Blockchain technologie

Het kan niemand ontgaan dat een nieuw technologisch fenomeen sterk in opkomst is: de blockchain technologie. Hoewel deze technologie voornamelijk invloed heeft op administratieve processen en minder zichtbaar is dan bijvoorbeeld 3D printing, kan de impact, in ieder geval op de financiële sector en de overheid, niet gemakkelijk worden onderschat. Om de ontwikkelingen te kunnen begrijpen en in perspectief te kunnen plaatsen is een basaal begrip van de werking van Bitcoin onontbeerlijk.

Auteur
Egbert van de Coevering[1]

In dit artikel nemen we de lezer mee langs de recente technische ontwikkelingen en beschrijven de belangrijkste karakteristieken van de techniek. De bedoeling is om de lezer uit te rusten met voldoende bagage om de te verwachten "tsunami" aan publicaties op het gebied van blockchain technologie op relevantie te kunnen sorteren en waarderen. Aan het eind van het artikel geven we aan waar blockchain technologie de wereld van de belegger op dit moment raakt.

De blockchain technologie staat weliswaar nog in de kinderschoenen maar de ontwikkelingen gaan razendsnel mede als gevolg van de enorme investeringen die in deze technologie worden gedaan en de technologische gemeenschappen die zich op het fenomeen storten. Het is zeer wel mogelijk dat dit artikel een half jaar na publicatie grotendeels herschreven zal moeten worden.

Dat de technologie voor beleggingsinstellingen interessant is mag blijken uit het feit dat Goldman Sachs in november 2015 een patent heeft aangevraagd in de VS voor de settlement van securities gebaseerd op de ideeën van het Bitcoin protocol.[2]

Blockchain 1.0: Bitcoin

Bitcoin kan worden vergeleken met het eerste vliegtuig van de gebroeders Wright. Zij toonden als eerste aan dat een vliegmachine werkt. De ontwerper van Bitcoin Satoshi Nakamoto heeft in 2008[3] aangetoond dat betrouwbare, min of meer anonieme, digitale transacties tussen twee partijen die elkaar niet kennen, niet vertrouwen en zonder tussenkomst van een centrale instantie mogelijk zijn. Een mijlpaal in de historie van het geld.

Bitcoin werd zeker bij aanvang in verband gebracht met crimineel geld. Daarvan kan gezegd worden dat uit de technische historie blijkt dat criminelen vaak als eersten nieuwe technologieën toepassen. Kijk naar de automobiel en de smartphone.

Criminelen zijn vermoedelijk vaak uitgegaan van de foute aanname dat Bitcoin anoniem is. Dat is niet het geval: Bitcoin is pseudoniem. Na een eerste transactie waar fiat geld (dollar, euro) aan te pas komt, is de eigenaar van de Bitcoin te traceren met alle transacties.[4]

Voor Bitcoin zijn er al wel initiatieven geweest om cryptografisch geld te creëren, maar deze initiatieven zijn alle mislukt. Het meest in de buurt komen b-money van Wei Dai (1998) en Bitgold van Nick Szabo (2005).[5]

Wat de oplossing van Satoshi Nakamoto onder andere briljant maakt, is dat hij een oplossing heeft gevonden voor het "double spending" probleem. De vraag is: hoe voorkom je dat een digitaal bedrag meer dan eens wordt uitgegeven? Dit probleem kan worden opgelost door een heel nauwkeurige timestamp te hanteren en daarmee consistentie te waarborgen. Men ziet dan tot op de nanoseconde welke transactie het eerst is ontstaan. Deze eerste transactie is dan geldig. Latere transacties hebben geen geldigheid. Google lost in zijn Spanner project dit probleem van consistentie over zijn wereldwijde datacenters op door een atoomklok en gps antennes. Voor Google is de volgordelijkheid en daarmee de consistentie van de transacties in zijn database altijd helder.

Aangezien Satoshi Nakamoto in een open source omgeving niet de mogelijkheid had van een kostbare atoomklok, heeft hij de oplossing gevonden in het Proof of Work. Het Proof of Work houdt kortgezegd in dat iedereen met een computer (open systeem) die een cryptografische puzzel kan oplossen, de door hem geaggregeerde transacties (block) aan het grootboek (blockchain) kan toevoegen. Als beloning staan daar twee vergoedingen tegenover: een fee per transactie (incentive) en Bitcoins uit een pool van nog niet uitgegeven Bitcoins (incentive). Het Bitcoin systeem en de Bitcoin blockchain worden voor uiterst betrouwbaar gehouden. Er zijn weliswaar hacks geweest van bewaarders van de Bitcoin sleutels (Mount Gox) maar nog nooit van Bitcoin zelf.[6]

Het Bitcoin protocol heeft ook een aantal nadelen. De generatie van blocks en nieuwe Bitcoins kost veel rekenkracht en daarmee elektriciteit. Het Bitcoin protocol is ook niet snel. Per 10 minuten wordt er een block aan de keten toegevoegd. Gemiddeld haalt Bitcoin daarmee 7 transacties per seconde wat in geen verhouding staat tot de 24.000 transacties gemiddeld per seconde die Visa bijvoorbeeld haalt. Om dit te versnellen worden er alternatieven voor het Proof of Work bedacht zoals bijvoorbeeld het Proof of Stake. In deze variant is het netwerk niet voor iedereen open maar mogen alleen de partijen die over een bepaalde kwantiteit aan coins beschikken, meedoen met het oplossen van de cryptografische puzzel. Een deel van de betrouwbaarheid wordt in het Proof of Stake model opgeofferd aan de snelheid.

Het Bitcoin protocol is open source, wat betekent dat de code door iedereen is te gebruiken en aan te passen. Dat is ook gebeurd en leidde tot de opkomst van de zogenaamde altcoins. Dit zijn op het Bitcoin protocol gebaseerde cryptocurrencies met aanpassingen. Op deze website is een overzicht te vinden van de beschikbare altcoins: http://mapofcoins.com.[7]

Blockchain 1.0+: Aanvullend gebruik van de Bitcoin blockchain

Het Bitcoin blockchain concept kent een aantal karakteristieken die het voor andere toepassingen interessant maken.

De Bitcoin blockchain levert de volgende karakteristieken:

- Consensus – er is overeenstemming tussen partijen die elkaar niet vertrouwen over de gedeelde feiten op de schaal van internet. Dat wil zeggen dat de hele (internet) wereld in potentie de vastgelegde feiten kan inzien.
- Validiteit – in de regels kan worden opgenomen wat een valide toevoeging is. Bijvoorbeeld: is er voldoende saldo, is er een vergoeding voor de transactie bepaald en is er een geldige private key.
- Uniciteit – de blockchain voorkomt "double spending", het dubbel uitgeven. Alle gevalideerde transacties zijn uniek.
- Onveranderlijkheid – dit betekent niet dat de gegevens niet veranderd kunnen worden, maar meer genuanceerd dat niemand anders een aangepaste transactie afkomstig van dezelfde bron zal accepteren.
- Authenticatie – een transactie is gekoppeld aan een "private key". Er is geen concept van een "master key" of "administrator" die overal toegang toe heeft.

Aan de hand van deze karakteristieken kunnen met gebruikmaking van het open source Bitcoin protocol nieuwe toepassingen worden ontwikkeld die desgewenst worden gekoppeld aan de bestaande Bitcoin blockchain.

Die nieuwe toepassingen kunnen alle karakteristieken overnemen, maar noodzakelijk is dat niet.

Ironisch is dat de banken de blockchain technologie omarmen, terwijl Bitcoin juist bedoeld is om de banken overbodig te maken. Het R3 consortium dat inmiddels meer dan 40 aangesloten grootbanken telt, ontwikkelt nieuwe applicaties gebaseerd op de karakteristieken van de technologie, zonder iedere karakteristiek in volle omvang te implementeren.

De banken hebben er geen behoefte aan om de consensus met betrekking tot de transacties over heel het internet te delen. Voor hen is het voldoende dat er consensus bestaat op transactieniveau en niet op grootboekniveau.

De nieuwe R3 applicaties zoals Corda zijn in wezen wel gedistribueerde digitale grootboeken, maar strikt genomen geen "blockchain".

De karakteristieken Validiteit en Onveranderlijkheid maken de Bitcoin Blockchain interessant om daar bijvoorbeeld notariële of kadastrale diensten aan te koppelen. In het Bitcoin protocol is een aantal records dat daarvoor niet is ontworpen, maar voor deze doelen kan worden gebruikt. Dit zeer tot ontzetting van enige Bitcoin gebruikers, die aan deze praktijk refereren als "bloating" (opblazen van Bitcoin).

Het Bitcoin protocol is door Satoshi Nakamoto bedoeld om peer2peer transacties te ondersteunen en daartoe strikt beperkt gehouden.[8] In het Bitcoin protocol is bewust geen programmeertaal opgenomen om te voorkomen dat anderen "logische bommen" in de software zouden kunnen introduceren en daarmee het systeem zouden kunnen opblazen.

Deze beperking weerhoudt anderen er niet van om applicaties aan te bieden die boven op de Bitcoin blockchain worden gebouwd en waarmee andere diensten kunnen worden uitgevoerd. Een bekende speler is Factom. Factom biedt aan Bitcoin gekoppelde en parallelle applicaties aan waarmee o.a. notariële en kadastrale registraties kunnen worden vastgelegd.

Blockchain 2.0: Ethereum – the world computer

Geheel los van Bitcoin heeft Vitalik Buterin, een Canadees van Russische afkomst, met hulp van de Nederlander Jeffrey Wilcke en de Engelsman Gavin Wood Ethereum bedacht en opgezet.

Anders dan Bitcoin is Ethereum niet bedoeld om alleen transacties uit te voeren. Ethereum gaat door waar Bitcoin ophoudt. Anders dan Bitcoin kent Ethereum wel een programmeertaal waarin zogenaamde "smart contracts" geprogrammeerd en uitgevoerd kunnen worden.

De term "smart contracts" is afkomstig van Nick Szabo.[9] Met "smart contracts" worden overeenkomsten bedoeld die zowel door een computer als mens te lezen zijn. Het oervoorbeeld is volgens Nick Szabo de cola automaat. Deze machine kan een koopovereenkomst sluiten en effectueren.

Door deze nieuwe functionaliteit voegt Ethereum nog nieuwe karakteristieken toe aan die van de Bitcoin blockchain:

- Zelfstandigheid – personen hebben accounts in Ethereum, maar contracten staan op zich zelf en hebben gelijke status (ergo ook zaken, goederen kunnen contracten aanmaken) ("contracts are autonomous agents").
- Transparantie – de code van smart contracts is transparant, voor iedereen in te zien en te (her) gebruiken.

In de Ethereum whitepaper wordt al aangegeven waar de ontwerpers de toepassingen voor hun world computer zien:

- Financiële applicaties. Overeenkomsten waar geld een zwaarwegende rol speelt. Denk aan derivaten, hedge contracten, testamenten, arbeidscontracten.
- Semi-financiële applicaties. Die overeenkomsten waar geld een rol speelt, maar er ook een niet-financiële component is. Bijvoorbeeld vergoedingen voor aangenomen werk (oplossen van computer problemen).
- Niet-financiële applicaties. Overheidsdiensten.
- Verzekeringen. Denk aan volledig geautomatiseerde "crop insurance".
- DAO. Afkorting van het Engelse Decentralized Autonomous Organization. Ook wel DAC, Decentralized Autonomous Corporation. In de algoritmes ligt besloten wie welke aandelen en rechten heeft om te stemmen. Ook het stemproces kan in Ethereum worden ingeregeld. Voor de toekomstige wijze van besturen is ook een naam bedacht "futarchy".
- Prediction markets. Het gedecentraliseerd voorspellen van toekomstige gebeurtenissen zoals bijvoorbeeld verkiezings- en sportuitslagen.

Hoewel de techniek van Ethereum zeker nog niet is uitontwikkeld, groeit het aantal startups dat op basis van dit open source platform applicaties maakt enorm.

De techniek staat nog behoorlijk in de kinderschoenen. De eerste release Frontier van Ethereum was nog niet "secure" wat nogal lastig is voor financiële applicaties. De begin 2016 uitgebrachte release met de naam "Homestead" is vooral bedoeld voor technici en niet geschikt voor het grote publiek. De daarop volgende geplande release met de naam "Metropolis" is bedoeld voor de massa. Ook mensen zonder software ontwikkelingsachtergrond zullen met deze release aan de slag kunnen.

In de laatste nu geplande release met de naam "Serenity" zal de overstap gemaakt worden van Proof of Work naar Proof of Stake. Hoe dat gaat gebeuren weet men nog niet, maar de community is optimistisch dat er een oplossing wordt gevonden die Ethereum snel maakt (vergelijkbaar met Visa en Mastercard) en open houdt voor iedereen die zijn

computer capaciteit wil inzetten om de blockchain uit te breiden.

Dat Ethereum potentie heeft, mag blijken uit het feit dat Microsoft een samenwerkingsverband met de Ethereum community is aangegaan.

Dat de Decentralized Autonomous Organzation op basis van Ethereum geen hersenspinsel is weten we sinds mei 2016 met de oprichting van de DAOhub. Deze DAO heeft – via gedecentraliseerde crowdfunding – naar verluidt het equivalent van meer dan 130 miljoen dollar opgehaald.

Relevantie voor beleggers

Het disruptieve karakter van de nieuwe technologie voor met name administratieve processen in financiële en overheidsorganisaties maakt dat beleggers de essentie van de technologie goed dienen te begrijpen en de verdere ontwikkeling van de technologie en de belangrijke spelers kritisch moeten volgen.

De blockchain technologie wordt door de financiële industrie volledig omarmd. Men kan zich afvragen of dit omarmen niet uitmondt in een smoren van de technologie en initiatieven die tot doel hebben financiële transacties zonder centrale autoriteit mogelijk te maken.

De financiële industrie vindt in de gesloten (private) blockchain technologie met het gedistribueerde digitale grootboek en cryptografische beveiliging voldoende voordelen om daarmee voor het eigen domein applicaties te ontwikkelen.

Een voorbeeld: Barclays bouwt in Corda van het R3 consortium derivaten in de vorm van smart contracts opgeslagen in een blockchain. In april 2016 werd een eerste test publiek gemaakt. De overeenkomsten tussen de partijen zijn gevat in een smart contract en met de wettelijk vereiste bijlagen opgeslagen in de (gesloten) blockchain. Voordeel voor de betrokken partijen is dat er consensus is over de overeenkomst, over de wijzigingen op het contract en over de wettelijke bijlagen. De blockchain geeft de toezichthouders de mogelijkheid de transactie direct te monitoren.

Conclusie

De blockchain zal hoe dan ook direct of indirect gevolgen hebben voor de beleggingsprofessional. Direct door de applicaties die zij gebruiken. Deze zullen wellicht niet als blockchain kunnen worden geduid maar meer en meer op cryptografische digitale grootboeken en smart contracts gebaseerd zijn, zodat vertrouwen tussen betrokken partijen en toezichthouders kan worden bereikt en kosten van de transacties kunnen worden gereduceerd.

Indirect via de beleggingsobjecten wanneer deze zich bevinden in de financiële sector of aan de overheid gerelateerde sectoren. Serieuze, of zelfs disruptieve veranderingen in de administratieve procesgang zullen op handen zijn.

Ook in de eigen administratieve procesgang van custody liggen veranderingen in het verschiet. Goldman Sachs zal zijn vorig jaar ingediende patentaanvraag op het gebied van security settlement ongetwijfeld willen verzilveren. Beleggers die geen klant willen worden van Goldman Sachs of een aangesloten instelling, kunnen overwegen zelf een Decentralized Autonomous Organization van beleggers op te zetten. De broncode van Ethereum is daartoe in ieder geval vrij beschikbaar.

Noten

1 Mr. Egbert M. van de Coevering Directeur van TM7 – Carp Technologies en XuRuX, een startup gespecialiseerd in blockchain technologie.
2 De samenvatting van de Goldman Sachs patentaanvraag: US Patent & Trademark Office onder nr: 20150332395
3 Satoshi Nakamoto – Bitcoin a Peer-to-Peer Electronic Cash System
4 Omdat er kennelijk behoefte bestaat aan werkelijk anonieme cryptocurrencies komen partijen als Monero en Dash (voorheen Darkcoin) met constructies die het technisch lastig maken de eigenaar "zonder enige twijfel" te traceren.
5 Onlangs claimde de Australische ondernemer Graig Wright dat hij Satoshi Nakamoto is. Hierover bestaat grondige scepsis binnen de Bitcoin community. Er zijn onderzoekers die menen aan de hand van de volgordelijkheid van publicaties over cryptocurrencies en smart contracts dat niet Craig Wright maar Nick Szabo Satoshi Nakomoto is.
6 Het aan derde partijen in bewaring geven van privte keys houdt een risico in. Als voorbeeld geldt de hack van Mount Gox waarbij door hackers de private sleutels van de aangeslotenen werden gestolen.
7 De website http://mapofcoins.com/ is tot september 2015 bijgewerkt. De site geeft weer welke stortvloed van copycats van bitcoin in een korte periode zijn ontstaan.
8 Andreas Antonoupoulos Mastering Bitcoin Unlocking Digital Cryptocurrencies
9 http://szabo.best.vwh.net/smart_contracts_2.html