Van oud naar nieuw: van internet naar smart contracts en van mensen naar code (II, slot)

4. Vertrouwen in wie en wat?

Het feit dat smart contracts op de blockchain decentraal draaien en zelfuitvoerend zijn, heeft veel gevolgen voor het vertrouwen dat partijen stellen in de wijze waarop hun overeenkomst wordt uitgevoerd. Daarbij verschuift immers het vertrouwen in personen naar vertrouwen in code, zoals hierna wordt toegelicht.

Mr. T.J. de Graaf*

4.1. Trustless of people en context

Aangezien voor de correcte uitvoering van een smart contract geen vertrouwen meer nodig is in personen, noch in de wederpartij noch in een tussenpersoon zoals een bank, borg of (andere) TTP, worden smart contracts ook wel aangeduid als *trustless*. Dat klopt als daarmee wordt gedoeld op trustless ten aanzien van personen dat ze doen wat ze zijn overeengekomen. Immers, als de code klopt, maakt het niet uit of de wederpartij betrouwbaar is of niet. Het verschil tussen vertrouwen in personen (*trust by communication*) en vertrouwen in code (*trust by computation*) komt ook tot uitdrukking in de verschillende manieren waarop op het internet en de blockchain gebruik wordt gemaakt van publieke en private sleutelparen. Bij het public key infrastructure (PKI) publieke en private sleutelpaar waar de eIDAS-verordening van uit gaat, ligt de nadruk op een gecentraliseerde TTP (certificatiedienstverlener) om personen te authenticeren (verifiëren dat ze zijn wie ze zeggen te zijn). In de blockchain komt er echter geen derde (persoon) aan te pas bij het overmaken van Ether door gebruikmaking van het betreffende publieke en private sleutelpaar. Vanuit het perspectief van Ethereum hoeft dat ook niet, want voor het veilig ontvangen en betalen van Ether is slechts relevant dat er een EOA is waarnaartoe en vanwaaruit veilig Ether kan worden overgemaakt, niet welke persoon daar achter schuilt en of die betrouwbaar is.

Vanuit het oogpunt van rechtszekerheid is dit vertrouwen in code winst; hoe smart contracts code zichzelf uitvoert is immers voorspelbaarder dan hoe personen handelen. Door bij de uitvoering van een smart contract geen menselijke tussenkomst meer mogelijk te maken, ontstaat iets dat meer rechtszekerheid biedt dan bijvoorbeeld een abstracte bankgarantie die betaalbaar is op eerste verzoek (*abstract first demand bank guarantee*), het traditionele instrument bij uitstek dat wordt gebruikt als betalingszekerheid met zo min mogelijk menselijke beoordelingsvrijheid gewenst is.

Op het eerste gezicht biedt zo'n bankgarantie veel zekerheid. Immers, de bank mag en hoeft alleen te controleren of de door de begunstigde van de bankgarantie overgelegde documenten (bijvoorbeeld *statement of default*) formeel (*face value*) overeenstemmen met de daaraan in de garantie gestelde eisen (beginsel van formele controle). Daarbij mag en hoeft de bank alleen te betalen als strikt aan alle in de bankgarantie opgenomen betalingsvoorwaarden is voldaan (beginsel van strikte conformiteit).[35] Toch blijft de uitbetaling van een bankgarantie afhankelijk van het al dan niet handelen van een bank, iets waar hard-core smart contracts voorstanders van zullen gruwen omdat niet (althans niet meteen) wordt betaald als de bank failliet gaat of als de bank, om hem moverende redenen, niet uitbetaalt. De zekerheid dat een smart contract uitbetaalt zonder afhankelijk te zijn van de beschikkingsbevoegdheid en (potentiële) willekeur van een derde, vormt de eerste reden dat een smart contract meer (betalings)zekerheid biedt dan een abstracte bankgarantie op eerste verzoek.

* Universitair docent burgerlijk recht aan de Universiteit Leiden.

35. R.I.V.F. Bertrams, 'De bankgarantie als zekerheidsinstrument bij internationaal contracteren', in: B. Wessels & T.H.M. van Wechem, *Contracteren in de internationale praktijk,* Deventer: Kluwer 2011, nr. 1.9.1.

De redenen waarom een bank niet uitbetaalt, kunnen overigens zeer wel valide zijn. Zo hoeft en mag een bank niet onder een abstracte bankgarantie op eerste verzoek uit te betalen als sprake is van fraude, bedrog of willekeur.[36] Dat brengt ons tot een tweede reden waarom smart contracts meer (betalings)zekerheid bieden dan traditionele instrumenten zoals zo'n bankgarantie: decontextualisering. Bij de beoordeling of sprake is van fraude, zal een bank immers, vaak gevoed door zijn klant, kijken naar de context: de omstandigheden buiten de letterlijke tekst van de bankgarantie. Of een rechter doet dat in kort geding en ge- of verbiedt de bank om uit te betalen. Ook die afhankelijkheid wordt in een smart contract geëcarteerd.[37] De code volgt haar 'if this, then that' structuur: als aan het 'this' is voldaan, dan volgt automatisch het 'that' of, in het voorbeeld van het 'raad het getal onder de tien' spel: als een speler het getal heeft geraden, volgt uitbetaling van de inleg van beide spelers aan hem. De omstandigheden van het geval doen daarbij niet ter zake,[38] zelfs niet als sprake is van fraude.

De vergelijking tussen smart contracts en abstracte bankgaranties betaalbaar op eerste verzoek is in zoverre goed dat in beide gevallen partijen gebruik maken van instrumenten om te abstraheren van de onderliggende rechtsverhouding teneinde (betalings)zekerheid te creëren; bij smart contracts door code op de blockchain te deployen, bij bankgaranties door TTP's (banken) in te schakelen. Ook bij de uitgifte van waardepapieren (zoals wissels, cheques en cognossementen) gebeurt iets soortgelijks. Uitgangspunt bij het uitgeven van een waardepapier is echter dat de uitgifte tussen de oorspronkelijke contractspartijen niet leidt tot het in het leven roepen van een abstracte verbintenis; de onderliggende rechtsverhouding blijft van belang.[39] Ook in dat opzicht leidt het deployen van smart contracts in de blockchain tot decontextualisering, terwijl partijen dat in hun onderliggende verhouding in de regel niet bereiken door het uitgeven van een waardepapier.

4.2. Trustful of code, maar bij The DAO hack toch niet?

Terug naar het credo 'code is law'. Als we dat zouden willen accepteren, dan veronderstelt dat dat we kunnen vaststellen of de code klopt. Dat legt echter een ander probleem bloot: hoe weten we dat die code klopt? Natuurlijk is het in de regel zo dat smart contracts volledig transparant zijn en iedereen de code kan controleren, maar wie beschikt over de expertise om dat te doen? In het voorbeeld van het 'raad het getal onder de tien' spel, is dat voor een gemiddelde programmeur niet zo moeilijk, maar naarmate de complexiteit van het smart contract toeneemt, zal het steeds lastiger worden die code te controleren, zeker voor de gemiddelde gebruiker. Dus zal die gebruiker een derde inschakelen om die code te controleren. Ironischerwijs is dat nu juist waar blockchain-adepten met hun disintermediation-mantra van af willen: vertrouwen in derden. En toch kan het vertrouwen in derden ook bij smart contracts een rol spelen en wel vooraf om code te controleren en in uitzonderingsgevallen zelfs achteraf om ongewenste gevolgen terug te draaien.

Neem de door Slock.it ontwikkelde *Decentralised Autonomous Organisation* (DAO), The DAO geheten. The DAO was een organisatie die uitsluitend als Ethereum smart contract bestond en op 30 april 2016 het levens-/cryptolicht zag. In het The DAO smart contract konden investeerders Ether storten in ruil voor verhandelbare tokens waarmee ze zeggenschap verwierven (*Initial Coin Offering* (ICO)[40]). Zodra voldoende Ether was opgehaald, begon The DAO echt te functioneren. Een bedrijf dat funding wilde aantrekken zou een businessplan indienen en als de meerderheid van de stemmen zou instemmen met het businessplan, zou vanuit het smart contract automatisch Ether naar het Externally Owned Account (EOA, zie hierboven) van het bedrijf worden overgemaakt. Een bug in de smart contracts code werd echter door een hacker ge-/misbruikt, waardoor op 17/18 juni 2016 al één derde van de funding (3,6 miljoen Ether) aan The DAO was onttrokken en geparkeerd in een ander smart contract, de zogeheten child DAO.[41] Volgens het Ethereum smart contract kon de Ether vanuit het child DAO pas na verloop van een moratorium van 28 dagen naar een EOA worden overgemaakt.

36. HR 26-3-2004, ECLI:NL:PHR:2004:AO2778, *NJ* 2004, 309 (*Anthea Yachting/ABN AMRO*) en R.I.V.F. Bertrams, 'De bankgarantie als zekerheidsinstrument bij internationaal contracteren', in: B. Wessels & T.H.M. van Wechem, *Contracteren in de internationale praktijk*, Deventer: Wolters Kluwer 2011, nr. 1.10.
37. Zie waarschuwend, in de zin dat (teveel) nadelige effecten moeten worden voorkomen, T.F.E. Tjong Tjin Tai, 'De redelijke derde en de blockchain', *WPNR* 2015/7072, p. 671-672.
38. Die omstandigheden doen alleen dan ter zake als ze in het smart contract zijn geprogrammeerd.
39. Zie voor cognossementen art. 8:441 lid 2 BW, voor wissels HR 25-4-2008, *NJ* 2008, 261 (*Somotex/Wiener*) en in algemene zin R. Zwitser, *Order- en toonderpapieren (Monografieën BW nr. A28)*, Deventer: Wolters Kluwer 2017, nr. 19. Michiel Spanjaart, *Vorderingsrechten uit cognossement (diss EUR). Deel 18 NTHR-reeks*, Zutphen: Uitgeverij Paris 2012, nr. 3.3 wijst erop dat partijen daar door middel van een *superseding clause* van kunnen afwijken.
40. https://bitcoinmagazine.com/guides/what-ico/.
41. https://www.coindesk.com/understanding-dao-hack-journalists/ en in algemene zin https://en.wikipedia.org/wiki/The_DAO_(organization).

Saillant detail is echter dat de makers van de The DAO code, Slock.it, in hun blog van 5 april 2016 trots lieten weten dat één van 's-werelds "leading security audit companies" Deja Vu Security een security review van het generieke The DAO smart contracts framework had verricht, waarbij "no stone was left unturned during those five whole days of security analysis".[42] Daarmee staat overigens niet vast dat Deja Vu Security iets over het hoofd heeft gezien. Onduidelijk is immers wat de scope en uitkomst van de audit was. Ook liet Deja Vu Security weten dat zij geen mededelingen zou doen zonder schriftelijke toestemming van Slock.it.[43] Duidelijk is wel dat Slock.it een derde inschakelde om haar code te controleren en door haar blog post over de audit vermoedelijk anderen ervan probeerde te overtuigen dat de code veilig was.

Hoewel met The DAO hack het Ethereum protocol niet werd gecompromitteerd, nam de Ethereum foundation (de maker van Ethereum) het op zich om de 'gestolen' Ether terug te krijgen. Nadat een minder ingrijpende *soft fork* vanwege veiligheidsproblemen niet een goed idee bleek,[44] bedacht de foundation een *hard fork* waardoor alle Ether die in The DAO en de child DAO zat in een nieuw smart contract (het *WithdrawDAO recovery contract*) terecht zou komen.[45] Dat nieuwe smart contract zou als enige doel hebben om de daarnaar overgemaakte Ether uit te betalen aan alle token houders (met een wisselkoers van 100 DAO tokens = 1 Ether). Die hard fork zou worden geïmplementeerd door middel van updates van de Ethereum clients (software die, zoals gezegd, op alle nodes draait en waarmee de nodes aan het peer-to-peer Ethereum netwerk deelnemen).[46] De Ethereum foundation vroeg de *community* te stemmen over het automatisch uitrollen van die hard fork met behulp van Carbonvote, een ad hoc stemprogramma waarmee iedere Ether houder met één stem per gehouden Ether kon stemmen. Uiteindelijk bleek 87% van de stemmen vóór de hard fork,[47] werd die fork uitgerold en mine'den al snel 85% van de miners op die fork.[48]

De manier waarop de hard fork werd voorgesteld, erover werd besloten en werd uitgerold bracht een aantal problemen aan het licht. De meeste aandacht ging uit naar de stammenstrijd tussen enerzijds degenen die de hack als misbruik kwalificeerden, haar tegen wilden gaan en de hard fork als gerechtigheid zagen, en anderzijds degenen die de hack niet als misbruik zagen, maar als slim gebruik van transparante code en de hard fork als misbruik van het systeem kwalificeerden. Parallellen werden getrokken met de bankencrisis en de *bail-out* van banken die *too-big-to-fail* waren. Het voorkomen van nog zo'n crisis en de daaropvolgende bail-out vormden juist een belangrijke aanleiding om de blockchain te ontwikkelen. De ironie wil dat de Ethereum hard fork wel erg op zo'n bail-out leek. Ook werden er vraagtekens geplaatst bij de wijze waarop de stemming bekend werd gemaakt (blog post, Twitter en Reddit), de duur van de stemming (24 uur) en het percentage van het totale aantal Ether houders dat een stem uitbracht.[49]

Vanuit juridisch oogpunt intrigeert niet zozeer de rechtvaardigheid van de uitkomst,[50] maar vooral de wijze van geschillenbeslechting tussen de hacker en de rest. Kennelijk achtten de Ethereum foundation en de softwareontwikkelaars van de clients zich gerechtigd om de regels van het spel te veranderen na daartoe, geheel onverplicht en wellicht zelfs op twijfelachtige wijze, de backing van een al dan niet representatief deel

42. https://blog.slock.it/deja-vu-dao-smart-contracts-audit-results-d26bc088e32e.
43. "*Hi Everyone, Adam Cecchetti CEO of Deja vu Security here. For legal and professional reasons Deja vu Security does not discuss details of any customer interaction, engagement, or audit without written consent from said customer. Please contact representatives from Slock.it for additional details*." https://www.reddit.com/r/ethereum/comments/4ota1q/the_truth_about_the_security_audit_stephen_tual/.
44. De soft fork werd voorgesteld in https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/ en https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/, en zou tot gevolg hebben dat de 'gestolen' Ether zou worden bevroren waardoor het niet zou kunnen worden uitgegeven. Het veiligheidsprobleem staat beschreven in http://hackingdistributed.com/2016/06/28/ethereum-soft-fork-dos-vector/ en https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork/.
45. Zie voor een algemene uitleg van forks https://www.coindesk.com/short-guide-bitcoin-forks-explained/ en voor een uitleg van de Ethereum DAO hard fork https://www.coindesk.com/understanding-dao-hack-journalists/.
46. Voor de meest gebruikte en door de Ethereum foundation uitgebrachte client (go-ethereum ofwel geth) zie https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/ en voor de steun van Slock.it zie https://blog.slock.it/what-the-fork-really-means-6fe573ac31dd.
47. http://v1.carbonvote.com.
48. https://blog.ethereum.org/2016/07/20/hard-fork-completed/. Een deel van de nodes die het met deze fork niet eens waren, hebben Ethereum Classic opgericht en zijn daarmee verder gegaan onder het motto code is law: https://ethereumclassic.github.io.
49. https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/.
50. Vergelijk voor een rechtvaardige uitkomst bij een geval van misbruik HR 19-10-2007, *NJ* 2007, 565 (*Vodafone/ETC*), in dat geval bereikt door gebruik te maken van het uitleg-leerstuk.

van de community te hebben verworven. Vervolgens was het aan de nodes van het netwerk om de update te installeren als zij het met die 'beslissing' eens waren en volgens de nieuwe regels van het spel verder wilden werken, of niet te installeren als zij het met die 'beslissing' niet eens waren en volgens de oude regels van het spel verder wilden werken. Opmerkelijk is ook dat door de Ethereum foundation de stemmen van Ether houders bepalend werden geacht, en niet de stemmen van de The DAO token houders en degenen die om funding vroegen (de deelnemers aan The DAO, de contractspartijen). Indachtig de hiervoor geciteerde oproep van Barlow valt een lans te breken voor het zelfregulerende vermogen van deze nieuwe vorm van technologie (in dit geval voor zelfregulering door de Ethereum foundation, de community en de softwareontwikkelaars van de clients), maar vanuit juridisch oogpunt valt deze vorm van zelfregulering (bijna) niet te billijken. Het recht is er immers (juist) om in individuele gevallen eigenrichting te voorkomen, zo nodig een minderheid te beschermen tegen een meerderheid en op z'n minst te waarborgen dat besluitvormingsprocedures op procedureel rechtvaardige wijze verlopen.

Door de rechtvaardigheid van de uitkomst zal al snel worden gedacht dat het doel de middelen heiligt, maar de geschetste risico's die inherent zijn aan deze wijze van zelfregulerend ingrijpen moeten daarbij niet uit het oog worden verloren. Die risico's kunnen nog beter zichtbaar worden gemaakt door een aantal (deels retorische) vragen over een lastiger scenario te stellen. Wat zou er zijn gebeurd als een kleine financier zijn inleg door een hack zou dreigen te verliezen aan de overige financiers? Overheerst dan het gevoel van rechtvaardigheid of de mantra code is law? En zouden de Ethereum foundation en de softwareontwikkelaars van de clients, in feite derden, zich in zo'n geval geroepen voelen in te grijpen? Zo ja, zouden zij dat handelen voor- of achteraf willen legitimeren en zo ja, op welke wijze? Dit wetende, hoeveel vertrouwen zouden kleine financiers hebben in zo'n DAO en wat betekent dat voor de geloofwaardigheid en (daarmee) het succes van die DAO?

In ieder geval blijkt uit het voorgaande dat zelfs in de blockchainwereld code niet law is en in uitzonderingsgevallen door derden ook aan zelfuitvoerende smart contracts een halt kan worden toegeroepen. Vertrouwen in code werd ineens halverwege de rit vervangen door vertrouwen in de developers, community en nodes. Ook bleek, en dat is zorgelijker, dat het zelfregulerend ingrijpen vanuit juridisch oogpunt twijfelachtig werd gelegitimeerd. De deelnemers aan Ethereum smart contracts, zo zagen we bij The DAO hard fork, zagen hun geschil niet door een rechter opgelost, maar door de Ethereum foundation, de softwareontwikkelaars van de clients en de meerderheid van de nodes.

5. Toepasbaarheid van internetregelgeving

Hoe past, met het voorgaande in het achterhoofd, de bestaande internetregelgeving op smart contracts? Die vraag is actueel omdat de Europese Commissie onlangs liet weten "the right enabling environment" voor blockchain te willen creëren.[51] Zodra gevraagd wordt iets nieuws in het leven te roepen, ligt het voor de hand eerst te onderzoeken of met het bestaande kan worden volstaan. In juridisch opzicht vergt dat dus een onderzoek naar vraag of bestaande internetregelgeving toepasbaar is op smart contracts. In dat kader is het nuttig terug te grijpen op de besproken ratio van de internetregeling. In wezen strekt die regelgeving ertoe de (veronderstelde) achterstand die een afnemer heeft bij een internetkoop ten opzichte van een koop bij een *brick-and-mortar* winkel weg te nemen en het vertrouwen van de afnemer in (het handelen van) de leverancier te versterken. Dat gebeurt deels door de leverancier te verplichten aan diens (potentiële) afnemers allerlei informatie over zichzelf en de wijze van contracteren te verstrekken, deels door hem te verplichten zijn contracteerproces op een bepaalde manier in te richten en de afnemer herroepingsrechten toe te kennen (richtlijn elektronische handel en richtlijn consumentenrechten). Ook wordt de (veronderstelde) onzekerheid die partijen hebben met betrekking tot de rechtsgeldigheid en bewijskracht van elektronische documenten ten opzichte van schriftelijke documenten met behulp van regelgeving opgelost (richtlijn elektronische handel, eIDAS-verordening en wet elektronisch rechtsverkeer). Dat gebeurt door de tussenkomst van een derde (TTP) te vereisen om een elektronisch document met elektronische hand-

51. Commissioner for the Digital Economy and Society Mariya Gabriel zei daarover: "*I see blockchain as a game changer and I want Europe to be at the forefront of its development. We need to establish the right enabling environment - a Digital Single Market for blockchain so that all citizens can benefit, instead of a patchwork of initiatives. The EU Blockchain Observatory and Forum is an important step in that direction.*", persbericht Europese Commissie, European Commission launches the EU Blockchain Observatory and Forum, 1-2-2018, http://europa.eu/rapid/press-release_IP-18-521_en.htm. Ook in Engeland wordt nagedacht over "*reviewing the current English legal and regulatory framework to ensure that it facilitates the use of smart contracts*.", zie https://www.lawcom.gov.uk/project/13th-programme-of-law-reform/. In Nederland experimenteert de Nederlandse overheid met blockchain, zie https://www.blockchainpilots.nl.

tekening automatisch gelijk te stellen met een schriftelijk document met een schriftelijke handtekening.

Veel commerciële partijen die op het internet producten of diensten willen verkopen hebben er belang bij aan die regelgeving te voldoen. Traditioneel verkopen zij meer als afnemers hen vertrouwen. En een manier om vertrouwen te winnen, is door informatie over jezelf te verschaffen en je aan de internetregelgeving te houden. De noodzaak dat te doen, is er niet of nauwelijks bij smart contracts. Doordat smart contracts zichzelf uitvoeren is vertrouwen in de code van belang, niet vertrouwen in de leverancier. Als de leverancier de noodzaak niet voelt zich aan die regelgeving te houden en (dus) ook geen informatie over zichzelf verschaft, heeft dat tot gevolg dat handhaving feitelijk moeilijk, zo niet onmogelijk is. Als de leverancier niet vindbaar is, kan er immers lastig tegen hem worden geprocedeerd en verhaal worden gezocht op zijn vermogensbestanddelen. Daar komt bij dat smart contracts zichzelf automatisch uitvoeren en de afnemer daardoor om technische redenen geen mogelijkheden heeft zijn rechten uit te oefenen tot aan het moment waarop het smart contract is uitgevoerd. Dat betekent bijvoorbeeld dat de uitoefening van opschortingsrechten illusoir is. Dit alles maakt dat er door smart contracts een machtsverschuiving plaats vindt, door Raskin aangeduid als "*subordination of state authority to individual autonomy*".[52] Zo lang de uitvoering van het smart contract helemaal on chain plaatsvindt, kunnen contractspartijen zich dus relatief makkelijk onttrekken aan regelgeving en overheden.[53] In dat geval komt de wens van Barlow toch nog uit.

Gelet op deze technische en feitelijke beperkingen om van het standaardrepertoire aan remedies en handhaving gebruik te maken, is het belangrijk(er) te bepalen hoe het vertrouwen in code kan worden vergroot. Immers, als code law is, dan ontstaat het risico dat *code-savvy* personen misbruik maken van *code-naive* personen[54] of, neutraler gezegd, er fouten in de code zitten die leiden tot ongewenste gevolgen die niet althans moeilijk zijn terug te draaien. Het ligt voor de hand dat risico in te dammen door op de kwaliteit van de code te focussen. Immers, als de code doet wat partijen ervan verwachten, ontstaan in de regel geen problemen en is er ook geen noodzaak achteraf te corrigeren. In zoverre verschuift de aandacht van het oplossen van problemen (voor, tijdens of na de uitvoering van de overeenkomst) naar het voorkomen daarvan (in de precontractuele fase). Dat betekent dat programmeurs samen met juristen betere smart contracts moeten maken. Dat betekent ook dat het verifiëren van de betrouwbaarheid van de code van cruciaal belang is. Aangezien de meeste afnemer dat niet zelf kunnen doen, zullen zij daarvoor een derde, een auditor, willen inschakelen. In dat licht zou aan de eIDAS-verordening[55] een deel kunnen worden toegevoegd over het auditen van smart contracts code. Het gebrek aan verhaalsmogelijkheden van de afnemer op diens leverancier zou vervolgens kunnen worden gecompenseerd door het introduceren van een aansprakelijkheidsregime ten aanzien van de auditor als de audit niet juist blijkt te zijn uitgevoerd. Ook zou aan de eIDAS-verordening een regime kunnen worden toegevoegd waarmee smart contracts op de blockchain waarnaar cryptocurrency is overgemaakt met gebruikmaking van sleutelparen zonder TTP, wat betreft rechtsgeldigheid[56] en bewijskracht automatisch gelijk worden gesteld met schriftelijke overeenkomsten met schriftelijke handtekeningen, al dan niet na een goedkeurende verklaring door een auditor.[57] In feite wordt de code dan eerst proefgedraaid, keurt de auditor de code goed en wordt de code dan pas voor echte transacties gebruikt. Gelijkenissen met acceptietesten doemen op. Ironischerwijs introduceren we door dit alles weer een TTP (de auditor), terwijl smart contractsadapten zo'n TTP juist willen ecarteren. Wellicht zou zo'n TTP op termijn geëlektronificeerd en geblockchained kunnen worden.

52. Max Raskin, 'The law and legality of smart contracts', *Georgetown Law Technology Review* 2017-1:2, p. 315, https://ssrn.com/abstract=2959166.
53. Zodra de uitvoering deels off chain (in de fysieke wereld) plaatsvindt, ontstaan er meer mogelijkheden voor juridische interventie. In dat geval bestaan smart contracts niet een juridisch vacuum, net zo min als cyberspace is afgesneden van de echte wereld, zoals verwoord door Martin von Haller Groenbaek, 'Blockchain 2.0, smart contracts and legal challenges', *SCL magazine* 2016-June/July, https://www.scl.org/articles/3668-blockchain-2-0-smart-contracts-and-legal-challenges.
54. Zie in waarschuwende zin Bill Marino & Ari Juels, 'Setting standards for altering and undoing smart contracts', *Rule technologies. 10th International Symposium, RuleML 2016, NY, USA, July 6-9* 2016-LNCS9718, p. 151-166, https://link.springer.com/content/pdf/10.1007%2F978-3-319-42019-6.pdf en Marcella Atzori, 'Blockchain technology and decentralized governance: is the state still necessary?', *SSRN* 2015-December 1, https://ssrn.com/abstract=2709713.
55. Vergelijk E. Valgaeren & J.J. Linnemann, 'Blockchain ontketend', *Computerrecht* 2017-6, p. 346, die menen dat door de blockchain mogelijkerwijs een deel van de eIDAS-regels overbodig worden of uit worden gehold, maar dat aspecten die door die eIAS-verordening worden gereguleerd als inspiratiebron kunnen dienen om bepaalde aspecten van de blockchain te reguleren.
56. Voor zover voor de betreffende overeenkomst een wettelijk vormvereiste geldt.
57. Op welke wijze aan deze ideeën uitvoering kan worden gegeven, gaat het bestek van deze bijdrage te buiten.

Het alternatief zou zijn de internetregelgeving één-op–één van toepassing te laten zijn op smart contracts en de daarbij betrokken partijen. Met name als de leveranciers zich daaraan houden, zouden de mogelijkheden toenemen voor afnemers om invoerfouten te herstellen en zich bij wanprestatie tot de leveranciers te wenden. Echter, in veel gevallen hebben leveranciers er, zoals gezegd, geen of nauwelijks belang bij zich te houden aan die regelgeving en kunnen afnemers en leveranciers niet of nauwelijks handhavend optreden. Leveranciers zijn immers vaak onbekend (waardoor het niet/nauwelijks mogelijks is tegen hen te procederen) en hun voor verhaal vatbare vermogensbestanddelen zijn vaak onbekend (waardoor verhaal niet/nauwelijks mogelijk is). In die gevallen is het beter door voornoemde audits en voornoemd gelijkstellingsregime het vertrouwen in de code te vergroten dan te vertrouwen op handhaving die niet of nauwelijks mogelijk blijkt.

6. Conclusie

Smart contracts verschillen, zo zagen we, wezenlijk van e-commerce via internet. Juridisch relevant is vooral dat in het internettijdperk veel vertrouwen wordt geplaatst in mensen en hun handelen (met name de leverancier, banken en (andere) trusted third parties). Door daarop betrekking hebbende internetregelgeving krijgt de afnemer middelen in handen om tegen een wanpresterende leverancier op te treden en wordt elektronisch met schriftelijk gelijk gesteld om aan vormvoorschriften te voldoen en gebruik te maken van bewijsrechtelijke voordelen. Dat vertrouwen in personen wordt bij smart contracts vervangen door vertrouwen in code. Die code is voor de gemiddelde gebruiker echter niet te begrijpen. The DAO hack liet zien dat als het faliekant mis gaat, uiteindelijk toch personen (moeten) ingrijpen, maar dat daar allerlei technische en juridische haken en ogen aan kleven. Weliswaar kan worden geprobeerd bestaande internetregelgeving op smart contracts toe te passen, maar die is daar lastig op toepasbaar. Dat komt door het verschil in uitgangspunten: vertrouwen in personen versus vertrouwen in code. Dat komt ook door technische en feitelijke beletselen: technisch gezien valt er vóór uitvoering door contractspartijen niet of nauwelijks in te grijpen en feitelijk gezien is het ná uitvoering niet of nauwelijks mogelijk om tegen een onbekende te procederen en zijn (dientengevolge) voor verhaal vatbare vermogensbestanddelen niet of nauwelijks te vinden. Al met al heeft het bij smart contracts meer zin problemen te voorkomen dan ze achteraf te corrigeren. Om die reden bepleit ik dat programmeurs samen met juristen betere smart contracts maken en dat de regelgever zich focust op regelgeving met betrekking tot het auditen van smart contracts code door trusted third parties en het wat betreft rechtsgeldigheid en bewijskracht automatisch gelijkstellen van smart contracts met schriftelijke overeenkomsten met schriftelijke handtekeningen. Hopelijk zal dat ertoe bijdragen permissionless smart contracts op de blockchain een grote vlucht te laten nemen.