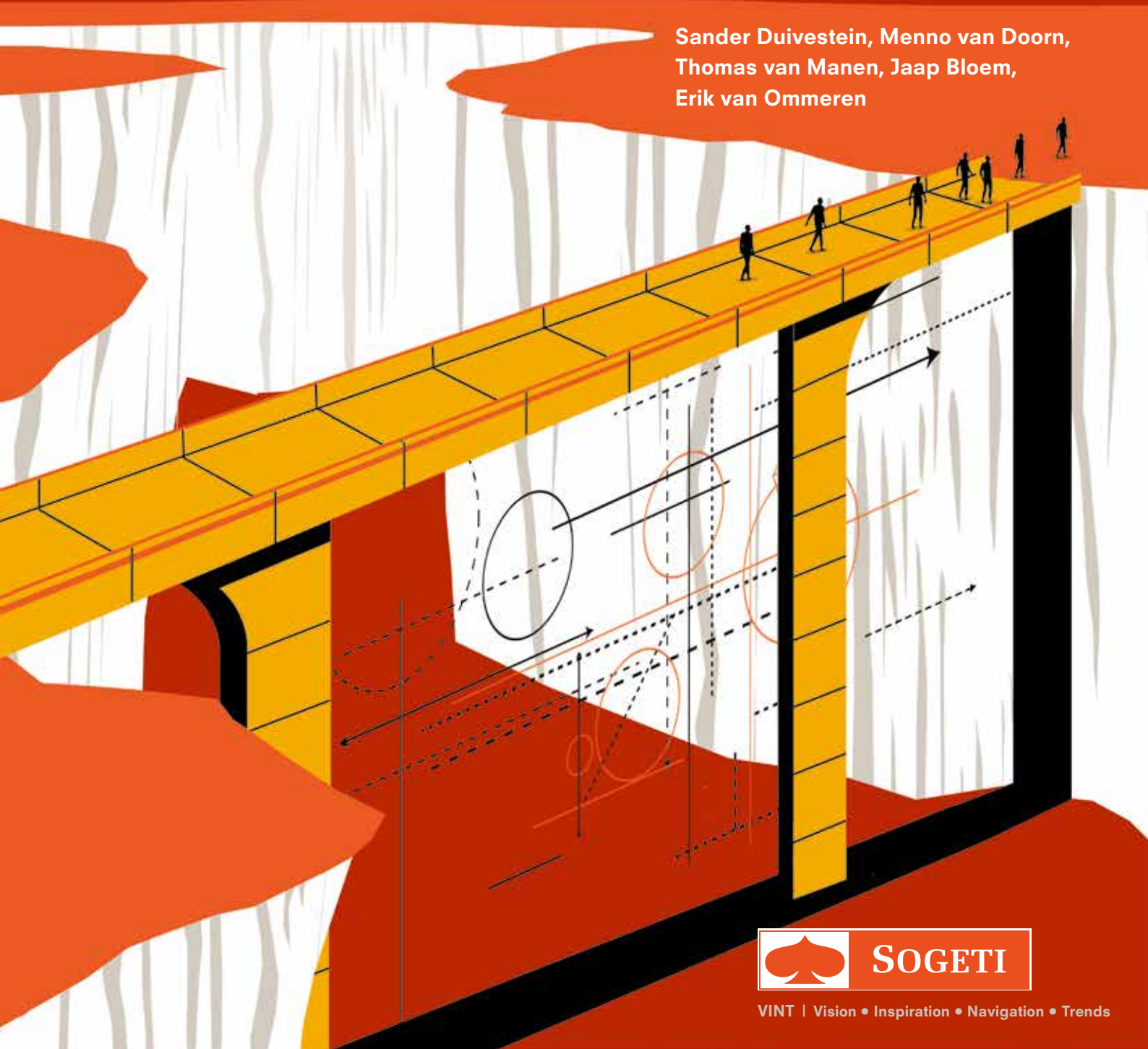


DESIGN TO DISRUPT

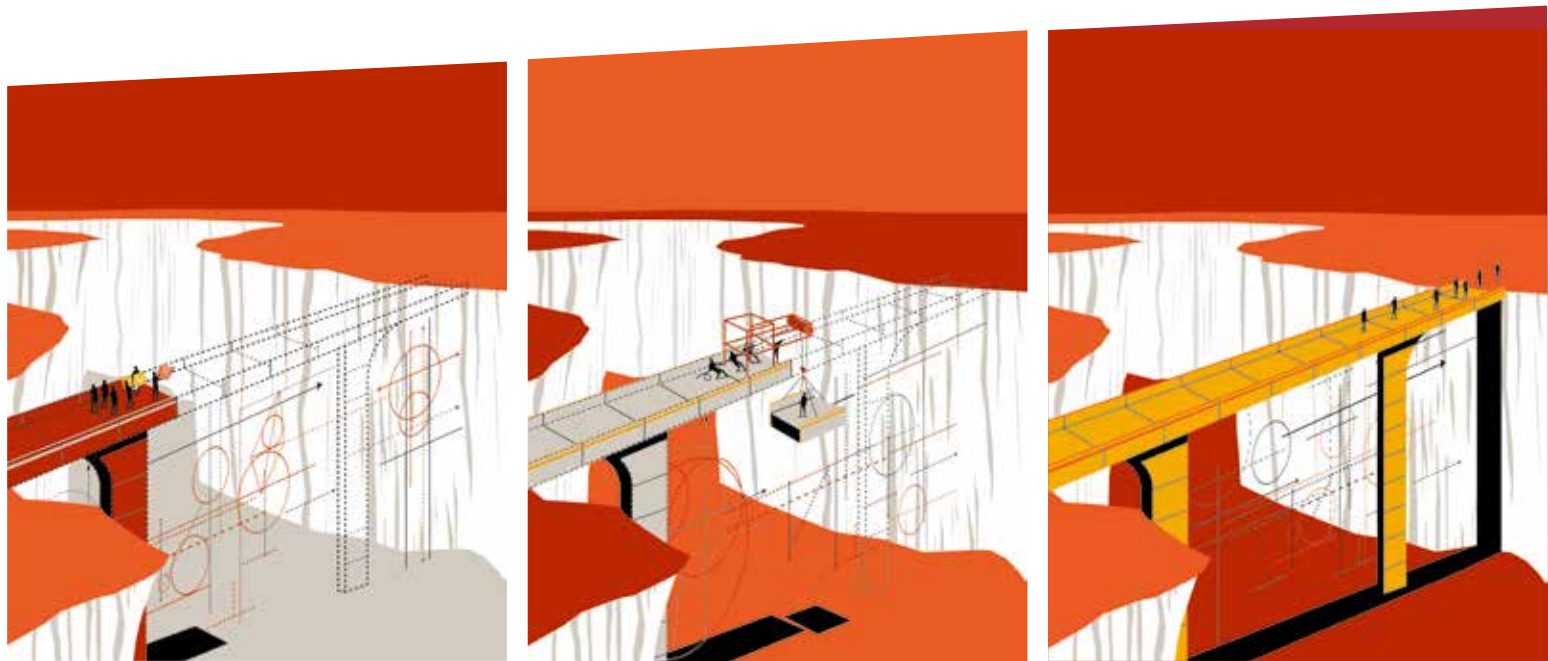
Blockchain: cryptoplatform voor een
frictieloze economie

Sander Duivestein, Menno van Doorn,
Thomas van Manen, Jaap Bloem,
Erik van Ommeren



SOGETI

VINT | Vision • Inspiration • Navigation • Trends



INHOUD

Design to Disrupt 3

Inleiding: een nieuwe vertrouwensbasis 4

Opbouw van dit rapport: drie versies van de crypto-economie 6

Hoofdstuk 1 Crypto-economie 1.0 – de munt 7

Zaaien op een vruchtbare bodem 7

Introductie in cryptovaluta 7

Wat is een bitcoin en wat is een blockchain? 8

Zijn er andere munten dan de bitcoin? 8

Hoe werkt Bitcoin? 8

Hoe worden bitcoins gemaakt? 10

Frauduleuze transacties uitsluiten met een cryptopuzzel 11

Shared single source of truth 11

De zeven voor- en nadelen van Bitcoin 12

Wie dan wel? A Bitcoin Governance Framework 16

Hoofdstuk 2 Crypto-economie 2.0 – slimme contracten en dingen 17

Een nieuw protocol 18

De Blockchain Application Stack 18

Bitcoin en het Internet of Things 22

Device Democracy 24

Slimme contracten 24

Slimme eigendomsrechten 26

Hoofdstuk 3 Crypto-economie 3.0 – de Robocorps 27

Tradenet 27

Robocorps, DAO's en DAC's 28

Taxi's, overheid, uitzendbureaus 29

Decentrale Autonome Overheden 29

Virtual reality en de blockchain 30

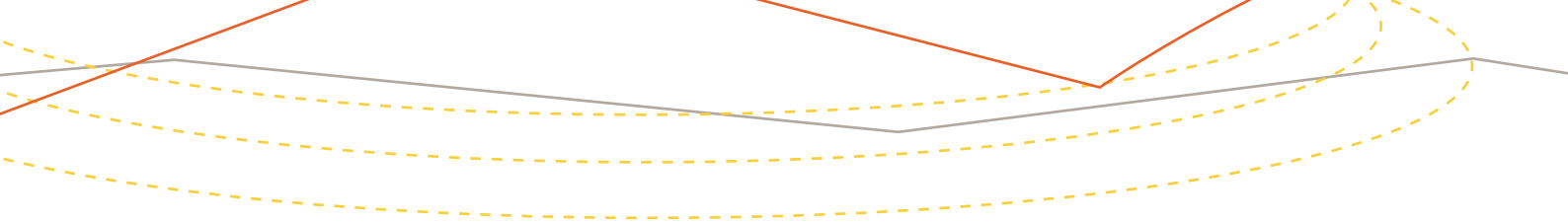
Tot slot: het nieuwe organisatieparadigma 30

De toekomst is decentraal 30

Tot slot: conclusie en overwegingen voor business executives 31

Verklarende woordenlijst 34

Literatuur 36



DESIGN TO DISRUPT

‘Disruptie is Het Nieuwe Normaal.’ Dat is de kernboodschap uit de executive introductie van deze publicatiereeks. In dat eerste rapport beschrijven we de exponentiële groei van digitale mogelijkheden. Start-ups duiken in het gat en dagen de gevestigde orde uit. Ook de snelheid waarmee innovaties aanslaan neemt toe. Tegenover die expansie staat de trage reactie van organisaties die de digitale wervelwind niet kunnen bijbenen. Van dit fenomeen, ook wel bekend als Eroom’s Law (de omgekeerde Wet van Moore), worden steeds meer organisaties zich bewust.

In de tweede notitie ‘Nieuwe digitale concurrentie’ stonden de uitdagers centraal. Weinig gevestigde organisaties hebben ze al vroeg in het vizier, want ze komen vaak van buiten de eigen sector en worden aanvankelijk niet serieus genomen. Hun vermeend inferieure proposities zetten toonaangevende spelers op het verkeerde been, terwijl die juist een open oog moeten hebben voor disruptieve innovatie. Dit innovatorsdilemma brengt ons terug bij de belangrijkste vraag van dit Design to Disrupt-project: hoe ontwerp je als organisatie je eigen disruptieve marktmogelijkheden?

Dit derde rapport staat in het teken van een geheel nieuw designprincipe. Het beschrijft de potentiële impact van blockchain, een nieuwe manier om vertrouwen te organiseren in de aanwezigheid van onbetrouwbare partijen. Deze is nu vooral bekend vanwege de munt, de bitcoin, maar de cryptografische capaciteiten van het netwerk kunnen op tal van andere manieren worden ingezet. Het is een speciaal soort platform, dat de basis vormt om tal van andere platformen op te bouwen. Een platform voor platformen dus. De relevantie hiervan voor organisaties zetten we uiteen in drie stappen: de crypto-economie 1.0, 2.0 en 3.0.

‘Think about the blockchain as another class of thing, like the Internet – a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money. In fact it is even more, the blockchain concept is a new organizing paradigm.’

Melanie Swan, Institute for Blockchain Studies

INLEIDING: EEN NIEUWE VERTROUWENSBASIS

Welkom in de wondere wereld van de complexe en fantasierijke crypto-economie. De wereld van blockchain en bitcoin, van miners, sandboxes en hashes. Wie nog helemaal niet ingevoerd is in deze materie, kan gauw in de ban raken van de fascinerende en snel groeiende crypto-omgevingen. Ook voor wie zich al meer in de materie heeft verdiept, blijven elementen van de crypto-economie vaak nog mysterieus en enigszins ongrijpbaar.

**“The first five times you think
you understand it, you don’t”**

Dan Kaminsky,
American Security Researcher



Het grapje waarschuwt voor de serieuze kost die u voorgeschoteld krijgt. Zowel de werking als de mogelijkheden van de blockchain kunnen soms een harde noot zijn om te kraken. Het leesadvies hierbij luidt: lezen, terugbladeren en herlezen, bronnen waarnaar we verwijzen erbij pakken en doornemen. Als u gegrepen bent en aan een eigen innovatie wilt gaan denken, blijf dan ook switchen tussen werking en mogelijkheden. Beide komen zoals gezegd aan bod in dit rapport.

De digitale notaris

Stelt u zich eens voor dat bij elke transactie die u doet op internet een notaris meekijkt om te checken of alles klopt. Dat zou een dure operatie worden. Maar als zo iets geautomatiseerd kan, wordt het een heel ander verhaal. In feite heb je dan een mogelijkheid gecreëerd om frictieloos zaken te doen, want de controle zit al ingebakken in de transactie. Dit gegeven leidt tot tal van nieuwe mogelijkheden. Het systeem waar we het over hebben bestaat. Het heet blockchain, een solide keten zonder zwakke schakels, en het biedt een oplossing voor een aantal bestaande problemen binnen de digitale economie. Wat de nieuwe mogelijkheden zijn, beschrijven we in dit rapport.

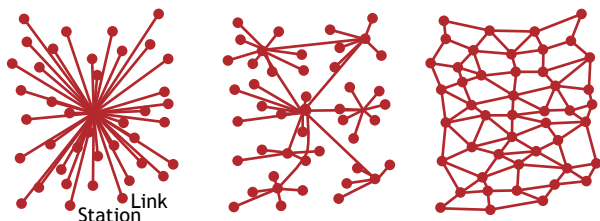
De zwakste schakel

Tot nu toe controleerden banken, instituten, toezichthouders en notarissen de transacties. Dit zijn ‘trusted third parties’. Deels doen ze hun werk geautomatiseerd, deels is het nog mensenwerk. Het loopt over veel schakels en als er ergens wat misgaat, dan komt een van die partijen in actie. De garantstelling van een bank of een creditcardmaatschappij zorgt ervoor dat we het systeem vertrouwen. Daarbij verlagen extra services, zoals een verzekering van producten die je met je Visa-kaart betaalt, de drempel om een transactie te doen.

De wrijving om de handel goed op gang te krijgen zou te groot zijn als deze vertrouwenspartijen niet bestonden. Sterker nog, de economie zou weinig voorstellen en ruilhandel – een koe voor drie varkens – zou de norm zijn. Toch gaan er nog dingen fout of moeten we lang wachten totdat de checks gedaan zijn en blijft de service achter omdat we nu eenmaal afhankelijk zijn van deze partijen. Ook moeten we ons realiseren dat de trusted-third-partyconstructie een behoorlijk prijskaartje heeft: de notarissen, banken en makelaars doen hun werk niet voor niets. Het alternatief echter, de blockchain, maakt het mogelijk om op zondagmiddag 100 miljoen euro naar Amerika over te maken: veilig, zonder transactiekosten en direct gestort. Probeer dit maar eens bij uw eigen bank.

De sterkste schakel

Deze trusted third parties zijn van origine niet ‘voor het internet ontworpen’. Inmiddels zijn ze digitaal wel te bereiken, maar meestal gebeurt dat door interfaces te bouwen boven op de bestaande legacysystemen. Het internet zelf heeft een heel ander ontwerpprincipe: de centraal, gedistribueerd, zonder eigenaar. We vertrouwen erop dat e-mails aankomen, dat we onze Facebook-pagina kunnen updaten of een Skype-call kunnen doen, simpel omdat het internet voorhanden is. Tegenover trusted third parties staat dus een trusted web. Beide moeten werken om de economie geolied te laten werken, maar de designprincipes zijn verschillend.



Waar is vertrouwen belegd: centraal, decentraal of in een gedecentraliseerd netwerk?

Als de sterkere schakel de zwakke schakels in het oude systeem kan vervangen, zien we opeens de potentie. De kosten kunnen naar beneden, het gaat sneller en er is geen single point of failure meer. Want als het ergens misgaat, gaat het ook goed mis. Dat zagen we een paar jaar geleden nog gebeuren bij Diginotar, een Nederlandse certificaatautoriteit die is opgericht door een groep van trusted-third-party notarissen. Terwijl de Nederlandse burgers hiermee digitaal hun belastingaangifte deden, werd er bij Diginotar ingebroken. De publieke sleutels die toegang geven tot onze belastingaangiften lagen op straat. De overheid zegde het vertrouwen op, inmiddels is Diginotar failliet.

Het rigoureuze antwoord op de fundamentele onveiligheid van centrale autoriteiten is een gedecentraliseerd systeem, zonder eigenaar, open source, volledig transparant en ondersteund met geavanceerde cryptografie. Dit zijn een aantal attributen van de blockchain. In een studie van MIT naar een blockchain-alternatief voor certificaatautoriteiten komt de blockchain als winnaar uit de bus¹.

¹ Conner, F., D. Velicanu & S. Yakubov, 'A Decentralized Public Key Infrastructure with Identity Retention', 2014

BLOCKCHAIN

Een publiek grootboek dat alle transacties bijhoudt en tegelijkertijd registreert op alle computers in dat netwerk. Dit is de nieuwe toezichhouder zonder een voor de hand liggende zwakke schakel die erom vraagt om getarget te worden. Iedere transactie wordt aan de hand van cryptografische puzzels gecheckt. De eerste computer die de puzzel oplost – en zo de transactie verifieert en goedkeurt – wordt betaald met nieuwe bitcoins. Als 51 procent van de computers in het netwerk de transactie heeft geverifieerd en goed bevonden, wordt de transactie bijgeschreven in het grootboek.

Omdat iedereen een exacte kopie heeft van dit grootboek, is het lastig om in de boeken te rommelen, want je moet ten minste 51 procent van de rekenkracht van alle computers die het netwerk beschermen onder controle hebben. Het computernetwerk van Bitcoin heeft veel meer rekenkracht dan de 500 snelste supercomputers bij elkaar. Iedereen kan meedoen aan dit netwerk en krijgt voor het rekenwerk een vergoeding in verhouding tot de toegevoegde rekenkracht. Op die manier hebben we nu te maken met een crowdfunded en crowd-owned publiek transparant en veilig transactiesysteem.

Blockchain: alle transacties van iedereen in een grootboek, gedistribueerd in een peer-to-peer netwerk.

HISTORISCHE VERGELIJKING

We kunnen een interessante historische parallel trekken met de introductie van het dubbel boekhouden in de dertiende eeuw. Aan de eerste vorm van dubbel boekhouden werd een stimulans van de economie toegeschreven. Het economisch verkeer versoepelde (lees bijvoorbeeld *Double Entry* van Jane Gleeson-White). Van de cryptovariant verwachten we nu ook weer zo'n 'goed oliën van de machine'-werking. We zien nog een andere mogelijke parallel: ook destijds werd het systeem niet goed begrepen en tegengewerkt door de machthebbers (zoals de paus) zoals nu door het huidige establishment.

OPBOUW VAN DIT RAPPORT: DRIE VERSIES VAN DE CRYPTO-ECONOMIE

Tot nu toe hebben we het nog niet gehad over de munt, de bitcoin, maar dat is wel waar de blockchain zijn bekendheid aan te danken heeft. Bitcoin is de voorlopige killer-applicatie van de blockchain. Het vertrouwen in de bitcoinmunt en het vertrouwen in het Bitcoin-platform (de blockchain) moeten wel gescheiden worden. Het ene vertrouwen hangt af van of het geld wel wat waard blijft, of als je bitcoins gestolen worden, de politie er wel achteraan gaat, dat soort zaken. Het andere vertrouwen gaat over een infrastructuur: of het netwerk down kan gaan, het systeem gehackt kan worden, of de snelheid van de transacties wel gegarandeerd kan worden.

Uiteindelijk gaat het om de toepassingen van de blockchain. Als én het netwerk én de toepassingen vertrouwd worden, is er een nieuwe basis gelegd voor waardetransacties. Aan ideeën voor deze nieuwe toepassingen is er geen gebrek. Start-ups storten zich op nieuwe killer-apps, proof-of-concepts komen naar buiten. Die toepassingen strekken zich uit van geld naar slimme contracten en slimme dingen tot aan autonoom opererende organisaties toe.

Crypto-economie 1.0

In drie stappen zetten we de potentiële impact van deze nieuwe toepassing uiteen. De eerste noemen we de *crypto-economie 1.0*. Die betreft de munt, de bitcoin, en

financiële transacties. Hier vindt u ook de broodnodige uitleg over de werking van het protocol. We geven zeven voor- en nadelen van de bitcoin, staan stil bij vragen over het toezicht op het systeem en eindigen met de officiële standpunten van de financiële autoriteiten.

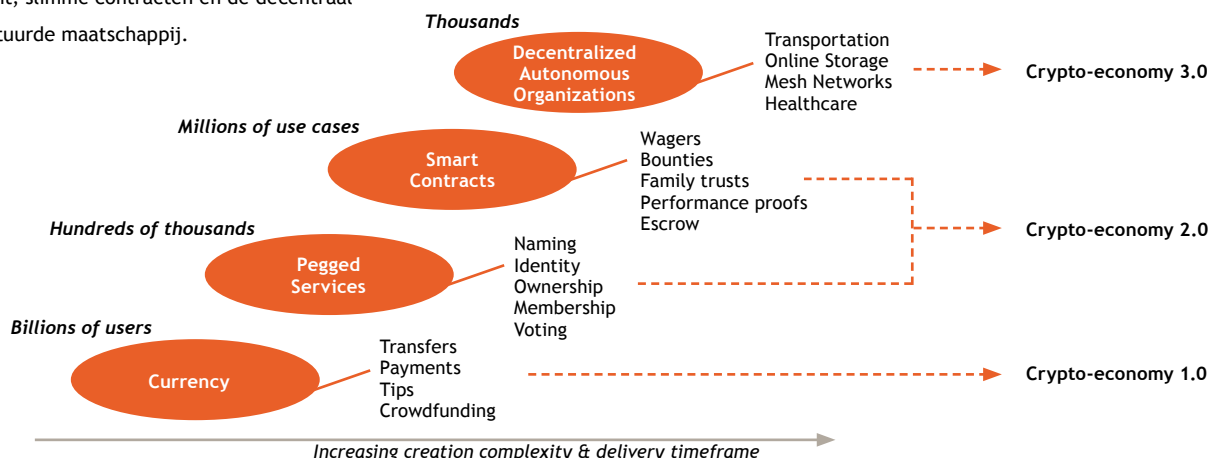
Crypto-economie 2.0

Bij de beschrijving van de *crypto-economie 2.0* gaan we dieper in op de andere mogelijkheden van de blockchain, ook wel 'bitcoin zonder bitcoin' genoemd. Dit betreft met name twee soorten toepassingen: slimme contracten en slimme producten en hoe hierdoor het economische verkeer kan worden versoepeld of, met andere woorden, de verspilling kan worden weggehaald.

Crypto-economie 3.0

Laten we onze fantasie de vrije loop, dan komen we uit op de *crypto-economie 3.0*. We beschrijven daar de DAC's (Decentralised Autonomous Corporations), ook wel 'Robocorps' genoemd. Het is een Internet-of-Things-scenario waarin objecten veel meer de vrije hand krijgen om beslissingen te nemen en de economie vooruit te trekken: een mogelijke voorbode van een 'zero marginal cost society'. Blockchain maakt dan deel uit van een 'collaborative commons', een ver doorgevoerde vorm van blockchaintechnologie in de maatschappij.

De crypto-economie in drie stappen: de munt, slimme contracten en de decentraal gestuurde maatschappij.



1 CRYPTO-ECONOMIE 1.0 – DE MUNT

*The Bank of England:
'It's a significant innovation that could transform the financial system more generally.'*

*Goldman Sachs:
'Innovations in network technology and cryptography could change the speed and mechanics of moving money.'*

Zaaien op een vruchtbare bodem

Het is niet verwonderlijk dat de impact voor de financiële sector steeds als eerste aan de orde komt, want over disruptie in de financiële sector wordt veel gespeculeerd. Niet in de laatste plaats natuurlijk vanwege wat er zich de afgelopen jaren heeft afgespeeld. Joris Luyendijk, antropoloog en journalist, publiceerde onlangs zijn bestseller 'Dit kan niet waar zijn'. The Guardian vroeg hem een analyse te maken van de financiële sector. Zijn conclusie, na honderden interviews, luidt dat een heel ander DNA nodig is voor een echte oplossing van de problemen. De blockchain zou een stukje van dat DNA kunnen zijn: een alternatieve manier om vertrouwen te organiseren. Ook vanwege de noodzakelijke transparantie in een inmiddels supercomplex systeem. Dit wordt misschien nog wel het duidelijkst onderstreept door een uitspraak van Andrew Haldan, de tweede man van de Bank of England, die in een interview met *Der Spiegel* zegt dat de balansen van grote banken nog steeds 'het zwartste aller zwarte gaten' zijn.

Bill Gates heeft ooit gezegd 'We need banking, we don't need banks', en die gedachte is voer voor durfinvesteerders die 'de Uber voor de financiële sector' willen vinden: een bank zonder bankkantoor, net als een taxicentrale zonder centrale. In 2012 werd er 2,3 miljoen dollar in bitcointechnologie geïnvesteerd, in 2013 was dat 95,81 miljoen, in 2014 347,29 miljoen en in de eerste twee maanden van 2015 was het 105,84 miljoen dollar. In 2013 kwamen er 200 bitcoin-start-ups bij en in 2014 meer dan 500. Ook de munt heeft de wind in de rug. Volgens cijfers van de Amerikaanse centrale bank² verdubbelt het aantal bitcoingebruikers iedere acht maanden: een exponentiële groeicurve. In oktober 2014 heeft een van de bekendste investeerders, Marc Andreessen, oprichter en maker van Netscape, zich zo uitgelaten in een interview met Bloomberg:

'Je hebt geen 100.000 mensen nodig, A-locaties in Manhattan en gigantische datacenters vol met mainframe-computers uit de jaren 70 om een online betaling te doen. Vandaag de dag zou je een financiële onderneming niet op dezelfde manier opbouwen. Voor mij staat de ontbundeling van banken centraal.'

Introductie in cryptovaluta

Bitcoin is een van de eerste incarnaties van een concept dat 'cryptovaluta' heet en dat voor het eerst in 1998 beschreven werd door Wei Dai op de Cypherpunks-mailinglist. Daar werd het idee gelanceerd van een nieuwe geldsoort die cryptografie gebruikt in plaats van een centrale autoriteit om de creatie van geld en om transacties te beheren. In 2009 werd de eerste specificatie en proof-of-concept op een cryptografie-mailinglist gepubliceerd door iemand met het pseudoniem Satoshi Nakamoto. Tegen het eind van 2010 verliet Satoshi het project, zonder veel over zichzelf te onthullen. Er zijn inmiddels diverse speurtochten ondernomen om zijn identiteit te

² Badev, Anton & Matthew Chen, 'Bitcoin: Technical Background and Data Analysis', 2014, www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf?p=cite_@inthepixels



achterhalen. Tot op heden hebben ze niet geleid tot de ontmaskering van de uitvinder van Bitcoin. Het feit dat het netwerkprotocol en de bijbehorende software onder een open-sourcelicentie zijn gepubliceerd, maakt de identiteit van de maker van ondergeschikt belang.

Zo ziet het hele plaatje eruit. Iemand doet een verzoek om bitcoins over te maken. De 'miners' pikken het verzoek op en beginnen met processen. Ongeveer tien minuten later wordt de eerste bevestiging ontvangen en begint de betrouwbaarheid van de transactie toe te nemen. Na nog eens tien minuten, wanneer de tweede bevestiging ook ontvangen is, is de transactie bijna honderd procent betrouwbaar. De goedgekeurde transacties worden in blokken aan het publieke grootboek toegevoegd. Zodoende ontstaat er een blokketen (de blockchain) waarin alle transacties zijn terug te lezen.

Wat is een bitcoin en wat is een blockchain?

Bitcoin is in wezen een consensusnetwerk dat een nieuw betaalsysteem en een nieuwe vorm van digitaal geld mogelijk maakt. Het is het eerste gedecentraliseerde door gebruikers gedreven peer-to-peer betalingsnetwerk zonder tussenkomst van een centrale autoriteit of andere tussenpersonen als een bank, notaris of verzekeraar. Een bitcoin is eigenlijk gewoon een uniek getal. Je kunt bitcoins dus heel makkelijk kopiëren en printen, maar als ze eenmaal worden uitgegeven, staan die unieke getallen in het grootboek en kunnen ze daarna niet nogmaals worden uitgegeven. De algoritmes zijn zo ontworpen dat er elke dag een vast aantal nieuwe bitcoins wordt gegenereerd. Elk dag wordt dat aantal iets minder, zodat ergens in 2140 het maximum is bereikt. Het aantal bitcoins groeit dan niet meer en dan zijn er 21 miljoen in omloop.

Zijn er andere munten dan de bitcoin?

De bitcoin is niet de enige cryptocurrency. In korte tijd zijn er veel meer alternatieve munten bij gekomen, zogeheten altcoins. De website Map Of Coins houdt al deze munten in de gaten. Op het moment van schrijven zijn er 705 cryptomunten, waarvan er in een maand tijd 45 stuks zijn bij gekomen.

Interessant aan deze altcoins is dat ze een nieuwe monetaire cultuur voor een bepaalde community faciliteren. Zo stelt FitCoin haar gebruikers in staat hun sportschoolbezoek te gelde te maken. Dankzij allerlei activity trackers en wearables wordt de gemeten hartslag van de sporter omgezet in de digitale munt. De oprichters van FitCoin hopen dat deze munt gebruikt kan worden om exclusieve artikelen te kopen van partners als Adidas om verzekeringspremies omlaag te brengen. Zelfs banken experimenteren met hun eigen altcoin. Citibank bijvoorbeeld heeft een testplatform voor digitale valuta en overweegt zijn eigen oplossing, CitiCoin.

Hoe werkt Bitcoin?

Voor we ingaan op de werking van Bitcoin, moeten we het eerst hebben over de rol van schaarste in een omgeving waar slechts overvloed te vinden is: het internet. Alles gaat daar razendsnel rond, wordt geliked en copy-paste doorgezonden of gewhatsappt. Maar voor geld, contracten en valutahandel is het juist belangrijk dat er unieke stukken zijn te identificeren. Hoe dat kort en goed in zijn werk gaat, leest u in ons overzicht op pagina 20 en 21.

Stel u zit ergens op een bankje en de persoon naast u geeft u een appel. U bedankt en neemt een hap. Zowel voor u als voor de persoon naast u op het bankje is dit een eenvoudig ritueel dat geen verdere uitleg behoeft. Met digitale transacties ligt dat anders. In dat geval stuurt iemand u een plaatje van een appel.



De eigenaar kan eenvoudig duizend kopieën maken en dezelfde appel naar duizend andere mensen sturen. Als het slechts een plaatje van een appel is, kan het u waarschijnlijk weinig schelen dat anderen ook kunnen meegenieten. Maar meer waardevolle dingen, zoals contracten, daarvan wilt u zeker weten dat de transactie klopt. U bent er niet bij met alle zintuigen, zoals op dat bankje, dus doet u een beroep op een arbiter, een trusted third party: een bank, notaris, marktplaats, creditcardmaatschappij of PayPal. Om hetzelfde niveau van vertrouwen te krijgen zal op de een of andere manier uniciteit ofwel 'digitale schaarste' georganiseerd moeten worden in de wereld van digitale overvloed. Met andere woorden, u moet zeker weten dat u de enige ontvanger bent van dit unieke exemplaar. Tot nu toe kon dat alleen via een centraal instituut, zoals een bank. Nu doet zich de mogelijkheid voor om dit technisch anders op te lossen. Het Bitcoin-protocol biedt deze mogelijkheid.

Om Bitcoin goed te kunnen begrijpen kun je Bitcoin het beste als een digitale rekening zien. Stel u voor dat u met een groep vrienden rond een tafel zit. Iedereen beschikt over een laptop en iedereen heeft tegelijkertijd toegang tot hetzelfde logboek, dat precies weergeeft hoeveel bitcoins elk van uw vrienden op ieder moment bezit.

Wanneer een van hen op een gegeven moment wat bitcoins aan een ander wil overmaken, moet hij iedereen rond de tafel daarvan op de hoogte brengen. Wanneer dat gebeurd is, voegt de hele groep die transactie aan het logboek toe, op voorwaarde dat allen de authenticiteit ervan hebben bevestigd. Ondanks het feit dat het geld in een dergelijk systeem digitaal is en geen fysieke vorm heeft, is het niet mogelijk om hetzelfde geld meer dan één keer uit te geven. 'Double spending' wordt door het netwerk immers meteen opgemerkt en bijgevolg verworpen.

In de realiteit maken alle deelnemers natuurlijk deel uit van een globaal peer-to-peernetwerk en vinden de transacties niet tussen individuen, maar tussen adressen in het netwerk plaats. Het verificatieproces van die adressen gebeurt door middel van cryptografie, zonder de werkelijke identiteit van de eigenaars te onthullen.

DOUBLE SPENDING

Tot op heden is er nog geen enkel geval van double spending bekend. In theorie is zo'n frauduleuze aanval echter wel mogelijk wanneer en zolang de hacker de controle heeft over minstens 51 procent van de rekenkracht van alle computers die het netwerk beschermen. Maar het misleiden van het netwerk gedurende de tijd die nodig is om één double spend te kunnen uitvoeren, zou vanuit economisch en organisatorisch oogpunt een slechte keuze zijn. Het computernetwerk van Bitcoin bezit vele malen meer rekenkracht dan de 100 snelste supercomputers bij elkaar. De poging tot double spending zou een te grote investering en complexe organisatie vergen. Daarnaast werd de broncode recent nog aangepast om de detectie en neutralisatie van dergelijke aanvallen makkelijker te maken – ongeacht de motivatie van de hacker.

Hoe worden bitcoins gemaakt?

Nieuwe bitcoins worden virtueel gedolven (het zogeheten mining) door een competitief en gedecentraliseerd proces. Bitcoin-miners verwerken transacties en beveiligen het netwerk met gespecialiseerde hardware. Voor hun bewezen diensten – het creëren, verhandelen en controleren van bitcoins – worden deze personen beloond met nieuwe bitcoins. Er bestaan zowel heel grote professionele miners, bijvoorbeeld ASCIMiner, als kleine eenpitters.



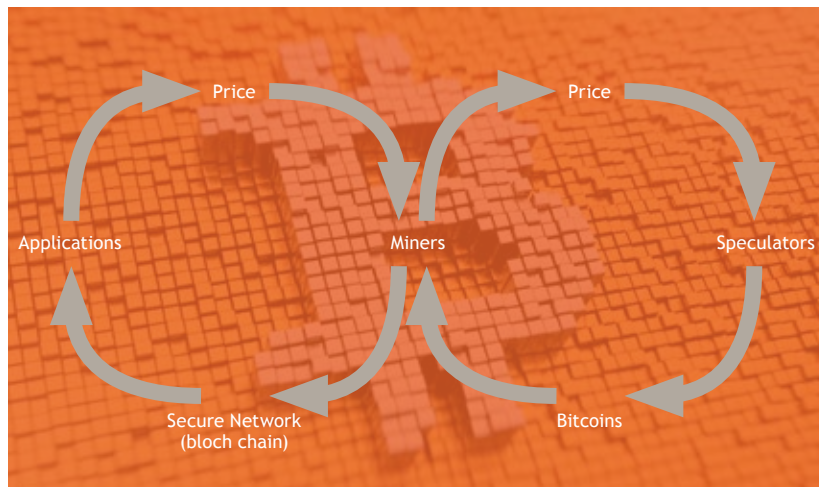
Voorbeeld van een moderne bitcoinmijn, ASCIMiner, in Hongkongs Kwai Chung. De koelinstallaties staan op het dak van het gebouw.

In het tweede onderzoeksrapport 'Design to Disrupt: Nieuwe digitale concurrentie' stonden we uitgebreid stil bij hoe diverse technologische platformen onze economie veranderen. Bitcoin is wat we een 'multi-sided platform' (MSP) noemen. Binnen dit platform hebben 'mi-

ners' een cruciale rol in het bespelen van de diverse zijden. Aan de ene kant delven zij de nieuwe cryptomuntten waarmee gespeculeerd kan worden, aan de andere kant bouwen en beheren ze de infrastructuur waarop allerlei applicaties gebouwd kunnen worden. De onderstaande figuur maakt ook meteen duidelijk dat de digitale munt niet losgekoppeld kan worden van het onderliggende netwerkprotocol. Miners hebben een incentive (= de bitcoinmunt) nodig om het netwerk in stand te houden. Wilt u zelf bitcoins gaan minen? Dan is de 'Beginner's Guide to Mining Bitcoin' die u kunt lezen op start-bitcoin.com een handige start.

Eric Nelson, een eenpitter die besloot om slechts 1 bitcoin te maken, rekent voor hoeveel hij aan de hele operatie verdient en wat zijn economische afwegingen zijn. Nelson rekent tegen een bitcoinprijs van 92 dollar, maar inmiddels staat de bitcoin op 260 dollar en dus zouden zijn inkomsten uitkomen op iets meer dan 8 dollar per dag.

'I decided to mine one bitcoin with my spare computer to see how it all works. I am part of "slush's pool", and running GULminer on Windows. When I shut down everything but my mining computer, my UPS reports that I am using 0.261 kw, or 6.264 kwh/day. I pay 12.5 cents per kwh, so I am paying 78.3 cents per day. I have averaged about 0.03 bitcoins per day so far (aprox 330 MHash with some video card that was the top of the line a year or two ago), with that number about to drop a lot since the ASIC rigs are coming online. Bitcoins are \$92, so my total revenue per day is \$2.76, with \$1.98 in profit [which is less than the depreciation on the machine]. I'm going to stop as soon as I hit one bitcoin though, as the extra heat in my office will be uncomfortable in the summer. This is more of a wintertime activity.'





Het Bitcoin-protocol is zo ontworpen dat nieuwe bitcoins in een vast tempo worden gecreëerd. Naarmate meer miners zich bij het netwerk voegen, wordt het steeds moeilijker om winst te maken en moeten miners naar efficiënte benaderingen zoeken om hun bedrijfskosten te drukken. Er zijn inmiddels diverse groepen actief op internet waar mensen samen kunnen zoeken naar het elektronische geld, door alle gezamenlijke rekenkracht van de computers in te zetten tijdens het delven, de 'mining pools'. Het systeem kan niet door een centrale autoriteit of ontwikkelaar worden beheerd of gemanipuleerd om de winst te verhogen. Elke Bitcoin-node in de wereld weigert elke vorm van een transactie die niet aan de regels van het systeem voldoet.

GOUD VERSUS BITCOINS

De miningmetafoor is niet toevallig gekozen. Je moet bitcoins delven (bitcoins maken), net als goud. Goud is met name handig omdat het niet snel vergaat, het klein genoeg is om op zak te dragen, je makkelijk namaak van echt kunt onderscheiden, enzovoort. Allemaal attributen die de bitcoin ook heeft. Het feit dat de bitcoin schaars is, net als goud, speelt een cruciale rol.

Frauduleuze transacties uitsluiten met een cryptopuzzel

Om zeker te weten dat alleen geldige transacties worden opgenomen in de blockchain, moeten alle aangesloten computers in het netwerk met elkaar in competitie een controlegetal uitrekenen, een cryptografische puzzel. De eerste die het controlegetal vindt, wordt aanvaankelijk vertrouwd en mag de transactie bijschrijven in de blockchain. Naarmate meer computers op hetzelfde getal uitkomen, wordt de uitslag betrouwbaarder. Omdat zeer veel computers op zoek zijn naar dezelfde oplos-

sing, is de kans erg klein dat een frauderende computer de oplossing (voor een frauduleuze transactie) mag bijschrijven in de blockchain. De kans dat zo'n transactie ook nog eens meerdere malen wordt bevestigd, is minimaal. Als meer dan de helft van de in het netwerk aanwezige rekenkracht ter beschikking staat van de correcte, betrouwbare algoritmes, is het statistisch onmogelijk de blockchain te vervalsen. Dit betekent overigens ook dat bitcointransacties pas na een paar minuten kunnen worden gerealiseerd. Inmiddels zijn er meerdere oplossingen bedacht om de transactietijd te omzeilen of te verkorten.

Shared single source of truth

De basis van bitcoin is dus de blockchain. De blockchain is voor bitcoin wat het grootboek is voor een bank. Een normale bank heeft ergens een grote berg geld in een kluis met daarbij het grootboek waarin wordt opgeschreven welk deel van het geld van wie is. Dit is essentieel: dit grootboek wordt door een bank beheerd. Daarom lopen alle transacties via die bank.

Bij bitcoin is het grootboek dus decentraal, oftewel: het hele netwerk is het grootboek (de blockchain). Niemand beheert het grootboek, want iedereen doet dat. Iedereen kan iets aan het grootboek toevoegen, maar niemand kan er iets uit verwijderen. Het grootboek bevat een onuitwisbare historie van alle transacties. Het is een financieel DNA dat fraude of anderzijds foutieve transacties praktisch onmogelijk maakt doordat hij wordt gecontroleerd en geverifieerd door tienduizenden servers over de hele wereld die gebruikmaken van de publieke en permanente overdrachtshistorie van het blokje code. Welke bitcoins aan welke wallets (adressen) zijn toegekend, wordt door alle knooppunten in het hele netwerk bijgehouden. Het is alsof een notaris iedere transactie nauwkeurig in de gaten houdt. Transacties lopen gewoon van wallet naar wallet, peer-to-peer.

De decentrale aard van de blockchain heeft veel voordelen en biedt de mogelijkheid tot het bedenken van allerlei nieuwe toepassingen die in een centraal georganiseerde wereld niet kunnen bestaan. Het feit dat (financiële) censuur door een enkele partij onmogelijk is, impliceert dat er geen single point of failure meer bestaat. Alleen dit concept al biedt legio mogelijkheden. In tegenstelling tot het grootboek van een bank heeft iedereen inzage in de blockchain. Het is een 'shared single source of truth'. Iedereen heeft de beschikking over dezelfde gedeelde versie van de waarheid. Bitcointransacties zijn om deze reden volledig transparant. De 'rekeningnummers' (bitcoinadressen) die in de blockchain worden bijgeschreven, zijn echter in principe anoniem. Dit geeft gebruikers van Bitcoin de keuze tussen anonimiteit of juist transparantie: eenieder die zijn adressen publiceert, geeft direct inzicht in zijn geldstromen, eenieder die ze verborgen weet te houden, blijft buiten zicht.

De zeven voor- en nadelen van Bitcoin

Pro 1: Vrijheid van betaling

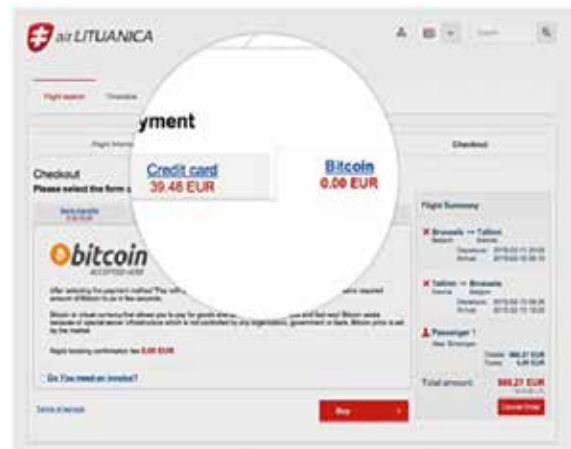
Bitcoin is als e-mail voor geld. Het is mogelijk om elk bedrag altijd en overal direct te verzenden en te ontvangen. Geen feestdagen. Geen grenzen. Geen opgelegde limieten. Binnen enkele minuten kan iemand met Bitcoin geld overboeken naar personen of bedrijven. Waar ook ter wereld, voor een fractie van de kosten die banken hiervoor vragen.

Contra 1: Je kunt er maar op weinig plekken mee betalen

Veel mensen weten nog niet van het bestaan van Bitcoin af. Dagelijks accepteren meer bedrijven bitcoins, omdat ze gebruik willen maken van de voordelen, maar het lijstje blijft kort en moet groeien om van netwerkeffecten te profiteren.

Pro 2: Zeer lage kosten

Bitcoinbetalingen worden momenteel zonder of tegen extreem lage kosten verwerkt. Gebruikers kunnen kosten aan transacties verbinden om prioriteitsverwerking te ontvangen, waardoor transacties sneller door het netwerk worden bevestigd.



Een vliegticket kopen kan met Bitcoin goedkoper uitpakken.

Daarnaast bestaan er exchanges om verkopers te helpen tijdens de verwerking van transacties, de conversie van bitcoins naar fiduciaire valuta en de dagelijkse rechtstreekse storting van geld op de bankrekening van de verkoper. Omdat deze diensten op bitcoin zijn gebaseerd, kunnen deze tegen veel lagere kosten dan bij PayPal of andere creditcardnetwerken worden aangeboden.

Contra 2: De waarde schommelt nogal

De totale waarde van bitcoins in omloop en het aantal bedrijven dat Bitcoin gebruikt zijn nog steeds erg gering vergeleken met wat het zou kunnen zijn. Relatief kleine marktveranderingen beïnvloeden de prijs dus aanzienlijk. Theoretisch gezien zal deze volatiliteit afnemen naarmate bitcoin een grotere positie in de markt krijgt en de technologie wordt verbeterd.



Koersverloop van de bitcoin. Eind maart 2015 was de munt ongeveer 260 dollar waard. Anderhalf jaar eerder lag de prijs nog boven de 600 dollar.

Pro 3: Microbetalingen gaan van een leien dakje

Bitcoin kan betalingen van een paar cent verwerken. Dit opent de weg naar nieuwe betalingsmodellen die met name voor de aanbieders van content interessant zijn. Aanbieders van content zijn beperkt in de manier waarop ze inkomsten genereren. Met Bitcoin kun je betalen voor een enkel stuk content, bijvoorbeeld voor een 'single listen' (het eenmalig luisteren naar een enkel nummer) of het kopen van bandbreedte van een wifi-hotspot per kilobyte. Uitgevers kunnen simpelweg bij hun artikelen een button plaatsen om het desbetreffende artikel zelf te verkopen voor een klein bedrag, een alternatief voor Blendle. Of wat te denken van de hinderlijke advertenties bij het bekijken van een YouTube-filmpje? Wat als je deze advertenties door een paar cent te betalen in een keer kunt overslaan? Helemaal mooi is de applicatie Streamium, een soort Periscope of Meerkat, maar dan op stereoïden. Kijkers naar een livestream betalen realtime per minuut via microbetalingen.

Contra 3: Het rammelt her en der, het is nog niet af

De Bitcoin-software bevindt zich nog steeds in een bètafase met veel onvolledige functies waaraan nog volop wordt gesleuteld. Nieuwe tools, functies en diensten worden ontwikkeld om Bitcoin voor het grote publiek veiliger en toegankelijker te maken. Een aantal daarvan is nog niet klaar voor iedereen. De meeste bitcoinbedrijven zijn nieuw en bieden nog geen verzekering. Bitcoin bevindt zich nog steeds in het proces richting volwassenheid.

Pro 4: Transparant en neutraal

Alle informatie inzake de bitcoin-geldtoevoer is direct beschikbaar in de blokken zodat iedereen deze in real-time kan verifiëren en gebruiken. Personen of organisaties kunnen het Bitcoin-protocol niet controleren of manipuleren omdat het cryptografisch beveiligd is.

Contra 4: Het faciliteert illegale handel en duistere praktijken

Er zijn sluiptwegen om op anonieme, ongecensureerde manier online handel te faciliteren, zoals via OpenBazaar en Silk Road, de Amazon van het darknet, en Dark Wallet. Die laatste is een plug-in voor Chrome en Firefox (Mac, Windows en Linux) die functioneert als een bitcoinportemonnee en anonieme betalingen garandeert. De Dark Wallet-software versleutelt en combineert de transacties van anderen. Het combineren van die transacties gebeurt volstrekt willekeurig: als Alice sokken koopt bij een bitcoinvriendelijke kledingzaak en Bob bestelt op hetzelfde moment lsd bij Silk Road (of zijn opvolgers), dan kunnen ze tot een enkele transactie worden gecombineerd, zelfs als Bob en Alice elkaar helemaal niet kennen. Overheden hebben op deze manier totaal geen inzicht in de gedane transacties.

Where are the unbanked?



Adults with an account at a formal financial institution (%)

0 - 20	61 - 80
21 - 40	81 - 100
41 - 60	no data

SOURCE: World Bank

Pro 5: Banking the unbanked

Volgens cijfers van de Wereldbank heeft meer dan de helft van de volwassen beroepsbevolking geen toegang tot allerlei financiële diensten om geld te sparen of te lenen. Dit komt neer op meer dan 2,5 miljard volwassenen wereldwijd die niet kunnen deelnemen aan het economisch verkeer. Dankzij Bitcoin heeft iedereen met internettoegang de mogelijkheid om te bankieren.

Contra 5: De overheid kan niet meer meeluisteren

Bitmessage is een P2P-communicatieprotocol om gecodeerde berichten te versturen naar een ander of naar vele abonnees. Het maakt gebruik van sterke authenticatie, wat inhoudt dat de afzender van een bericht niet kan worden vervalst, en het probeert 'niet-content'-gerelateerde gegevens (zoals de zender en ontvanger van boodschappen) te verbergen voor luistervinken zoals de NSA.

Pro 6: Beveiliging en controle

Bitcoingebruikers hebben de volledige controle over hun transacties. Het is voor verkopers onmogelijk om kosten af te dwingen zoals bij andere betaalmethoden wel kan gebeuren. Bitcoinbetalingen worden gedaan zonder dat er persoonlijke gegevens aan de transactie zijn verbonden. Dit zorgt voor een sterke bescherming tegen identiteitsdiefstal. Bitcoingebruikers kunnen hun geld daarnaast beschermen via back-ups en versleuteling.

Contra 6: Bitcoins kun je stelen

De gegevens waarmee je de controle over je bitcoins uitoefent, kunnen op verschillende manieren bewaard worden: in een digitale portefeuille, de zogenaamde wallet, of via websites die bitcoinaccounts aanbieden. Ook buiten de digitale weg om kun je die informatie bewaren: schrijf het op een papiertje (een zogenaamde cold wallet) of onthoud het zelf gewoon. Met die gegevens kunnen bitcoins vervolgens via het internet worden overgedragen aan iedereen die over een bitcoinadres beschikt, wat je kunt vergelijken met het versturen van e-mail. Punt is wel dat net zoals in de fysieke wereld cryptogeld gestolen kan worden. Al meerdere malen zijn mensen opgeschrikt doordat bitcoins uit hun wallet verdwenen waren omdat ze hun gegevens niet goed afgeschermd hadden.

Pro 7: Minder risico's voor verkopers

Bitcointransacties zijn veilig, zijn onomkeerbaar en bevatten geen gevoelige of persoonlijke informatie van klanten. Op deze manier zijn verkopers beschermd tegen verliezen door fraude of frauduleuze storneringen en is PCI-compliance niet nodig. Verkopers kunnen eenvoudig nieuwe markten betreden waar creditcards niet beschikbaar zijn of het fraudepercentage onacceptabel hoog is. De nettoresultaten zijn lagere kosten, grotere markten en minder administratiekosten.



Contra 7: Wennen aan andere vorm van toezicht

Er is weinig regulering vanuit de overheid of vanuit een andere toezichthouder. Dat is de belangrijkste reden om sceptisch te zijn. Er is geen centrale instantie zoals een centrale bank die de munt uitgeeft of controleert of er valse munten in omloop zijn. Dat komt onder andere omdat de bitcoin door deze instanties niet als munt wordt beschouwd.

Het idee dat vertrouwen op een andere manier georganiseerd kan worden, in code en systemen, vraagt een 'mindshift'. Het zal dus wel even duren voordat de waardevolle attributen van de bitcoin (en blockchain) bij een groter publiek zullen aanslaan. Het centrale contrapunt is hier dus niet het feit dat er weinig regulering is vanuit de overheid, maar dat we moeten wennen en gaan begrijpen dat het ook anders opgelost kan worden.

Op dit moment maken de mensen van de Europese Centrale Bank (ECB) zich overigens niet ongerust. Bitcoin stelt in hun ogen niet veel voor, leidt een marginaal bestaan, en ze zien dat er geen grote ongelukken mee gebeurd zijn. Het gevaar dat ze voorzien is dat wanneer er klappen gaan vallen in de bitcoineconomie, ook het vertrouwen in de officiële munten en e-payments kan worden ondermijnd. En dat willen ze te allen tijde voorkomen, daar is de ECB immers voor in het leven geroepen.

Een goed beeld van hoe de verschillende wereldwijde toezichthouders er nu tegenaan kijken geeft het rapport 'Virtual currency schemes – a further analysis' (2015) van de ECB. Om te beginnen zegt de ECB dat de bitcoin geen geld is: 'They are something else, different from known currencies'. Een logische conclusie wellicht, omdat de essentie van geld is dat het algemeen geaccepteerd is en de bitcoin is (nu nog) verre van dat. Maar in een eerdere definitie uit 2012 van de ECB kwam het woord 'geld' nog wel voor, daar neemt de centrale bank nu dus bewust afstand van. Misschien valt er dan

een last c.q. verantwoordelijkheid van de schouders van de financiële toezichthouders, want die moeten vooral het geld bewaken. Ook het woord 'unregulated' heeft de ECB uit de definitie geschrapt, want, zo zegt de ECB: 'regulation has caught up with innovation'. De ECB ziet de bitcoin dus als iets anders dan geld en beschouwt het op een bepaalde manier als gereguleerd, al dan niet door andere instanties dan de traditionele financiële instituten. Het idee dat de regelgever geen regels voor de bitcoin hoeft in te stellen wordt door de Amerikaanse Federal Reserve ondersteund:

'The Federal Reserve simply does not have the authority to regulate the bitcoin in any way.'

De directeur van de Amerikaans consumentenbond, Richard Cordray, maakt zich dan ook zorgen:

'Virtual currencies are not backed by any government or central bank, and at this point consumers are stepping into the Wild West when they engage in the market.'

Waarschuwingen voor de bitcoin zijn legio, die geven de toezichthouders wel. Van de BAfin, de Duitse financiële autoriteit, tot de Franse, de Nederlandse en de Belgische centrale bank. Daarbuiten zijn het de People's Bank of China, de Reserve Bank of India, de monetaire autoriteit van Singapore en onder andere de bank van Indonesië die waarschuwen. Naast waarschuwen en vooral benadrukken dat de bitcoin geen officieel (juridisch) betaalmiddel is, geven in sommige landen banken licenties uit voor bepaalde bitcoindiensten. Zo heeft Zweden een licentie voor de handel in bitcoins (de bitcoin exchange). In Duitsland mag je ze van de financiële instanties gewoon gebruiken, kopen, verkopen en minen, maar voor aanvullende diensten kunnen licenties noodzakelijk zijn.



China heeft de handel en het betalen in bitcoins verboden. De Thaise bank ook, maar die heeft naar verluidt niet de middelen voor enige vorm van handhaving van dat besluit. De vraag is ook welk land wel voldoende middelen heeft. Rusland ziet de bitcoin als 'substitute money' en om die reden is het verboden; volgens de Russen is het een mogelijk bewijs dat je je met dubieuze transacties bezighoudt.

De grote vraag is vooral in hoeverre de algoritmes achter de bitcoinmunt te vertrouwen zijn. De code is open source en een netwerk van computers garandeert dat fraude onmogelijk is, maar toch voelt het vreemd om een hypotheekakte via de blockchain te laten passeren. Welke instantie garandeert dat het door mij aangekochte huis ook daadwerkelijk van mij is? Welk instituut zorgt ervoor dat mijn in de blockchain bewaarde testament ook wordt uitgevoerd?

Wie dan wel? A Bitcoin Governance Framework

Voorsnog blijft het koffiedik kijken. Op dit moment is het niet duidelijk hoe regulering van de cryptomunt in de toekomst zal plaatsvinden. De verwachting is dat het een mix zal zijn van overheden, centrale instanties en het onderliggende algoritme. Een rapport en inventarisatie gedaan door Global Solution Networks propageert een 'multi-stakeholder solution to the challenges of the cryptocurrency'. Zo luidt ook de ondertitel van het rapport 'A Bitcoin Governance Framework'. Veel van deze

uitdagingen zijn verwoord in de lijst van zeven contra's hierboven. Speerpunten van een nieuw governance framework zijn met name Anti-Money Laundering (AML), Know Your Client (KYC) en Combating the Finance of Terrorism (CTF). De partijen die bij de governance van bitcoin/blockchain betrokken moeten worden zijn bijvoorbeeld het Worldwide Web Consortium (W3C), de ICANN, de Internet Engineering Task Force (IETF) plus de overheden. Voor alle partijen is het inmiddels overduidelijk dat het Bitcoin-protocol een aantal voordelen herbergt. Boven op dit zogeheten 'vijfde protocol' kunnen allerlei toepassingen worden gebouwd die het bestaande (en verouderde) financiële systeem op vele fronten verbeteren. Het is geen geld, zo zei de ECB al. Het is ook een netwerk, een digitale infrastructuur, een nieuw protocol en nieuwe mogelijkheden. Het volgende hoofdstuk gaat over deze nieuwe toepassingen.



2 CRYPTO-ECONOMIE 2.0 – SLIMME CONTRACTEN EN DINGEN

Heeft uw organisatie iets te doen met de volgende zaken, dan kan de crypto-economie 2.0 interessant voor u worden.

Geld, aandelen, hypotheken, paspoorten, geboorteregister, stempasjes, schietvergunningen, kentekenregistraties, digitale identiteiten, hotelreserveringen, softwarelicenties, track & trace van pakketten, medische dossiers, contracten, testamenten, handtekeningen, diploma's, DNA, huissleutels, sleutels van kluisjes, coupons, vouchers, domeinnamen, patenten, bioscoopkaartjes, simkaarten, auteursrechten.

En verder alle fysieke apparaten die een internetverbinding zouden kunnen krijgen (Internet of Things).

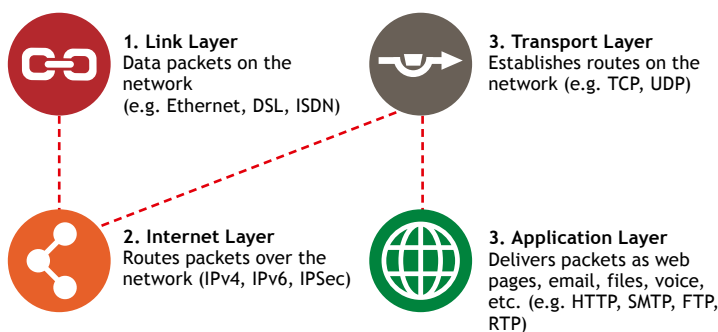
De hele lijst van immateriële activa (zoals contracten) en materiële activa (alle apparaten) kan een nieuwe dimensie krijgen dankzij de mogelijkheden van de blockchain. Hier gaat het om slimme contracten en slimme dingen. Volgens Melanie Swan, oprichter van het Institute for Blockchain Studies, vormen deze twee de basis voor de nieuwe mogelijkheden, een 'Blueprint for a New Economy'. Zo luidt ook de titel van haar laatste boek. We betreden met deze vorm van crypto-economie een nieuw terrein. Zoals gezegd het is nog 'early days', Swan spreekt nadrukkelijk nog over een blauwdruk, maar op basis daarvan kan wel worden gebouwd en getest, en dat gebeurt volop.

De opsomming waar we dit hoofdstuk mee begonnen bevat allemaal voorbeelden van afspraken die we met elkaar maken om de fysieke wereld te organiseren. Volgens Andreas Antonopoulos, de schrijver van het boek *Mastering Bitcoin* en eind 2014 door de bitcoin-community verkozen tot de meest invloedrijke bitcoinexpert, kunnen we de fysieke wereld nu anders gaan inrichten. Volgens hem kunnen we geld beschouwen als data, als een nieuw *contenttype*. Digitaal geld bestaat uiteraard uit niets anders dan nullen en enen. Geld wordt door de blockchain getransformeerd tot programmeerbare eenheden, waardoor het – en allerlei andere vormen van waarde en eigendom – net zoals webpagina's, e-mail, video en muziek zonder frictie over het internet kan stromen. We kunnen geld dus bepaald gedrag meegeven aan de hand van vooropgestelde regels. Nu is dat vaak vastgelegd in regels die via bureaucratische processen worden gecontroleerd. Geen wonder dat sommige banken bang zijn voor de mogelijke gevolgen van de blockchain. Of zoals Johann Palychata, financial securities research analyst bij BNP Paribas, het zegt: *'Its core is the first successful attempt for a secure and decentralized register. It should be considered as an invention like the steam or combustion engine. [...] In its purest form, a distributed blockchain system allows all market participants direct access to the DSD (Decentralised Securities Depositary), to the exchange and to the post-trade infrastructure (clearing and settlement). If this setup develops then existing industry players might be redundant.'* Met behulp van een mechanisme als de blockchain kunnen we deze regels dus programmeren in het geld zelf. Compliance vooraf dus. Zo zouden zorgverzekeraars gebruik kunnen maken van een zogeheten 'zorgcoin' voor persoonsgebonden budgetten. Deze coins kunnen alleen uitgegeven worden wanneer ze besteed worden aan vooraf geprogrammeerde doelen.

Dan gaat het dus om de creatie van een compleet nieuw netwerk met alle mogelijkheden van dien: van internetgeld naar een internet van geld.

Een nieuw protocol

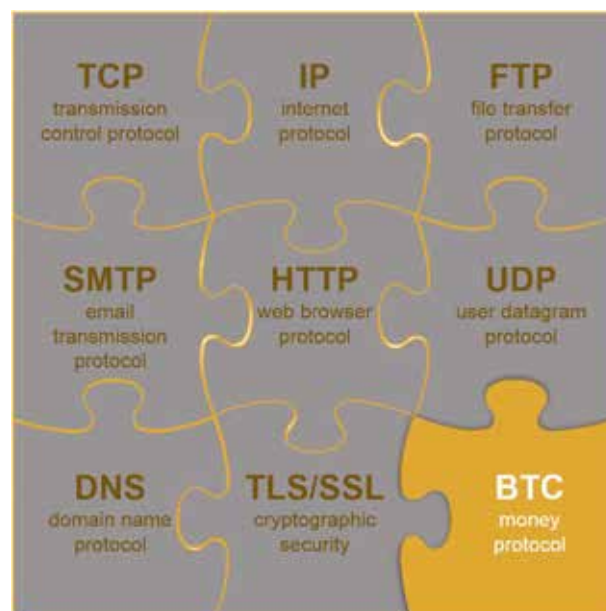
Sinds 1960 is er gebouwd aan het grootste datanetwerk ter wereld. Dit netwerk, dat we het internet noemen, verstuurt pakketjes data over en weer door gebruik te maken van diverse communicatieprotocollen. Die staan te boek als de Internet Protocol Stack en die bestaat uit vier lagen: een datalinklaag (voor transport van de data over een verbinding), een netwerklaag (voor het doorgeven van de pakketjes over het netwerk), een transportlaag (voor het probleemloze transport van data voor de applicaties) en een applicatielaag (hier bevinden zich de internettoepassingen zoals HTTP, SMTP en FTP).



Bron: Winklevoss, Cameron & Tyler Winklevoss (2014): 'Money Is Broken; Its Future Is Not', Money20/20.tv, December 1, 2014

Dit netwerk is in de loop der jaren erg behulpzaam geweest voor het uitwisselen van gegevens, maar niet voor de intrinsieke overdracht van waarde. Dankzij het internet kunnen we nu wereldwijd met elkaar handel drijven, alleen het simpelweg elkaar toesturen van geld en het overdragen van waarde of eigendom is nog een probleem. Het Bitcoin-protocol, de blockchain, lost dit probleem op en houdt dus een enorme belofte in. Vandaar dat het provocatieve statement 'The Fifth Protocol' door de bitcoinexperts ook wel wordt gevoerd als we het hebben over de potentie van de blockchain.

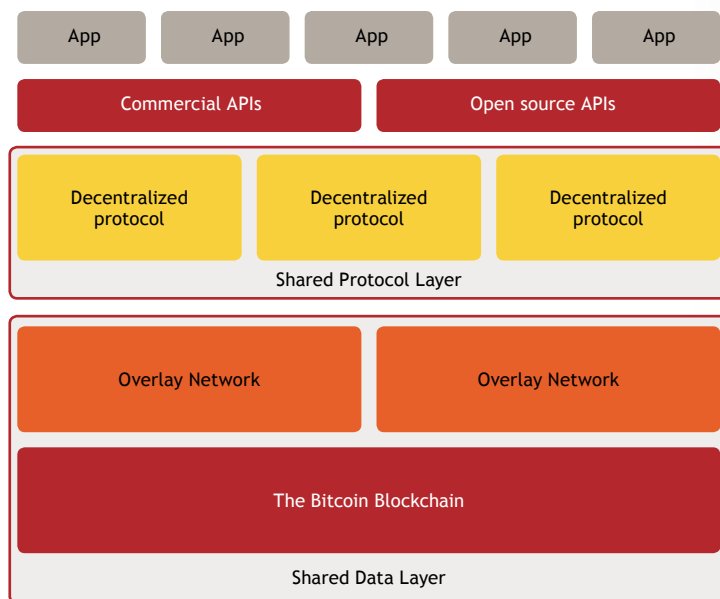
Een internet waarbij 'echt geld, goederen, diensten of andere activa tegen minimale frictie van eigenaar kunnen veranderen over grote afstanden': de blockchain is het ontbrekende puzzelstukje om het Internet van Waarde mogelijk te maken.



Bron: Reddit, zie: http://www.reddit.com/r/Bitcoin/comments/2x5de0/the_final_piece_of_the_protocol_puzzle/

De Blockchain Application Stack

Een van de bitcoinexperts die stelt dat de blockchaininfrastructuur belangrijker is dan de cryptomunt, is Joel Monegro. Hij werkt voor het investeringsbedrijf Union Square Ventures van Fred Wilson en ontwikkelde de Blockchain Application Stack. Deze architectuur laat zien hoe het mogelijk is om met behulp van Bitcoin decentrale applicaties te maken. Volgens Monegro ging de eerste fase van Bitcoin om het installeren van een infrastructuur – gateways, consumer wallets, developer platforms, merchant services enzovoort. De hierop volgende fase betreft het bouwen van *native* Bitcoin-applicaties, die nog nooit eerder gebouwd konden worden. Deze applicaties moeten ervoor zorgen dat Bitcoin eindelijk mainstream wordt.



Bron: Monegro, Joel, "The Bitcoin Application Stack", November 25, 2014, <http://joel.mn/post/103546215249/the-blockchain-application-stack>

Nu is de tijd voor ontwikkelaars gekomen om allerlei soorten applicaties met gebruiksvriendelijke interfaces op dit platform te bouwen. De strijd om de killer-apps kan beginnen.

CLOUDCOMPUTING IS KANDIDAAT-KILLER-APP

Een kandidaat is de applicatie Storj. Dit is een gedecentraliseerde cloudoplossing om bestanden op te slaan. Gebruikers kunnen op hun computer een applicatie installeren waarmee ze een gedeelte van hun harde schijf aan de cloud geven zodat andere gebruikers vervolgens hun files beveiligd en versleuteld daarop kunnen bewaren.

Op internet is inmiddels een Mega-Master Blockchain List³ terug te vinden die via een Twitter-brainstorm is gecreëerd. Die mogen we beschouwen als een goede in-

ventarisatie van killer-appmogelijkheden. Deze lijst bevat inmiddels 84 verschillende toepassingen die zijn onderverdeeld in 6 categorieën waarin de blockchain gebruikt kan worden. Een redelijk concrete vertaling van die lijst naar mogelijke diensten komt uit een onderzoek van William Mougayar. Hij heeft in februari 2015 uitgebreid onderzoek gedaan naar het cryptotechnologielandschap. In totaal heeft Mougayar zo'n 430 bedrijven geïnventariseerd die zich allemaal richten op het ontwikkelen van allerlei applicaties voor de blockchain. Hij onderscheidt vier categorieën: applicaties, middlewarediensten, ondersteunende diensten en infrastructuur en platformen.

³ <http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list>

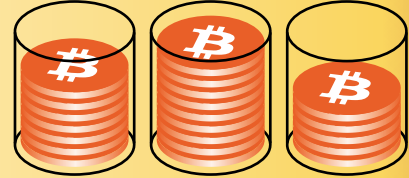
THE BITCOIN BLOCKCHAIN AT WORK IN FIVE EASY STEPS

Online retailer CashCoin accepts bitcoins and Betty wants to pay with the currency from her wallet.

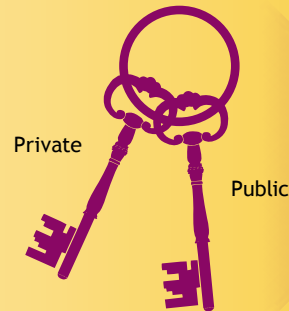
Wallets and Addresses



Both CashCoin and Betty have virtual Bitcoin wallets on their computer. These files provide access to Bitcoin addresses. Each address is a string of letters and numbers and contains a certain amount of bitcoins.



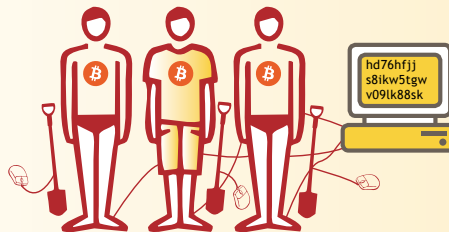
The signage of a message with your private key (which only you know) can be verified by anyone on the network using the matching public key (which everyone knows). Cashcoin's new Bitcoin address is a unique public key that is published on the network, while the corresponding private key is safely stored in the company's wallet.



Submitting a Payment

Verifying the Transaction

Jill, Jack and John are Bitcoin miners. Their computers bundle the transactions of the past ten minutes into a new transaction block to be added to the Bitcoin blockchain.



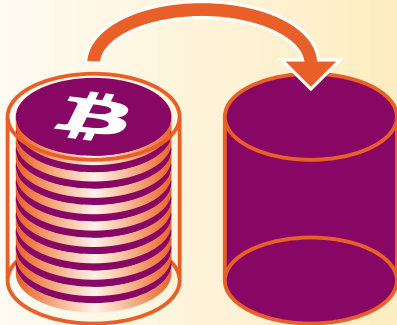
The block is identified by a new cryptographic hash value, i.e. a fixed-length string of numbers and letters, since Jill's Jack's and John's computers are set up to do so.

Every new Bitcoin hash value must have a specific form and must start with a certain number of zeroes. There is no way of predicting which nonce will generate the required number of zeroes. For Jill, Jack, John, and all other Bitcoin miners this is a trial and error process that needs enormous computing power.



When the coinbase that is part of every transaction block on the Bitcoin blockchain has been hit - let's say by John - this winning Bitcoin miner is rewarded 25 newly minted bitcoins by the Bitcoin system. John receives an address in his wallet which represents the money he earned for his successfully accomplished transaction verification effort.

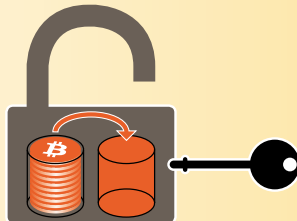
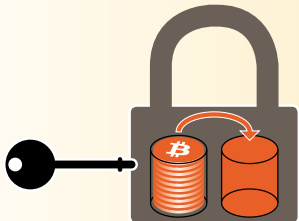
Creating a New Address



At CashCoin, the cashier replies to Betty's payment request by creating a new Bitcoin address where the money can be submitted. By creating the address a cryptographic key pair is being generated, consisting of a private key and a corresponding public key.

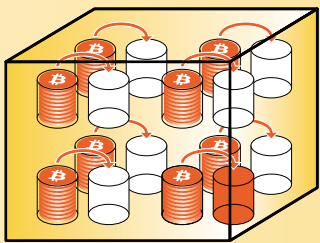
Private

Public

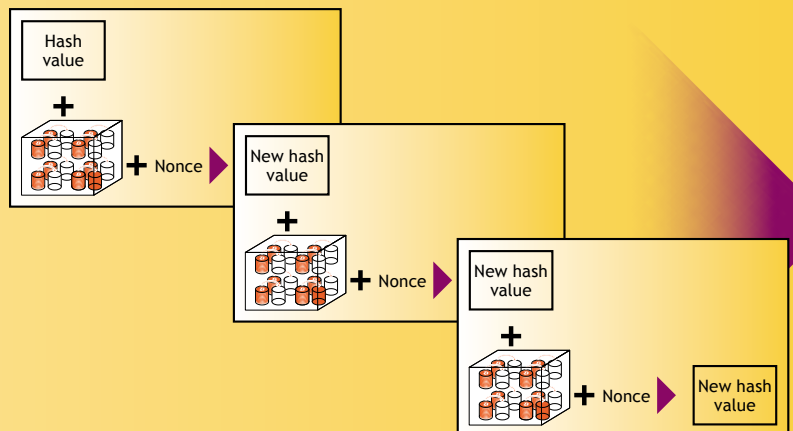


Betty's Bitcoin wallet holds the private key for each of the addresses it contains. The Bitcoin program on her computer signs Betty's transaction request with the private key of the address that she chooses to transfer bitcoins from.

Anyone on the Bitcoin network can verify with the public key whether the transaction request is actually coming from Betty.



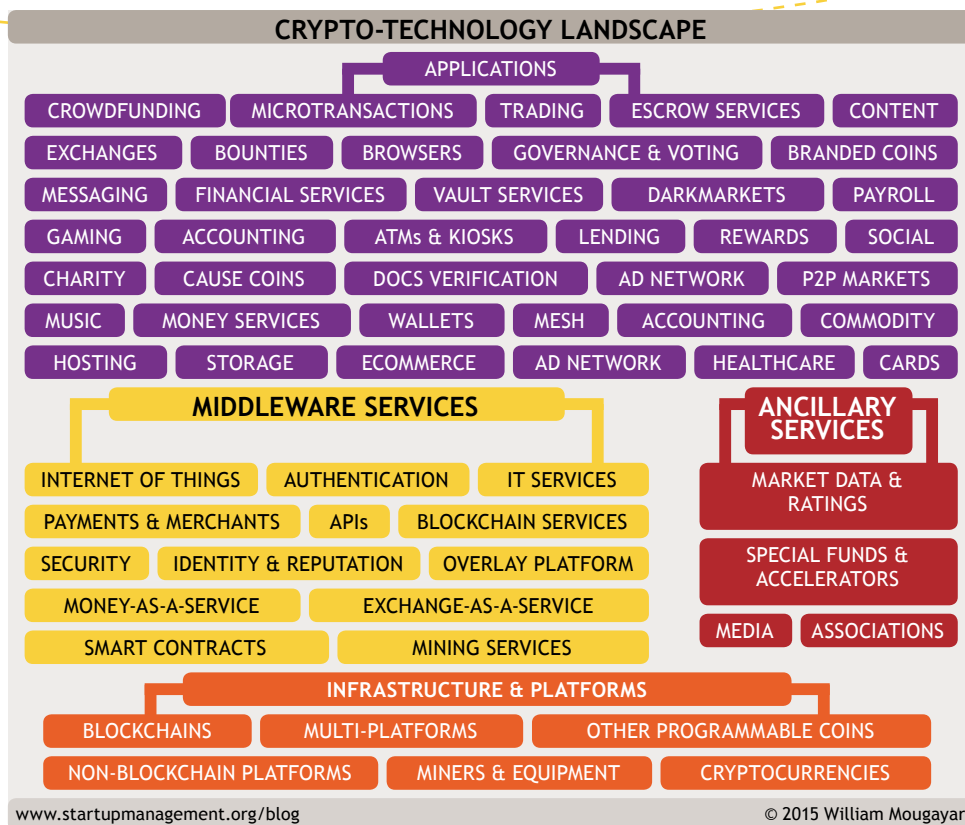
Each new hash value in the Bitcoin blockchain contains information about ALL previous Bitcoin transactions. A nonce is a random number that is added prior to hashing. The computers of Jill, Jack and John create new hash values based on a combination of the previous hash value, the new transaction data block, and a nonce.



Want to Break the Bitcoin or Any Other Blockchain System?

Anyone aspiring to takeover the Bitcoin system would have to redo what John did and all subsequent miners. That is practically impossible.





Uit de bovenstaande figuur blijkt in een oogopslag de diversiteit van het totaal aan gebouwde applicaties. Bitcoin-kenners beweren dat de komende jaren tal van applicaties ontwikkeld zullen worden, met name rond het Internet of Things en de slimme contracten en eigendomsrechten.

Bitcoin en het Internet of Things

De Samsung-wasmachine W9000 is uitgerust met een nieuwe informatiearchitectuur van IBM: ADEPT (Autonomous Decentralised Peer-To-Peer Telemetry) op basis van de blockchain. De wasmachine kan zelf wasmiddelen bestellen, zoekt in haar netwerk van 'peers' naar de juiste leverancier, communiceert, kan onderhandelen, bestellen en het afleveradres geven en betalen. Ook gaat zij op zoek naar de beste onderhoudsmonteur als zij ergens een storing signaleert (zich niet lekker voelt) en om energie te besparen gaat zij zelfstandig in gesprek met de energiemaatschappij of met de tv. Zij kan om piekbelasting te voorkomen de tv verzoeken zichzelf uit te zetten (maar de tv kan dit verzoek afslaan).

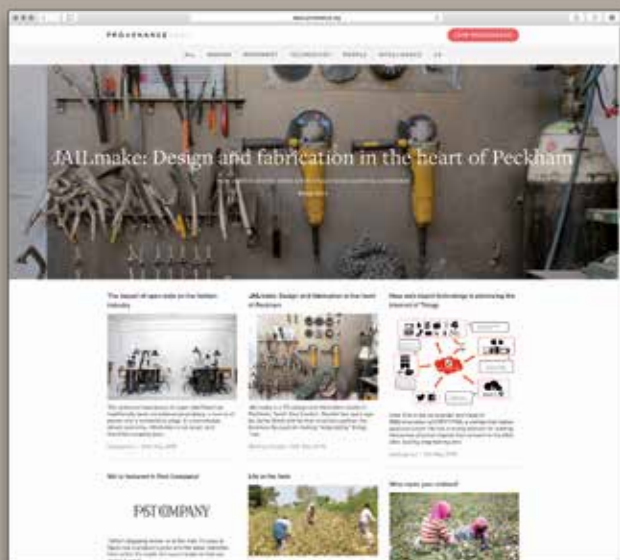


De Samsung W9000, werkend met blockchain, uitgewerkt en beschreven in het IBM paper 'ADEPT: an IoT Practitioner Perspective'.

De Samsung W9000 blockchain-wasmachine is een 'proof-of-concept' en slimme contracten zijn alleen nog een 'blauwdruk' voor een toekomstige praktijk. Op grote schaal wordt de blockchain nog niet gebruikt. Toch kan het interessant zijn om zo'n toekomst te verkennen. Vanaf het moment dat een product de productielijn afrolt, kan het door de fabrikant worden geregistreerd in

een universele blockchain en representeert dit het begin van het leven van het bewuste product. Een simpele wasmachine kan een semiautonom apparaat worden dat in staat is de levering van zijn eigen verbruiksartikelen te beheren, onderhoud te regelen en te onderhandelen met andere peer-apparatuur teneinde zo efficiënt en effectief mogelijk om te gaan met zijn omgeving. Een vorm van autonoom Product Lifecycle Management dus, waarbij de producten zelfstandig hun levensduur, levensbeëindiging en voortbrenging van nieuwe producten bepalen (we komen hier bij de crypto-economie 3.0 op terug).

Het Engelse bedrijf Provenance ('herkomst') heeft een softwareservice ontwikkeld waarmee onderdelen van producten worden vastgelegd en gedeeld op basis van de blockchain. 'Made in', 'made of'- en 'made by'-informatie kan door de makers aan hun producten worden meegegeven. De waarde ligt volgens Provenance in de mogelijkheid andere verhalen te vertellen over je product. De API's kunnen praten met de grotere e-commerceplatformen, zodat dit soort informatie eenvoudiger beschikbaar komt op grotere platformen dan Provenance.



The Provenance platform

Using Provenance it's simple for maker to add products and open up information using our online tools in three simple sections:

Made in

Locations: Making, materials and business addresses

Made Of

Materials, accreditations, certifications and processes

Made By

Maker stories, company information, employees

Device Democracy

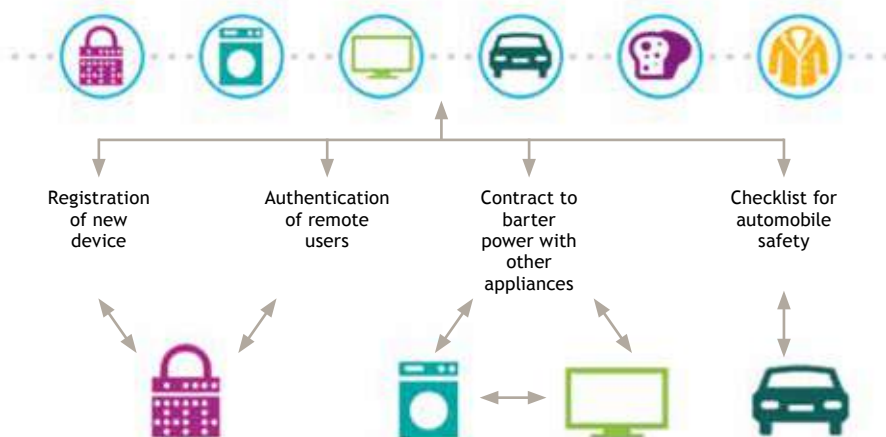
Een van de bedrijven die munt probeert te slaan uit bovenstaand gedachtegoed is het bedrijf 21 Inc. In de afgelopen jaren hebben venture capitalists – zoals Andreessen en Horowitz, chipmaker Qualcomm en de oprichters van bedrijven zoals eBay, PayPal, Dropbox, Expedia en Zynga – meer dan 161 miljoen dollar in het bedrijf geïnvesteerd. Pas in mei 2015 maakte het bedrijf zijn plannen bekend. Het heeft een speciale miningchip ontwikkeld, genaamd Bitshare, die in ieder mobiel apparaat past: *'21 Inc. will insert ASIC chips for bitcoin mining into such daily devices as routers, gaming consoles, USB battery chargers, toasters, set-top boxes, and chipsets'*. Conceptueel gezien transformeert de chip Bitcoin hiermee in 'een fundamentele systeembron die een op een te vergelijken is met CPU, bandbreedte, hardeschijfruimte en RAM'. Ieder apparaat kan met behulp van deze chip zijn eigen stroom aan digitale valuta genereren en deze vervolgens gebruiken om elkaar te betalen voor de geleverde diensten. Volgens een van de ontwikkelaars van 21 Inc. zijn het in de toekomst ook niet de mensen die transacties verrichten, maar juist de machines: *'Everyone assumes that humans will be driving transactions, not the case.'*

Driekwart van de opbrengsten van het miningwerk gaat naar 21 Inc. Onderdeel van het plan zou zijn om producten gratis te maken en daardoor snel nieuwe klanten te kunnen werven. De winst komt immers uit een andere bron. Dit model sluit aan bij de trend die door IBM is beschreven in hun rapport over Device Democracy.

Slimme contracten

Bij het 'verblockchainen' van contracten gaat het met name om het idee dat allerlei regels en afspraken die in contracten besloten zitten, nu simpelweg te programmeren zijn op de blockchain. Bemiddeling en vastlegging door een centrale instantie zoals een notaris of een bank is dan niet langer vereist voor de opstelling en naleving van een contract. Een slim contract staat in dit geval gelijk aan een klein geprogrammeerd stukje code waarin contractuele afspraken worden belegd die geverifieerd worden door de blockchain met automatische transacties of uitstel van betalingen als de blockchain weet wanneer afspraken wel of niet zijn nagekomen.

Universal digital ledger



De blockchain functioneert als een universeel digitaal grootboek dat allerlei apparaten kunnen gebruiken om met elkaar diverse typen van transacties aan te gaan.

Bron: Brody, Paul & Veena Pureswaran (2014): 'Device democracy – Saving the future of the Internet of Things', IBM, September, 2014

DIGITALE NOTARISSEN

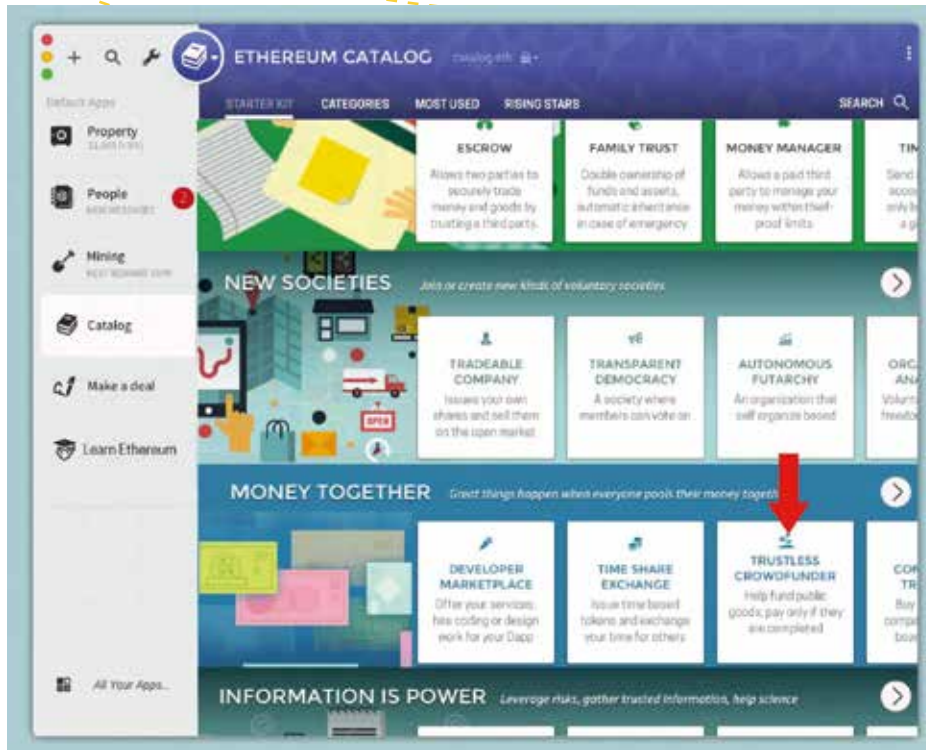
Er bestaan al enkele concrete implementaties waarin de blockchain voor notariële functies wordt gebruikt. Zo ontwikkelde de Argentijnse ontwikkelaar Manuel Araoz Proof of Existence. Deze dienst maakt het mogelijk de echtheid van een document op een bepaald moment publiekelijk vast te leggen door het van een unieke code (sha256-hash) te voorzien en te registreren in de blockchain. Daarmee kan bijvoorbeeld een journalist of advocaat aantonen dat hij op een bepaald tijdstip een zeker document in handen had, zonder dat de inhoud ervan publiekelijk wordt gedeeld. Virtual-Notary, Bitnotar, Chronobit, Pavilion.io en btcluck zijn diensten die een soortgelijke functionaliteit bieden.

Online gokken zou zich uitstekend lenen voor deze slimme contracten. De code vraagt de uitslag van een sportwedstrijd en betaalt eventueel uit volgens de opgestelde regels. Daarmee wordt de organisator van bijvoorbeeld een gokspel geheel overgeslagen. Augur is een volledig gedecentraliseerde voorspellingsmarkt die gebruikmaakt van het blockchainmechanisme. Met Augur is het bijvoorbeeld mogelijk de uitslag van de toekomstige presidentsverkiezingen te voorspellen of een weddenschap aan te gaan wie er dit jaar landskampioen in het voetbal wordt.

Het bedrijf Ethereum regelt en organiseert heel veel van dit soort slimme contracten en is marktleider in deze zich pas ontwikkelende markt. Ethereum is een open-sourceplatform dat waardetokens, genaamd 'ethers', distribueert via de blockchain. Via een WYSIWYG-interface, de Mist-browser, kan iedereen slimme contracten bij elkaar klikken. Het platform biedt een aantal templates voor het maken van zulke contracten. Een kind kan de was doen, lijkt het.

Naast contracten wil Ethereum ook andere financiële toepassingen mogelijk maken, zoals het openen van een spaarrekening, het opstellen van een testament en het uitgeven van aandelen. Ook worden semifinanciële toepassingen mogelijk geacht, zoals het belonen van iemand die lastige rekenklussen uitvoert op zijn systemen. Daarnaast wordt nagedacht over andere decentrale processen, zoals het opzetten van een systeem om veilig te kunnen stemmen, maar ook om een 'concurrent' voor Dropbox op te zetten.





Slimme eigendomsrechten

Een belangrijk onderdeel van een contract kan het eigendomsrecht zijn. Dit eigenaarschap kan belegd worden in de blockchain en door de programmeerbaarheid weten de activa in kwestie wie hun eigenaar is. Denk aan een gestolen auto die niet start omdat de blockchain weet dat de auto is ontvreemd. De blockchain fungeert hier als een controledatabase gelinkt aan een unieke digitale 'vingerafdruk' die onrechtmatig gebruik onmogelijk maakt. Een bedrijf als Mine gebruikt een combinatie van identiteit, reputatie historie, digitale documentatie en de blockchain als een bewijs van eigenaarschap. Dit levert interessante kansen op voor nieuwe online marktplaatsen die volledig gedecentraliseerd zijn en waar iedereen handel met elkaar kan drijven op basis van het gestelde vertrouwen in het netwerk. Of voor bestaande marktplaatsen: wanneer een auto wordt verkocht via een marktplaats, wordt het eigenaarschap pas overgedragen als de betaling binnen is. Een voorbeeld van zo'n P2P-marktplaats is OpenBazaar. Dit is een nieuwe ma-

nier om op een anonieme, ongecensureerde manier online handel te faciliteren. Het maakt gebruik van technologieën als BitTorrent, Tor en Bitcoin. Volgens oprichter Brian Hoffman is het niet de bedoeling dat allerlei illegale producten en diensten worden verhandeld, maar dat is gezien de aard van het project niet te voorkomen. Naast OpenBazaar bestaat ook nog het soortgelijke Bit-Markets.

Een ander voorbeeld is Airlock.me, een nieuwe manier om sloten open te maken. Er is niet langer een fysieke sleutel vereist, maar de deur kan van het slot worden gehaald met behulp van cryptocurrencies. Zo is het bijvoorbeeld mogelijk via Airbnb een appartement te huren. Zodra de huurder het bedrag in bitcoins heeft overgemaakt, verstrekt de Bitcoin-blockchain na verificatie toegang tot het appartement voor de duur van de afgesproken periode. Het is een combinatie van slimme contracten en slimme dingen.



Lockmasters

A Lockmaster connects their smart lock to Airlock. A lock can be public or private and is always communicating with the Airlock network.

Keyholders

A keyholder is granted access to a Lock by its owner. Access can be open-ended, limited by date and time, or one-time only, as determined by the Lockmaster.



3 CRYPTO-ECONOMIE 3.0 – DE ROBOCORPS

Juist omdat we de blockchain zo duidelijk positioneren als een platformtechnologie met meerdere mogelijke uitkomsten en toepassingen, loont het om ons te laven aan de fantasierijke denkers die zich in de wereld van de blockchain begeven. Degene die daar bij uitstek toe in staat is, is Mike Hearn. Hij is een voormalige ingenieur van Google, een van de ontwikkelaars achter bitcoin, en tevens een wereldwijde autoriteit op blockchaingebed. Zijn toekomstvisie heet Tradenet.

Tradenet

Niet de elektrische auto's van Tesla of de omstreden taxidiens Uber zijn de toekomst, maar geëmancipeerde auto's die op eigen houtje zakendoen. Hearn gaat er in zijn theoretische experiment van uit dat zelfrijdende auto's in de toekomst volledig normaal zijn en dat de meeste mensen daardoor niet langer zelf een auto bezitten. Als die zelfrijdende taxi's bovendien niet langer eigendom zijn van een groot bedrijf maar volledig autonoom werken, worden ook de ritten goedkoper.

Echt interessant wordt het als die autonome auto's helemaal naar onze wensen geprogrammeerd kunnen worden. Hearn: 'We kunnen ze zo programmeren dat ze een heel klein beetje winst mogen maken, maar geen excessieve hoeveelheden. We kunnen zo de meest morele en sociaalvoelende kapitalisten ooit maken.'

De auto's communiceren met klanten en infrastructuur via een nieuw online handelssysteem: Tradenet. Je zou een app gebruiken die inlogt op Tradenet en zegt: 'Hier ben ik, hier wil ik naartoe, geef me de beste prijzen.'

De autonome taxi's zullen dan hun beste tarieven doorgeven, gebaseerd op waar ze zijn, hoeveel brandstof ze hebben, de kwaliteit van hun programmering... Jijzelf of je telefoon kiest vervolgens het beste aanbod, niet alleen op basis van de beste prijs maar ook op basis van rijgegevens en hoe aangenaam de wagen is.

Hearn benadrukt dat de auto's wel zelfstandig werken, maar geen bewustzijn hebben. Ze kunnen echter wel zo geprogrammeerd worden dat ze zichzelf bijvoorbeeld updaten. Zo kunnen ze het geld dat ze verdienen gebruiken om menselijke softwareontwikkelaars in te huren om hun code aan te passen, maar ook om te betalen voor onderhouds- of tankbeurten. De auto's kunnen vervolgens ook de kans krijgen om hun 'spaargeld' samen te leggen om nieuwe auto's te laten maken. Om 'kinderen' te krijgen dus. Als een nieuwe auto van de productieband rolt, zou die in concurrentie gaan met de bestaande wagens. Daardoor zou de nieuwe auto een deel van zijn inkomsten moeten afstaan aan zijn 'ouders'. Je kunt het zien als een soort 'geboortelening', die de wagen aan zijn ouders moet afbetalen voordat hij volledig zelf-





standig wordt. Volgens datzelfde principe is ook de dood verwerkt in het systeem, om verouderde modellen van de straat te halen of om in te spelen op een veranderende markt. Als er op een bepaald moment te veel auto's zijn voor het aantal mensen, zouden sommige auto's zichzelf in een langetermijnparking kunnen zetten en uitschakelen. Volgens datzelfde principe zouden auto's ook kunnen uitwijken naar andere steden om daar werk te zoeken, aldus Hearn.

Omdat banken – zeker in het begin – wellicht zouden weigeren om geld te geven aan machines, zouden de wagens werken met virtueel geld zoals bitcoins. Voor klanten zou zakendoen met machines volgens Hearn veel transparanter zijn dan zakendoen met mensen.

'Je loopt geen enkel risico dat ze je afzetten en er is geen kans op misverstanden.'

Robocorps, DAO's en DAC's

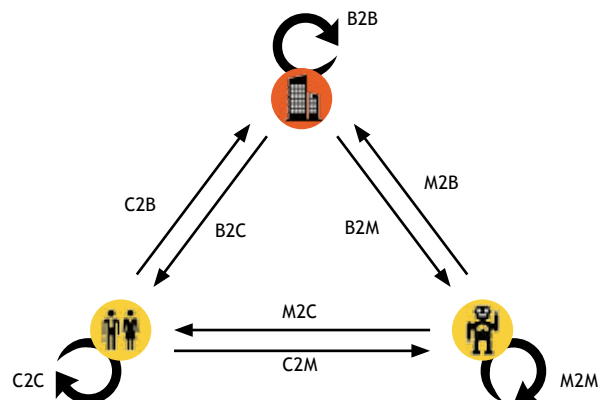
De visie van Hearn is een uitleg van een breder gedragen gedachtegoed in de wereld van de blockchain en de bitcoin: gedecentraliseerde autonome organisaties (DAO's) gaan een belangrijke rol spelen in de maatschappij. Centrale instanties en hiërarchieën zijn steeds minder no-

dig. De machines regelen het onderling veel efficiënter. Een dergelijke efficiëntie – waarin robotbedrijven niets anders zijn dan een commodity – komt in de buurt van het nieuwe paradigma dat Jeremy Rifkin in zijn boek *The Zero Marginal Cost Society* presenteert. Gemeenschappelijk gebruik van auto's verlaagt de kosten extreem en transactiekosten nemen af door gedecentraliseerde autonome machinebeslissingen. Rifkin noemt dit een 'collaborative commons'.

Een gedecentraliseerde autonome organisatie (DAO), ook wel 'Fully Automated Business Entity' of 'Distributed Autonomous Corporation / Distributed Autonomous Company' genoemd (FAB en DAC), is een gedecentraliseerd netwerk van autonome agenten die een productiefunctie hebben, gebaseerd op outputmaximalisatie. Deze DAO's, FAB's en DAC's functioneren zonder menselijke tussenkomst en op basis van businessregels die naar verluidt niet corrupteerbaar zijn.

'You become a stakeholder by buying "stock" in the (DAO) company or being paid in that stock to provide services for the company. This stock may entitle you to a share of its "profits", participation in its growth, and/or a say in how it is run.'

Stan Larimer,
president of Invictus Innovations



Naast een business-to-business- en business-to-consumereconomie voorziet de blockchain in een autonome machine-to-machinetoekomst.

Iedere persoon en elk object heeft zodoende de mogelijkheid om een bankrekening te bezitten en financiële transacties te verrichten. Een wereld waarin een frisdrankmachine een zelfstandige economische entiteit is, met een eigen (bitcoin)bankrekening, die zelf verantwoordelijk is voor het beheer en de verkoop van haar eigen drankvoorraad, behoort hiermee tot de mogelijkheden. Een machine die dus naast het zelfstandig verkopen van een drankje aan de consument (M2C), ook zelf een order kan plaatsen bij bedrijven (B2M). Ze kan zelfs een order plaatsen bij consumenten (C2M) om de voorraad aan te vullen. IBM-architect en blockchainexpert Richard Gendal Brown verwoordt het als volgt:

'Op de Blockchain weet niemand dat je een koelkast bent.'

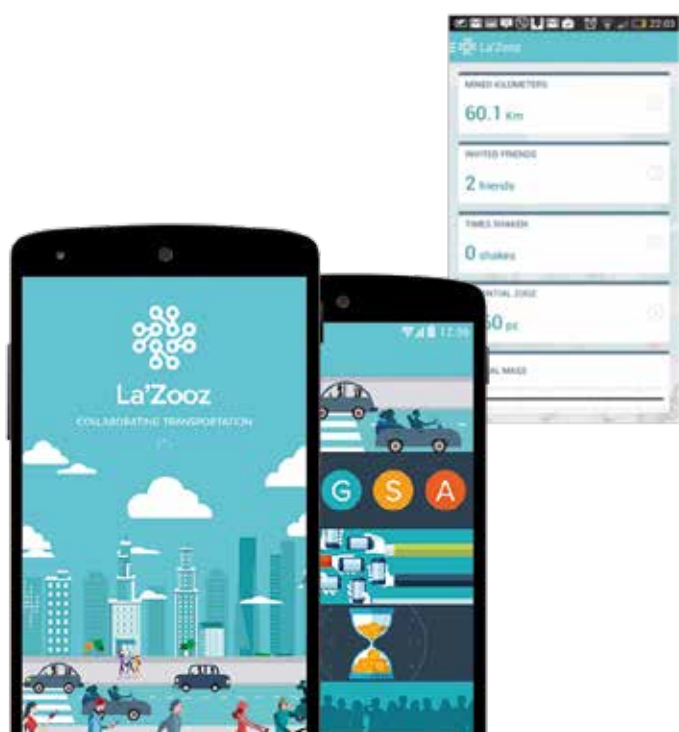
Taxi's, overheid, uitzendbureaus

Het bedrijf La'Zooz is een voorbeeld van een gedecentraliseerde autonome organisatie. Je kunt geld verdienen (een Zooz) als je iemand een lift geeft. Een centraal register van afgelegde kilometers met een lifter vormt de basis van het systeem. Het is een soort Uber of Lyft, maar dan zonder een centraal orgaan. La'Zooz werkt volgens 'proof-of-movement'. De smartphone met de La'Zooz-app erop registreert de kilometers (bewijs dat er gereden is). Iedere keer dat meer dan 20 kilometer is afgelegd, verdient de bestuurder een Zooz en kan hij die weer inzetten als hij zelf een rit nodig heeft.

Het hoeft niet op te houden op bij een frisdrankmachine, een koelkast of een zelfrijdende auto. Bedrijfsstrategieën kunnen verpakt worden in een stuk code dat na executie zelfstandig kan acteren in de economie. Maar denk bijvoorbeeld eens aan een uitzendbureau. Wanneer je nu iemand nodig hebt om werk voor je te verrichten, bel je het uitzendbureau, leg je uit wat er verlangd wordt van de werknemer en zorgt het bureau ervoor dat de ideale kandidaat op het juiste moment komt opdagen. Maar hoe moeilijk is het om deze taken te automatiseren in de vorm van een algoritme? De blockchain kan ook de basis zijn van een heel nieuw zzp-model. De ondernemers die ook Layar in de markt hebben gezet, zijn hiermee bezig. Hun nieuwe bedrijf heet Clock en stelt zich ten doel een wereldwijde 'Networked Autonomy' te creëren, inclusief een grootboek waarin alle waarde-uitwisselingen plaatsvinden via de blockchain, zoals microbetalingen voor inspiratie van de ene naar de andere deelnemer in het netwerk.

Decentrale Autonome Overheden

Ook voor de overheid kan bovenstaande gedachte opgaan. De Bitcoin-software kan grote delen van overheidstaken zoals het verstrekken van een geboortecertificaat, het uitreiken van een paspoort, het aankopen van grond en het stemmen op politieke partijen overnemen. Melanie Swan noemt dit idee een DAS (Decentralised Autonomous Society). Bitnation is in de conceptualisering van de blockchaingedachte voor de overheid het verst. Hun slogan is 'Blockchains, not borders'. Bitnation is volgens oprichtster Susanne Tarkowski Tempelhof het beste te omschrijven als een Do It Yourself-overheid. Een van de pilotprojecten is het verstrekken van een blockchain ID. Met behulp van de blockchain wordt nu ook geprobeerd om in Australië de politieke partij van de toekomst op te richten. Oprichter May Kay noemt de partij de Neutral Voting Bloc (NVB). Het is in zijn ogen een 'politieke app' waarbij het electoraat via de digitale achterban verneemt hoe het moet kiezen. Geen verborgen politieke agenda's meer: alle politieke beslissingen zijn op deze manier via de blockchain open en transparant. Het is wat Kay een 'true democracy' noemt.



Ook vanuit de niet-Bitcoin-hoek worden overigens stappen ondernomen om de overheid te veranderen in een gedecentraliseerd orgaan. Een mooi voorbeeld hiervan is het e-burgerschap van Estland. Buitenlanders kunnen vanaf eind 2014 een e-burgerschap aanvragen, waarmee ze toegang krijgen tot alle 'digitale services' van Estland.

Virtual reality en de blockchain

Simon de la Rouviere, auteur van het boek *The Blockchain: Mapping the Decentralized Future*, gaat nog een stapje verder. Hij ziet een toekomst voor zich waar mensen steeds meer tijd doorbrengen (en ook hun geld verdienen) in een virtuele wereld – zoals Second Life, Eve: Online en World of Warcraft – en beargumenteert dat de blockchain al deze alternatieve realiteiten kan ondersteunen: 'alternatieve realiteiten als een legitiem middel om op verschillende manieren te "leven". Door gebruik te maken van een combinatie van decentrale financiën, onroerend goed, handel, organisaties, kunstmatige intelligentie en de wet, schept het niet alleen een gedecentraliseerde basis voor onze huidige realiteit, maar ook voor elke andere.' Een voorbeeld hiervan is Decentraland, een open-source initiatief voor het bouwen van een gedecentraliseerde virtuele realiteit. Er wordt blockchaintechnologie gebruikt om land te claimen en over te dragen en een eigendomsregistratie bij te houden.

Tot slot: het nieuwe organisatieparadigma

De blockchain is een nieuw organisatieparadigma. Maar de decentrale autonome organisaties die we hierboven beschreven, zijn nauwelijks organisaties te noemen. Het is software met een heel hoge mate van autonomie. Dit lijkt een revolutionaire ontwikkeling: je hebt geen bedrijven meer nodig, algoritmes doen het werk. Het is een 'verdwijnpunt' voor organisaties. Het valt goed te rijmen met de uitspraak van Marc Andreessen: 'Software is eating the world'. Alles wat gedigitaliseerd kan worden, wordt gedigitaliseerd, dus ook organisaties in al hun facetten.

Door de lens van de geschiedenis bekeken is het minder revolutionair. De blockchain modus operandi is slechts een logisch automatiseringsvervolg. Automatiseren be-

tekt immers machines zoveel mogelijk het werk laten doen. Sinds internet weten we dat decentralisatie en peer-to-peernetwerken hiervoor ook sterke schakels zijn. Een belangrijke vraag die overblijft, is welke organisaties deze leemte gaan vullen en hoe sterk ze kunnen worden. 'Wie is de eigenaar van de toekomst?' is de kritische vraag die we nu moeten stellen. Wordt het een democratisch spel of gaan we het Uber- en Google-tijdperk van de blockchain in? Dat laatste scenario is een extra overweging om vroegtijdig geïnformeerd te raken over de mogelijkheden en zelf te gaan experimenteren.

De toekomst is decentraal

Wel vereist het denken in blockchaintermen een compleet andere mindset. De wijze waarop we gewend zijn om onze economie en samenleving te organiseren, het 'oude denken', wordt dankzij de blockchain volledig op zijn kop gezet. De vaak gehoorde uitspraak 'de toekomst is decentraal' vereist dat mensen en organisaties het verleden loslaten, out-of-the-box denken, sterker nog, heel de box weggooien en opnieuw beginnen. Terug naar de tekentafel dus. En dit is lastig. Bedrijven proberen immers het probleem in stand te houden waarvoor ze zelf ooit de oplossing waren.

In 2004 schreven de economen Frank Levy en Richard Murnane in hun boek *The New Division of Labor* dat zelfrijdende auto's nooit realiteit konden worden: 'But executing a left turn against oncoming traffic involves so many factors that it is hard to imagine discovering the set of rules that can replicate a driver's behaviour [...]'. Zes jaar later, in oktober 2010, kondigde Google aan dat ze al een tijd lang in diverse Toyota Priussen rondreden die volledig autonoom waren. Zoals we reeds aantoonde in ons eerste rapport 'Design to Disrupt: Een executive introductie' neemt het tempo van technologische innovaties toe. Bedrijven moeten deze versnelling omarmen om zichzelf te kunnen veranderen. Blockchain staat misschien nog in de kinderschoenen, maar nu is de tijd om ermee aan de slag te gaan.

TOT SLOT: CONCLUSIE EN OVERWEGINGEN VOOR BUSINESS EXECUTIVES

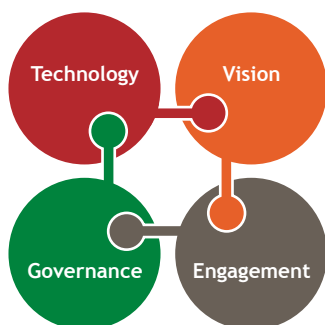
Als leidraad voor digitale disruptie presenteerden we in de vorige rapporten het vierfasenmodel uit 'Leading Digital'. We deden een oproep aan de CIO en de business executives om de leiding te nemen in de digitale verandering.

Leading Digital in Four Steps

Fuse IT and business to build digital skills and transform technology platforms

Create a shared transformative vision of the digital future

Establish strong digital governance to steer the course



Engage employees at scale to make vision a reality

Met de blockchain, met al zijn technische details en onzekerheden, kun je je afvragen bij wie of waar de 'Leading Digital'-actie komt te liggen. 'Nergens, totdat we werkelijk de technologie begrijpen' is het meest waarschijnlijke antwoord. Maar hoe lang kunt u wachten voordat een transformatieve kijk op uw eigen digitale toekomst op basis van de blockchain gemaakt moet worden?



Internet Yellow Pages: alle adressen van het internet in een boek.

Early days

De blockchain is een fascinerend fenomeen. Het doet denken aan het internet voordat er webbrowsers waren. Toen paste het hele internet nog in een boek (Internet Yellow Pages) waarin alle adressen stonden waar je naartoe kon gaan. Later kwamen pas de killer-apps, Google, Facebook en veel later mobile banking en WhatsApp.

We staan aan de vooravond van het Netscape-moment voor de blockchain. De toepassingen zijn volop in ontwikkeling, het is wachten op de nieuwe Google of Spotify van dit nieuwe netwerk. Als de basis echt zo solide blijkt, vergeten we de 'sterkste schakel' en zullen de ogen gericht zijn op de toepassingen zelf. Het schaart zich dan onder de andere solide bouwblokken van het moderne IT-landschap: SMOAT (Social, Mobile, Analytics, Cloud and Things), straks mogelijk B-SMOAT ('be smashed'). Hiermee is nog niet gezegd welk pad u dient te bewandelen om hiervan de vruchten te plukken en wanneer het voor u interessant wordt om in te stappen.

Wie neemt de lead?

Het is te verwachten dat de nieuwe toepassingen in uw markt van organisaties zullen komen waar u nog nooit van gehoord hebt, zoals Coinometrics, Helloblock, Kraken, BTCJam, BlockCypher, DigitalTangibleTrust, Bifubao en Bitpagos, om maar eens wat te noemen.

Hier ligt ook de essentie van de disruptie zoals beschreven in de executive introductie: de uitdagers komen van buiten de eigen sector en worden in het begin niet serieus genomen. Het zijn de concurrenten met ogenschijnlijk 'crappy' producten en diensten waar in eerste instantie voor gewaakt moet worden. Dit is de les die innovatiegoeroe Clayton Christensen ons leert.

De telco's, de banken, de IT-sector

De reden waarom telco's er vroeg bij willen zijn is waarschijnlijk omdat ze IT-infrastructuurinnovaties eerder begrijpen, omdat het hun business is. Telecomgigant Orange is in gesprek met bitcoin/blockchain-start-ups en legt geld op tafel voor investeringen. George Nahon, CEO van Orange Silicon Valley (OSV):

'There's something intriguing in this technology, so we want to be there as early as possible.'

Maar ook van DoCoMo, T-Mobile en Perseus Telecom is al bekend dat ze investeren in deze nieuwe technologie. Het Japanse DoCoMo heeft in januari 2015 nog mee geïnvesteerd in de injectie van 75 miljoen dollar in 'coinbase'.

Voor de financiële sector, en dan met name de banken, ligt het erg voor de hand om navolging te geven aan wat UBS heeft gedaan: een Bitcoin Innovation Lab openen en daar serieus in investeren. De CIO van UBS, Oliver Bussmann, heeft de blockchain al genoemd als de belangrijkste potentiële disruptor voor zijn markt.

'The blockchain is the technology with the biggest potential to disrupt financial services and trigger massive simplification of banking processes and cost structure, changing not only the way we do payments but also the whole trading and settlement topic.'

Infosys gaat al een stap verder en kondigde in april 2015 aan om de blockchain te integreren in zijn 'core banking software' Finacle, met name om het mobiel betalingsverkeer veiliger te maken.⁴

Meer leren

Voor de meeste organisaties, die geen innovatielab willen opzetten maar de blockchain al wel willen opnemen in hun coreprogrammatuur of die geld durven steken in start-ups, is er nog genoeg te doen: de blockchain en de bitcoin beter leren begrijpen. Dat kan een individuele actie zijn, een opdracht zo u wilt, voor de lezer van dit rapport. Graag geven we ter afsluiting de volgende lijst van tien tips.



⁴ <http://www.livemint.com/Companies/ITLjqp5nmZFeNXsF4AfA3M/Infosys-revamps-core-banking-software-with-eye-on-future.html>

1. **Volg een online cursus.**

Bijvoorbeeld bij de Khan University: <https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it>

Of schrijf u in voor de MOOC van de universiteit van Nicosia:

<http://digitalcurrency.unic.ac.cy/free-introductory-mooc>

2. **Bekijk een van deze zes bitcoindocumentaires:**

<http://www.coindesk.com/six-bitcoin-documentaries-watch>

3. **Open een bitcoin wallet bij www.coinbase.com en koop een bitcoin.**

4. **Voeg bitcoin toe aan uw Microsoft-account en koop een game.**

Geld toevoegen aan uw Microsoft-account met Bitcoin:

1. Meld u met uw Microsoft-account aan bij Microsoft-account – Betaling en facturering.
2. Kies **Betalingsopties > Microsoft-account > Bitcoins wisselen.**
3. Selecteer het bedrag dat u wilt toevoegen en klik op Volgende.
4. Controleer het benodigde Bitcoin-bedrag en voltooi de transactie binnen 15 minuten met uw digitale portemonnee.
 - Op uw computer: kies Betalen met Bitcoin en betaal met uw Bitcoin-portemonnee op hetzelfde apparaat.
 - Op uw smartphone: scan de QR-code die wordt weergegeven op de pagina om te betalen via uw mobiele Portemonnee-app.
 - Als uw portemonnee zich op een ander apparaat bevindt, kunt u het ontvangstadres en het BTC-bedrag kopiëren naar de portemonnee op uw apparaat of het web en vervolgens uw aankoop doen.

5. **Verricht een micropayment via [ChangeTip.com](http://www.chargetip.com), de ‘love button’ voor het internet.**

6. **Installeer een miningprogramma en lees de ‘Beginner’s Guide to Mining Bitcoins’: <http://startbitcoin.com>**

7. **Bekijk een transactie op de blockchain. www.blockchain.info**

8. **Bouw een eigen slim contract op Ethereum binnen een uur: <http://forum.ethereum.org/discussion/1402/how-to-get-started-your-first-dapp-under-one-hour>**

9. **Inventariseer de bestaande bitcoin/blockchain-kennis onder uw medewerkers en **organiseer een blockchainavond.****

10. **Bekijk uw eigen organisatie met een decentrale blik. Welke centrale onderdelen van uw organisatie kunt u middels een decentrale blockchainoplossing vervangen?**



VERKLARENDE WOORDENLIJST

Altcoin – Bitcoin is de bekendste cryptovaluta. Er zijn echter nog honderden alternatieve digitale valuta op de markt met vaak net iets andere eigenschappen. Een overzicht van alle altcoins vindt u op de website Map of Coins.

Bitcoin – Bitcoin is een vorm van elektronisch geld en tevens de naam van de open-sourcesoftware die is ontworpen om dit te gebruiken. Het is een van de eerste implementaties van een concept genaamd cryptocurrency oftewel cryptografisch geld, dat voor het eerst in 1998 beschreven werd door Wei Dai op de Cypherpunks-mailinglist en in 2009 werd geïmplementeerd door Satoshi Nakamoto (pseudoniem van een onbekende persoon of groep).

Blockchain – Een publiek decentraal grootboek dat alle transacties bijhoudt en tegelijkertijd registreert op alle computers in dat netwerk.

Cryptogeld – Cryptogeld (ofwel cryptovaluta) is een soort digitale munteenheid, die vaak gebruikt wordt als alternatief geldsysteem voor de reguliere geldsoorten. Cryptogeld is gebaseerd op cryptografie (versleutelings-systemen) en gaat gepaard met een proof-of-worksche-ma, dat gebruikt wordt om het geld te genereren, om het te controleren op echtheid en om ermee te han-delen. In feite bestaat cryptogeld uit een stuk versleutelde code waarin de transacties worden opgeslagen. Steeds als er een transactie plaatsvindt, wordt de code aange-vuld of veranderd met een nieuw versleuteld blokje code.

DAC's (Decentralised Autonomous Organisations) ofwel Robocorps – Dit zijn een nieuwe type bedrijven. Het gaat om software die boven op de Bitcoin-blockchain draait en zelfstandig opereert.

Ethereum – Ethereum is een gedecentraliseerd mining-netwerk en de ontwikkeling van een softwareplatform ineen dat mensen in staat zal stellen hun eigen altcoins met ontelbare eigenschappen te creëren. Maar naast een miningnetwerk is het ook een soort van besturings-systeem waarop je cryptocurrency-'apps' kunt laten draaien. Mensen schrijven die applicaties met behulp van programmeertaal die is ontworpen door het Ethe-reum-team. Zodra de applicatie geschreven is, publice-ren ze die op het systeem in de vorm van een 'contract'. Een contract is een geautomatiseerde agent op het Ethe-reum-netwerk samen met een Ethereum-adres. Het kan transacties ontvangen en verzenden en slaat de saldi op van deze transacties.

Hash – Een hashfunctie maakt van een willekeurige lan-ge rij cijfers een unieke 'handtekening' van 128 of 256 bits (~ 40 of 80 decimale cijfers). Een goede hash maakt het onmogelijk om de oorspronkelijke rij, of zelfs maar een deel daarvan, te reconstrueren. Een hash ziet er als volgt uit: 1NkbuV2VLU2u8s1Y2kSA3YqXBb1ty6x6Up

Public key / Private key – De beveiliging van Bitcoin(-transacties) is gebaseerd op een cryptografisch principe van publieke sleutels en privésleutels (public en private keys). De private key is gekoppeld aan de public key, maar is niet te achterhalen door iemand die de public key heeft. Je kunt met de private key aantonen dat de public key van jou is. Om bitcoins te kunnen overmaken heb je voor elk bitcoinadres een unieke sleutel (private key) nodig waarmee je een digitale handtekening maakt om aan te tonen dat je de eigenaar bent. Bitcoinadres-sen zijn afgeleid van de public key. Ze bestaan uit een combinatie van meestal 34 cijfers en letters, beginnend met een 1, waarbij één bepaalde private key hoort. Hiermee kun je transacties ondertekenen om te bewij-zen dat je eigenaar bent van de te versturen bitcoins.



Een bitcoinadres wordt willekeurig gegenereerd. Dit kan omdat er zó veel mogelijke bitcoinadressen zijn dat de kans dat er ooit een dubbele bitcoin gegenereerd wordt verwaarloosbaar klein is. Om je een idee te geven: het aantal mogelijke bitcoinadressen is grofweg vergelijkbaar met het aantal atomen op aarde (in één zandkorrel zitten al vele malen meer atomen dan een miljoen miljard!).

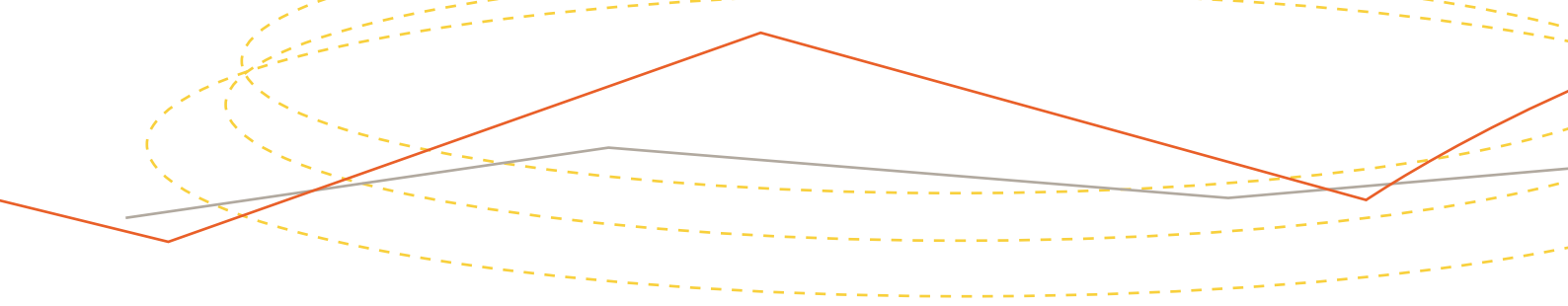
Mining – De bitcoin dient virtueel ‘gedolven’ te worden. Elke dag wordt er een bepaalde hoeveelheid vrijgegeven aan mensen die de bitcoin delven (‘mining’). Dit wordt gedaan door het inzetten van de rekenkracht van computers. Er zijn inmiddels op internet diverse groepen actief waar mensen samen kunnen zoeken naar het elektronische geld door alle gezamenlijke rekenkracht van de computers in te zetten tijdens het delven, de zogeheten ‘mining pools’.

Sidechains – Nieuwe kettingen die inhaken op de kernstructuur van de blockchain, stellen ontwikkelaars in staat features en functionaliteit toe te voegen aan het systeem zonder de kern aan te passen. De sidechain is niets anders dan een sandboxomgeving op de blockchain. Hierdoor kan men sneller experimenteren en is het systeem flexibeler.

Wallet – Een wallet is te vergelijken met een digitale portemonnee waar je geld in kunt stoppen en uit kunt halen om te betalen. Met een wallet kunt je zien hoeveel bitcoins je bezit, kun je ze overmaken of ermee betalen. In tegenstelling tot wat vaak verteld wordt, bevat een wallet geen bitcoins. Wat zich wel in een wallet bevindt zijn de ‘private keys’. Deze private keys (privésleutels) geven toegang tot je bitcoins. Zonder deze sleutels kun je nergens bij. Het is dus zeer belangrijk dat je de wallet (en de private keys die zich daarin bevinden) goed bewaart.

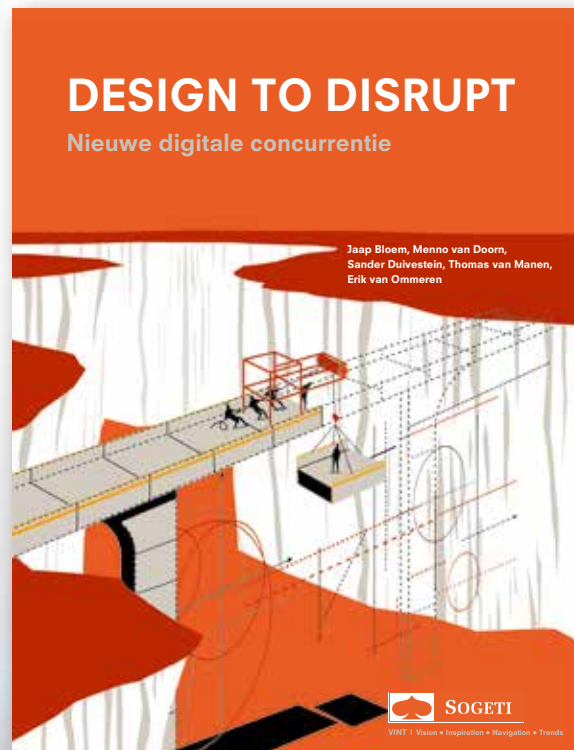
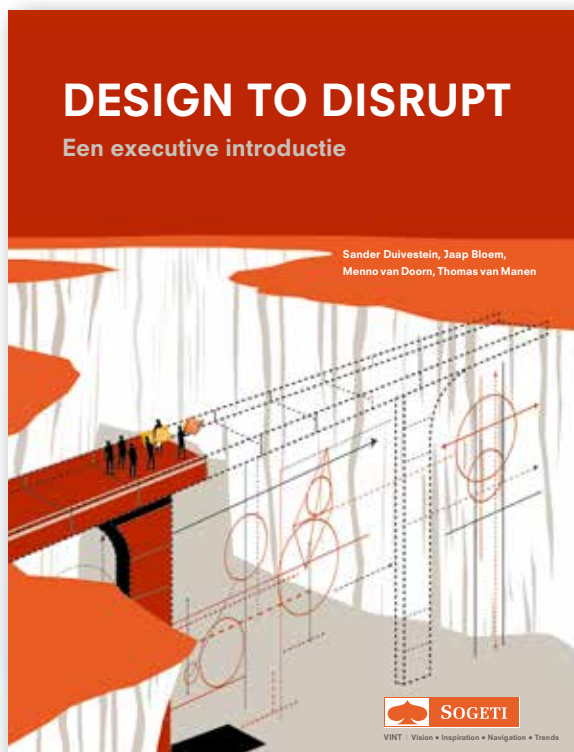
LITERATUUR

- Andreessen, Marc (2011): 'Why Software Is Eating the World', *The Wall Street Journal*, 20 augustus 2011, <http://www.wsj.com/articles/SB10001424053111903480904576512250915629460>
- Antonopoulos, Andreas (2014a): 'Bitcoin and the Evolution of Money As a Content Type', BitcoinSouth, 8 d 2014, <http://vimeo.com/113833922>
- Antonopoulos, Andreas (2014b): *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*
- Arnold, Martin (2014): 'Barclays' Antony Jenkins Calls End of Universal Banking', *Financial Times*, 17 december 2014, <http://www.ft.com/intl/cms/s/0/ef588b42-860a-11e4-b248-00144feabdc0.html>
- Assange, Julian (2014): 'Bitcoin is Much More Than Just a Currency', The Nantucket Project, 3 oktober 2014, https://www.youtube.com/watch?v=MaB3Zw5_p9c
- Back, Adam, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón & Pieter Wuille (2010): 'Enabling Blockchain Innovations with Pegged Sidechains', 22 oktober 2010, <http://www.blockstream.com/sidechains.pdf>
- Badev, Anton & Mathew Chen (2014): 'Bitcoin: Technical Background and Data Analysis', FED, 7 oktober 2014, http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf?p=cite_@inthepixels
- Bartlet, Jimmy (2014): 'Soon the Internet Will Be Impossible to Control', *The Telegraph*, 10 december 2014, <http://www.telegraph.co.uk/technology/internet/11284538/Soon-the-internet-will-be-impossible-to-control.html>
- Beikverdi, Alireza (2015): 'Blockchain Technology Could Have Prevented Louisiana's Deadly Bacteria Leak', *Coin Telegraph*, 3 maart 2015, <http://cointelegraph.com/news/113595/blockchain-technology-could-have-prevented-louisianas-deadly-bacteria-leak>
- Bloem, Jaap, Menno van Doorn, Sander Duivestein & Thomas van Manen (2015): 'Design to Disrupt: Nieuwe digitale competitie'
- Brinker, Gijs den (2013): 'Wellink: "Bitcoin erger dan tulpenmanie"', *Financieel Dagblad*, 4 december 2013, <http://fd.nl/economie-politiek/40311/wellink-bitcoin-erger-dan-tulpenmanie>
- Brody, Paul & Veena Pureswaran (2014): 'Device Democracy – Saving the Future of the Internet of Things', IBM, september 2014, <http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF>
- Cohen, David & William Mougayar (2015): 'After the Social Web, Here Comes the Trust Web', TechCrunch, 18 januari 2015, <http://techcrunch.com/2015/01/18/after-the-social-web-here-comes-the-trust-web>
- Conner, F., D. Velicanu & S. Yakubov (2014): 'A Decentralized Public Key Infrastructure with Identity Retention', <https://eprint.iacr.org/2014/803.pdf>
- Custodio, Nik (2013): 'Explain Bitcoin Like I'm Five', Medium, 12 december 2013, <https://medium.com/@nik5ter/explain-bitcoin-like-im-five-73b4257ac833>
- Duivestein, Sander (2014): 'Het algoritme is de nieuwe eindbaas', LinkedIn, 30 juni 2014, <https://www.linkedin.com/pulse/20140630185158-13303287-het-algoritme-is-de-nieuwe-eindbaas>
- Duivestein, Sander (2015a): 'Bitcoin Is the World's Most Dangerous Idea', The Next Web, 16 april 2015, <http://thenextweb.com/insider/2015/04/16/bitcoin-is-the-worlds-most-dangerous-idea/>
- Duivestein, Sander (2015b): 'De blockchain is de nieuwe Matrix', LinkedIn, 15 april 2015, <https://www.linkedin.com/pulse/de-blockchain-nieuwe-matrix-sander-duivestein?trk=mp-reader-card>
- Duivestein, Sander (2015c): 'Een Bitcoin mining chip in elk apparaat en in elke hand', LinkedIn, 19 mei 2015, <https://www.linkedin.com/pulse/een-bitcoin-mining-chip-elk-apparaat-en-elke-hand-sander-duivestein?trk=mp-reader-card>
- Duivestein, Sander (2015d): 'Why Bitcoin Is Changing How Banks Do Business', The Next Web, 3 maart 2015, <http://thenextweb.com/insider/2015/03/03/why-bitcoin-is-changing-how-banks-do-business/>
- Duivestein, Sander & Patrick Savalle (2014): 'Bitcoin: It's the Platform, Not the Currency, Stupid!', The Next Web, 15 februari 2014, <http://thenextweb.com/insider/2014/02/15/bitcoin-platform-currency/>
- Effinger, Anthony (2014): 'Marc Andreessen on Finance: "We Can Reinvent the Entire Thing"', Bloomberg, 7 oktober 2014, <http://www.businessweek.com/news/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing>
- Gleeson-White, Jane (2012): *Double Entry: How the Merchants of Venice Shaped the Modern World – and how Their Invention Could Make or Break the Planet*, Allen & Unwin
- Hayase, Nozomi (2014): 'The Blockchain and the Rise of Networked Trust', CoinDesk, 22 november 2014, <http://www.coindesk.com/blockchain-rise-networked-trust>

- 
- Hearn, Mike (2013): 'Future of Money', Turing Festival, 28 september 2013, <https://www.youtube.com/watch?v=Pu4PAM-FPo5Y>
- Higgins, Stan (2015): 'IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things', CoinDesk, 17 januari 2015, <http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/>
- Irrera, Anna (2014): 'UBS CIO: Blockchain Technology Can Massively Simplify Banking', *Wall Street Journal*, 27 oktober 2014, <http://blogs.wsj.com/digits/2014/10/27/ubs-cio-blockchain-technology-can-massively-simplify-banking/>
- Isaacson, Walter (2014): 'Big Idea 2015: The Coming Micropayment Disruption', *TIME*, 22 december 2014, <http://time.com/3636720/2015-micropayment-disruption/>
- Ismail, Salim, Mike Malone & Yuri van Geest (2014): 'Exponential Organizations (ExO)', Singularity University
- Kaplan, Robert. S. (2000): *The Nothing that Is: A Natural History of Zero*, Oxford University Press
- Kearns, Jeff (2013): 'Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value', Bloomberg, 4 december 2013, <http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.html>
- Kelion, Leo (2015): 'Could Driverless Cars Own Themselves?', BBC, 16 februari 2015, <http://www.bbc.com/news/technology-30998361>
- King, Brett (2014): 'Why the Facebook of Banking Won't Have a Charter', LinkedIn, 28 december 2014, <https://www.linkedin.com/pulse/why-facebook-banking-wont-have-charter-brett-king>
- Koenraadt, Mathijs (2014a): 'The Protocol Wars: Bitcoin and the Internet of Value', Medium, 10 oktober 2014, <https://medium.com/bitcoin-and-society/the-protocol-wars-bitcoin-and-the-internet-of-value-badc174bae4d>
- Koenraadt, Mathijs (2014b): 'The Decentralize Everything Manifesto', LinkedIn, 25 november 2014, <https://www.linkedin.com/pulse/20141125151550-259980788-the-decentralize-everything-manifesto>
- Kopstein, Joshua (2013): 'The Mission to Decentralize the Internet', *The New Yorker*, 13 december 2013, <http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html>
- Krugman, Paul (2013): 'Bitcoin Is Evil', *New York Times*, 28 december 2013, <http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>
- Lanier, Jaron (2014): 'The Myth of AI', Edge, 14 november 2014, <http://edge.org/conversation/the-myth-of-ai>
- Lent, Adam (2014): 'Farewell Corporate Power: How the Rise of the Blockchain Could Change Everything', City A.M., 16 december 2014, <http://www.cityam.com/205708/farewell-corporate-power-how-rise-blockchain-could-change-everything>
- Levy, Frank & Richard J. Murnane (2005): *The New Division of Labor: How Computers Are Creating the Next Job Market*, Princeton University Press
- Libbenga, Jan (2014): 'Van Bitcoin hype naar Blockchain revolutie', Emerge, 15 december 2014, <http://www.emerge.nl/interviews/efinancials-bitcoin-hype-blockchain-revolutie>
- Ludwin, Adam (2014): 'Why Bitcoin Apps and Bitcoin Speculators Need Each Other', Chain, december 2014, <http://blog.chain.com/post/105287860141/why-bitcoin-apps-and-bitcoin-speculators-need-each>
- Manen, Thomas van (2015): 'Het 1994 moment voor Bitcoin en de blockchain: een internet van vertrouwen', Medium, 12 februari 2015, <https://medium.com/@thomasvanmanen/het-1994-moment-voor-bitcoin-en-de-blockchain-een-internet-van-vertrouwen-743f90a293f4/>
- Monegro, Joel (2014): 'The Bitcoin Application Stack', 25 november 2014, <http://joel.mn/post/103546215249/the-blockchain-application-stack>
- Morozov, Evgeny (2013): *To Save Everything, Click Here: The Folly of Technological Solutionism*, Penguin
- Morris, David (2015): 'Are We Ready for Companies That Run Themselves?', Aeon, 26 januari 2015, <http://aeon.co/magazine/technology/are-we-ready-for-companies-that-run-themselves/>
- Mougayar, William (2014a): 'Blockchain Apps: Moving from the Jungle to the Zoo', Startup Management, 30 december 2014, <http://startupmanagement.org/2014/12/30/blockchain-apps-moving-from-the-jungle-to-the-zoo>
- Mougayar, William (2014b): 'The Blockchain Is the New Database, Get Ready to Rewrite Everything', Startup Management, 27 december 2014, <http://startupmanagement.org/2014/12/27/the-blockchain-is-the-new-database-get-ready-to-rewrite-everything/>
- Mougayar, William (2015): 'The Crypto-Technology and Bitcoin Landscape', Startup Management, 3 maart 2015, <http://startupmanagement.org/2015/03/03/the-crypto-technology-and-bitcoin-landscape/>

- Muller, Thor (2014): 'How the Ledger Unlocked Modern Business', Medium, 3 juni 2014
- Nakamoto, Satoshi (2008): 'Bitcoin: A Peer-to-Peer Electronic Cash System', bitcoin.org, 31 oktober 2008, <https://bitcoin.org/bitcoin.pdf>
- Peck, Morgan E. (2012): 'Bitcoin: The Cryptoanarchists' Answer to Cash', IEEE Spectrum, 30 mei 2012
- Popper, Nathaniel (2015): *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper
- Ravikant, Naval (2014): 'The Fifth Protocol', Start Up Boy, 1 april 2014, <http://startupboy.com/2014/04/01/the-fifth-protocol/>
- Reijerman, Dimitri (2014): 'De kracht van de blockchain – Innovaties met de ruggengraat van bitcoin', Tweakers, 15 december 2014, <http://tweakers.net/reviews/3781/de-kracht-van-de-blockchain.html>
- Rifkin, Jeremy (2014): *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, Palgrave Macmillan Trade
- Roberts, Daniel (2015): 'Bitcoin: will 2015 be a make-or-break year?', *The Guardian*, 3 februari 2015, <http://www.theguardian.com/technology/2015/feb/03/bitcoin-2015-make-or-break-year>
- Rosenfeld, Everett (2014): 'Bitcoin Tech and the Future of Business', AlleyWatch, 14 november 2014, <http://www.alleywatch.com/2014/11/bitcoin-tech-and-the-future-of-business/>
- Rouviere, Simon de la, 'The Blockchain: Mapping the Decentralized Future', GitHub
- Rouviere, Simon de la (2015): 'Virtual Reality & Blockchains: Towards a more empathic society', Medium, 22 mei 2015, <https://medium.com/@simondlr/virtual-reality-blockchains-towards-a-more-empathic-society-9eada83719e3>
- Schneier, Bruce (2013): 'The Battle for Power on the Internet', The Atlantic, 24 oktober 2013, <http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/>
- Seife, Charles (2000): *Zero: the Biography of a Dangerous Idea*, Penguin Publishing Group
- Sood, Varun (2015): 'Infosys revamps core banking software with eye on future', LiveMint, 13 april 2015, <http://www.livemint.com/Companies/ITLjqp5nmZFENXsF4AfA3M/Infosys-revamps-core-banking-software-with-eye-on-future.html>
- Sparkes, Matthew (2014): 'The Coming Digital Anarchy', *The Telegraph*, 9 juni 2014, <http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html>
- Srinivasan, Balaji, S. (2015): 'A Bitcoin miner in every device and every hand', Medium, 18 mei 2015, <https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821>
- Swan, Melanie (2015): *Blockchain: Blueprint for a New Economy*, O'Reilly Media
- Swanson, Tim (2014): *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management*, Amazon Digital Services
- Szabo, Nick (2014): 'The dawn of trustworthy computing', Unenumerated, 11 december 2014, <http://unenumerated.blogspot.nl/2014/12/the-dawn-of-trustworthy-computing.html>
- Valkenburg, Peter van (2015): 'Bitcoin: Our Best Tool for Privacy and Identity on the Internet', Coin Center, 3 maart 2015, <http://coincenter.org/2015/03/bitcoin-our-best-tool-for-privacy-and-identity>
- Vigna, Paul & Michael J. Casey (2015): *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*, St. Martin's Press
- Westerman, George, Didier Bonnet & Andrew McAfee (2014): *Leading Digital: Turning Technology into Business Transformation*, Harvard Business Review Press
- Winklevoss, Cameron & Tyler Winklevoss (2014): 'Money Is Broken; Its Future Is Not', Money20/20.tv, 1 december 2014, <https://www.youtube.com/watch?v=ciGr-v7fZt0>
- Wohlsen, Marcus (2014): 'Tech Giants Are Splitting Up Because They Do Too Much at Once', *Wired*, 7 oktober 2014, <http://www.wired.com/2014/10/tech-giants-splitting-much>
- <https://bitcoin.org/nl/>
- <https://bitonic.nl/>
- <http://nl.wikipedia.org/wiki/Cryptogeld>
- <http://www.bitcoinspot.nl/>
- <http://www.debitcoin.org>
- <http://www.watisbitcoin.nl/>

Het rapport dat voor u ligt, is nummer drie in een reeks van in totaal vier publicaties over het thema Design to Disrupt. De eerste twee kunt u downloaden via <http://labs.sogeti.com/downloads>. Daar vindt u onder meer ook de VINT-rapporten over het Internet of Things en Big Data, plus ons Cyber-security-boek.





Design to Disrupt

Over VINT labs.sogeti.com

Het Verkenninginstituut Nieuwe Technologie van Sogeti, VINT, is onderdeel van SogetiLabs. VINT geeft invulling aan de koppeling tussen bedrijfsprocessen en nieuwe IT. In elke rapportage over een verkenning die het instituut heeft uitgevoerd, zoekt VINT het juiste midden tussen feitelijke beschrijving en beoogde toepassing. Op die manier inspireert VINT organisaties om nieuwe technologie in beschouwing te nemen of zelfs te gaan gebruiken.

De onderzoeken van VINT worden uitgevoerd onder auspiciën van de Commissie van Aanbeveling bestaande uit:

- H. Wesseling (voorzitter), Bestuursadviseur ICT • H.W. Broeders, directievoorzitter Jaarbeurs Holding N.V.
- P. Dirix, directeur Operatie NS Reizigers • F.M.R. van der Horst, hoofd CIO Office ABN AMRO Bank N.V. • D. Kamst, Chief Executive Officer Klooker • T. van der Linden, Group Information Officer Achmea • Prof. dr. ir. R. Maes, hoogleraar Informatie- en communicatiemanagement Academy for I & M • P. Morley, Lid Raad van Commissarissen TLS
- E. Schuchmann, Chief Information Officer Academisch Medisch Centrum • W.H.G. Sijstermans, CIO a.i. Nederlandse Zorgautoriteit (NZa) • K. Smaling, Chief Information Officer Aegon Nederland N.V. • J. Tas, Chief Executive Officer Philips Healthcare Informatics Services Solutions • M. Boreel, Chief Technology Officer Sogeti Group • J.P.E. van Waayenburg, Chief Executive Officer Sogeti Group • P.W. Wagter, Chief Executive Officer Sogeti Nederland B.V.

Over SogetiLabs labs.sogeti.com

SogetiLabs is een netwerk van meer dan 120 technologieleiders binnen Sogeti wereldwijd. SogetiLabs biedt een breed scala aan deskundigheid op het gebied van digitale technologie: van embedded software, cyber security, simulaties en cloud tot business information management, mobiele apps, business analytics, testen en het Internet of Things. Het doel is altijd om technologie, systemen en applicaties met een zo groot mogelijk resultaat in actuele bedrijfssituaties in te zetten. Samen met VINT zorgt SogetiLabs voor inzicht, onderzoek en inspiratie met artikelen, presentaties en video's. Deze zijn altijd te downloaden op de uitgebreide website, online portals en social media van SogetiLabs.

Over Sogeti www.sogeti.com

Sogeti is een toonaangevende dienstverlener op het gebied van digitale technologie en software testing, gespecialiseerd in application, infrastructure en engineering services. Sogeti biedt state-of-the-art oplossingen op het gebied van testing, business intelligence & analytics, mobile, cloud en cyber security. Dit alles op basis van de beste methoden en het wereldwijde Rightshore® delivery-model. Sogeti telt meer dan 20.000 professionals in 15 landen en is in Europa, de VS en India lokaal sterk aanwezig op meer dan 100 locaties. Sogeti is onderdeel van Cap Gemini S.A. dat is genoteerd aan de beurs van Parijs.

SOGETILABS