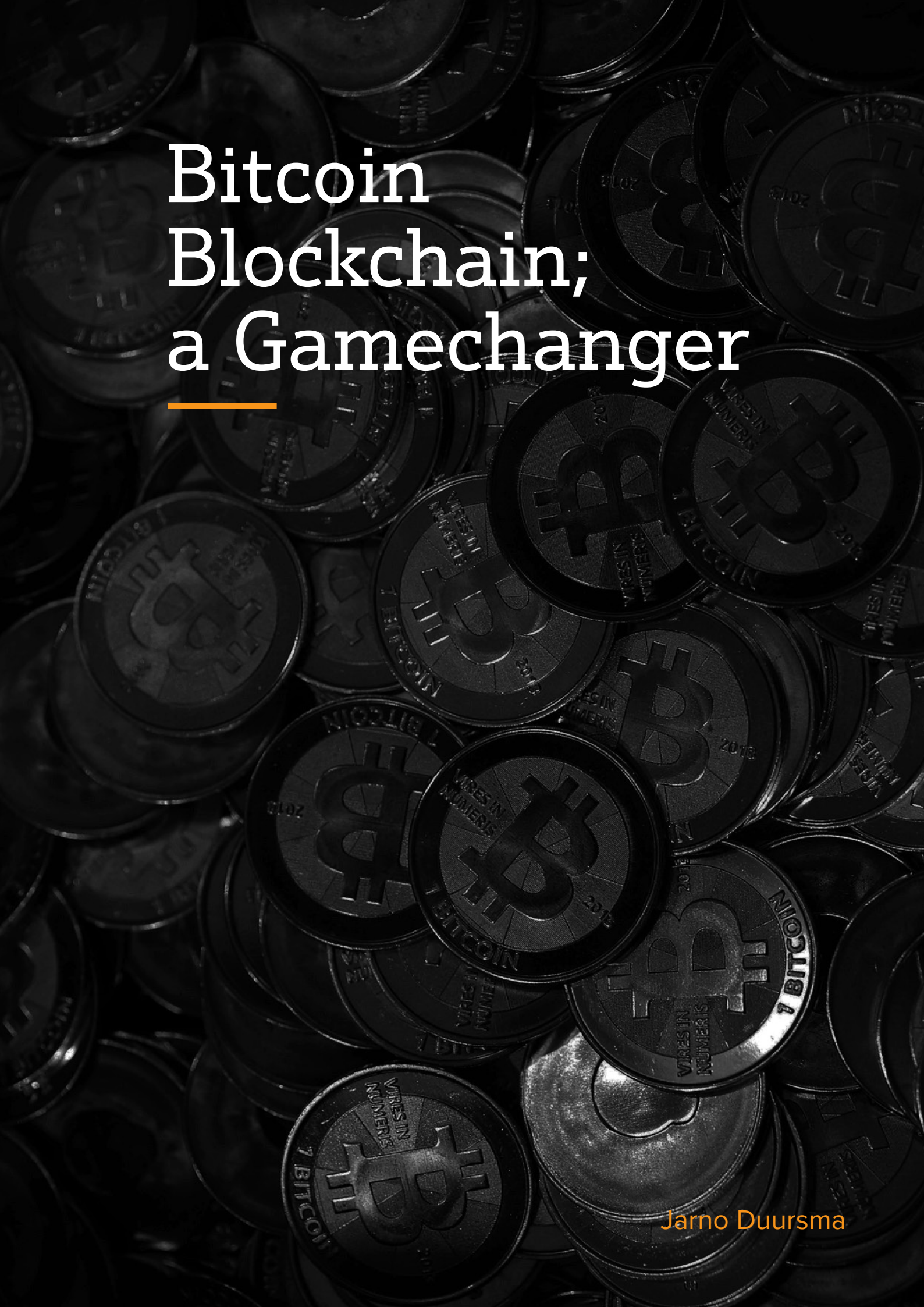
# Bitcoin Blockchain; a Gamechanger




Jarno Duursma

*“The blockchain protocol threatens to disintermediate almost every process in financial services.”*

*- The World Economic Forum*

*“But the real innovation is the blockchain itself, a protocol that allows for secure, direct (without a middleman), digital transfers of value and assets (think money, contracts, stocks, IP). Investors like Marc Andreesen have poured tens of millions into the development and believe this is as important of an opportunity as the creation of the Internet itself.”*

*- Peter Diamandis, Futurist and the author of “Abundance”*

*“The Disruptive Potential of Bitcoin and blockchain: “blockchain promises to be as disruptive a technology as the internet.”*

# Inhoudsopgave

# Inleiding

Halverwege 2014 ben ik begonnen met het schrijven van een boek over digitale trends, waaronder kunstmatige intelligentie, internet of things, de circulaire economie en ook Bitcoin blockchain. Hoewel ik al vergevorderd was, is het boek nooit voltooid. Andere zaken vroegen mijn aandacht en met een dergelijk boek word je al snel op alle vlakken ingehaald door de actualiteit. Toch heb ik besloten van het onderwerp bitcoin blockchain een aparte uitgave te maken. Dat rapport ligt nu voor je.

Het is namelijk een technologie die heel veel impact gaat hebben en heel vernieuwend is. Het is alsof het gehele kaartenspel van technologieën en protocollen wordt uitbreid met een extra onderdeel: niet alleen harten, klaveren, schoppen en ruiten, maar een compleet nieuwe kleur. Vanuit deze fascinerende constatering en mijn eigen enthousiasme heb ik dit rapport geschreven.

En dat deze nieuwe technologie serieus voet aan de grond krijgt bewijst een initiatief in Estland. via Bitnation is het mogelijk voor (virtuele) bewoners van dit land om hun huwelijksakte, geboortecertificaten, zakelijke contracten in de blockchain notarieel te bekrachtigen. En dat niet alleen; vorig jaar werd de mijlpaal bereikt van een totaal van $1 miljard aan investeringen in bitcoin bedrijven.

In dit rapport staat meer informatie over bitcoin, de blockchain en voorbeelden van toepassingen. Eerst zal ik iets uitleggen over Bitcoin en over de meerwaarde van deze digitale munt. Daarna wordt uitgebreid stilstaan bij de blockchaintechnologie. Ik maak daarbij de verdeling in slim eigendom, slimme contracten en slimme dingen. Tot slot komen ook nog de beperkingen van deze kersverse technologie aan de orde.

Een voetnoot aan alle bitcoin programmeurs en hardcore experts: een aantal processen en beschrijvingen heb ik versimpeld om dit rapport niet te technisch te maken en tevens begrijpelijk te houden. Zo breng ik voor de versimpeling in dit rapport soms bijvoorbeeld een verschil aan tussen bitcoin en blockchain. Wanneer ik schrijf over bitcoin gaat het veelal over de digitale munt en wanneer ik schrijf over blockchain gaat het veelal over de technologie van aan elkaar gekoppelde blocks die in een globaal gedistribueerd grootboek een ‘single source of truth’ vormen.

Er zijn, ook onder de mensen die er verstand van hebben, vele verschillende visies en er is vaak verschil van inzicht. Niet alleen over wat bitcoin is en zou moeten zijn, maar ook over de manier waarop technische processen ingezet zouden moeten of kunnen worden. De blogs die elkaar inhoudelijk tegenspreken op dit vlak zijn niet meer bij te houden.

Mijn doel is dan ook om licht te laten schijnen op de technologie en de impact ervan. Tegelijkertijd begrijpelijk voor iedereen, zonder te vervallen in technische verhandelingen en zonder tekort te doen aan de inhoud.

Heb je vragen, opmerkingen of aanvullingen? Laat het me horen.
Veel leesplezier!

met hartelijke groet,

Jarno Duursma
Trendverkenner

Twitter: *@jarnoduursma*
E-mail: *info@jarnoduursma.nl*
Web: *http://www.jarnoduursma.nl/blockchain*

# 1. Bitcoin

## 1.1 Wat is bitcoin?

Bitcoin is een open source en peer-to-peer systeem voor transacties. Een nieuwe vorm van transactietechnologie. Het werd in 2009 door Satoshi Nakamoto uitgelegd in een openbaar document. ‘Open source’ wil zeggen dat de broncode openbaar is, dus het staat iedereen vrij de software te gebruiken en ontwikkelen. Bekende voorbeelden van andere open source software zijn Wordpress, Linux, MySQL en OpenOffice. Peer-to-peer wil zeggen dat computers onderling contact met elkaar hebben, zonder tussenkomst van derden.

Bijzonder is dat Bitcoin de eerste vorm van decentrale digitale valuta is. Decentraal betekent in dit geval dat men onderling direct transacties kan uitvoeren zonder tussenpersoon of andere partij, zoals een bank.

De bitcoin als munt om betalingen mee te doen is veelvuldig in het nieuws geweest. Dat is niet alleen vanwege de fluctuaties van de koers, maar ook vanwege excessen als witwassen, failliete wisselkantoren en het gebruik als betaalmiddel bij criminele activiteiten. De media zetten bitcoin daarbij geregeld weg als het betaalmiddel van de onderwereld, maar niks is minder waar, zoals hieronder zal blijken.


De koers van bitcoin is in de afgelopen jaren van een paar cent gestegen tot boven de $1000 in 2013. Nieuwsbronnen spraken al snel over bitcoin-miljonairs: jongens (soms meisjes) die ooit voor een habbekrats bitcoins kochten en nu door de waardestijging miljonair waren geworden. De koers is daarna een paar keer flink gedaald en schommelt nu tussen de 300 en 450 dollar.

Ooit is bitcoin begonnen als een project van 20 programmeurs die in hun vrije tijd aan deze techniek werkten. Als je dat bedenkt, zie je dat het bijzonder is dat er op dit moment ongeveer 120.000 transacties per dag mee worden verwerkt. De echte meerwaarde van bitcoin is door alle negatieve berichten in de media onderbelicht gebleven, helaas.

Bitcoin wordt overigens soms met en soms zonder hoofdletter geschreven. Wanneer er een hoofdletter gebruikt wordt, gaat het meestal over het gehele netwerk van Bitcoin of Bitcoin als concept. Bij een kleine letter gaat het doorgaans om de valuta, de munt.

## 1.2 Bitcoin als betaalmiddel

Bitcoin begint als betaalmiddel beetje bij beetje serieuze vormen aan te nemen. Tegenwoordig zijn er bijvoorbeeld al meerdere bedrijven en organisaties, waar je kunt betalen (of doneren) met bitcoin. Voorbeelden in Nederland zijn thuisbezorgd.nl, onlinedrogist.nl, de Piratenpartij en Voys telecom. In het buitenland wordt bitcoin geaccepteerd door onder meer Wikipedia, Wordpress, Apple App Store, Tesla, Amazon, Victoria's Secret, Zynga, Expedia, Dell, Microsoft en Overstock. Deze partijen wisselen aan de achterkant de ontvangen bitcoins direct om in euro's en dollars. Toch is het een duidelijk signaal dat bitcoin steeds serieuzer wordt genomen en zich naar mainstream verplaatst. Duitsland heeft de digitale munteenheid zelfs als officiële valuta erkend, als eerste land ter wereld.

Om bitcoin uit te leggen is het goed eens te kijken naar wat geld eigenlijk is. Zoals we weten sinds de huizen-, krediet-, banken- en andere financiële crises sinds 2008, is geld niks anders dan vertrouwen. Geld is een middel waarvoor we hebben afgesproken wat het waard is. Verder willen we garanties dat die waarde intact blijft en inwisselbaar is. Geld is dus een middel dat vertrouwen uitdrukt. Niet meer en niet minder. Je kunt dus ook prima je eigen 'geld' maken, zoals onderstaand voorbeeld in Brazilië laat zien.

### *Zelf geld creëren*

*Een Braziliaanse sloppenwijk kampte met twee grote problemen. Er was enorm veel zwerfafval en er was een zeer hoge werkloosheid. Bewoners die naar de stad wilde reizen om daar werk te zoeken, konden de bus echter niet betalen. Lokale bestuurders probeerden jarenlang vergeefs een budget los te peuteren bij de centrale overheid. Toen besloot men dan maar zélf geld te maken: blauwe plastic muntjes. Wie een vuilniszak vol zwerfafval inleverde, kreeg als beloning een muntje. Met dat muntje kon men een busrit naar de stad betalen om werk te zoeken. Zo'n systeem kan functioneren zolang de gebruikers erop vertrouwen dat de buschauffeur het blauwe muntje accepteert als betaalmiddel.*

Net als in dit voorbeeld heeft Bitcoin waarde omdat wij die eraan toekennen, zoals het geval is bij iedere vorm van geld. Het vertegenwoordigt een bepaalde waarde. Met als gevolg dat je er in de reële wereld spullen, diensten of contant geld voor terug kunt krijgen.

## 1.3 Voordelen

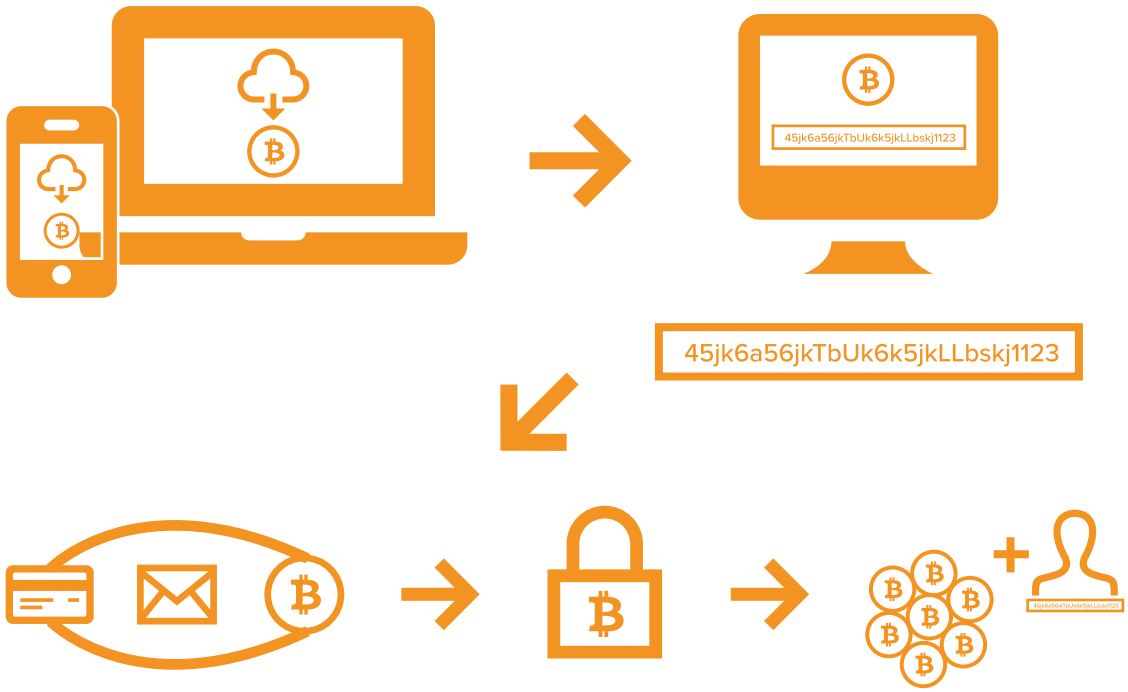
Bitcoin is anders dan andere betaalmiddelen, hoeveel parallellen er ook zijn. Het grootste verschil als betaalmiddel is de soevereiniteit; dat het zonder overheid, bank en centrale regulering plaatsvindt. Er zijn geen tussenpersonen nodig om een transactie te versturen, te ontvangen of af te ronden. Je betaalt namelijk rechtstreeks aan de ontvangende partij middels een persoonlijke code. Het maakt niet uit of de ontvangende partij een webshop-eigenaar, een ´reguliere´ winkelier of je grootmoeder is. Wat dat betreft is het te vergelijken met een transactie in contant geld: ook hier zijn immers geen tussenpersonen (zoals banken) nodig om de transactie uit te voeren. Bitcoin maakt bankloos betalen mogelijk.

Een ander verschil met veel andere betaalmiddelen is dat Bitcoin geen materiële variant heeft (zoals munten, bankbiljetten of andere waardepapieren). Het is enkel een vorm van elektronisch geld en bestaat dus alleen digitaal, als bits & bytes.

Dat maakt het gebruik van bitcoin als betaalmiddel grote voordelen heeft. Het eerste voordeel is natuurlijk dat je direct van persoon tot persoon (ook heel grote) betalingen kunt doen, zonder tussenkomst van een bank of een centrale organisatie. Je regelt het onderling.

Het tweede voordeel is dat de kosten van het gebruik van bitcoin bijzonder laag zijn. Je hoeft immers geen banksysteem (medewerkers, overhead en dividend) mee te financieren. Tevens is het makkelijk dat je bitcoin internationaal kunt gebruiken. Er zijn geen landsgrenzen die het gebruik in de weg staan. En betalen via bitcoin gaat snel en het bijbehorende betalingsverkeer wordt niet belemmerd door contracten met kleine lettertjes, graaibonussen of woekerpolissen.

Nadeel van de bitcoin als betaalmiddel is wel dat er nog veel fluctuaties in prijs zijn. In dezelfde week kan er $200,- prijsverschil zitten in een bitcoin. En dat is onwenselijk.

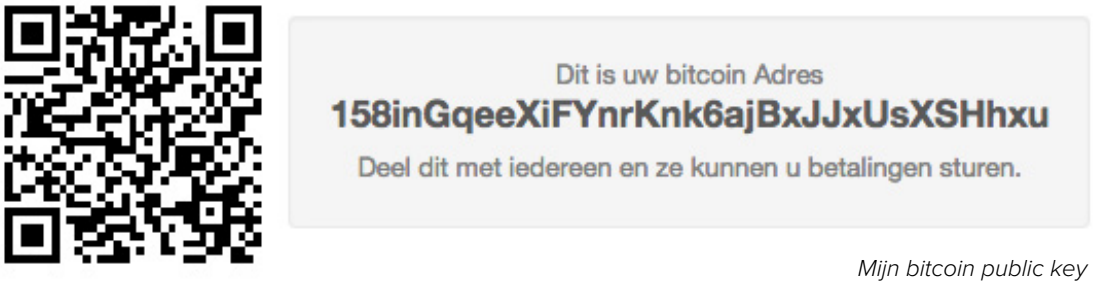


## 1.4 Transacties met bitcoin

Zoals gezegd is het systeem van Bitcoin gebouwd op een open source platform.
Iedereen kan het protocol, de zogeheten code, van Bitcoin gebruiken om verschillende toepassingen op te bouwen.

Bovendien is Bitcoin decentraal geregeld. Er is dus geen bank, overheidsinstelling of commerciële onderneming die de onderlinge transacties reguleert. Het verwerken van de transacties en het creëren van nieuwe valuta, bitcoins, gebeurt door de gebruikers op het netwerk.

Iedereen die gebruik wil maken van Bitcoin, moet daarvoor een persoonlijke, digitale portemonnee hebben, de zogeheten wallet. Deze portemonnee kun je online onderbrengen bij een externe partij, maar ook op je eigen computer plaatsen. Aan de wallet zijn twee ‘keys’ verbonden: een ‘private key’ en een ‘public key’. Je ‘private key’ geeft toegang tot je bitcoins. Je ‘public key’ is een code waarmee je je bitcoin-transacties doet.

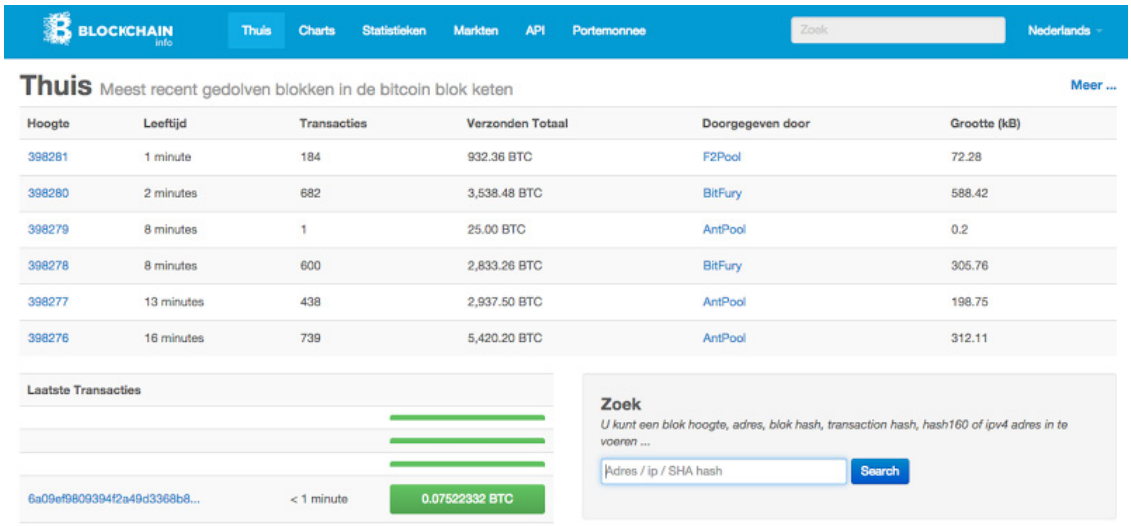



*Mijn bitcoin public key*

De vergelijking met een e-mailadres is misschien het makkelijkst. Je e-mailadres kan openbaar zijn en iedereen kan er mailtjes naartoe sturen. Maar de enige die de mailtjes kan openen is degene die de inloggegevens tot het account heeft.

Zo gaat het ook bij een Bitcoin-transactie. Als je iemand je ‘public key’ geeft, kan deze een betaling naar je sturen vanuit zijn of haar wallet. Maar je kunt dat geld er alleen afhalen als je een ‘handtekening’ (signature) hebt, die wordt aangemaakt door de ‘private key’. Je private key hou je altijd voor jezelf. Als je deze kwijtraakt, heb je geen toegang meer tot je bitcoins. Je leest het: dit is allemaal zo geregeld dat de tussenkomst van een bank niet meer nodig is: Bitcoin maakt bankloos betalen mogelijk.

De bitcointransacties zijn allemaal transparant en inzichtelijk. Ze zijn te bekijken in de blockchain. Via een explorer zoals www.blockchain.info kun je de transacties van een bij jou bekend adres bekijken en volgen. Bij een transactie wordt het pseudoniem van iemands public key gebruikt. Aan deze public key is geen identiteit gekoppeld. Je ziet in de blockchain dus geen naam, adres of bankrekeningnummer.




*Afb: Blockchain.info*

De privacy wordt op die manier gewaarborgd. En het is veilig. De transacties worden namelijk versleuteld middels cryptografie. Dat betekent dat van de transacties tussen de wallets een onleesbare code wordt gemaakt. Bitcoin wordt daarom ook wel cryptocurrency genoemd: valuta versleuteld middels cryptografie.

### *Viral succes: Jamaicaanse bobsleeërs*

*Bitcoin is de meest bekende, maar zeker niet de enige vorm van digitale valuta. Er zijn ook andere cryptocurrencies, zoals Litecoin, Gulden en Dogecoin. Deze laatstgenoemde digitale munt kwam in de publiciteit toen het werd gebruikt om het Jamaicaanse bobsleeteam te voorzien van de financiële middelen om naar de winterspelen van 2014 in Sotsji te gaan. Deze actie ging door een samenspel van factoren snel viral en binnen een paar uur werd er meer dan 26 miljoen Dogecoin, goed voor in totaal 30.000 dollar, geschonken.*

Een ander leuk voorbeeld is een student die tijdens het TV programma “College Gameday” een spandoek omhoog hield met de tekst “Hi Mom send Bitcoin” met een afbeelding van zijn publieke Bitcoin adres verpakt in een QR code. De foto van het spandoek met de QR code  ging viraal en leverde de student binnen een week $24.000 dollar op aan donaties van bitcoin fans.

## 1.5 Toekomst van bitcoin als betaalmiddel

Gaat de bitcoin de euro vervangen binnen nu en tien jaar? Het antwoord is nee. Bitcoin als vervangend alternatief is op dit moment nog niet zo relevant; en we zijn in Nederland gewend aan een heel hoog service niveau als het gaat om het doen van financiele transacties. En hoewel in Nederland het bitcoin-gebruik per hoofd van de bevolking het hoogste ter wereld is, zijn de bitcoin-transacties in Nederland in absolute zin nog niet zo groot, minder dan duizend per dag. Dat steekt schril af tegen de ruim 16 miljoen euro-betalingen die er dagelijks plaatsvinden. Zelfs marktpartijen die nu bitcoins accepteren, maken zogezegd vrijwel allemaal gebruik van een ‘payment services provider’ die de bitcoins meteen weer omzetten in euro’s of dollars.

Ook is de koers van bitcoin nog te gevoelig voor nieuws uit de media en staat hij nog sterk onder invloed van speculatie. En er is een kleine kans dat een slecht beveiligde online-wallet-dienst gehackt wordt of failliet gaat.

Dan kun je over het algemeen fluiten naar je geld, wanneer je ze niet offline of op je eigen computer hebt bewaard. Bitcoin als betalingssysteem zal de komende jaren in Nederland dus niet significant een rol spelen als vervanger van de euro.

Toch kan juist de functie van betaalmiddel voor gebruikers ook in andere landen interessant zijn. Er zijn op dit moment zeven miljard mensen op de wereld, van wie er zes miljard geen bankrekening hebben, zoals in Azië en Afrika. Deze mensen beschikken wel over geld, maar hebben geen rekening of creditcard om financiële transacties uit te voeren. Wanneer zij met bitcoin zouden betalen, kan het als betaalmiddel snel groot worden en daardoor - voor wie het wil weten - in waarde stijgen.

Een voordeel voor gebruikers uit deze landen zou zijn dat bij Bitcoin de transactiekosten zeer laag zijn. Terwijl de transactiekosten bij bijvoorbeeld Western Union juist vaak erg hoog zijn voor het internationaal overmaken van geld. Bovendien gebeurt het overmaken bij Bitcoin relatief snel. Het is mogelijk dat er in die continenten fysieke loketten komen waar je contant geld om kunt laten zetten naar een digitale valuta zoals Bitcoin, zodat je vanaf je eigen computer of smartphone heel snel en heel goedkoop internationale betalingen of overschrijvingen kunt doen. Want, zoals gezegd; niet iedereen heeft een betaalrekening om bitcoins mee te kopen.

# 2. Blockchain

*Bitcoin zou ondenkbaar zijn zonder de techniek van blockchain, waarop dit hoofdstuk nader ingaat. De blockchain wordt een van de beste uitvindingen genoemd sinds de uitvinding van het internet zelf. De techniek is enorm innovatief en heeft alle potentie om de toekomst te veranderen.*

## 2.1 Wat is blockchain?

De blockchain is een globaal, decentraal gedistribueerd grootboek waarbij vele duizenden computers wereldwijd werken aan de verwerking van transacties. Over de inhoud van het grootboek hebben ze ondubbelzinnig overeenstemming. Ze bezitten allemaal een eigen en identieke kopie van het grootboek. In het wereldwijd gezamenlijk gedistribueerde grootboek worden alle transacties bijgehouden, zodat iedereen weet wat van wie is. Je kunt dus zo een wereldwijde decentrale database van bezittingen maken.

Dankzij deze techniek kunnen wij onderling (decentraal) alles wat digitaal is snel, veilig, waterdicht en ondubbelzinnig van eigendom laten wisselen. We hebben dus geen partijen meer nodig die ons het vertrouwen van de transactie garanderen; de ‘trusted third party’ is overbodig.

Wat nu bijvoorbeeld de bank, het kadaster, het RDW, de notaris en KvK doen, kan worden overgenomen door deze nieuwe open source techniek. En de snelheid waarmee bedrijven formeel contracten met elkaar kunnen sluiten, kan dan enorm versnellen. Door de blockchain is het net alsof er bij iedere transactie die je doet een (virtuele) notaris aanwezig is.

## 2.2 Bitcoin Blockchain Technologie

Hoe gaat dit in z'n werk? Tijd om even onder de motorkap te kijken.
De blockchain bestaat uit blocks (zoals de naam al aangeeft). Wanneer er een bitcoin-betaling plaatsvindt van de ene partij naar de andere, via een smartphone of website, wordt deze betaling samen met andere vastgehouden. Bij een bepaalde hoeveelheid transacties wordt er een block van transacties gevormd. Middels cryptografische berekeningen bevestigt elk block in de keten de validiteit van de vorige block. Zo ontstaat er een waterdichte keten van geaccepteerde blokken, die in geen andere volgorde waar kan zijn.
Daardoor wordt het onmogelijk om vastgelegde transacties achteraf aan te passen.

De blockchain is een transactiedatabase. Het staat geregistreerd op duizenden computers en kan door iedereen wordt geraadpleegd. Ieder computer in het netwerk (een node) heeft een eigen kopie van de blockchain. Alle transacties van de virtuele valuta bitcoin staan er dus in. De nodes delen onderling de nieuwste transacties met elkaar. Ze houden hun eigen kopie van de blockchain up-to-date en verspreiden de wijzigingen onder elkaar.
En omdat iedere node gelijktijdig in bezit is van het hetzelfde gehele grootboek, is rommelen met de blockchain onmogelijk. Het is een 'single source of truth'.

*"Wat in de blockchain geregistreerd staat is onweerlegbaar, onomkeerbaar en ondubbelzinnig waar."*

*- Lykle de Vries*

De blockchain registreert dus alle transacties tussen personen en bedrijven (of, om het in technische termen zeggen: tussen de verschillende versleutelde adressen). Transacties gaan in principe van de ene wallet naar de andere. Welke bitcoins en transacties bij welke wallets horen, wordt door alle computerknooppunten (nodes) in het netwerk geregistreerd.

‘Elke node in het netwerk bewaart zijn eigen kopie van de blockchain. Zo wordt de eigendom van elke afzonderlijke bitcoin in de loop der tijd steeds en onafhankelijk geverificeerd. Ongeveer zes keer per uur wordt een block, een nieuwe groep van geaccepteerde transacties, gecreëerd en toegevoegd aan de blockchain. Dat wordt direct gepubliceerd aan alle andere nodes. Dat stelt de bitcoin software in staat te bepalen wanneer een bepaald bedrag aan bitcoins is uitgegeven. Dat is nodig om te voorkomen dat dezelfde bitcoin twee keer wordt uitgegeven in een omgeving zonder centraal toezicht.’ (Wikipedia)

## 2.3 Mining

Wanneer je een transactie hebt gedaan via het bitcoin-netwerk, moet je heel even wachten totdat jouw transactie is gecontroleerd en geverifieerd door de zogenaamde ‘miners’. Een miner is dus een computer met veel rekenkracht. Maar het kan ook een netwerk van computers zijn die daar samen over beschikken.

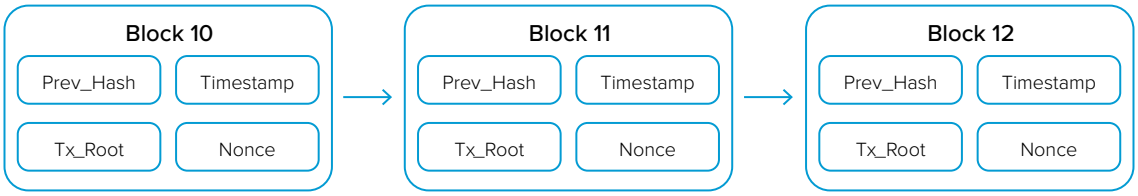
Je kunt een transactie hogere prioriteit geven door een ‘transaction fee’ eraan mee te geven. Dat betekent dat je bereid bent voor de transactie een kleine vergoeding te betalen aan de miners. Dat maakt dat de transaction fee een stimulans en de bitcoin-gebruiker heeft meer zekerheid dat een bepaalde transactie wordt opgenomen in het volgende block.

Voordat een blok geaccepteerd kan worden moeten miners met elkaar in competitie om een verificatiegetal uit te rekenen.

De moeilijkheid van het verificatiegetal wordt door het algoritme aangepast zodat er ongeveer iedere 10 minuten een nieuwe blok gegenereerd wordt.

Omdat er onweerlegbaar een bepaalde mate van rekenkracht nodig is om tot de oplossing van het verificatiegetal te komen noemen ze het bewijs van het beschikbaar stellen van rekenkracht ook wel ‘proof of work’. De rekenkracht van de miners is dus het kloppende hart van de blockchain technologie.
Een proof of work uitvoeren is computertechnisch een intensief en grillig proces van trial and error voordat het verificatiegetal wordt gevonden. Daardoor is het onvoorspelbaar welke miner het block mag toevoegen.

De miner die de proof of work puzzel oplost wordt door het algoritme beloond met nieuwe bitcoins (de ‘block-reward’) en de ‘transaction fees’ van alle bitcoin-transacties die op het block geplaatst worden. De beloning voor de miner van het beschikbaar stellen van zijn (dure) rekenkracht zijn dus bitcoins.



De blockchain lijkt op een schakelketting waar steeds nieuwe schakels aan worden toegevoegd. Blocks zijn aan elkaar gelinkt. Een block bevat namelijk altijd een verwijzing naar het vorige block. Middels cryptografische berekeningen bevestigt elk blok in de keten de validiteit van de vorige block. Daarom wordt bitcoin ook wel een consensusnetwerk genoemd. Zo ontstaat er een keten van geaccepteerde blokken, die in geen andere volgorde waar kan zijn. Op deze wijze wordt het onmogelijk om vastgelegde transacties achteraf aan te passen.

Om fraude te kunnen plegen en een foute transactie te kunnen toevoegen, moet je dus een supercomputer hebben die meer dan 51% van de rekenkracht bezit om een malafide blok toe te kunnen voegen. Maar dat is vrijwel onmogelijk; Op dit moment is het vermogen van het volledige Bitcoin-netwerk te vergelijken met 300 tot 400 maal de gecombineerde kracht van de top 500 supercomputers van de wereld. Daar kun je dus niet tegenop.

### Verificatie

De miner heeft in principe twee functies. Allereerst verwerkt en verifieert de miner alle voorgaande transacties binnen het netwerk. De miners verifiëren samen alle transacties, verpakt in de blocks. Daarmee zijn de miners een cruciaal onderdeel van het netwerk; ze zijn het kloppende hart van de blockchain technologie.

## Bitcoins maken

De tweede functie van het systeem van miners is dat ze nieuwe bitcoins genereren. De miner die de proof of work als eerste afrondt en de de transactie mag bijschrijven in de blockchain, krijgt immers nieuwe bitcoins.

Tevens deelt de miner zijn ontdekking met de andere miners, zodat het grootboek gesynchroniseerd kan worden. Nodes checken de validiteit; iedere node in het netwerk heeft een exacte kopie van de blockchain. Ze delen de transacties onderling en daarom kan de munt niet worden gekopieerd of twee keer worden uitgegeven. Dat maakt het tot een waterdicht systeem.

*Ter illustratie:* er wordt ongeveer iedere tien tot vijftien minuten een block toegevoegd aan de blockchain. Er komt dan ongeveer 25 bitcoin vrij. Als je dat naar dagwaarde omgerekend met een koers van ongeveer € 380 per bitcoin, is dat ongeveer € 1,4 miljoen per dag.

Het algoritme maakt het wel steeds moeilijker om de de proof of work te voltooien. Het wordt dus ook moeilijker om de beloning van een bepaald aantal bitcoins te verkrijgen. Bovendien worden er steeds minder bitcoins gegeven als beloning voor het minen van een block.

Zo is er in de zomer van 2016 weer een blokhalvering op komst. In theorie kan dat de waarde van een bitcoin ook weer doen laten stijgen. De verhouding tussen vraag en aanbod wordt immers beïnvloed; minder nieuwe bitcoins betekent een hogere prijs.
Het systeem reguleert zo zelf de hoeveelheid bitcoins die binnen een bepaalde tijd worden uitgedeeld. Je hebt als miner steeds meer rekenkracht nodig voor een lagere beloning; miners worden dus steeds meer gedwongen om kostenefficiënt te gaan werken.

Wanneer je het proces op deze manier bekijkt, lijkt het creëren van nieuwe bitcoins op het ophalen van waardevolle metalen uit een digitale mijn. Het kost na verloop van tijd steeds meer energie om nieuwe blocks te verwerken en er is ook steeds meer rekenkracht nodig om de 64-cijferige cryptografische code te kraken. Uiteindelijk neemt het aantal bitcoins dat je als beloning krijgt dus af. Om waardevermindering te voorkomen is er in het systeem vastgelegd dat er uiteindelijk maar 21 miljoen bitcoins zullen worden uitgegeven. Berekend vanuit de gemiddelde snelheid waarmee een block wordt verwerkt en nieuwe bitcoins worden gegenereerd, is 2140 het jaar dat de laatste bitcoins gemined gaan worden.

## Hoe kom je aan bitcoins?

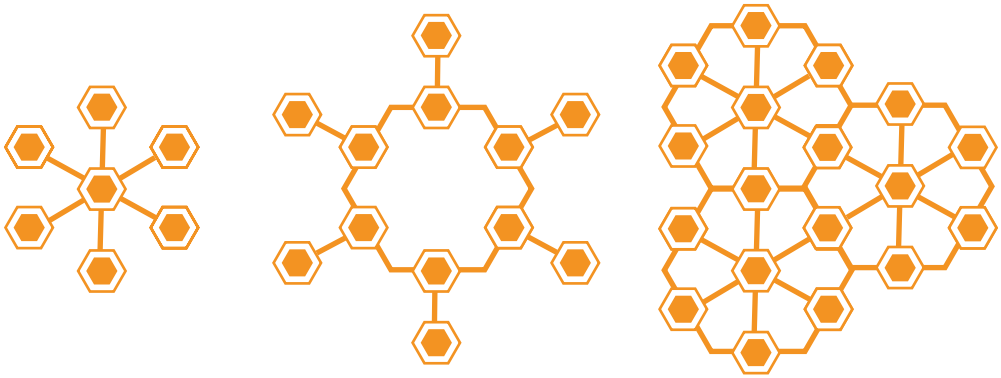
Even voor ‘gold diggers’ in spe: het minen van bitcoins met een huis-tuin-en-keuken-computer is bijzonder moeilijk. Het minen van bitcoins wordt steeds moeilijker. Weliswaar zijn er speciale chips ontwikkeld die erg goed zijn in rekenen en oplossen van die wiskundige sommen en daarnaast relatief weinig energie gebruiken. Met deze zogenaamde ASIC-chips (Application-Specific Integrated Circuit) kun je een eigen ‘bitcoinminer’ bouwen. Maar daar is wel flink wat computerkennis en een stevig budget voor nodig. Daarom wordt dat voornamelijk door professionele bedrijven gedaan. Deze bevinden zich veelal in China en andere delen van de wereld waar de energieprijzen ook aanzienlijk lager liggen dan bijvoorbeeld in Nederland.


*Voorbeeld van een ASIC Chip*

Toch hoef je niet zelf te gaan minen om aan bitcoins te komen. Er zijn bijvoorbeeld diverse bitcoin pinautomaten waar je met contant geld bitcoins kunt kopen. Je kunt ze ook aanschaffen bij een webshop voor bitcoins of rechtstreeks vanaf een beurs zoals Kraken. Een Nederlandse  aanbieder van bitcoins is de website van Bitonic. Lees je eerst wel even goed in voordat je bitcoins gaat kopen.

# 3. Overdracht van eigendom

*Bitcoin als munt heeft een bepaalde meerwaarde, maar het is vooral interessant wanneer het gaat om de blockchain, de onderliggende technologie. De blockchain is een openbaar register van transacties en eigendom. Het is een slimme vorm van transactietechnologie, uitermate geschikt voor het ondubbelzinnig overdragen van eigendomsrechten. Bitcoin als systeem zou je dus een "globally distributed asset register" kunnen noemen: een wereldwijd eigendomsregister. Een transactiedatabase met een 'single source of truth'.*



Centralised Decentralised Distributed

## 3.1 Grootboekfunctie

De blockchain een globaal, decentraal gedistribueerd grootboek waarbij vele duizenden computers wereldwijd werken aan de verwerking van transacties. Over de inhoud van het grootboek hebben ze ondubbelzinnig overeenstemming. Ze bezitten allemaal een eigen en identieke kopie van het grootboek.

In het wereldwijd gezamenlijk gedistribueerde grootboek worden alle transacties bijgehouden en zo weet iedereen wat van wie is. Je kunt dus een wereldwijde decentrale database van bezittingen maken.

Technisch beschouwd is de blockchain een platform van complexe algoritmes dat transacties van digitale producten op een veilige, transparante en betrouwbare manier mogelijk maakt zonder de tussenkomst van derden. Het is een gedecentraliseerd systeem voor de registratie en de overdracht van al het denkbare eigendom. De techniek zorgt ervoor dat alles wat je in de blockchain plaatst, ondubbelzinnig vastgesteld is. Wat in de blockchain staat is waar.

En je kunt met het Bitcoin protocol en zelf-te-schrijven software dus digitale ‘producten’ op een snelle, betrouwbare, decentrale manier van eigenaar laten wisselen.

Wanneer je met je persoonlijke sleutel een transactie doet, kun je daar dus informatie aan toevoegen, zoals de concrete beschrijving van een bepaald product dat je van eigendom wilt laten wisselen.

Trendwatchers Sander Duivestein en Patrick Savalle schrijven: ‘Dankzij de bitcoin technologie is voor het eerst in de geschiedenis mogelijk om eigendom en eigendomsrechten van digitale activa (zoals aandelen, certificaten, digitaal geld, enzovoorts) over te dragen zonder tussenkomst van centrale instanties zoals de overheid, een notaris, een bank of een verzekeringsmaatschappij. Het netwerk als geheel is de trusted party.’

Dat biedt immense kansen. Overal waar je digitaal eigendom wilt laten veranderen van eigenaar kan de blockchain zijn werk doen.

Registratie van kentekens, rijbewijzen, trouwaktes, diploma’s, vastgoed, eigendomsbewijzen, loyaliteitsprogramma’s, intellectueel eigendom, echtheidscertificaten van kunst en aandelen; het kan allemaal in de blockchain geregistreerd worden. Decentraal en zonder tussenkomst van derden die het geregistreerde normaal gesproken moeten oormerken als “waar”. De waarheid zit in de blockchain. Duizenden computers uit het netwerk hebben immers consensus over wat is vastgesteld. Alsof er bij iedere transactie een notaris meekijkt en de transactie beoordeeld als ‘waar’.

*Afb: PricewaterhouseCoopers*

Vrijwel iedereen die zijn boterham verdient als “onafhankelijke derde partij” (trusted third party) zal in de toekomst te maken krijgen met de Bitcoin blockchain. Accountants en notarissen voorop. En dan gaat het niet alleen over contracten en eigendomsbewijzen. We leven nu in een tijd waarin praktisch alles gedigitaliseerd kan worden. Sterker nog: ieder fysiek product kan in een digitale beschrijving worden gegoten.

*“Met blockchain kunnen we beschrijvingen toevoegen aan iedere transactie en zo vastleggen wat je van eigendom laat veranderen. Je kunt deze eigendommen wiskundig versleutelen en zonder tussenkomst van derden aan elkaar overhandigen. Dan is het ondubbelzinnig van eigenaar verwisselt. Wat op de blockchain staat is waar en daar kun je niet aan tornen”*

*- Roel Boer, Nocks*

Wanneer je de ‘overschrijving’ doet van het ene account naar het andere, voeg je daar dus tevens een beschrijving aan toe van het digitale (of gedigitaliseerde) product.
Zo verplaats je via de blockchain de eigendom en weet iedereen wat van eigenaar verwisselt.

In het kort: het geheel van API- en bitcoin-protocol bij elkaar betekent dat er nu een digitaal peer-to-peer verificatiesysteem is, waarop je allerlei digitale toepassingen kunt bouwen. Je kunt behalve technische features bijvoorbeeld uitgebreide informatie toevoegen aan de transactie, waarna het syteem zorgt voor een waterdichte verificatie. Dankzij blockchain kun je digitaal (of gedigitaliseerd) eigendom ondubbelzinnig, snel, veilig en decentraal van eigenaar doen veranderen.

Wanneer we dit op macroniveau bekijken, zou bijvoorbeeld de publieke registratie van de eigendom van huizen, grond en auto’s in Nederland decentraal geregeld kunnen worden, in zogenaamde ‘decentralised digital asset registers’. Denk eens aan wat de Kamer van Koophandel, het kadaster en de gemeenten doen op het gebied van eigendom en transacties. Dat zou met blockchain dus decentraal geregeld kunnen worden in een bestaand systeem wat op die manier enorm veel kosten kan besparen.

Mensen kunnen het dan immers onderling regelen, waarbij iedere gebruiker op het netwerk een bouwsteen en dus altijd samen tot consensus dient te komen. Er is niet één iemand de baas over het netwerk.

*Afb: Uk Government*

Ook een notaris kan gebruik maken van blockchain. Het zou onderdeel kunnen worden van bepaalde boekhoudsoftware. Alles wat je erin registreert wordt waterdicht vastgelegd. Nu betaal je de notaris voor het opmaken en het laten passeren van een akte. Bij het opmaken worden de aktes op maat gemaakt, naar gelang de wensen van de klant. Dit blijft het werk van de notaris, die dat vaak uitvoert op basis van een persoonlijk gesprek. Het laten passeren van de akte kan plaatsvinden door gebruik te maken van een programma dat geschreven is op basis van het Bitcoin-protocol.

Met een druk op de knop wordt het (versleutelde) document of een registratie daarvan vastgelegd in de blockchain. Ook op het gebied van logistiek zou je je kunnen voorstellen dat het Bitcoin-protocol en -software een registratiefunctie hebben.

## 3.2 Smart contracts

De blockchain maakt het ook mogelijk om aan een transactie vantevoren regels toe te voegen. Dat zijn bijvoorbeeld voorwaarden die je aan een bepaalde transactie stelt, voordat deze geaccordeerd wordt. Dankzij de voorwaarden en de regels die je kunt inprogrammeren in de blockchain, kun je ‘smart contracts’ maken: contracten die ‘self executing’ zijn waar de overeenstemming over voorwaarden vooraf zijn vastgelegd. Wat je afspreekt leg je dus vantevoren vast in computercode. Vertrouwen geprogrammeerd in een “slim contract”. Als-dit-dan-dat, zo-niet-dan-dat etcetera.

*“A key aspect is the programmable smart contract: code stored on the blockchain that automatically executes when certain conditions have been met.”*

- *Paul Levy, phys.org*

Met smart contracts kun je bijvoorbeeld vastleggen hoe de uitvoering van een testament dient plaats te vinden. Je stelt van tevoren voorwaarden op die ingaan bij het overlijden van desbetreffende persoon. Je zet afspraken in de code die door een computer worden uitgevoerd. Voordeel is dat dit geheel geautomatiseerd en autonoom plaatsvindt, zoals eerder afgesproken. Zo is er van alles mogelijk. Het slimme contract kan autonoom scripts uitvoeren wanneer het een bepaalde transactie ontvangt. Ethereum is een voorloper op het gebied van slimme contracten. Het is een crowd-funded platform dat werkt met een eigen cryptocurrency. (Meer hierover in de link naar de bookmarks).

Je zou ook een contract kunnen maken waarbij je gratis MP3's stuurt naar mensen die jou 0,00001 bitcoin sturen en tevens volgen op Facebook of Twitter bijvoorbeeld.

Blockchain wordt al toegepast om orders te verwerken op de NASDAQ middels een systeem genaamd Linq. Via hele kleine transacties worden uit te voeren orders op de beurs gecommuniceerd en versleuteld en overhandigt op en via de blockchain. Dit levert natuurlijk niet alleen een enorme tijdswinst op, maar vermindert ook het papierwerk aanzienlijk.

## 3.3 Eigenschappen

De mogelijkheden van Bitcoin als protocol zijn schier oneindig. Met behulp van de API kun je allerlei features toevoegen die betrekking hebben op de wisseling van eigendom. In de Bitcoin blockchain zijn, zoals gezegd, ‘slimme contracten’ te programmeren; we kunnen het bepaald gedrag meegeven aan de hand van door onszelf ingestelde regels en voorwaarden. Omdat de regels vantevoren zijn ingeprogrammeerd neemt het onderlinge vertrouwen toe en worden de risico’s geminimaliseerd. Tegelijkertijd voeg je bijvoorbeeld de datum in waarop het contract (oftewel: eigendomswisseling) ingaat.

### Automatisch

Transacties kunnen dus autonoom plaatsvinden, zonder tussenkomst van mensen. Het kan zelfs zo zijn dat een computerserver straks zelf gaat onderhandelen met klanten over de kosten van computerruimte en van de opbrengsten daarvan extra ruimte inkoopt. Volledig autonoom.

Een struikelblok voor de ontwikkeling van smart contracts is dat het lastig is met zekerheid vast te stellen wat in de echte wereld plaatsvindt.

In de digitale wereld is dit makkelijk: wanneer ik een e-mail stuur, wanneer ik een bitcoin overmaak, wanneer ik een mp3 beluister of een website bezoek: het is digitaal, dus kan dit gelezen worden door een slim contract.

*“Maar hoe registreer je in de echte wereld of een pakje daadwerkelijk is bezorgd? Of dat je daadwerkelijk iets tegen iemand hebt gezegd, of dat iemand daadwerkelijk kennis heeft genomen van bepaalde informatie?”*

*- Lykle de Vries*

## Locktime

Laten we eens kijken naar de feature die je kunt inprogrammeren in een slim contract; zo’n feature is ‘locktime’, waarmee je een transactie op een later tijdstip kunt laten uitvoeren. Dat betekent dat op hetzelfde moment dat er digitaal eigendom wordt verplaatst, ook de betaling direct plaatsvindt. Zo hoef je nooit meer iemand te wantrouwen, want de transactie werkt volgens het principe van ‘gelijk oversteken’. De blockchain heeft daarnaast features waarmee je voorwaarden kunt stellen aan een bepaalde overeenkomst, voordat er definitief een ‘signature’ onder komt. Bijvoorbeeld de hoogte van een bepaald bedrag in bitcoins.

## Simulfunding

Met het protocol kun je ook het principe van ‘Simulfunding’ waarborgen. Simulfunding wil zeggen dat mensen of bedrijven apart van elkaar een deel van een financiering voor hun rekening nemen, bijvoorbeeld als onderdeel van een crowdfunding-project. Je kunt het protocol dusdanig programmeren dat de definitieve afschrijving pas plaatsvindt op het moment dat de laatste partij de betaling doet. List en bedrog behoren daarmee tot het verleden, net als de situatie dat bepaalde partijen besluiten toch niet te betalen. Met Bitcoin gaat de transactie pas in de blockchain wanneer de laatste betaling binnenkomt. Onderling vertrouwen is dus niet meer nodig: het ‘slimme contract’ en het gehele netwerk zorgt voor de garantie dat alles volgens afspraak verloopt.

Een voorbeeld van zo’n Bitcoin-applicatie is Lighthouse. Lighthouse is een crowdfunding-platform waar het Bitcoin-protocol als basis dient. Het bitcoin-netwerk signaleert wanneer er voldoende geld is toegezegd om het beoogde doel van het project te bereiken. Vervolgens wordt het bedrag vrijgemaakt voor de uitvoerder van het crowdfunding project wanneer aan alle voorwaarden is voldaan. Ook hier is vertrouwen dus niet meer nodig. Het kan vooraf worden vastgelegd in de blockchain. En dat is nieuw.

## Ingeprogrammeerd vertrouwen

Rutger van Zuidam van intobitcoin.com schetste in een gesprek twee voorbeelden:

Verzekeraars kunnen deze nieuwe technologie toepassen met voorgeprogrammeerde behandelingen. In het contract dat je met je zorgverzekeraar hebt, zitten dan al een aantal randvoorwaarden versleuteld: bijvoorbeeld wanneer je je enkel verstuikt, dat je je geld uit kunt geven bij vooraf geselecteerde maatschappen van fysiotherapie.

Nog een voorbeeld: je kunt een transactie ook zo programmeren dat deze bij binnenkomst wordt onderverdeeld; gesplitst naar drie betaalrekeningen. Bijvoorbeeld een horecaondernemer die bij een bitcointransactie op de ene betaalrekening automatisch de btw reserveert, op een andere rekening de te verwachtte inkomstenbelasting en op een derde rekening zijn te besteden liquide middelen. Bitcoin blockchain maakt een hoge mate van automatisering mogelijk. Daardoor zullen zal er miljoenen bespaard worden op processen.

# 4. Overige toepassingen

*We hebben gezien dat de blockchain als onderliggende techniek van bijzondere waarde kan zijn bij onder meer financiële transacties en wisseling van eigendom. Hieronder een aantal andere mogelijke toepassingen van blockchain: verkiezingen, auteursrechten en journalistiek. Tot slot gaan we in op een geheel nieuwe wereld die zich opent: the Internet of Things.*

## 4.1 Verkiezingen

De blockchain zou een stemkastje kunnen zijn, in combinatie met een speciaal voor de verkiezingen uitgegeven token. Iedere Nederlander krijgt dan één zo'n token en ieder token is geoormerkt als aparte stem. Iedere token kan maar eenmaal ingediend worden. Een prima methode om makkelijk mee te democratiseren. Zo zouden we er dus fraudevrije verkiezingen mee kunnen houden.

## 4.2 Auteursrechten

*“And beyond financial transactions, cryptographic ledgers (zoals de blockchain, red.) could be used to exchange the information needed to validate a physical transaction – perhaps as a way of adding proof of authenticity to art, or registration documents for machinery, or even as a way to prevent copying of digital content.”*

*- The Economist*

De blockchain zou een middel kunnen zijn voor de beveiliging van digitale items waarvan je niet zou willen dat ze gereproduceerd worden. Stel dat je een Coin-identifier kunt koppelen aan een bestand, waardoor het bewijsbaar uniek wordt en (onbeperkt) kopiëren onmogelijk wordt. Zou dat geen middel zijn tegen het ongebreidelde en onbeperkt kopiëren van auteursrechtelijk beschermd materiaal?

Zo zou je iedere digitaal bestand een unieke eigenaar kunnen geven die niet zonder de auteur of uitgever te belonen van eigendom kan wisselen. Dat wil zeggen, iedere keer dat auteursrechtelijk beschermd materiaal van eigenaar wisselt, wordt de auteur of uitgever beloond met een percentage van de transactie of wordt er een deel transactiekosten toegekend. Dit zou kunnen met muziek en e-books, maar eigenlijk met alle digitale producten.

## 4.3 Journalistiek

Een bitcoin kan geknipt worden in een honderdste miljoenste bitcoin (0.00000001 BTC). Dat wordt ook wel een Satoshi genoemd, naar de bedenker van de bitcoin. Omdat het in kleine stukken kan worden geknipt, maakt het microbetalingen mogelijk.

Micropayments in de journalistiek zijn met dank aan Blendle heel populair geworden in Nederland. Het zou echter met behulp van blockchain-technologie en de daarbij behorende snelle micropayments nóg makkelijker en sneller kunnen, wanneer iedereen met zijn of haar browser online afrekent voor de gebruikte content. Bijvoorbeeld via een browser-plugin, die de lezer direct toegang tot een artikel verschaft na afrekenen, waarna de auteur van een artikel direct zijn deel ontvangt.

Zo zouden alle opbrengsten automatisch verdeeld kunnen worden conform de overeengekomen afspraken op de blockchain en de gebruikte currency.  Dit zou een oplossing kunnen zijn voor het probleem dat journalistieke inkomsten dalen doordat veel mensen veelal gratis hun nieuws lezen en ook advertentie-blockers gebruiken. Ook kan het gebruikt worden om micro-betalingen te doen aan muzikanten of filmakers voor het afspelen van hun content.

De Amerikaanse start-up Watchmybit probeert dit principe te verwezenlijken.

## 4.4 Internet of Things

Het Bitcoin-protocol en blockchain zouden ook hand in hand kunnen gaan met the Internet of Things (IoT). The internet of things wordt ook wel the internet of objects genoemd. En dat is logisch. Want waar we met de opkomst van social media een Internet of People kregen (waarbij mensen zich met elkaar kunnen verbinden via het internet) gaat het bij IoT om 'smart' (slimme) fysieke objecten gingen.

Deze slimme objecten bevatten ingebouwde technologie om te communiceren met het internet, met elkaar en met mensen. Ze hebben dus de mogelijkheid om waarnemingen te doen, maar kunnen ook waarnemingen van andere apparaten opvangen en verwerken. Soms met tussenkomst van mensen, soms niet. Soms volledig geautomatiseerd, soms niet. In de industrie wordt dit al langer toegepast, maar nu ook steeds meer in andere gebieden.

De sensoren die daarbij in allerlei objecten geplaatst worden zijn in staat om velerlei natuurkundige grootheden te meten.

Ze detecteren bijvoorbeeld informatie over hun omgeving zoals temperatuur, vochtigheidsgraad, beweging, nabijheid of locatie. Andere sensoren meten bijvoorbeeld massa, tijd, lichtsterkte, druk, elektrische spanning, snelheid, versnelling of magnetische veldsterkte. Sensoren werken op deze manier als extra en externe zintuigen van de mens. Beter, uitgebreider, sneller dan de mens. En sensoren worden nooit moe.

## Slimme spullen

Wanneer we spreken over fysiek objecten, dan hebben we het over vrijwel alle spullen om ons heen, zoals meubels, huishoudelijke apparaten, industriële machines, kleding en complete steden die met het internet verbonden kunnen worden. Door verbonden te worden aan het internet worden alledaagse objecten dus ‘smart’ of intelligent.

Je kunt fysieke objecten en apparaten dus verrijken met een digitale identiteit. Dankzij de blockchain kun je ze ook voorzien van een economische identiteit. Een object of apparaat dat dus in staat is financiële transacties te verrichten, zelfs zonder menselijke tussenkomst. Dat schept een wereld aan mogelijkheden.

Een (afwas-) machine kan dus theoretisch onderhandelen met de energieleverancier over het te betalen bedrag aan energiekosten. Bij een huurauto of (zelfrijdende) taxi zou je bijvoorbeeld per gereden minuut of kilometer kunnen afrekenen, zonder dat je ooit je portemonnee hoeft te pakken.

*“In this “futuristic” world, a soda machine can be an independent economic entity that is responsible for managing and selling its own store of drinks. It will be a machine that, in addition to selling drinks to consumers (M2C), will also be able to place orders with companies (B2M). It can even place orders with consumers (C2M) to fill its store.” (...) “The bitcoin protocol enables a “smart” machine to participate as a third economic agent alongside humans and organizations in the marketplace”*

En wat als je iedere simkaart zou voorzien van een bitcoin-adres? Zo kun je geld via je telefoon overmaken. Je telefoon als economische identiteit. En wanneer je bedenkt dat miljarden mensen een smartphone bezitten, brengt dat vele mogelijkheden met zich mee. TWYP van ING heeft dit principe onlangs min of meer gelanceerd, maar dan (nog) zonder blockchain/technologie.

Een bank zal overigens eerder een eigen digitale munt uitgeven met een private blockchain dan gebruik te maken van Bitcoin. Toch is het interessant om te zien dat de toepassingen hun intrede maken in de maatschappij.

## 4.5 Kinderziekten

Is het dan alleen maar halleluja rondom blockchain? Nee, dat is zeker niet het geval. Omdat de technologie ingewikkeld is en zich nog in een pril stadium bevindt en omdat beslissingen met instemming van de grote meerderheid moeten worden genomen, kent blockchain ook een aantal stevige kinderziektes. Op moment van schrijven, februari 2016, kan blockchain maximaal vijf transacties per seconde herbergen. De technologie is op dit moment nog onvoldoende in staat om vele transacties aan te kunnen. Wanneer het bitcoin netwerk meer kan ‘schalen’ zou het dus meer transacties per tijdseenheid kunnen verwerken. Er wordt actief gezocht naar een oplossing voor dit probleem.

Voor een wereldwijde adoptie van deze nieuwe technologie zou het ook nodig zijn dat transacties in real time meerdere keren bevestigd zouden kunnen worden. En dat de technologie voor de massa ook te begrijpen valt. En op dit moment is het gebruik van bitcoin technologie natuurlijk nog niet heel gebruiksvriendelijk.

En er zijn ook niet veel toepassingen gemaakt die het voor de gewone gebruiker makkelijk maakt om deze technologie in te zetten.

Uiteindelijk zal deze technologie geïmplementeerd worden aan de achterkant van vele toepassingen. We zullen dan minder in de gaten hebben dat de blockchaintechnologie de drijvende kracht is. Net zoals we nu ons op het internet weinig meer bezighouden met DNS en https zal dat ook met blockchain ook zo zijn. Waarschijnlijk zal het in de toekomst meer aan het oog onttrokken zijn.

# Conclusie

Het moge duidelijk zijn dat de nieuwe techniek van bitcoin blockchain een hele nieuwe wereld van mogelijkheden creëert. En hoewel de technologie zich nog in een prille en experimentele fase bevindt, zijn de contouren helder.

Als we kijken naar de toekomst van bitcoin als digitale munt is het niet de verwachting dat wij in West-Europa over een paar jaar massaal hiermee zullen betalen. In andere delen van de wereld krijgt bitcoin wellicht meer voet aan de grond omdat minder mensen een betaalrekening hebben maar wel een internetverbinding en omdat de transactiekosten hoger zijn bij euro's of dollars.

De onderliggende technologie, blockchain is in staat om bijzonder veel impact te kunnen hebben. Het stelt ons namelijk in staat om

- (Financiële) transacties te verrichten zonder tussenkomst van bank
- Eigendoms(recht) vast te leggen in een wereldwijd gedistribueerd grootboek
- Slimme contracten te creëren die geautomatiseerd hun taken uitvoeren
- Met-het-internet-verbonden objecten om een economische identiteit aan te nemen en transacties zelfstandig uit te kunnen voeren.

Met dit rapport heb ik hopelijk mijn licht kunnen laten schijnen op deze nieuwe technologie en de mogelijkheden die het herbergt. Dank voor het lezen.

Bijzonder veel dank aan Lykle de Vries van bitcoinevangelist.nl (@BTCevangelist), Rutger van Zuidam van Intobitcoin.com (@IntoBitCoin) en Roel Boer (@roelbuerra) voor hun uitleg, voorbeelden, meelezen en inzichten. Dankzij hen is het rapport beter geworden.
Dank Gert Gritter voor de tekstuele aanpassingen.
Mark en Marten voor design.

Wil je MEER lezen over bitcoins en blockchain? Kijk dan voor de bookmarks op http://www.jarnoduursma.nl/bitcoinblockchain/

Je kunt me ook boeken voor een lezing over bitcoin blockchain!

met hartelijke groet,

Jarno Duursma
Trendverkenner

*http://www.jarnoduursma.nl/*
*info@jarnoduursma.nl*