Van oud naar nieuw: van internet naar smart contracts en van mensen naar code (I)

Mr. T.J. de Graaf*

1. Inleiding

Smart contracts staan de laatste tijd volop in de belangstelling. Smart contracts zijn, kort gezegd, *"little programs that execute 'if this happens then do that'"*.[1] Smart contracts die op de blockchain draaien, dat wil zeggen gedecentraliseerd worden opgeslagen op en uitgevoerd door computers die met elkaar in een netwerk verbonden zijn, zijn lastiger kort en krachtig te definiëren. Ze zouden aan de hand van een aantal kenmerken omschreven kunnen worden als softwareprogramma's:

1. die zonder tussenpersoon gedecentraliseerd op diverse computers (*nodes*) worden opgeslagen en uitgevoerd, die onderling in een netwerk met elkaar verbonden zijn en aan verschillende personen toebehoren (*disintermediated peer-to-peer*);
2. die uit zichzelf '*if this then that*' commando's uitvoeren waardoor (contractuele) afspraken automatisch worden uitgevoerd (*autonomous & self-executing*);
3. ten aanzien waarvan (als opschortende voorwaarde) geldt dat verschuiving van waarde (vaak: betaling door afnemer aan leverancier) alleen kan plaatsvinden als minimaal 51% van de nodes hebben vastgesteld dat de uitvoering van het smart contract heeft plaatsgevonden conform de in het smart contract geprogrammeerde eisen (vaak: verrichten van de prestatie door leverancier) (*consensus*); en
4. waarvan de vastlegging in een grootboek op alle nodes plaats vindt, publiek is en niet kan worden gewijzigd (*secure public ledger with a single source of truth*).

Zoals bij elke nieuwe technologische ontwikkeling rijzen een aantal juridische vragen.[2] Teneinde deze nieuwe ontwikkeling en de mogelijkheden daarvan beter te kunnen begrijpen, zal ik de ontwikkeling van smart contracts in historisch perspectief plaatsen en gaandeweg afzetten tegen bestaande technische en juridische vormen waarmee soortgelijke resultaten kunnen worden bereikt: internet, bankrekeningen, bankgaranties en waardepapieren. Dat doe ik aan de hand van een chronologische bespreking. Eerst bespreek ik hoe het internet opkwam en welke wetgeving werd uitgevaardigd om e-commerce via internet juridisch te ondersteunen en reguleren. Vervolgens leg ik uit hoe blockchaintechnologie en smart contracts werken en hoe het gebruik ervan leidt tot een verschuiving van vertrouwen (van vertrouwen in mensen naar vertrouwen in code). Aan de hand van een bespreking van The DAO hack en de daarbij gerezen problemen vraag ik me af of die vertrouwensverschuiving zo absoluut is als vaak wordt gedacht. Tot slot onderzoek ik in hoeverre de bestaande internetregelgeving kan helpen de ontwikkeling van smart contracts te ondersteunen en zo niet, wat daar wel voor nodig is. Dit alles doe ik aan de hand van Ethereum, een smart contracts platform waaraan iedereen deel kan nemen (*permissionless*) en dat op dit moment toonaangevend is.[3] Daarbij ga ik ervan uit

* Universitair docent burgerlijk recht aan de Universiteit Leiden.

1. https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/. Zie voor een beknopte uitleg van smart contracts ook https://www.uitlegblockchain.nl/smart-contracts/.
2. Zie in algemene zin T.F.E. Tjong Tjin Tai, 'Smart contracts en het recht', *NJB* 2017-3, p. 176-182, J.J. Linnemann, 'Juridische aspecten van (toepassingen van) blockchain', *Computerrecht* 2017-6, p. 319-324, H. Schuringa, 'Enkele civielrechtelijke aspecten van blockchain', *Computerrecht* 2017-6, p. 372-378 en Smart Contract Werkgroep - Dutch Blockchain Coaltion, 'Smart contracts als specifieke toepassing van de blockchain-technologie. Eerste verkenning naar vragen rond wet- en regelgeving en opleidingsbehoeften als gevolg van blockchain en meer specifiek smart contracts', 2017, https://www.dutchdigitaldelta.nl/uploads/pdf/Smart-contract-rapport-DBC.pdf. Zie over uitleg van smart contracts J.B Schmaal & E.M. van Genuchten, 'Smart contracts en de Haviltex-norm', *Tijdschrift voor Internetrecht* 2017-1, p. 12-17 en over smart contracts en onvoorziene omstandigheden Eefke Janssen, 'Smart contracts en onvoorziene omstandigheden', in: H.N. Schelhaas, A.I. Schreuder & K.K.E.C.T. Swinnen, *Nieuwe technologieën, nieuw privaatrecht?*, Den Haag: Boom juridisch 2017.
3. Zie voor een beknopte uitleg van Ethereum https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/ en voor een uitgebreidere http://www.ethdocs.org/. In deze bijdrage worden *permissioned* blockchain platformen niet besproken. Dat zijn blockchain platformen waarvan de toegang kan worden afgeschermd door middel van een zogeheten *access control layer* en per gebruiker (of gebruikerssoort) verschillende bevoegdheden kunnen worden toegekend.

dat de smart contracts uitsluitend op de blockchain worden opgeslagen en daar worden uitgevoerd, zonder met de fysieke wereld (*off chain*) verbonden te zijn.

2. De opmars van het internet

Rond 1990 begint de opmars van het internet. Naast vele andere toepassingen biedt het internet, in tegenstelling tot gesloten EDI-systemen,[4] ondernemingen mogelijkheden geautomatiseerd producten en diensten aan te bieden en te verkopen aan wederpartijen met wie voordien geen rechtsverhouding bestond (*one-to-many e-commerce*). In algemene zin rijst de vraag of overheden zich wel met internet zouden mogen bemoeien. Zo schrijft John Perry Barlow, één van de oprichters van de Electronic Frontier Foundation, in 1996 in zijn Declaration of the Independence of Cyberspace:

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. … Where there are real conflicts, where there are wrongs, we will identify them and address them by our means."[5]

De wensen van Barlow komen niet uit, integendeel. De Europese Unie neemt, nog afgezien van privacy- en sectorspecifieke regelgeving, gedetailleerde richtlijnen aan op grond waarvan zij, via haar lidstaten, met name internetverkoop minutieus regelde teneinde e-commerce juridisch te faciliteren en tegelijkertijd zwakkere partijen te beschermen. Voorbeelden zijn de (minimumharmonisatie) B2C richtlijn koop op afstand uit 1997[6] (inmiddels vervangen door de (maximumharmonisatie) B2C richtlijn consumentenrechten uit 2011[7]) en de B2B&B2C richtlijn elektronische handel uit 2000.[8] In de toekomst krijgen we waarschijnlijk te maken met een richtlijn digitale inhoud en een richtlijn verkoop (die aanvankelijk alleen zag op online verkoop, maar waarvan het toepassingsbereik inmiddels is uitgebreid tot ook andere vormen van verkoop).[9]

2.1. Informatieverplichtingen en verplichtingen met betrekking tot de wijze van contracteren

Op grond van de richtlijn elektronische handel en de richtlijn consumentenrechten wordt het leveranciers die via internet producten of diensten willen verkopen makkelijker gemaakt. Een country-of-origin principe wordt geïntroduceerd waardoor ze bijvoorbeeld voor het opstarten van hun activiteiten alleen hoeven te voldoen aan de regelgeving van het land van waaruit zij handelen (art. 3 lid 4 Richtlijn elektronische handel, geïmplementeerd in art. V-1 Aanpassingswet elektronische handel[10]). En lidstaten worden gedwongen het elektronisch sluiten van overeenkomsten mogelijk te maken (art. 9 lid 1 Richtlijn elektronische handel, geïmplementeerd in art. 6:227a BW, waarover hieronder meer).

Tegelijkertijd wordt een grote hoeveelheid verplichtingen aan de leverancier opgelegd. Zo moet de leverancier veel informatie verschaffen over zichzelf, de aangeboden producten en diensten, de wijze waarop het contracteerproces is ingericht en uitgevoerd, en de door hem gehanteerde (contracts- en algemene) voorwaarden (art. 3:15d, 6:234 lid 2, 6:227b, 6:227c lid 2 BW en, in B2C-situaties, 6:230m en 6:230v BW). Ook moet de leverancier zijn contracteerproces op zodanige wijze inrichten dat invoerfouten kunnen worden hersteld (art. 6:227c lid 1 BW) en de afnemer een aanbod niet kan aanvaarden dan nadat hij erop is gewezen dat zijn bestelling een betalingsverplichting inhoudt (in B2C-situaties, art. 6:230v lid 3 BW). Consumenten hebben veel dwingendrechtelijke bescherming, waaronder het recht de op afstand gesloten overeenkomsten te herroepen (zonder reden te ontbinden) gedurende een termijn van (inmiddels) 14 dagen na aflevering van de producten of het sluiten van de dienstenovereenkomst (art. 6:230o BW). Die regelgeving strekt in grotendeels toe de (veronderstelde) achterstand die een afnemer heeft bij

4. Zie over EDI: R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht (diss. KU Nijmegen)*, Deventer: W.E.J. Tjeenk Willink 1999, hoofdstuk 2.1, p. 13-14 die EDI als volgt definieert: "EDI is de elektronische uitwisseling van gestructureerde en genormeerde berichten tussen informatiesystemen" en M.B. Voulon, *Automatisch contracteren (diss. Leiden)*, Leiden: Leiden University Press 2010, hoofdstuk 2.2.1, p. 11-12 voor het volgende voorbeeld: kassières scannen in een supermarkt producten in hun kassasystemen (*Points of Sale*), die PoS versturen die gegevens naar het warehouse management systeem (WMS) van de supermarkt en het WMS plaatst automatisch elektronisch een order bij de toeleverancier als de voorraad van het product onder een vooraf ingesteld niveau daalt.
5. https://www.eff.org/cyberspace-independence.
6. Richtlijn koop op afstand 97/7/EG.
7. Richtlijn consumentenrechten 2011/83/EU.
8. Richtlijn elektronische handel 2000/31/EG.
9. Voorstel voor een richtlijn digitale inhoud COM(2015) 624 final respectievelijk Voorstel voor een richtlijn verkoop van goederen COM(2017) 637 final, waarover onder andere V. Mak, 'Op weg naar een Europese 'Digital Single Market'. Twee nieuwe richtlijnvoorstellen voor het Europees contractenrecht', *NJB* 2016-8, p. 518-524 en M.B.M. Loos, 'Europese harmonisatie van online en op afstand verkoop van zaken en de levering van digitale inhoud (I) en (II)', *NtEr* 2016-3 & 4, p. 114-120 & 148-156.
10. Aanpassingswet richtlijn elektronische handel, *Stb.* 2004/210.

een internetkoop ten opzichte van een koop bij een *brick-and-mortar* winkel weg te nemen. Overigens, om een idee te geven van de mate van detail: om dit alles in het BW te implementeren, had de Nederlandse wetgever rond de 5,500 woorden nodig, zo'n 12 A4'tjes.[11]

2.2. Gelijkstelling elektronische overeenkomsten met schriftelijke overeenkomsten waarvoor een vormvereiste geldt

Naarmate steeds vaker elektronisch overeenkomsten worden gesloten maakt men zich zorgen over de rechtsgeldigheid daarvan. Sommige regelgeving eist immers dat overeenkomsten schriftelijk worden gesloten. Schending van zo'n vormvereiste leidt, tenzij uit de wet anders voortvloeit, tot nietigheid (art. 3:39 BW). In Nederland valt te denken aan de cessie- (art. 3:94 BW) en pandakte (onder andere art. 3:237 lid 1 en 3:239 lid 1 BW) waarvoor een schriftelijkheids- en ondertekeningsvereiste geldt (art. 156 lid 1 Rv). Op EU-niveau wordt geprobeerd barrières voor het elektronisch contracteren weg te (doen) nemen en het elektronisch contracteren te (doen) vergemakkelijken.

Zo verplicht de net genoemde richtlijn elektronische handel uit 2000 de lidstaten er voor te zorgen "dat hun rechtsstelsel het sluiten van contracten langs elektronisch weg mogelijk maakt" en dienen die lidstaten zich ervan te vergewissen "dat de regels met betrekking tot de totstandkoming van contracten geen belemmering vormen voor het gebruik van langs elektronische weg gesloten contracten, noch ertoe leiden dat dergelijke contracten, omdat zij langs elektronische weg tot stand zijn gekomen, zonder rechtsgevolg blijven en niet rechtsgeldig zijn." (art. 9 lid 1, waarvan zijn uitgezonderd de contracten opgenomen in art. 9 lid 2, zoals de transportakte die nodig is voor de levering van een woonhuis). Nederland gaf daaraan gevolg door het opnemen van art. 6:227a BW, waarvan de hoofdregel (opgenomen in lid 1) luidt:

> "Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is totstandgekomen en a. raadpleegbaar door partijen is; b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is; c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld."

Voor alle duidelijkheid, art. 6:227a BW geldt alleen als de wet voorschrijft dat een overeenkomst "slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt". Bij gebreke aan zo'n vormvereiste is een elektronisch gesloten overeenkomst net zo geldig als een schriftelijke of mondelinge overeenkomst.

2.3. Gelijkstelling elektronische handtekening met schriftelijke handtekening

Op EU-niveau komt ook regelgeving tot stand om elektronische handtekeningen gelijk te stellen met schriftelijke handtekeningen: in 1999 door de Richtlijn elektronische handtekeningen,[12] die in 2016 is vervangen door de eIDAS verordening.[13] Interessant aan die verordening is dat alleen een bepaalde vorm van een elektronische handtekening, de gekwalificeerde elektronische handtekening, *automatisch* dezelfde rechtsgevolgen heeft als een handgeschreven handtekening (art. 25 lid 2 eIDAS verordening).[14] De meest gebruikte vorm van zo'n gekwalificeerde elektronische handtekening kan als volgt worden omschreven.[15]

Ten eerste, een elektronische handtekening bestaat uit een sleutelpaar: een publieke en een private sleutel. Wil een persoon (afzender) een bericht sturen naar een andere persoon (geadresseerde), dan versleutelt de afzender het bericht met de publieke sleutel van de geadresseerde en ontsleutelt de geadresseerde dat bericht na ontvangst met gebruikmaking van zijn private sleutel. Wordt het bericht onderschept, dan kan de onderschepper niets met dat bericht.

11. Het gaat daarbij om art. 3:15d-f, 6:227a-c, 6:267 lid 1, 6:234 lid 2 en afdeling 6.5.2B, paragrafen 1, 3 en 5 BW.
12. Richtlijn elektronische handtekeningen 1999/93/EG.
13. eIDAS verordening 910/2014.
14. Zie voor een uitleg van elektronische handtekeningen en de gelijkstelling tussen schriftelijke en elektronische handtekeningen Marten Voulon, 'Digitalisering en het Nederlands Burgerlijk Wetboek', in: Vereniging voor de vergelijkende studie van het recht van België en Nederland, *Preadviezen 2017. Digitalisering en digitale producten in het privaatrecht*, Den Haag: Boom juridisch 2017, p. 311-348.
15. Naast de gekwalificeerde elektronische handtekening bestaan de geavanceerde en de 'gewone' elektronische handtekening. Daaraan hoeft niet een hierna te beschrijven certificatiedienstverlener of andere TTP te pas te komen. Die handtekeningen hebben echter alleen hetzelfde rechtsgevolg als een schriftelijke handtekening als "de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval." (art. 3:15a BW). Van een *automatische* gelijkstelling tussen zo'n geavanceerde/gewone elektronische handtekening en een schriftelijk handtekening is in zo'n geval dus geen sprake.

Zonder private sleutel van de geadresseerde kan hij het bericht niet ontsleutelen en ziet hij dus een bericht vol onbegrijpelijke tekens. Ook wijzigen en daarna doorsturen van het bericht van de geadresseerde heeft geen zin. Als de geadresseerde het aldus gewijzigde bericht probeert te ontsleutelen, zal de technologie hem erop attenderen dat het bericht is gewijzigd.

Ten tweede moet die handtekening van de geadresseerde, wil zij gekwalificeerd zijn, zijn gebaseerd op een daarop betrekking hebbend certificaat dat is afgegeven door een certificatiedienstverlener:[16] een verlener van vertrouwensdiensten die een certificaat uitgeeft en die door een toezichthoudend orgaan de status van gekwalificeerde heeft gekregen (art. 3 onderdeel 20, 19, 16, 15 en 14 eIAS Verordening). Zo'n certificatiedienstverlener is een voorbeeld van een zogeheten *trusted third party* (TTP). Die certificatiedienstverlener heeft geverifieerd dat de persoon die een certificaat wil gebruiken degene is die hij zegt te zijn (dat zeggen heet: identificeren, dat verifiëren heet: authenticeren[17]) en geeft vervolgens een certificaat uit dat gekoppeld is aan diens publieke sleutel. Heeft de afzender met behulp van zo'n certificaat geverifieerd dat de publieke sleutel (waarmee hij het bericht wil versleutelen) bij de geadresseerde hoort en versleutelt en verstuurt de afzender vervolgens een bericht naar de geadresseerde met gebruikmaking van zo'n publieke sleutel, dan kan de afzender er (in theorie) vanuit gaan dat alleen die geadresseerde het bericht kan lezen. Dit hele systeem wordt ook wel *public key infrastructure* (PKI) genoemd.

2.4. Bewijsrechtelijke gelijkstelling elektronische onderhandse akte met schriftelijke

Bepaalde regelgeving verbindt bewijsrechtelijke voordelen aan schriftelijke stukken ondertekend met een schriftelijke handtekening. Zo leveren ondertekende geschriften, bestemd om tot bewijs te dienen (dat zijn onderhandse akten in de zin van art. 156 lid 3 Rv) dwingend bewijs op (art. 157 lid 2 Rv): ze worden kort gezegd geacht waar te zijn, behoudens tegenbewijs (art. 151 Rv). Het gaat daarbij met name om twee eisen: geschrift en schriftelijke handtekening. Ook in dat kader is wetgeving gekomen om elektronisch met schriftelijk gelijk te stellen, in dit geval een elektronische onderhandse akte met een elektronische. Aan het vereiste van geschrift kan in elektronische zin worden voldaan als aan de eisen van art. 156a lid 1 Rv wordt voldaan.[18] Dat artikel bepaalt:

> "Onderhandse akten kunnen op een andere wijze dan bij geschrift worden opgemaakt op zodanige wijze dat het degene ten behoeve van wie de akte bewijs oplevert, in staat stelt om de inhoud van de akte op te slaan op een wijze die deze inhoud toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de akte bestemd is te dienen, en die een ongewijzigde reproductie van de inhoud van de akte mogelijk maakt."

Aan het vereiste van ondertekening kan in elektronische zin worden voldaan als aan de eisen van art. 25 lid 2 eIDAS verordening althans art. 3:15a BW wordt voldaan (zie hierboven).

2.5. Tussenconclusie

Het combineren van alle bovenstaande internetregelgeving levert het volgende beeld op. Ten eerste, de regelgeving legt een grote nadruk op informatie die de elektronische handelende leverancier moet verschaffen alsmede op de wijze waarop hij zijn contracteerproces moet inrichten en moet contracteren. Door aldus zoveel nadruk te leggen op de leverancier, maakt de (Europese) wetgever duidelijk dat hij vertrouwen in de leverancier en diens handelen wil scheppen.[19] Ten tweede, voor overeenkomsten waarvoor geen vormvereiste geldt (zoals bijna alle overeenkomsten), kan alleen door middel van een elektronische onderhandse akte van het bewijsrechtelijke voordeel van dwingend bewijs (art. 157 jo. 151 Rv) worden geprofiteerd als voldaan is aan de vereisten van art. 156 Rv (vereisten akte) in combinatie met art. 156a lid 1 Rv (gelijkstelling elektronisch bestand met schriftelijk stuk) en art. 25 lid 2 eIDAS verordening althans art. 3:15a BW (gelijksteling elektronische handtekening met

16. Deze term is afkomstig uit de oude Richtlijn elektronische handtekeningen om een dienstverlener te omschrijven die certificaten afgeeft in verband met elektronische handtekeningen (art. 2 onder 11 Richtlijn elektronische handtekeningen) en zal in deze bijdrage gemakshalve worden gebruikt omdat de eIDAS verordening slechts de meer generieke omschrijving 'gekwalificeerde verlener van vertrouwensdiensten' kent (art. 3 onder 19 eIDAS verordening).
17. Dat kan bijvoorbeeld door een persoon langs te laten komen, vast te stellen dat zijn gezicht overeenkomt met de foto op zijn paspoort en de schriftelijke handtekening die hij ter plekke zet te vergelijken met de handtekening in zijn paspoort. Gewoon fysiek dus.
18. Deze bepaling is in ons BW terecht gekomen als gevolg van de Wet elektronisch rechtsverkeer, *Stb.* 2010/222.
19. Vergelijk *Kamerstukken II*, 2001-2002, 28 197, nr. 3 (MvA), p. 24: "De artikelen 10 en 11 van de richtlijn beogen de afnemers door middel van een informatieplicht voor de dienstverlener en beginselen die in acht moeten worden genomen bij het plaatsen van een order met behulp van technologische middelen meer duidelijkheid en transparantie te verschaffen, waardoor het vertrouwen van afnemers, en in het bijzonder de consument, in het elektronisch zaken doen wordt verhoogd."

schriftelijke handtekening). Ten derde, voor overeenkomsten waarvoor een vormvereiste van een akte geldt (zoals de cessieakte ex art. 3:94 BW), moet (strikt genomen) voor het elektronische equivalent daarnaast worden voldaan aan de eisen gesteld in art. 6:227a BW (gelijkstelling van elektronische overeenkomsten met schriftelijke in geval van een vormvereiste).[20] Opvallend bij de twee laatste punten is vooral dat in de beschreven situaties alleen dan van een *automatische* gelijkstelling van een elektronisch bestand met een schriftelijk stuk sprake kan zijn als sprake is van een gekwalificeerde elektronische handtekening en daarvoor de tussenkomst van een *trusted third party* (TTP, in dit geval een certificatiedienstverlener) is vereist. Door aldus zoveel nadruk te leggen op een TTP, maakt de (Europese) wetgever duidelijk dat hij met name vertrouwen schept in het centraliseren van vertrouwen, te weten bij een TTP. Deze nadruk op de leverancier en een TTP ontbreekt bij smart contracts, zoals hierna zal blijken.

3. Smart contracts doen hun intrede

De bedenker van smart contracts, Nick Szabo, definieert smart contracts in 1994 als volgt:

> "A smart contract is a computerized transaction protocol that executes the terms of a contract."

en voegde daaraan toe:

> "The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries."[21]

Neem het voorbeeld van *smart property* dat Szabo toen ook noemde: een op afbetaling gekochte auto waarmee niet kan worden gereden als de koper niet op de daarvoor afgesproken tijdstippen aan zijn betalingsverplichtingen heeft voldaan. Zonder blockchain zou die wens als volgt worden geïmplementeerd. De verkoper laat een startonderbreker in de auto van de koper installeren, zoals dat ook bij een alcoholslot gebeurt. Voordat de auto start, checkt de startonderbreker met gebruikmaking van mobiele datatransmissie bij de bank van de verkoper (of, neutraler, bij een TTP op wiens escrow rekening de koper steeds betaalt) of de koper alles heeft betaald wat hij op dat moment moet betalen. Is dat wel zo, start de auto. Is dat niet zo, start de auto niet. Deze wijze van implementatie vereist vertrouwen in de verkoper (dat hij geen misbruik maakt van de technologie door zelf een instructie te geven aan de startonderbreker om niet te starten) en diens bank of een TTP (die vaststelt of alle op dat moment vereiste betalingen door hem zijn ontvangen).

Het vernieuwende aan smart contracts op de blockchain in combinatie met cryptocurrency is dat de uitvoering van het contract (het verrichten van de prestatie en de daartegenover staande betaling van waarde) automatisch en decentraal gebeurt. Anders dan bij gecentraliseerd handelen van één leverancier (*server-based*, web 2.0), vindt uitvoering nu gedecentraliseerd plaats (*peer-to-peer*, web 3.0). Daardoor kunnen de ideeën van Szabo, die het bovenstaande schreef toen er nog geen blockchain was, veel beter in de praktijk worden gebracht. Een eenvoudig voorbeeld kan dit verduidelijken. Iemand wil graag samen met iemand anders een 'raad het getal onder de tien' spel spelen.[22] Hij stelt zich dat spel als volgt voor: twee personen leggen bij het begin van ieder spel evenveel geld in, het smart contract kiest een willekeurig getal en de spelers raden net zo lang tot dat ze het door het smart contract gekozen getal raden. Degene die het getal raadt, krijgt zijn inleg terug en wint de inleg van de ander. Als het spel via een (gecentraliseerde) internetsite zou worden gespeeld, zouden de spelers ten eerste veel vertrouwen moeten hebben: in elkaar dat de ander ook inlegt en in het internetbedrijf dat het bedrijf uitbetaalt aan de winnaar en niet vals speelt. Ten tweede zouden transactiekosten moeten worden betaald, door de spelers aan het internetbedrijf en door het internetbedrijf aan een *payment service provider* (PSP) die de inleg ontvangt en

20. Volgens R.E. van Esch, 'De vermogensrechtelijke gelijkstelling van een elektronisch gegevensbestand met een geschrift', Computerrecht 2011/123 kunnen partijen, ingeval zij een elektronische onderhandse akte hebben gebruikt, "zich voor de gelijkstelling met het vormvereiste van een (ondertekend) geschrift beroepen op zowel art. 6:227a BW als art. 156a Rv." Hij geeft in dat geval de voorkeur aan een beroep op art. 156a Rv omdat aan de daarin gestelde eisen gemakkelijker kan worden voldaan dan aan de in art. 6:227a BW gestelde eisen.
21. Hoewel het lastig is een betrouwbare bron te vinden voor Szabo's artikel, lijken velen ervan uit te gaan dat het hier te vinden is: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.
22. Het voorbeeld is bewust zo gekozen, dat het eenvoudig is en het hele contract kan worden vastgelegd in en de uitvoering daarvan op de blockchain (*on chain*) plaats kan vinden. Complexiteit die ontstaat door de uitvoering van het smart contract afhankelijk te laten zijn van een beslissing van een derde in de fysieke wereld (*off chain* door middel van een zogeheten *oracle*) kan daardoor buiten beschouwing worden gelaten.

uitbetaalt. Ten derde hebben beide spelers pech als het internetbedrijf gehackt wordt of uit de lucht is (*single point of failure*). Door gebruik te maken van een smart contracts platform, Ethereum, is dat vertrouwen niet nodig, kunnen de transactiekosten worden gereduceerd en is er geen *single point of failure*. Ethereum werkt door de volgende combinatie van cryptocurrency en smart contracts.

3.1. Het cryptocurrency deel

Voor het gebruik van smart contracts is Ether nodig. Ether is een cryptocurrency (net zoals bitcoin[23]), die net als andere cryptocurrencies door middel van hierna uit te leggen blockchaintechnologie functioneert en die wordt gehouden in een zogeheten *Externally Owned Account* (EOA, hierna ook wel: "account") (vergelijk: een bankrekening) met een uniek adres (vergelijk: een bankrekeningnummer) waarnaartoe en vanwaaruit Ether kan worden overgemaakt.[24] De toegang tot ieder account is beveiligd door middel van een sleutelcombinatie, bestaande uit een publieke en een private sleutel. Die sleutelcombinatie is opgenomen in een zogeheten *key file*, een tekstbestand dat in een text editor kan worden geopend en bekeken. Het privésleutel gedeelte van de key file is versleuteld en kan alleen worden ontsleuteld door middel van een wachtwoord dat wordt gekozen bij het aanmaken van het account. Om toegang te krijgen tot een account om vervolgens Ether over te maken zijn dus twee dingen nodig: de keyfile (iets dat je hebt) en het wachtwoord waarmee het privé sleutel gedeelte van de keyfile is versleuteld (iets dat je weet). Het unieke adres waarnaartoe en vanwaaruit Ether kan worden overgemaakt, bestaat uit de laatste 20 bytes van de publieke sleutel.

Wil iemand Ether naar een account overmaken, dan maakt hij het over naar dat unieke adres. Vervolgens kan alleen degene die beschikt over de keyfile en het wachtwoord waarmee het privé sleutel gedeelte van de keyfile is versleuteld, bij de naar dat account overgemaakte Ether. Tot dusver is het overmaken naar één Ethereum account naar een ander Ethereum account vergelijkbaar met het overmaken van giraal geld van de ene naar de andere bankrekening met *two-factor authentication*. Ook daarvoor is nodig: iets dat je hebt (smartphone&app) en iets dat je weet (wachtwoord/pincode). Er is echter één belangrijk verschil tussen beiden, en dat heeft te maken met het feit dat het openen van accounts en het overmaken van Ether van en naar accounts gedecentraliseerd in de blockchain plaats vindt, in plaats van centraal op de servers van één of meerdere banken. Dat verschil vergt wat meer uitleg.

De Ethereum blockchain houdt de actuele status van elk account bij, evenals alle transacties tussen die accounts. Dat gebeurt in een gedecentraliseerd grootboek (*distributed ledger*). Dat grootboek staat op alle computers die aan het Ethereum netwerk deelnemen (*nodes*). Op al die nodes draait zogeheten *client software*,[25] waaronder de zogenaamde *Ethereum Virtual Machine* (EVM). De EVM zorgt er onder andere voor dat het grootboek tussen alle nodes gesynchroniseerd wordt en dus iedere node uitgaat van dezelfde realiteit (*shared single source of truth*). Voor het synchroniseren wordt gebruik gemaakt van een *peer-to-peer network protocol*, denk aan BitTorrent. Zodra iemand een transactie wil verrichten, zeg het overmaken van x Ether van account a naar account b, moet worden vastgesteld of er x Ether in account a beschikbaar is en zo ja, x Ether van account a naar account b kan worden overgemaakt. Dat gebeurt door middel van miners. Dat zijn nodes die volledig automatisch verschillende transacties samen verpakken in *blocks* en er door het volledig automatisch oplossen van een ingewikkelde cryptografische puzzel naar streven de eerste te zijn wiens block aan de blockchain wordt toegevoegd. Degene die als eerste de puzzel heeft opgelost[26] (winnaar van de *speed competition*) wint het recht voor te stellen om het aldus geminde block aan de blockchain toe te voegen. Hij heet daarom *proposer*.

Vervolgens krijgen de andere nodes te kans te bewijzen dat de proposer het niet bij het juiste eind heeft (in de *quality competition*).[27] Als een van de nodes bewijst dat de proposer ongelijk heeft (en dus de quality competition wint), begint het proces van voor af aan en hebben alle nodes weer de kans proposer te worden. Als minimaal 51% van de nodes het met elkaar eens zijn dat de proposer het bij het juiste eind heeft, is sprake van consensus. Op dat moment wordt die transactie, samen met de andere geverifi-

23. Zie voor een simpele uitleg van bitcoin https://medium.freecodecamp.org/explain-bitcoin-like-im-five-73b4257ac833.
24. http://www.ethdocs.org/en/latest/account-management.html#accounts.
25. Er zijn zo'n acht verschillende implementaties van clients, zie http://ethdocs.org/en/latest/ethereum-clients/choosing-a-client.html.
26. In de praktijk werken miners samen in zogeheten *mining pools* en delen de eventuele winst die zij ontvangen (zie hierna) als hun pool wint.
27. Ik heb niet kunnen vaststellen of Ethereum net als bitcoin met een quality competition werkt, maar ga er toch van uit dat dat zo is.

eerde transacties in dat block, als block toegevoegd aan de blockchain. Dat block is onveranderbaar in die zin, dat elk block door middel van een zogeheten *hash pointer* terugverwijst naar het vorige block. Daardoor is elke wijziging in een block meteen zichtbaar en zal zo'n wijziging niet worden geaccepteerd. De proposer wiens block aan de blockchain wordt toegevoegd wordt daarvoor beloond doordat hij (i) nieuwe Ether krijgt van het netwerk (*block reward*) en (ii) *gas*,[28] zeg maar transactiekosten, ontvangt van degenen wiens transacties in het toegevoegde block zitten.

Deze gedecentraliseerde vorm van het bereiken van consensus zorgt ervoor dat Ethereum transacties bijna foutloos geschieden, de data die is opgeslagen in de blockchain niet kan worden gewijzigd en Ethereum bijna nooit uit de lucht is. Immers, als één of meerdere nodes gehackt worden of uit de lucht zijn, blijven de overige nodes gewoon functioneren en gaan ze door met hun werk alsof er niets aan de hand is. Dat lijkt op wat er met het internet gebeurt als een internetknooppunt eruit ligt, maar is fundamenteel anders bij een bank. Als een bank wordt gehackt of uit de lucht is, is er een risico dat zijn rekeninghouders (tijdelijk of zelfs permanent) niet meer over hun geld kunnen beschikken. Tot dusver past deze beschrijving grosso modo op vrijwel iedere cryptocurrency, waaronder bitcoin. Wat Ethereum bijzonder maakt en onderscheidt van een cryptocurrency sec, is het smart contracts deel.

3.2. Het smart contracts deel

Het Ethereum platform biedt de mogelijkheid een smart contract volledig automatisch en decentraal (peer-to-peer) te laten uitvoeren. Toegepast op het 'raad het getal onder de tien' spel werkt dit als volgt. Een programmeur programmeert het spel als een smart contract in bijvoorbeeld Solidity (een programmeertaal die speciaal is ontworpen voor het maken van smart contracts) of een andere gebruikersvriendelijke programmeertaal die gemodelleerd is op bestaande programmeertalen zoals JavaScript of Python.[29] De code waarin de programmeur het spel heeft geprogrammeerd heet de *source code* of, in Ethereum termen, de *contract source*. Zodra de contract source van het smart contract klaar is, gebruikt de programmeur software (een *compiler*) om de contract source om te zetten (compileren) naar een code die door de Ethereum Virtual Machine (EVM) op alle nodes kan worden uitgevoerd (*EVM bytecode*).[30] Die EVM bytecode wordt vervolgens, in de regel met behulp van een browser (de Mist browser), in de blockchain gezet (*gedeployed*) waardoor het decentraal op alle nodes zal worden opgeslagen. Die EVM bytecode en (in de regel ook) de contract source zijn openbaar.[31] Iedereen kan die code inzien en beoordelen of de code klopt en juist zal worden uitgevoerd.

Belangrijk bij dit alles is dat in het smart contract een zogeheten *contract account* wordt geprogrammeerd.[32] Op het contract account kan, net als op een EOA, Ether worden ontvangen en overgemaakt. Het overmaken van Ether van een EOA naar een contract account is ook de eerste stap die nodig is om de uitvoering van een smart contract op de Ethereum blockchain in gang te zetten. Zonder zo'n eerste overmaking gebeurt er niets. In ons voorbeeld 'start' het smart contract dus pas als één van de deelnemers zijn inleg vanuit zijn EOA naar het smart contract heeft overgemaakt en die inleg door het smart contract is ontvangen. Als dat is gebeurd, wacht het smart contract vervolgens op de ontvangst van de Ether van de andere deelnemer, waarna het spel begint. Zit de inleg eenmaal in het smart contract, dan kan alleen de uitvoering van de code tot uitbetaling leiden. In ons voorbeeld maakt de code de inleg van beiden over naar het EOA van degene die het spel wint. En de code is zelfuitvoerend en staat gedecentraliseerd in de blockchain, dus kan niet meer worden stopgezet door de programmeur van die code of de deelnemers aan het spel.[33] Het smart contract maakt de gewonnen Ether vanuit het

28. Gas is een cryptofuel waarvan de prijs wordt bepaald aan de hand van de beschikbare rekenkracht van de nodes. Gas kan worden gekocht met Ether. Gas is verschuldigd om nodes te belonen voor het verifiëren van transacties, maar ook om ervoor te zorgen dat de nodes niet overbelast worden door DDoS aanvallen (het door meerdere computers tegelijkertijd bombarderen van een node met onzin verkeer) of het berekenen van infinite loops (het tot in het oneindige uitvoeren van dezelfde berekening).
29. Zie voor een experiment om het opschortingsrecht van een koper in code te vertalen T.F.E. Tjong Tjin Tai, 'Formalizing contract law for smart contracts (September 18, 2017)', *Tilburg Private Law Working Paper Series* 2017-6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038800.
30. http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html#what-is-a-contract.
31. De code kan worden gecheckt op https://etherscan.io. Hoewel het mogelijk is de EVM bytecode zonder de contract source in de blockchain te deployen, is dat eigenlijk niet de bedoeling omdat alleen met behulp van de contract source kan worden geverifieerd of de code klopt en juist zal worden uitgevoerd.
32. http://ethdocs.org/en/latest/account-management.html#accounts.
33. Stopzetten kan alleen als een mogelijkheid daartoe in het smart contract is geprogrammeerd en dat is iets dat zich, zoals hierna zal blijken, zich slecht verdraagt met de filosofie van een smart contract.

contract account over naar het EOA van de winnaar zodra minimaal 51% (=consensus) van de nodes het met elkaar eens dat de code juist is uitgevoerd (waardoor zo'n vorm van gokken ook wel aangeduid als *provably fair gambling*).

Dat de code zichzelf uitvoert en niet kan worden gestopt, wordt in de woorden van Lessig omschreven als '*code is law*' en in de woorden van Wright en De Filippi als '*lex cryptographia*'.[34] Het is belangrijk dat te benadrukken: als er eenmaal Ether in het smart contract zit, dan bepaalt *enkel en alleen* de uitvoering van de zelfuitvoerende code of en zo ja, wanneer en naar welk EOA Ether wordt overgemaakt. Dus, bij een EOA kan een persoon beschikken over de Ether in dat account, bij een smart contract komt die 'bevoegdheid' niet toe aan een persoon, maar aan de code.

(wordt vervolgd)

34. L. Lessig, *Code version 2.0,* New York: Basic Books 2006, http://codev2.cc respectievelijk Aaron Wright & Primavera De Filippi, 'Decentralized blockchain technology and the rise of lex cryptographia', *SSRN* 2015-March 10, https://ssrn.com/abstract=2580664.