Joost Linnemann[1]

Juridische aspecten van (toepassingen van) blockchain

Computerrecht 2016/218

In dit artikel beschrijft de auteur de techniek achter blockchain. Op hoofdlijnen wordt aandacht besteed aan juridische aspecten van blockchain en van de toepassingen daarvan.[2]

1. Inleiding

Blockchain is hot. Een enkeling voorspelt dat banken zullen verdwijnen door de opkomst van blockchain.[3] Een ander dat blockchain de wereld zal veranderen.[4] Toekomstmuziek wellicht, maar de rechten voor het gebruik van de muziek van Hardwell worden vandaag al daadwerkelijk verdeeld via de blockchain.[5]

Blockchain is de technologie onder de virtuele munteenheid bitcoin. Over bitcoin is al de nodige jurisprudentie[6], en over juridische aspecten van de digitale munt wordt al uitgebreid geschreven[7]. Veel van wat aan blockchain wordt toegedicht heeft echter niets met bitcoin te maken. Juridische literatuur over blockchain als zodanig is er in Nederland nog nauwelijks, noch over andere toepassingen daarvan dan voor bitcoin.[8]

Dit artikel beoogt in de eerste plaats uit te leggen wat blockchain is. Daarbij zal ik proberen blockchain zelf af te bakenen van concrete toepassingen, zoals bitcoin. Bij de uitleg valt er niet aan te ontkomen – ik waarschuw maar vast – om aandacht te besteden aan een aantal cryptografische technieken. Diezelfde technieken worden gebruikt bij digitale handtekeningen. In het notenapparaat zal daarom bij de bespreking van een techniek worden verwezen naar relevante bepalingen van de wetgeving op het terrein van elektronische handtekeningen.[9]

Vervolgens wordt kort een aantal toepassingen van blockchain beschreven, zoals *smart contracts*. Zoals zal blijken, kleven aan blockchain als zodanig niet veel bijzondere juridische aspecten. Voor een aantal van de mogelijke toepassingen is dat zeker anders, bijvoorbeeld omdat datgene wat blockchain zou kunnen vervangen, wettelijk is geregeld. Het gaat het bestek van dit artikel te buiten om van een groot aantal toepassingen de juridische aspecten met enige diepgang te bespreken. In dat opzicht is het ambitieniveau van dit artikel laag. Wel beoogt dit artikel een basis te leggen waarop toekomstige artikelen over de juridische aspecten van toepassingen van de blockchain kunnen voortbouwen. In dat opzicht is het ambitieniveau dan weer bepaald hoog.

Nog een opmerking vooraf. Het is gebruikelijk om te spreken over 'de' blockchain, ook als het gaat over het concept blockchain. Dat is verwarrend. Het doet namelijk vermoeden dat er maar één blockchain is. Dat is niet zo. Ik spreek hierna dan ook alleen over 'de' blockchain als het gaat om een specifieke blockchain, bijvoorbeeld de blockchain onder bitcoin.

2. Wat is blockchain?

In dit deel van dit artikel wordt technisch uitgelegd wat blockchain is, hoe gegevens in een blockchain zijn beveiligd tegen manipulatie, wat er in een blockchain kan worden opgeslagen en hoe gegevens aan een blockchain kunnen worden toegevoegd.

Zoals gezegd is blockchain de technologie onder bitcoin. Satoshi Nakamoto, de mysterieuze bedenker van bitcoin[10], wilde komen tot een "*purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without going through a financial institution*".[11] De blockchain onder bitcoin is complex door een aantal specifieke kenmerken die uit deze doelstelling voortvloeien. Een toepassing waarvoor niet alle eisen gelden die bitcoin stelt, zoals de eis dat transacties zonder tussenkomst van een financiële instelling moeten kunnen worden gedaan, kan volstaan met een minder complexe blockchain.

Op hoog abstractieniveau kan een blockchain worden omschreven als een openbaar grootboek (of database) van onveranderbare transacties. Kenmerkend voor een grootboek en de meeste databases is dat die worden bijgehouden door een organisatie. Als onderneming A iets verkoopt aan onderneming B, leggen beide ondernemingen die transactie vast in hun eigen grootboek. Dat grootboek is gewoonlijk alleen voor de desbetreffende onderneming toegankelijk. Die onderneming bepaalt ook wat wel en niet in het grootboek wordt vastgelegd en kan desgewenst wijzigingen in

1 Joost Linnemann is advocaat bij Kennedy Van der Laan in Amsterdam.
2 NVDR. Deze bijdrage vormt een inleiding op een themanummer dat in het volgende jaargang zal verschijnen.
3 https://fd.nl/beurs/1170837/banken-verdwijnen-door-opkomst-blockchain.
4 www.ad.nl/nieuws/blockchain-gaat-de-wereld-veranderen~a4697f98/.
5 www.emerce.nl/nieuws/wereldprimeur-dj-hardwell-blockchain. Hardwell maakt gebruik van de technologie van startup Rightsshare.
6 Zie bijvoorbeeld Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219 en HvJ 22 oktober 2015, C-264/14.
7 Bijvoorbeeld W.F. Dammers, 'Bitcoins: een vreemde zaak?', *Tijdschrift voor Internetrecht*, nr. 3, september 2015, p. 110 waarin beide in de vorige noot genoemde uitspraken worden becommentarieerd.
8 Een uitzondering: T.F.E. Tjong Tjin Tai, 'De redelijke derde en de blockchain', *WPNR* 2015/7072, p. 671-672 over de rol die de blockchain kan spelen bij bankgaranties.
9 In het bijzonder Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna: Verordening elektronische identificatie en vertrouwensdiensten.
10 Het is nog steeds onduidelijk wie Satoshi Nakamoto is. Zie onder (veel) meer www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair.
11 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf.

het grootboek aanbrengen. Aldus zijn er meerdere vastleggingen van dezelfde transactie, waarbij het ook niet is uitgesloten dat er discrepanties zijn tussen die vastleggingen. Een blockchain is in een aantal opzichten anders. In de eerste plaats is een blockchain decentraal. Het grootboek is niet op één computer opgeslagen (zoals de server van onderneming A). Volledige exemplaren van het grootboek (de blockchain) zijn opgeslagen op alle computers in een zogenaamd peer-to-peer netwerk. Toevoegingen aan het grootboek worden op die computers in het netwerk doorgevoerd. Op die manier kijken alle deelnemers aan het netwerk naar dezelfde informatie. Zou de hiervoor beschreven transactie tussen onderneming A en B aan een blockchain zijn toegevoegd, dan is er dus één eenduidige vastlegging van de transactie die kan worden geraadpleegd door beide partijen (en trouwens door alle deelnemers aan de blockchain). Uiteraard is voor een dergelijk decentraal systeem cruciaal dat gegevens niet zomaar kunnen worden gewijzigd en dat er een manier is om te bepalen welke data aan de blockchain wordt toegevoegd. In de volgende paragraaf wordt beschreven hoe een blockchain is opgebouwd, en welk mechanisme garandeert dat gegevens daarin niet zomaar kunnen worden gewijzigd.[12]

2.1 *Opbouw van een blockchain*

Gegevens in een blockchain worden om redenen van efficiency vastgelegd in blokken. Vandaar 'block' in blockchain. Een blok kan bijvoorbeeld bestaan uit een aantal bitcointransacties, maar kan – zoals we later zullen zien – ook bestaan uit heel andere gegevens en zelfs uit computerprogramma's. De blokken staan in een onderlinge verhouding tot elkaar: ze zijn aan elkaar gekoppeld. Vandaar 'chain' in blockchain. De manier waarop blokken in de blokchain aan elkaar zijn verbonden zorgt ervoor dat het wijzigen van gegevens achteraf praktisch onmogelijk is. Mocht toch een wijziging worden aangebracht, dan kan die wijziging makkelijk worden opgespoord. Daartoe wordt gebruik gemaakt van zogenaamde *hashing*. Goed begrip daarvan vereist een kleine cryptografische uitstap.

Een belangrijke bouwsteen van een blockchain is namelijk de cryptografisce hashfunctie. Het gaat hier om een wiskundige functie die wordt gebruikt om data van willekeurige omvang (de invoer) te vertalen in een – meestal kleinere – vaste hoeveelheid data (de uitvoer, ook wel aangeduid als de hashwaarde). Een bekende cryptografische hashfunctie is SHA-256[13]. Aan een cryptografische hashfunctie worden onder meer de volgende eisen gesteld:

– De hashfunctie moet het onmogelijk te maken om de invoer af te leiden uit de uitvoer. Een hashfunctie heeft iets van een gehaktmolen: zoals het onmogelijk is om te komen tot het oorspronkelijke stuk vlees door de gehaktmolen terug te draaien, is het onmogelijk om aan de hand van een hashwaarde te bepalen welk document tot die hashwaarde heeft geleid.
– De hashfunctie mag weinig 'botsingen' veroorzaken. Dit betekent dat het praktisch onmogelijk moet zijn om dezelfde uitvoer te vinden voor verschillende invoer.

De laatstgenoemde eigenschap van een hashfunctie betekent niet alleen dat verschillende invoer tot verschillende uitvoer moet leiden, maar ook dat dezelfde invoer steeds tot dezelfde uitvoer moet leiden. Deze eigenschap maakt het mogelijk om efficiënt te bepalen of twee documenten identiek zijn door alleen de hashwaardes van die documenten met elkaar te vergelijken. Zijn de hashwaardes identiek, dan zijn ook de documenten identiek. Zo kan ook worden vastgesteld of aan een document iets is gewijzigd. Stel dat de verzender van een document de hashwaarde van dat document berekent voordat het wordt verzonden naar de ontvanger. Als de ontvanger op zijn beurt van het ontvangen document de hashwaarde berekent, en die hashwaarde is gelijk aan de door de verzender berekende waarde, dan staat daarmee vast dat er tussen verzending en ontvangst niets aan het document is gewijzigd. Was dat immers wel gebeurd, dan zou toepassing van de hashfunctie door de ontvanger noodzakelijk hebben geleid tot een andere hashwaarde dan de waarde die eerder door de verzender was berekend.[14]

Elk blok in een blockchain bevat een zogenaamde hash pointer die verwijst naar het voorafgaande blok. Een hash pointer is een verwijzing naar de locatie van data waarin ook de hashwaarde van die data is vastgelegd. Het gebruik van hash pointers maakt het mogelijk om een wijziging in een blok te detecteren. Als iemand een wijziging in een blok zou aanbrengen, bijvoorbeeld om de waarde van een in dat blok vastgelegde transactie te wijzigen, dan zou door die wijziging noodzakelijkerwijs ook de hashwaarde van dat blok veranderen. Probleem is echter dat de oorspronkelijke hashwaarde onderdeel is van de hash pointer in het daaropvolgende blok. Om te voorkomen dat de wijziging zou worden gedetecteerd zou een onverlaat dus ook de hash pointer in het daaropvolgende blok moeten veranderen. Die verandering leidt echter weer tot een wijziging van dat blok en dus van de hashwaarde van dat blok die weer in het daaropvolgende blok is vastgelegd. Enzovoort, enzovoort. Het volstaat dus niet om een wijziging aan te brengen in het blok dat je wilt wijzigen: om dat ongemerkt te doen moet je alle daaropvolgende blokken wijzigen. Als je in een boek een pagina zou willen vervalsen, kun je in beginsel volstaan met wijziging van de desbetreffende pagina (je vervangt bijvoorbeeld de oorspronkelijke pagina 10 door een nieuwe pagina 10). Om te voorkomen dat een vergelijkbare wijziging van een blok in een blockchain zou worden ontdekt,

12 De technische beschrijving van blockchain in dit artikel is in belangrijke mate gebaseerd op Narayanan, Bonneau, Felten, Miller en Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press 2016.

13 Dit staat voor Secure Hash Algorithm – 256 bit.

14 Artikel 26 van de Verordening elektronische identificatie en vertrouwensdiensten stelt als een van de eisen aan een geavanceerde elektronische handtekening dat zij op zodanige wijze aan de daarmee ondertekende gegevens is verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord. Uit het voorgaande volgt dat aan deze eis kan worden voldaan door gebruik te maken van een cryptografische hashfunctie.

zou je niet alleen pagina 10 moeten vervangen, maar ook alle daaropvolgende pagina's. In een boek geeft een paginanummer de volgorde aan (pagina 11 komt na pagina 10) maar is er overigens geen noodzakelijke relatie tussen de pagina's. In een blockchain wordt door het gebruik van hash pointers de volgorde niet alleen gekoppeld aan de locatie van het vorige blok, maar ook aan de inhoud daarvan. Om de gegevens in een blok in een blockchain te veranderen moet je dus (veel) meer wijzigen dan alleen het desbetreffende blok. Daarnaast bevatten blockchains mechanismen die ervoor zorgen dat wijzigen ook nog eens moeilijk is. In het geval van bitcoin wordt dit bereikt door het hierna te bespreken mechanisme van *proof-of-work*, maar er zijn ook andere mechanismen. Daardoor is niet alleen wijziging door onbevoegden lastig, maar is het ook voor bevoegden vrijwel onmogelijk om gegevens in het midden van de blockchain te wijzigen. Per saldo betekent dit dat gegevens alleen aan het einde van de blockchain kunnen worden toegevoegd.

2.2 *Wat zit er in de blockchain?*

Hiervoor is beschreven hoe de blockchain is opgebouwd. Dat zegt echter nog niets over welke gegevens in de blockchain zijn opgeslagen. De bitcoin-blockchain bevat bitcointransacties, maar in beginsel kan in een blockchain van alles worden opgeslagen, inclusief computerprogramma's. Alvorens die andere mogelijkheden onder ogen te zien, is het goed om te bekijken hoe een bitcoin transactie werkt. Daarbij wordt gebruikgemaakt van de techniek van digitale handtekeningen. Een in dit verband belangrijk kenmerk van een digitale handtekening is (net als van een handgeschreven handtekening) dat alleen de betrokkene die kan zetten, maar dat iedereen kan verifiëren of de handtekening echt is. Ook moet de handtekening onlosmakelijk verbonden zijn met bepaalde gegevens (bijvoorbeeld een bitcointransactie) om te voorkomen dat de handtekening wordt misbruikt met betrekking tot andere gegevens[15]. Een systeem voor digitale handtekening bestaat uit drie algoritmes:

- Een algoritme dat een sleutelpaar genereert: een sleutelpaar bestaat uit een cryptografisch onlosmakelijk met elkaar verbonden geheime sleutel en een openbare sleutel. De geheime sleutel wordt – de naam zegt het al – geheimgehouden en gebruikt om te ondertekenen. De openbare sleutel kan vrijelijk worden gedistribueerd en kan door iedereen die erover beschikt worden gebruikt om te verifiëren dat een handtekening geldig is.[16]
- Een algoritme dat een handtekening genereert: op basis van een geheime sleutel en te ondertekenen gegevens genereert dit algoritme ondertekening van de desbetreffende gegevens.
- Een algoritme waarmee een handtekening kan worden geverifieerd: dit algoritme bevestigt of weerlegt op basis van het document, de handtekening en de openbare sleutel van de ondertekenaar dat het document is ondertekend met de bijbehorende geheime sleutel.

Elk sleutelpaar vormt in zekere zin een identiteit. De houder van de geheime sleutel kan die identiteit vertegenwoordigen. Bitcoin kenmerkt zich door zogenaamd decentraal identiteitsbeheer. Er is niet een centrale autoriteit die bepaalt wie de gebruikers van het systeem zijn: iedereen kan gebruiker zijn en elke gebruiker kan zoveel identiteiten maken als hij of zij wil, namelijk door een nieuw sleutelpaar te genereren. Dat de houder van een geheime sleutel zich kan identificeren als degene die een handtekening heeft gezet, wil nog niet zeggen dat aan de hand van die handtekening de ware identiteit van de betrokkene kan worden achterhaald: de sleutels zijn niet meer dan getallen van 256 respectievelijk 512 bits. In die zin is bitcoin een anoniem systeem.[17] Die anonimiteit is echter relatief: omdat alle bitcointransacties voor alle deelnemers zichtbaar zijn in de blockchain, hoeft maar één transactie aan een persoon te kunnen worden gekoppeld (bijvoorbeeld door netwerksurveillance) om eenvoudig alle transacties van die persoon te vinden. Om die reden is het niet ongebruikelijk om voor elke bitcointransactie een nieuw sleutelpaar te genereren.

Sterk vereenvoudigd bestaat een bitcointransactie uit een bitcoinwaarde, het adres van de betaler, het adres van de ontvanger en de digitale handtekening van de betaler. Een bitcoinadres is niets anders dan de hashwaarde van de openbare sleutel van de betrokkene. Op onderstaande foto heeft een demonstrant zijn bitcoinadres gecodeerd in een QR-code op zijn spandoek. De demonstrant kan toegang krijgen tot de bitcoins die zijn moeder stuurt doordat hij beschikt over de geheime sleutel die hoort bij (de publieke sleutel in) het bitcoinadres op het spandoek.

15 Vergelijk de definitie van elektronische handtekening in artikel 3 van de Verordening elektronische identificatie en vertrouwensdiensten: gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen (onderstreping auteur).

16 Ook de hier genoemde begrippen zijn terug te vinden in de Verordening elektronische identificatie en vertrouwensdiensten. Zo voldoet de hier beschreven geheime sleutel aan de definitie van gegevens voor het aanmaken van elektronische handtekeningen (unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken), en de publieke sleutel aan de definitie van valideringsgegevens (gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren).

17 Hiervoor verwees ik al enkele malen naar de regeling van elektronische handtekeningen in de Verordening elektronische identificatie en vertrouwensdiensten. Die Verordening bepaalt in artikel 25 lid 2 dat een elektronische handtekening die aan bepaalde voorwaarden voldoet, dezelfde rechtsgevolgen heeft als een handgeschreven handtekening. Een van die eisen is dat uit de handtekening, anders dan bij bitcoins, wél de identiteit blijkt. Die koppeling tussen publieke sleutel en een natuurlijke persoon wordt bereikt door gebruik van een zogenaamd certificaat voor elektronische handtekeningen, volgens de Verordening "een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt". Certificaten spelen in de bitcoin-blockchain geen rol.

Om te voorkomen dat al zijn eerdere bitcointransacties – na identificatie aan de hand van de foto – eenvoudig aan hem kunnen worden gekoppeld, zal de demonstrant vermoedelijk speciaal voor dit verzoek een nieuwe identiteit (ofwel sleutelpaar) hebben gegenereerd.

Decentraal identiteitsbeheer en anonimiteit, zoals bij bitcoin, zijn geen noodzakelijk kenmerk van een blockchain. Het is goed denkbaar dat aan een blockchain alleen gegevens kunnen worden toegevoegd door gebruikers aan wie vooraf, door een centrale autoriteit toegang is verleend. In dat geval zouden digitale handtekeningen kunnen worden gebruikt om aan te tonen dat een in de blockchain vastgelegde transactie ook daadwerkelijk is gedaan door een bevoegde gebruiker.

In de bitcoin-blockchain worden geen direct identificerende gegevens vastgelegd. Er zijn echter zeker toepassingen denkbaar waarbij dat wel gebeurt.

Kortom: in een blockchain kunnen allerlei gegevens worden opgeslagen. De kring van gebruikers kan onbeperkt zijn, maar dat hoeft niet. En gegevens kunnen anoniem worden vastgelegd, maar ook dat is geen noodzakelijk kenmerk van een blockchain.

2.3 *Toevoegen van gegevens aan een blockchain*

We hebben gezien dat van alles in een blockchain kan worden opgeslagen. Resteert de vraag hoe wordt bepaald welke gegevens aan een blockchain worden toegevoegd. Een voor de hand liggende oplossing is dat dat gebeurt door een centrale autoriteit. Zo bepaalt in het eerdere voorbeeld onderneming A welke transacties aan 'haar' grootboek worden toegevoegd. Maar zoals in de inleiding opgemerkt, was een van de doelstellingen van bitcoin om betalingen mogelijk te maken zonder tussenkomst van een bank. De vraag is hoe in een dergelijk systeem, bij gebreke van een centrale autoriteit, kan worden bepaald welke transacties geldig zijn en aan de blockchain moeten worden toegevoegd, en in welke volgorde. Het antwoord is dat dit gebeurt door het decentraal bereiken van consensus.

Degene die gegevens wil toevoegen aan de blockchain, zendt die gegevens aan alle computers die deel uitmaken van het peer-to-peernetwerk. Elk van die computers voegt de gegevens samen met andere nog niet in de blockchain opgenomen gegevens in een blok en gaat vervolgens op zoek naar het zogenaamde *proof-of-work* voor dat blok. Daartoe moeten zogenaamde hash-puzzels worden gedaan: een computer die het proof-of-work wil leveren gaat – simpelweg door steeds een ander getal te proberen – op zoek naar een getal dat aan een bepaalde eis voldoet. Die eis is dat de hashwaarde van de som van dat getal, de inhoud van het voorgestelde blok en de hash pointer naar het vorige blok in de blockchain, valt binnen een bepaald klein doelgebied. Het vinden van een getal dat aan die eis voldoet vereist veel rekenkracht.[18] Als een computer erin slaagt het getal te vinden, zendt de computer het blok naar alle andere computers op het netwerk. In het blok wordt ook het gevonden getal opgenomen. Andere computers in het peer-to-peernetwerk zullen het nieuwe blok als geldig accepteren als de inhoud van het blok geldig is én het getal aan de eis voldoet. Zij kunnen dat laatste eenvoudig vaststellen door de hashwaarde van de onderdelen van het blok te berekenen en te verifiëren dat die hashwaarde inderdaad valt binnen het doelgebied. Aldus is het moeilijk, althans vergt het veel rekenkracht om het proof-of-work te leveren, maar is het heel eenvoudig om vast te stellen of dat ook inderdaad is gebeurd. Een computer in het netwerk accepteert het voorgestelde nieuwe blok door bij het werken aan een nieuw blok, in dat nieuwe blok de hashwaarde van het geaccepteerde blok te gebruiken.

Het decentraal bereiken van consensus vergt dus veel rekenkracht. Die rekenkracht kost geld. Het systeem moet een incentive hebben om gebruikers ertoe te bewegen rekenkracht ter beschikking te stellen. In het geval van bitcoin bestaat die incentive uit bitcoins[19]. Diegene die erin slaagt een nieuw blok aan de blockchain toe te voegen mag namelijk in dat blok een speciale *coin creation* transactie toevoegen. En zo worden bitcoins gecreëerd. Dit is zelfs de enige manier waarop bitcoins kunnen worden gecreëerd. Daarom wordt het leveren van proof-of-work ook wel aangeduid als *mining* van bitcoins.

De inspanning die wordt verricht om decentraal consensus te bereiken wordt in bitcoin dus beloond met bitcoins. Elke blockchain, ook een die niet onderdeel is van een systeem van virtueel geld, zal incentives moeten hebben om decentraal consensus te bereiken. Alternatief is natuurlijk dat consensus centraal wordt bereikt. In een dergelijk systeem is er een centrale autoriteit die bepaalt wat het volgende blok in de blockchain wordt. Zo'n systeem kan technisch veel eenvoudiger zijn, maar is niet geschikt voor toepas-

18 Hoeveel rekenkracht benodigd is, is variabel. In het geval van bitcoin wordt de benodigde hoeveelheid rekenkracht (of liever: de grootte van het hiervoor beschreven doelbereik) periodiek aangepast aan de totale hoeveelheid beschikbare rekenkracht. Zo wordt bewerkstelligd dat ongeveer elke 10 minuten een nieuw blok aan de blockchain wordt toegevoegd, ook als de totale hoeveelheid beschikbare rekenkracht toeneemt.

19 Bitcoin kent nog een andere incentive, de zogenaamde transactievergoeding. Die laat ik hier echter onbesproken.

singen waarin het juist de bedoeling is om zonder centrale autoriteit te werken.

3. Toepassingen van blockchain

Blockchain is de techniek onder bitcoin. Maar zoals uit het voorgaande blijkt, kan in de blockchain veel meer worden opgeslagen dan bitcointransacties. De complexiteit van de bitcoin-blockchain, die samenhangt met specifieke aspecten en doelstellingen van die virtuele munteenheid, is zeker niet voor alle toepassingen nodig.

3.1 *Toepassingen waarbij aanspraken worden vastgelegd*

Eén categorie van toepassingen van blockchain is die waarbij aanspraken worden vastgelegd in een blockchain. De aanspraak staat dan onomstotelijk vast en is door iedereen te raadplegen. Zo kan het opnemen van de beschrijving van een auteursrechtelijk beschermd werk in een blockchain helpen bij het bewijzen dat degene die die beschrijving in de blockchain vastlegde de rechthebbende is.[20] In die zin zou de blockchain de vroegere functie van de registratie van een onderhandse akte bij de Belastingdienst kunnen vervangen. De mogelijkheid daartoe is sinds wijziging van de Registratiewet 1970 per 1 januari 2013 vervallen. Een andere mogelijkheid is het vastleggen van de aanspraak op toegang tot een evenement. De houder van een doorverkocht e-ticket kan er bij de ingang van dat evenement achter komen dat aan iemand anders al toegang is verleend tot dat evenement op basis van hetzelfde e-ticket. Was de aanspraak vastgelegd in een blockchain, dan zou voor iedereen – ook de controleurs van de concertzaal – duidelijk zijn wie de enige en echte rechthebbende is.

Aan dergelijke toepassingen kleven juridische aspecten (een bewijspositie wordt versterkt, contractuele relaties worden helder vastgelegd), maar die aspecten zijn beperkt en overzichtelijk.

3.2 *Toepassingen waar vertrouwen nu wordt ontleend aan een centrale autoriteit*

Voor een andere categorie van toepassingen geldt dat de juridische aspecten complexer zijn. Veel toepassingen beogen namelijk een systeem te vervangen dat op dit moment gebaseerd is op vertrouwen in een centrale autoriteit. Bitcoin is daarvan een goed voorbeeld. Zoals we zagen is een van de kerndoelstellingen van bitcoin het faciliteren van betalingen zonder tussenkomst van een bank. En de gevestigde orde maakt zich zorgen. Traditionele financiële instellingen vrezen 23% van hun business te verliezen aan nieuwkomers.[21] Oprukkende blockchain-toepassingen vormen een bedreiging van het notariaat, stelde Jef Oomen, voorzitter van de Koninklijke Notariële Beroepsorganisatie tijdens de algemene ledenvergadering van dit jaar.[22]

In veel gevallen is de rol van een centrale autoriteit wettelijk verankerd, en is ook het toezicht op de autoriteit wettelijk geregeld. Vervanging van de bestaande systemen is daarom niet alleen een technisch en organisatorisch complexe aangelegenheid. Ook juridisch zijn dergelijke wijzigingen complex. Vervanging van de registratie van het Kadaster door een blockchain vereist wijziging van de Kadasterwet. Beperking van de rol van het notariaat ten gunste van blockchaintoepassingen vereist wellicht aanpassing van de Wet op het notarisambt, maar ook van specifieke wettelijke regelingen. Denk bijvoorbeeld aan de betrokkenheid van de notaris bij de levering van aandelen[23] en bij de levering van onroerende zaken[24]. Als al zou worden overwogen dergelijke functies aan blockchaintoepassingen over te laten, ligt het ook voor de hand om op de een of andere manier het toezicht op die blockchaintoepassingen wettelijk te verankeren.

3.3 *Inpassing van blockchain toepassingen in bestaande systemen*

Een laatste categorie van toepassingen van blockchain is het gebruik van blockchain-technologie door bestaande partijen, zoals banken. Traditionele banken zetten zwaar in op het gebruik van blockchain. Zo hebben ING en ABN AMRO zich aangesloten bij een groep internationale banken die de mogelijkheden onderzoekt van blockchain[25] en werkt ABN AMRO met het Havenbedrijf Rotterdam aan een experiment om scheepsladingen die in de haven komen te registreren via een blockchain.[26] ABN AMRO, ING, Rabobank, SNS Bank en Betaalvereniging Nederland onderzoeken gezamenlijk de toepasbaarheid van blockchain-technologie. De Nederlandsche Bank is als waarnemer bij het onderzoek betrokken.[27] Betrokkenheid van de toezichthouder bij een dergelijk onderzoek verbaast niet. Het is evident dat gebruik van blockchain-technologie door onder toezicht staande banken ook eisen stelt aan de toezichthouder.[28] Die moet immers beoordelen of banken, ook bij gebruik van blockchain, voldoen aan de wettelijke eisen.

Al met al zijn banken dus zeer actief op het terrein van blockchain. Het is opmerkelijk dat de techniek achter bitcoin

20 Daarbij is het, zoals we in paragraaf 2.2 gezien hebben, niet noodzakelijk dat de identiteit van de maker blijkt uit de blockchain. Ook is het niet nodig om de beschrijving van het werk zelf in de blockchain op te nemen. Volstaan kan worden met het opnemen van de hashwaarde van die beschrijving, voorzien van een digitale handtekening van de maker. Ook dan kan de maker later met behulp van de blockchain bewijzen dat hij op het moment van aanmaken van het desbetreffende blok beschikte over de beschrijving van het werk.

21 https://fd.nl/ondernemen/1157228/fintech-bedreigt-kwart-omzet-financiele-sector.

22 www.knb.nl/nieuwsberichten/bedreiging-trustfuctie-notaris-bij-blockchain-toepassingen.

23 Artikel 2:86 lid 1 BW en 2:196 lid 1 BW.

24 Artikel 5:89 lid 1 BW.

25 https://fd.nl/beurs/1127974/ing-sluit-zich-aan-bij-blockchain-collectief en https://www.abnamro.com/nl/newsroom/nieuws/2016/abn-amro-lid-van-r3.html.

26 https://www.nrc.nl/nieuws/2016/06/21/banken-zien-blockchain-ook-wel-zitten-2834727-a1506434.

27 https://www.betaalvereniging.nl/werkterreinen/innovaties/.

28 Die implicaties voor het toezicht onderzoekt De Nederlandsche Bank in zijn rapport *Technologische innovatie en de Nederlandse financiële sector, Kansen en risico's voor gevestigde instellingen, nieuwkomers & het toezicht*.

vooral wordt ingezet door dezelfde financiële instellingen die bitcoin beoogt buiten spel te zetten. Dit betekent dat in veel van die toepassingen niet steeds behoefte bestaat aan alle elementen van de bitcoin-blockchain, zoals decentraal identiteitsbeheer en het decentraal bereiken van consensus.

Ook in andere sectoren zijn traditionele spelers aan de slag met blockchain. Zo zijn er voorbeelden in de energiesector en in de zorg.[29] Ook hier gaat het om gereguleerde sectoren, zodat aan de inzet van blockchaintechnologie onvermijdelijk juridische aspecten kleven, al was het maar in het kader van toezicht. Zoals gezegd, gaat het de kaders van dit verkennend artikel te buiten om aan die specifieke aspecten aandacht te besteden.

Overigens zou toepassing van blockchain in de zorg kunnen vereisen dat de gegevens in de desbetreffende blockchain worden versleuteld. Dit met het oog op de bescherming van de persoonlijke levenssfeer van de betrokkenen. Ook daarbij zal ongetwijfeld gebruik worden gemaakt van sleutelparen van geheime en openbare sleutels. Het zou hier gaan om een verzwaring ten opzichte van de bitcoin-blockchain: de gegevens in die blockchain zijn namelijk niet versleuteld.

3.4 *Smart contracts*

Een bijzondere categorie van toepassingen van de blockchain wordt gevormd door de zogenaamde smart contracts. Bij smart contracts worden in de blockchain geen gegevens opgeslagen, maar computerprogramma's. Die overeenkomst is dan niet (alleen) vastgelegd in contractuele bepalingen (tekst), maar in een computerprogramma. De gedachte is dat daardoor de uitvoering van een overeenkomst kan worden geautomatiseerd. Die uitvoering is dan niet langer afhankelijk van de nukken van partijen. Als zich bepaalde condities voordoen, voert het smart contract bepaalde handelingen uit, zoals het doen van een betaling. De uit te voeren handelingen kunnen complex zijn en worden getriggerd of worden beïnvloed door externe input. Denk bijvoorbeeld aan het automatisch indexeren van een overeengekomen vergoeding op basis van een koppeling van het smart contract aan de systemen van het Centraal Bureau voor de Statistiek. Of aan het starten van de termijn van het herroepingsrecht bij een koop op afstand op basis van track and trace informatie van de vervoerder om op basis daarvan te bepalen of het verkochte tijdig is geretourneerd. Omdat het smart contract is opgeslagen in de blockchain, kan het niet door een van de partijen worden gewijzigd.

Bij de uitvoering van een overeenkomst is vaak uitleg van de bepalingen nodig. De Hoge Raad heeft daarvoor – in de woorden van Drion – zelfs een unieke love baby geschapen, met een befaamde over en weer formule en een dubbel geobjectiveerde subjectieve uitlegmaatstaf.[30] Het is mijns inziens dan ook een illusie te denken dat alle overeenkomsten zich lenen voor automatische uitvoering. Maar ook bij overeenkomsten waarvoor dat wel geldt, spelen juridische vragen, zoals de vraag of wat een smart contract doet wel altijd kan worden toegerekend aan de contractspartijen, zeker in een systeem waarbij automatisch nieuwe overeenkomsten worden gesloten.[31] Met deze kanttekeningen zijn er ongetwijfeld vele nuttige toepassingen van smart contracts denkbaar.

Aan smart contracts zitten ook veiligheidsrisico's. Eerder dit jaar ontstond een groot probleem op Ethereum, een platform voor smart contracts. DAO, een Ethereum smart contract, begon bedragen uit te keren aan een onbekende derde. Die bedragen werden uitgekeerd in *ether*, het virtuele geld van Ethereum (vergelijkbaar met bitcoin). Hierboven is al uiteengezet hoe moeilijk het is om oudere transacties te wijzigen. Het voorkomen daarvan is zelfs een belangrijk kenmerk van blockchain. Het ongedaan maken van dergelijke malversaties blijkt dan ook een groot probleem, wat ondermijnend werkt voor het vertrouwen in smart contracts.[32]

4. Conclusie

In dit artikel is een uitleg gegeven van blockchain-technologie. Daarbij is geïdentificeerd welke kenmerken van de bitcoin-blockchain gelden voor alle blockchains en welke kenmerken verband houden met de specifieke doelstellingen van bitcoin en met het feit dat het bij bitcoin gaat om virtueel geld. Vervolgens is een aantal toepassingen van blockchain besproken, waarbij de mogelijke juridische aspecten zijn aangestipt.

29 www.nrc.nl/nieuws/2016/06/21/banken-zien-blockchain-ook-wel-zitten-2834727-a1506434.

30 C.E. Drion, 'De historie van Haviltex', *NJB* 2016/1391, afl. 28, p. 1961. In het licht van zoveel uitleg-fijnzinnigheid lijkt het smart contract ineens een stuk minder smart.

31 Zie over dit onderwerp uitgebreid M.B. Voulon, *Automatisch contracteren* (diss. Leiden), Leiden University Press 2010, p. 241-286 en J.J. Linnemann en J.B. Schmaal, 'Intelligent contracteren', *Computerrecht*, 2010/6, 175.

32 Zie www.coindesk.com/ethereum-dao-hacker-getting-away-classic/.