Smart contracts en het recht

Tjong Tjin Tai, Eric

Published in:
NJB

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Smart contracts en het recht

Eric Tjong Tjin Tai[1]

Smart contracts bieden de mogelijkheid om automatisch, zonder centrale autoriteit, complexe betalingstransacties uit te laten voeren. De gedachte is nu dat dit een bedreiging vormt voor de gehele praktijk van contractjuristen. Teneinde dit te onderzoeken wordt in dit artikel ingegaan op wat smart contracts zijn, uitgaande van de bitcoin en de blockchain. Aan de hand van de eerste ervaringen worden daarna diverse kanttekeningen geplaatst en toekomstmogelijkheden geschetst.

1. Inleiding

In de algemene media vindt men regelmatig berichten over aandacht van het traditionele bedrijfsleven voor wat wordt genoemd de 'blockchain'. In het bijzonder banken tonen zich hoogst geïnteresseerd: zij investeren in wat men in bredere zin aanduidt als 'fintech'. Een van de aandachtsgebieden betreft zogenaamde 'smart contracts'.[2] In dit artikel zal ik dit aandachtsgebied aan een preliminaire juridische analyse onderwerpen.

Wat zijn smart contracts? In het Nederlands zou men spreken over 'slimme contracten', of beter, 'zelfexecuterende overeenkomsten'. Deze zijn te beschouwen als een verdere ontwikkeling op basis van de blockchaintechnologie. Smart contracts bieden de mogelijkheid om automatisch, zonder centrale autoriteit, complexe betalingstransacties uit te laten voeren. De gedachte is nu dat dit een bedreiging vormt voor de gehele praktijk van contractjuristen. Teneinde dit te onderzoeken zal ik eerst uitleggen wat smart contracts zijn, uitgaande van bitcoin en de blockchain. Aan de hand van de eerste ervaringen plaats ik diverse kanttekeningen en schets ik toekomstmogelijkheden.

2. Bitcoin en de blockchain

Bitcoin heeft veel aandacht ontvangen in de populaire media en in de (rechts)wetenschap.[3] Zij bieden de functionaliteit van banken maar zonder enkele van de bezwaren die sommigen tegen het bankwezen hebben.

Banken werken door het bijhouden van een centrale administratie van tegoeden, waar klanten door middel van overboekingen (transacties) over kunnen beschikken. Daarmee staat eenduidig vast wat het tegoed op ieder moment is. Als het tegoed te laag is, wordt de transactie geweigerd. De centrale administratie is echter niet alleen positief.

Ten eerste zijn banken in zoverre kwetsbaar voor hackers, dat men maar toegang tot één computer hoeft te verkrijgen om frauduleuze transacties uitgevoerd te krijgen.[4] Een voorbeeld is de hack van de Centrale Bank van Bangladesh.[5]

Ten tweede is het systeem kwetsbaar voor aanvallen tegen het centrale systeem: een Ddos aanval maakt het onmogelijk om gedurende de aanval betalingen uit te voeren, omdat klanten geen verbinding krijgen met de centrale server.[6]

Ten derde heeft de centrale autoriteit de mogelijkheid om transacties tegen te houden of te beïnvloeden, controles uit te voeren. Banken zijn niet louter neutrale doorgeefluiken, zij functioneren ook als poortwachters. Dit betekent bijvoorbeeld dat zij verdachte transacties kunnen en onder omstandigheden ook moeten tegenhouden.[7] Partijen kunnen dit onwenselijk vinden, bijvoorbeeld als een bank weigert onder een bankgarantie te betalen ofschoon strikt genomen aan de voorwaarden voor betaling is voldaan.[8] Deze controle kan overigens ook welkom zijn: de hack van de Centrale Bank van Bangladesh werd ontdekt doordat een andere bank een van de transacties verdacht vond.

De techniek van bitcoin en de blockchain omzeilt deze bezwaren: door de gedistribueerde aard van verwerking van transacties is dit niet kwetsbaar voor aanvallen en menselijke interventie.[9] Sommigen zien bitcoin als een voorbeeld van een nieuw soort organisaties: Decentralised Autonomous Organisations (DAO's).[10] In essentie werkt het als volgt.[11]

Er is een netwerk van computers (aangeduid als nodes), waarbij elke node een compleet register van alle transacties, en daarmee de tegoeden aan bitcoin, bijhoudt (de blockchain). Als een gebruiker een transactie het netwerk instuurt wordt dit door alle nodes geverifieerd en door het gehele netwerk gecommuniceerd. Maar hoe wordt nu de administratie bijgewerkt? Het antwoord is dat er niet één eenduidige administratie is. Ieder node

kan proberen de blockchain bij te werken, door een reeks transacties te verzamelen in een nieuw blok. Maar om dit blok geaccepteerd te krijgen moet er een ingewikkelde wiskundige 'puzzel' worden opgelost. Het is niet van te voren te zeggen welke node de eerste is die dit oplost. De winnaar krijgt als beloning enkele nieuwe bitcoin. Het nieuwe blok wordt verspreid door het netwerk, en daarmee is dan de blockchain overal bijgewerkt. Als toevallig een tweede node de puzzel ook oplost kan het zijn dat er twee verschillende blokken zijn. In dat geval is er tijdelijk een ambigue situatie. Deze lost zich op doordat de nodes steeds verder werken aan de langste nieuwe keten van blokken, en na enige tijd zal altijd een van de ketens langer zijn en blijven dan de andere.

Smart contract-initiatieven nemen het blockchain-mechanisme van bitcoin over en gebruiken dit vooral om een systeem voor contracten op te zetten

De blockchain is dus een gedistribueerd register van betalingstransacties, dat op gedistribueerde wijze wordt bijgewerkt. Door een ingenieuze koppeling tussen enerzijds de verificatie en acceptatie van transacties en anderzijds de toekenning van nieuwe bitcoin wordt consensus bereikt over welke transacties aanvaard zijn en wat de saldi zijn.

Het bitcoin-systeem zelf is primair bedoeld voor betalingstransacties, dat wil zeggen: A betaalt X bitcoin aan B. Deze transacties worden uitgevoerd door de nodes die onderdeel uitmaken van het bitcoin netwerk. Deze nodes kunnen echter, als de script-taal van de munteenheid dit toelaat, ook ingewikkelder transacties uitvoeren. Bijvoorbeeld: A betaalt X aan B over drie maanden. Of: A betaalt X aan B als voorwaarde Y is vervuld. *Smart contract*-initiatieven nemen het blockchain-mechanisme van bitcoin over en gebruiken dit niet zozeer ten behoeve van valuta maar juist en vooral om een systeem voor contracten op te zetten.

3. Smart contracts

De term 'smart contracts' stamt uit de jaren negentig.[12] De oorspronkelijke gedachte was dat de toegang tot zaken als auto's en huizen zou kunnen worden gecontroleerd via een ingebouwde computer waar contractuele regels in zouden worden opgeslagen en uitgevoerd, die bijvoorbeeld de toegang van de lessor tot een zaak zouden afsluiten na betaling van de laatste termijn, of omgekeerd juist de toegang van de verkrijger afsluiten indien deze in verzuim is met betaling.[13] Door de ontwikkeling op basis van bitcoin is de nadruk komen te liggen op de implementatie in programmatuur, code. Een kernachtige omschrijving van wat men er nu onder verstaat is: 'they are little programs that execute "if this happens then do that", run and verified by many computers to ensure trustworthiness.'[14]

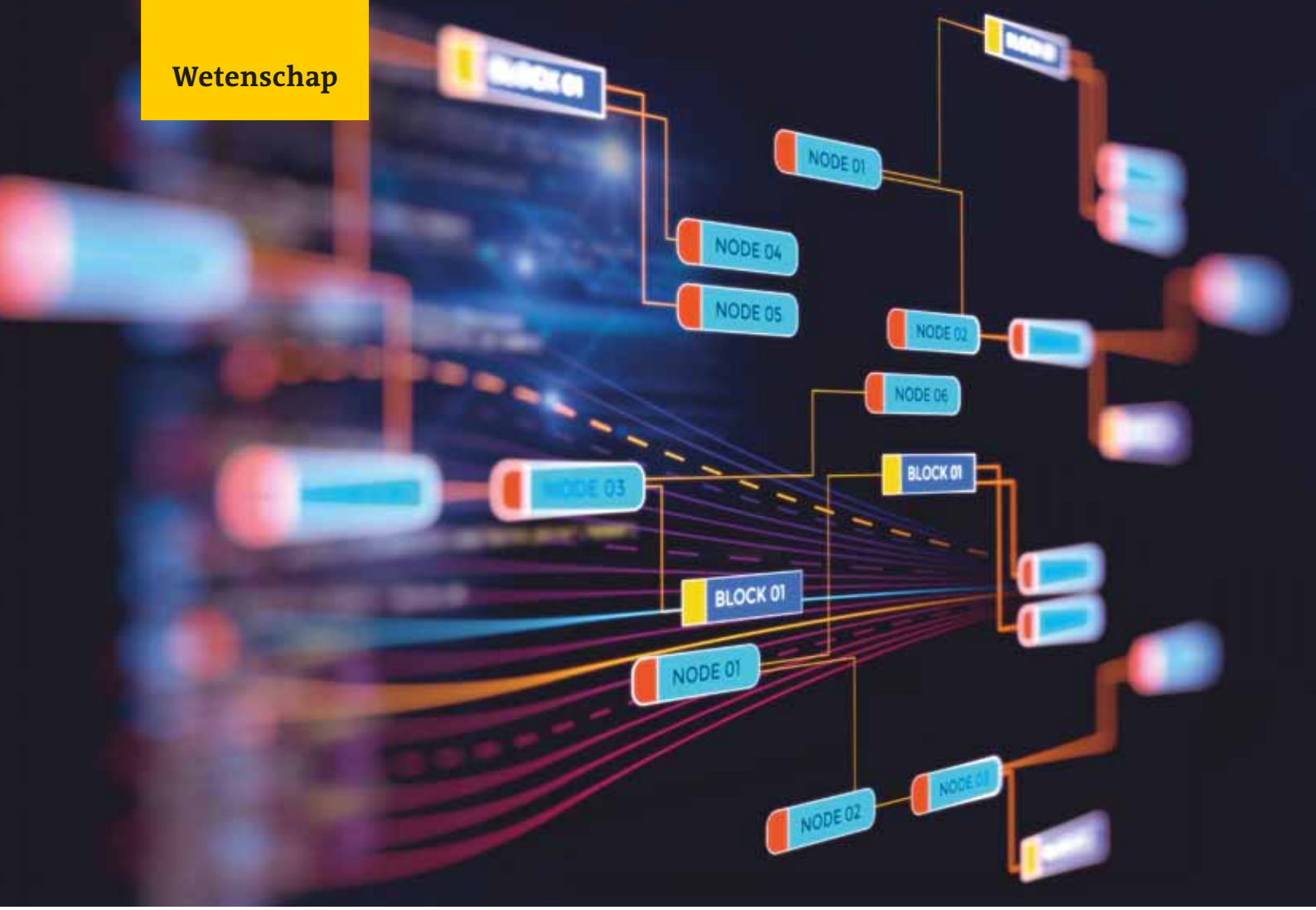
Er zijn al diverse initiatieven en waarschijnlijk nog veel meer in ontwikkeling. Het succesvolst is, of was in elk geval tot voor kort, Ethereum.[15] Ik zal dit als voorbeeld nemen. In essentie heeft Ethereum het systeem van bitcoin overgenomen en daar allerlei wijzigingen op aangebracht om het systeem beter hanteerbaar te maken. Men begon met een inschrijving op 'ether' (de valuta van Ethereum) om te zorgen dat er waarde in het systeem zat: dit leidde tot aankopen van $ 18 439 086. De totale waarde van ether liep in 2016 op tot boven de $ 1 miljard.[16] Een

Auteur

1. Prof. mr. T.F.E. Tjong Tjin Tai is hoogleraar Privaatrecht aan Tilburg University, en onderzoeker bij het Tilburg Instituut voor Privaatrecht (TIP).

Noten

2. Bijv. W. van Noort, 'Grote banken ontwikkelen een eigen munteenheid', *NRC* 24 augustus 2016, verwijzend naar een initiatief van onder meer UBS en Deutsche Bank.
3. J. Boersma e.a., *Bitcoins: Civiele en fiscale aspecten in beeld*, Deventer, 2015; Van den Berg, Van der Velden & Vergouwen, *MvV* 2014, p. 128-134; Rank, *AAe* 2015, p. 177-185; Bierens, *Ondernemingsrecht* 2014/25; Jongbloed, *TvPP* 2015, p. 77-83; Spaas & Van Roey Thomas, *Computerrecht* 2015/84; Jongbloed, *TvPP* 2015, p. 83.
4. Het is overigens mogelijk dat banken ervoor zorgen dat transacties niet uitsluitend door één enkele computer worden uitgevoerd.
5. https://en.wikipedia.org/wiki/2016_Bangladesh_Bank_heist.
6. T.F.E. Tjong Tjin Tai, 'Zorgplichten van banken tegen DDoS-aanvallen', *NJB* 2013/1969, afl. 32, p. 2196-2200.
7. In elk geval kan er een verplichting tot melden of waarschuwen zijn, die kan uitmonden in een verplichting transacties te blokkeren. Zie de Wet ter voorkoming van witwassen en financieren van terrorisme, en voor gevallen van financiële fraude; HR 23 december 2005, *NJ* 2006/289 (*Safe Haven*) en HR 27 november 2015, *NJ* 2016/245 (*ABN AMRO/St. Gedupeerde Beleggers vd B*).
8. T.F.E. Tjong Tjin Tai, 'De redelijke derde en de blockchain', *WPNR* 2015/7072.
9. Er zijn wel enkele nadelen en mogelijkheden van hacks; deze laat ik hier buiten beschouwing.
10. www.maciejolpinski.com/blog/on-risks-rewards-and-the-evolution-of-daos/.
11. Zie verwijzingen in noot 3, verder bijv. www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/; http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2016-06/1_blockchain-plan_efelten.pdf; en het oorspronkelijke paper van Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', op https://bitcoin.org/bitcoin.pdf.
12. De bedenker is Nick Szabo. Zie een artikel dat kennelijk reeds in 1994 verscheen: http://szabo.best.vwh.net/smart.contracts.html, ook www.virtualschool.edu/mon/Economics/SmartContracts.html, en uit 1997: 'Formalizing and Securing Relationships on Public Networks', *First Monday* 1997, vol. 2, nr. 9, op http://firstmonday.org/ojs/index.php/fm/article/view/548/469.
13. Overigens worden tegenwoordig 'starter cut-off devices' gebruikt om wanbetalers te verhinderen in hun auto te rijden. Zie bijv. http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_r=0 en www.stltoday.com/business/local/starter-cut-off-devices-keep-car-payments-coming/article_be4dfa8d-48bb-5d4c-9734-c93404c63250.html. Men spreekt over 'Automated Collection Technology'. Dit is géén smart contract omdat het gaat om een apparaat dat de schuldeiser naar eigen keuze activeert, het algoritme is dus niet overeengekomen door beide partijen. Wel laat dit zien dat het toepassen van een eenvoudige, heldere regel in de praktijk als onbillijk wordt ervaren.
14. https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/.
15. Zie een beschrijving bij https://en.wikipedia.org/wiki/Ethereum.
16. en.wikipedia.org/wiki/Ethereum.



verschil met bitcoin is overigens dat er een concrete organisatie is die de ontwikkeling van Ethereum regisseert: de Ethereum foundation, in Zwitserland gevestigd.[17]

Ethereum werkt, anders dan bitcoin, niet louter met een lijst transacties, maar met accounts. De blockchain houdt de complete lijst accounts bij.[18] Als incentive bij Ethereum fungeert op dit moment een systeem zoals dat bij bitcoin: een Proof of Work dat veel rekenkracht kost[19] en als beloning ether geeft. Er is overigens aangekondigd dat in de toekomst zal worden overgegaan op een zogenaamd consensus-algoritme[20] gebaseerd op Proof of Stake.[21] Het huidige Proof of Work-systeem gebruikt tevens een transaction fee, zogenaamd 'Gas'.[22]

Op zichzelf is Ethereum niet meer dan een platform voor gedecentraliseerde apps[23] waar derden specifieke toepassingen op kunnen plaatsen. In de documentatie van Solidity, de programmeertaal van Ethereum, worden voorbeelden gegeven van een crowdfunding contract en wat ze een 'democracy DAO' noemen.[24]

4. Waarom smart contracts?

De toegevoegde waarde van smart contracts draait om twee gerelateerde kenmerken: ze zijn zelfuitvoerend, en er is geen tussenpersoon of centrale instantie nodig.

Gewone overeenkomsten worden doorgaans nagekomen doordat partijen eigener beweging hun verplichtingen nakomen: dit kan men terugvoeren op de diepgewortelde morele notie van 'wat je beloofd hebt, moet je ook doen'. Voor het geval partijen toch de neiging zouden hebben zich aan hun verplichtingen te onttrekken is er de dreiging van gedwongen nakoming door middel van executie van een veroordelend vonnis: ofwel een rechterlijk gebod tot nakoming, al dan niet versterkt met een dwangsom, ofwel een verplichting tot schadevergoeding die evenzeer een prikkel tot nakoming vormt. In sommige situaties is de dreiging met executie minder effectief. Bijvoorbeeld als men niet bekend is met de (betrouwbaarheid van de) wederpartij, of als executie op moeilijkheden stuit door fysieke afstand of kosten. Voor dergelijke gevallen zijn er instrumenten ontwikkeld als wissels, cognossementen, bankgaranties. Dergelijke instrumenten werken doorgaans aldus dat zij 'vrijvallen', uitbetalen, als er bepaalde gebeurtenissen plaatsvinden.[25]

Bij smart contracts zal de nakoming automatisch door het systeem worden verricht, dat immers het contract (bestaande uit een programma) zelf uitvoert: het contract zorgt zelf voor de nakoming, als aan de door het systeem waarneembare criteria is voldaan. De schuldenaar hoeft dus niet meer een betalingsopdracht te geven: het systeem betaalt vanzelf voor hem. Dit werkt vooral goed bij betaling onder opschortende voorwaarde: dit lijkt op een (abstracte) bankgarantie.[26]

Overigens zijn er op dit moment nog drie praktische problemen. Ten eerste zouden er voor versterking van de functionaliteit van smart contracts mogelijkheden moeten komen om feitelijke handelingen of veranderingen in de fysieke wereld rechtstreeks af te dwingen: deze zijn er nu nog niet,[27] maar kunnen er in de nabije toekomst komen.[28] Ten tweede zijn smart contracts afhankelijk van I/O functies voor contact met de buitenwereld, wat vooral een praktisch probleem zal zijn als hier een menselijke beoordeling bij nodig is.[29] Ten derde vereisen smart contracts op dit moment dat de schuldenaar zijn toekomstige betaling alvast vastlegt, terwijl de schuldeiser noch een

derde daar intussen alvast over kan beschikken.[30] Dit leidt tot een verlies aan liquiditeit zonder het voordeel dat banken in de tussentijd hier toegevoegde waarde over kunnen genereren. Bij normale contracten hoeft de schuldenaar niet vooraf zijn betaling te reserveren.[31] Deze praktische problemen beperken voorlopig het toepassingsgebied van smart contracts. Het is echter niet uitgesloten dat hier oplossingen voor worden bedacht.

Dat smart contracts zelfuitvoerend zijn brengt met zich dat er geen tussenpersonen nodig zijn

Dat smart contracts zelfuitvoerend zijn brengt met zich dat er geen tussenpersonen nodig zijn. De vrees bij banken en advocaten is dan ook dat hun business zal worden *disrupted*. Het omzeilen van tussenpersonen wordt gezien als een belangrijk voordeel. Niet alleen bespaart dit kosten voor tussenpersonen, maar ook zou dit ervoor zorgen dat tussenpersonen niet kunnen bewerkstelligen dat de intentie van het contract wordt verdraaid. Men spreekt wel over 'corruption' in de zin van verderven, maar ook met de bijbetekenis van corruptie. Zie bijvoorbeeld een opmerking over het – hierna te bespreken – probleem bij The DAO: 'The entire point of cryptocurrencies to get around corrupt humans. And that's what trying to repair this problem is – corruption. It's a violation of TheDAO's own contract, which says the code is the contract, not to be superseded by human re-interpretation.'[32] Of: 'Zou dat niet ideaal zijn als ik via een smart contract een (corrupte) overheid/bank/tussenleveranciers kan omzeilen?'[33]

Dit wordt verwoord in een ideaal waarin niet langer het recht regeert, maar computercode:[34] *code is law.* Dit kan twee dingen betekenen. Als eerste gaat het om code *as* law: de deelnemers aan smart contracts hebben er kennelijk voor gekozen om hun rechtsverhouding te laten regelen door code, niet door rechtsregels. Hiertegen zou men kunnen inbrengen dat het recht nog steeds op de achtergrond aanwezig is: het recht op toegang tot de rechter is immers fundamenteel (art. 6 EVRM), men kan altijd nog naar de rechter stappen. Maar dan komt de tweede kant van *code is law* om de hoek. In de blockchain is het feitelijk niet meer nodig om op de schaduw van het recht te vertrouwen. Smart contracts voeren zichzelf uit onder de regels van het systeem. Sterker nog, doordat het systeem gedecentraliseerd is heeft het geen locatie en is het niet of nauwelijks vatbaar voor menselijke, juridische interventie. Het is dus feitelijk niet meer mogelijk rechtsbescherming te verkrijgen: *code is law*.

5. De hack van The DAO

De belofte van smart contracts is onlangs op de proef gesteld door een hack in een toepassing binnen Ethereum, genaamd 'The DAO'.[35] The DAO beoogde te werken als een *venture capital* of *crowdfunding* platform, waar investeringsvoorstellen (proposals)[36] konden worden gedaan die werden gepresenteerd in de vorm van code, waar dan door investeerders op kon worden ingeschreven door een kleine betaling van Ether, waarna zij erover konden stemmen.[37] The DAO kreeg in eerste instantie veel aanhang,[38]

17. www.ethereum.org/foundation.

18. www.ethdocs.org/en/latest/introduction/what-is-ethereum.html#how-does-ethereum-work.

19. www.ethdocs.org/en/latest/introduction/what-is-ethereum.html#how-does-ethereum-work; http://ethdocs.org/en/latest/mining.html. Het precieze type werk is anders, opdat het niet mogelijk is gespecialiseerde hardware te benutten.

20. Hierover bijv. www.coindesk.com/stellar-ripple-hyperledger-rivals-bitcoin-proof-work/.

21. Onder de naam Casper. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ Nader http://ethereum.stackexchange.com/questions/9/why-does-ethereum-plan-to-move-to-proof-of-stake, ook http://ethereum.stackexchange.com/questions/118/whats-the-difference-between-proof-of-stake-and-proof-of-work.

22. https://ethereum.gitbooks.io/frontier-guide/content/costs.html, https://github.com/ethereum/wiki/wiki/Mining.

23. http://ethdocs.org/en/latest/introduction/web3.html.

24. https://github.com/ethereum/go-ethereum/wiki/Contract-Tutorial. Andere voorbeelden bij https://medium.com/@AroundTheBlock_/a-current-list-of-use-cases-for-ethereum-b8caa5807553#.r5bhzhwag.

25. Het kan gaan om vereisten als ondertekening, afgifte van papieren document.

26. Tjong Tjin Tai, 2015.

27. Vergelijk opmerkingen van Gideon Greenspan, geciteerd in www.ibtimes.co.uk/how-are-banks-actually-going-use-blockchains-smart-contracts-1539789.

28. Bijv. als systemen reageren op signalen uit de blockchain. Zie bijv. www.ibtimes.co.uk/ethereum-based-slock-reveals-first-ever-lock-opened-money-1527014, of de eerdergenoemde startonderbrekers.

29. Dit wordt ook wel opgemerkt als reden waarom slechts bepaalde soorten contracten geschikt zijn voor automatisering, namelijk diegene die door robots gecontroleerd kunnen worden, en niet die welke menselijk oordeelsvermogen nodig hebben om te bezien of ze zijn nagekomen. www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874.

30. Vergelijk over dit punt ook www.ibtimes.co.uk/how-are-banks-actually-going-use-blockchains-smart-contracts-1539789.

31. Echter bij crowdfunding is dit wel vereist.

32. http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html.

33. doctor boo, commentaar 21 juli 2016 21:04 bij https://tweakers.net/nieuws/113805/ethereum-community-voert-hard-fork-uit.html.

34. Bijv. 'An organization/community that operates by rules of code, in a world where organizations/communities have historically been bound by legalese and human managerial interactivity, is revolutionary and potentially a lot more efficient. Not to mention, it's a big part of what Ethereum is about.' jonesyjonesy, commentaar bij www.reddit.com/r/ethereum/comments/4xf6bz/what_is_slockit_doing_nowadays_when_can_we_expect/.

35. Zie voor informatie https://en.wikipedia.org/wiki/The_DAO_(organization). De eigen website is https://daohub.org. De website laat op dit moment (oktober 2016) een bericht zien dat erop duidt dat The DAO wordt geliquideerd vanwege de hierna te beschrijven hack. Verder https://medium.com/edge-cases-multisig-phf-official-channel/the-daos-edge-cases-multisig-post-hard-fork-2f107380bd61#.lach36fh6.

36. https://github.com/slockit/DAO/wiki/How-to-create-a-proposal.

37. Zie bijv. https://medium.com/@simondlr/a-laymans-intro-to-thedao-why-history-is-being-made-41eac393b8c5, ook www.coingecko.com/buzz/the-dao-inevitable-result-ethereum?locale=en.

38. Er werden miljoenen aan Ether (dat miljoenen dollars waard was) opgehaald: https://en.wikipedia.org/wiki/The_DAO_(organization), verwijzend naar www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html.

De hack van The DAO legt een diepliggende onenigheid bloot onder de verschillende aanhangers van smart contracts

ook al waren er diverse lastig op te lossen veiligheidsproblemen en andere problemen gesignaleerd.[39]

Op The DAO werd in mei 2016 een proposal geplaatst dat gebruik maakte van een zwakte in de programmeertaal, waardoor het proposal (dat slechts één betaling leek te vragen) ervoor kon zorgen dat de portefeuille van de wederpartijen geheel geleegd werd (de betaling werd via recursie steeds opnieuw uitgevoerd).[40] De deelnemers die hun geld kwijt raakten wilden dit uiteraard terug.

De logische oplossing zou zijn om de transacties terug te draaien. Dat is technisch gezien mogelijk door het aanpassen van het systeem, dus verandering van de regels, en het creëren van een uitzondering voor dit proposal.[41] Dit komt in software-termen neer op het maken van een afsplitsing van de oorspronkelijke code, een *fork*.[42] Maar om dat te doen is het nodig om in te breken in het automatisme dat Ethereum propageerde. De bedoeling was immers juist dat contracten onaantastbaar zouden verlopen zonder menselijk ingrijpen of correctie. Dit is dan ook hoogst omstreden.[43] Een wijziging is niettemin mogelijk als de meerderheid van de deelnemers het voorstel volgt. Uiteindelijk is de fork aangekondigd[44] en uitgevoerd.[45]

Een deel van de participanten was het niet eens met de fork: zij beschouwden dit als een fundamentele aantasting van het uitgangspunt van Ethereum. Deze groep heeft zich verenigd onder de naam Ethereum Classic (ETH Classic) met het principe 'Code is law'.[46] Er is dus daadwerkelijk een splitsing ontstaan: zo'n 20% van de Ether zit in ETH Classic, de overigen hebben de aanpassing gevolgd. Dit leidt tot allerlei problemen over geldigheid van betalingen, mogelijkheden voor fraude.[47] Een argument dat tegen het terugdraaien was aangevoerd was dat er geen sprake was van oplichting: het contract was volledig open en iedereen kon nagaan wat de uitkomst zou zijn volgens de regels.[48] De regels waren niet genegeerd, er was integendeel gewoon slim gebruik gemaakt van de regels.

De hack van The DAO legt een diepliggende onenigheid bloot onder de verschillende aanhangers van smart contracts. Dit betreft twee aspecten: governance, en het primaat van de bedoeling.

6. Governance

Allereerst laat de reactie op de hack zien dat er geen systemen zijn zonder menselijke correctiemogelijkheden. Weliswaar is het mogelijk dat een systeem geen snelle correctiemogelijkheid heeft, maar uiteindelijk kan elk door mensen gemaakt systeem ook door mensen worden overruled. Althans geldt dit als het systemen betreft die sociale werking hebben: we kunnen er als groep voor kiezen die werking te negeren of ontkrachten. De respons van de founder van slock.it, Christoph Jentzsch, was: 'We just found out that we have a supreme court, the community!'[49] Anders gezegd: men ontdekte ineens de institutionele randvoorwaarden die bij ieder systeem aanwezig zijn.[50] Maar dit betekent dat op de achtergrond van DAO's altijd algemenere principes van inspraak, zorg, en rechtvaardigheid aanwezig zijn. Men kan er voor kiezen om DAO's te beschouwen als vrije ruimten waarin we deze principes tijdelijk buiten spel zetten (zoals ook bij bordspelen), maar men kan ze nooit geheel uitschakelen.

Dit is in de praktijk mogelijk lastig te executeren als er geen centrale server is, wat zou betekenen dat in de praktijk de DAO wel onaantastbaar zou zijn. Bij grootschalige systemen zoals The DAO en Ethereum is er echter genoeg financieel belang om de kosten voor een procedure voor lief te nemen en de aansprakelijke of verantwoordelijke partijen aan te pakken. Daarnaast zijn bij The DAO en Ethereum, zo blijkt, wel degelijk centralere partijen die grotere invloed hebben dan gewone deelnemers, en deze hebben dan mogelijk enige zorgplicht of verantwoordelijkheid.[51] Bovendien is mogelijk dat, als er geen centrale partij is, de deelnemers zelf worden aangesproken:[52] zij kunnen immers gezamenlijk kiezen voor wijziging.

Smart contracts blijven dus kwetsbaar voor juridische interventie. Theoretisch zou het mogelijk zijn om een smart-contractsysteem op te zetten en dit zoveel mogelijk af te sluiten van mogelijkheden voor latere inmenging. In zekere zin is bitcoin hier een voorbeeld van: de bedenker is anoniem en het systeem ontwikkelt zich op basis van losse groepen vrijwilligers. Bezwaar is dan dat je dan ook geen geld verdient met het opzetten van zo'n systeem. Als de bedenker toch betrokken blijft, is het niet uitgesloten dat hij aansprakelijk kan zijn omdat hij heeft nagelaten een mogelijkheid van inmenging op te nemen.[53] Anders gezegd: willen we eigenlijk wel een systeem dat nooit terug te draaien is? Er is op gewezen dat DAO's gelijkenis vertonen met de boeman van science fiction: Skynet.[54]

De mogelijkheid van aansprakelijkheid zou voor een organisatie als Ethereum reden kunnen zijn om een uitdrukkelijke overeenkomst te sluiten met deelnemers waarin forumkeuze, rechtskeuze, en exoneraties worden opgenomen. Bezwaar daarvan is dat men daarmee erkent dat smart contracts niet buiten het recht staan. Bij gebreke van zulke overeenkomsten met beschermende voorwaarden is het systeem echter inherent kwetsbaar voor procedures.

7. Het primaat van de bedoeling

Misschien nog belangrijker is dat de hack een fundamentele tegenstelling bloot legt: is het wenselijk om uitsluitend de code te volgen, of is het wenselijk om ook menselijke correctiemogelijkheden te hebben?[55] Het lijkt erop dat de meerderheid van de deelnemers aan The DAO *niet* wenste dat 'code is law', maar een andere opvatting heeft van overeenkomsten, een opvatting die in overeenstemming is met het recht.[56] Dit is de aloude tegenstelling tussen tekst versus bedoeling.

De vraag is of de code doet wat de bedoeling is.[57] Als de code niet doet wat de programmeur bedoelde, spreekt men van een bug. Het komt echter ook voor dat de code

iets anders doet dan de gebruiker verwachtte. Dan hoeft het niet om een bug te gaan, maar gewoon om een eigenschap van het systeem. Het antwoord is dan regelmatig: 'it's not a bug, it's a feature'. Bij smart contracts zou de code zelf het gehele contract uitmaken.[58] Het lijkt er nu echter op dat mensen dus *niet* geheel willen vertrouwen op de code.[59]

De reden hiervoor is dat het voor de gewone deelnemers niet goed mogelijk is de code te begrijpen.[60] Sterker nog: ook voor veel computerdeskundigen is het lastig om smart contracts geheel te doorgronden. Dat veronderstelt kennis van programmeren en bekende computertalen, maar ook van de specifieke eigenaardigheden van het specifieke systeem, naast kennis van de bijzonderheden van blockchain-technologie (zoals speltheoretische en netwerkaspecten). Het blijkt lastiger dan gedacht om goede code te schrijven.[61] Voor het goed coderen van dergelijke contracten zijn daarom specialistische – dus dure – programmeurs nodig.[62] En deelnemers die op veilig willen spelen zullen een audit nodig hebben om te verzekeren dat er geen onverwachte kanten aan het contract zitten. Dit is echter precies wat juristen in de contractspraktijk doen: opstellen en beoordelen van contracten. Anders gezegd: in plaats van juristen zou men kostbare Ethereum-deskundigen nodig hebben.[63]

Dit heeft ook juridische gevolgen. Het feit dat smart contracts niet goed te begrijpen zijn voor leken roept de vraag op in hoeverre voorlichting vereist is. Mogelijk zou een beroep op dwaling kunnen slagen als de voorlichting incorrect is. Daarnaast eisen diverse EU-richtlijnen (geïmplementeerd in hierna te noemen BW-artikelen) additionele voorlichting. Smart contracts zijn waarschijnlijk een vorm van elektronische dienstverlening in de zin van art. 3:15d BW, en ook een vorm van elektronisch contracteren (art. 6:227a BW). Daarvoor gelden tal van informatieplichten ten aanzien van consumenten (art. 3:15d en 15e, 227a-227c BW), naast algemene informatieplichten voor dienstverlening (art. 230b-d, 230m-230z BW). Deze regels eisen bijvoorbeeld dat de identiteit en het fysieke adres van de wederpartij duidelijk wordt medegedeeld: overtreding

39. Deze zijn nogal technisch van aard en daarom niet eenvoudig beknopt uit te leggen. Zie bijv. http://vessenes.com/advice-for-dao-2-0s/ en http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/, iets toegankelijker https://techcrunch.com/2016/05/22/all-the-cool-kids-are-doing-ethereum-now/.

40. Hierover www.americanbanker.com/news/bank-technology/what-the-attack-on-the-dao-means-for-banks-1081575-1.html, en meer technisch http://vessenes.com/deconstructing-thedao-attack-a-brief-code-tour/. In essentie komt het neer op misbruik van een recursieve functieaanroep waardoor de 'betaal'functie steeds weer wordt aangeroepen. Zie ook bijv. http://nakamotoinstitute.org/mempool/ethereum-is-doomed/.

41. Overigens waren er nog meer mogelijkheden; het voert te ver om hier diep op in te gaan. Onder meer ging het om een verschil tussen een 'hard fork' en een 'soft fork' (hierover bijv. http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html). Daarnaast was er een 'white hat' hack (goedbedoelde hack) om fondsen tijdelijk veilig te stellen.

42. Het ligt iets ingewikkelder: bij gewone software is een fork een splitsing van de hoofdlijn van de code. Bij de blockchain spreekt men echter ook van een fork bij (tijdelijke) discrepanties bij het uitrollen van nieuwe versies van de software. Men onderscheidt dan bovendien tussen een 'soft fork' en 'hard fork'.

43. Zie bijv. de discussie bij http://vessenes.com/point-counterpoint-ethereum-miners-should-blacklist-thedao-theft/.

44. https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/.

45. https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

46. https://ethereumclassic.github.io/assets/ETC_Declaration_of_Independence.pdf.

47. http://vessenes.com/do-not-mess-with-eth-classic-it-will-f-you-up/.

48. http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html.

49. https://blog.slock.it/what-an-accomplishment-3e7ddea8b91d#.wnz2yp6sp.

50. www.americanbanker.com/news/bank-technology/what-the-attack-on-the-dao-means-for-banks-1081575-1.html wijst erop dat dit vragen oproept over de governance van dergelijke systemen.

51. https://bitcoinmagazine.com/articles/the-securities-law-implications-of-the-dao-hack-and-proposed-ethereum-hard-fork-1467215402.

52. Vergelijk www.coindesk.com/how-to-sue-a-decentralized-autonomous-organization/.

53. Vergelijk de aansprakelijkheid voor het niet kunnen terugdraaien van een foutieve effectenorder: https://en.wikipedia.org/wiki/Mizuho_Securities#Massive_sale_order_of_J-COM_share_incident; ook T. Tamai, 'Software engineering view of a large-scale system failure and the following lawsuit', *Proceeding SER&IP* 2015, p. 18-24, op http://dl.acm.org/citation.cfm?id=2821387.2821394.

54. www.zdnet.com/article/bitcoin-laying-the-foundation-for-a-real-world-skynet/, ook https://cyber.harvard.edu/events/luncheon/2014/04/difilippi en transcriptie op www.guerrillatranslation.org/2014/11/20/ethereum-freenet-or-skynet/.

55. Evenzo www.cio.com/article/3086207/cloud-computing/a-blockchain-smart-contract-could-cost-investors-millions.html.

56. Vergelijk Brett Scott, 'How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?', *UNRISD Working Paper* 2016-1, p. 13: 'Contracts are representations of frequently ambiguous, unpredictable and messy relationships between imperfect humans with imperfect knowledge. Such relationships cannot easily be pre-programmed, and much of the work of lawyers involves resolving and interpreting contracts in light of changing realities.'

57. Vergelijk 'The contract for The DAO did run exactly as programmed – although not, perhaps, exactly as intended' (www.cio.com/article/3086207/cloud-computing/a-blockchain-smart-contract-could-cost-investors-millions.html).

58. Daarom twijfelden diverse deskundigen of dit wel als bug of hack kon worden aangemerkt: www.cio.com/article/3086207/cloud-computing/a-blockchain-smart-contract-could-cost-investors-millions.html.

59. Vergelijk www.cio.com/article/3086207/cloud-computing/a-blockchain-smart-contract-could-cost-investors-millions.html: 'For The DAO investors in particular, it's the ultimate test of whether they truly want to be part of a decentralized economy, with no central authority to judge and to impose redress.'

60. Overigens is er ook een lopend debat of de DAO-hack er verband mee hield dat Solidity, de taal van Ethereum, teveel mogelijkheden heeft (technisch gesproken: Turing-compleet is), terwijl Bitcoin veiliger is doordat het maar enkele mogelijkheden biedt. Zie bijv. www.ibtimes.co.uk/dr-gide-on-greenspan-blockchain-design-academic-work-shouldnt-just-be-decided-by-banks-1520754; www.ibtimes.co.uk/how-are-banks-actually-going-use-block-chains-smart-contracts-1539789.

61. Zie bijv. comments van Sunny McJoyride en kieranelby[S] op de site www.reddit.com/r/ethereum/comments/44h1m1/a_new_ðapp_king_of_the_ether_throne/czqyomf en www.kingoftheether.com/postmortem.html; ook http://vessenes.com/advice-for-dao-2-0s/ die wijst op diverse safeguards die regelmatig worden vergeten, evenzo www.americanbanker.com/news/bank-technology/what-the-attack-on-the-dao-means-for-banks-1081575-1.html?pg=2; www.rsk.co/blog/lessons-from-the-dao-incident; http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/; www.coingecko.com/buzz/the-dao-inevitable-result-ethereum?locale=en.

62. Vergelijk www.coingecko.com/buzz/the-dao-inevitable-result-ethereum?locale=en.

63. Evenzo bijv. www.rsk.co/blog/lessons-from-the-dao-incident; http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html. Deze bieden zich al aan, zie bijv. 'I and my team are available for smart contract creation, auditing and specification' op het eind van http://vessenes.com/advice-for-dao-2-0s/. Het is mogelijk dat deze wel goedkoper zijn dan advocaten. Zie voor U.S. securities law: https://bitcoinmagazine.com/articles/the-securities-law-implications-of-the-dao-hack-and-proposed-ethereum-hard-fork-1467215402.

van art. 3:15d en 15e BW kan daarnaast een economisch delict vormen (art. 1, slot Wet op de Economische Delicten). Ook is mogelijk dat financiële regelgeving van toepassing is, afhankelijk van wat de smart contracts doen. De toekomstige EU-regelgeving over digitale inhoud (COM(2015)634) zou nog verdere verantwoordelijkheden en aansprakelijkheden kunnen opleveren: het valt immers te verdedigen dat een smart contract kwalificeert als 'digitale inhoud'.

Een onzekerheid hierbij is dat niet geheel zeker is of een smart contract wel onder de EU valt: het is mogelijk dat het systeem buiten de EU moet worden gelokaliseerd. Echter ook elders zijn er financiële regels.[64] Daarbij komt dat het mogelijk is dat weliswaar niet de directe aanbieder van een DAO of een smart contract aan te spreken is (omdat deze anoniem is), maar dat wel andere partijen die bemiddelen bij of bijdragen aan een DAO onder EU-jurisdictie vallen. Zij zouden onder omstandigheden kunnen worden aangesproken voor die medewerking,[65] in het bijzonder als er dingen mis gaan zoals bij de The DAO-hack. Het is dan ook bepaald niet zonder risico's als gevestigde Europese financiële instellingen zich begeven op dit terrein.[66] Om een achterstand van de EU te vermijden zou de EU om deze reden er voor kunnen kiezen om uitzonderingen te maken op de gewone regels, teneinde smart contracts te stimuleren. Dit zou een rechtspolitieke keuze zijn, die ten koste gaat van consumentenbescherming.

8. Wat moeten contracten regelen?

Een interessant theoretisch punt is het volgende. In de discussie na de The DAO-hack is erop gewezen dat het maken van smart contracts veel meer regels vergt dan alleen een opgeschorte betaling of een sanctie op te late betaling. Smart contracts zouden voor alle eventualiteiten oplossingen moeten bevatten: daarvoor zouden dan best practices moeten worden ontwikkeld.[67]

Dit inzicht is interessant omdat de bedoelde gevallen en oplossingen in het contractenrecht te vinden zijn. Men kan verdedigen dat het contractenrecht in essentie bestaat uit kennis en ervaring over wat er kan gebeuren bij contracten en wat de beste oplossingen daarvoor zijn. Dit zou een interessant onderzoek kunnen opleveren: het contractenrecht zou moeten worden vertaald naar best practices. Omgekeerd zou dit kunnen leiden tot een rationalisatie en harmonisatie van het contractenrecht, dat in ieder land weer een ander lastig te doorgronden systeem van remedies kent.

Een probleem blijft overigens dat het contract zelf niet aan te passen is, zelfs niet als alle partijen het daar over eens zijn. Een mogelijke oplossing zou zijn om een exit-optie in te bouwen waarmee het contract bij voldoende stemmen beëindigd wordt en de saldi overgezet worden naar een nieuw, dan aan te wijzen, contract. Een nadeel hiervan is dat dan kan worden verdedigd dat de ontwikkelaar verantwoordelijk is om indien nodig zo'n upgrade te verzorgen.[68]

9. De toekomst van smart contracts

De slotsom van deze bedenkingen is dat er op dit moment nog significante juridische onzekerheden en risico's zijn rond smart contracts. Dit is in het bijzonder riskant als men via smart contracts grote investeringen wil afhandelen: dan is er immers voldoende financieel belang om de onzekere weg van juridische procedures te vervolgen. Dit betekent niet dat smart contracts niet gebruikt zullen worden. Voor (consumenten)transacties van geringe waarde zou bijvoorbeeld een rol kunnen zijn weggelegd. Denk als voorbeeld aan internetbestellingen met automatische betaling bij aflevering. De risico's voor de consument zijn dan gering, en bovendien gaat het om een standaardsituatie waar een standaardcontract bij kan helpen. Op dit moment vindt in wezen al een zekere uniformering plaats van de financiële afhandeling van internetbestellingen, in de vorm van de dispute resolution systemen van giganten als eBay, Amazon, en PayPal (onderdeel van eBay).[69] De geconstateerde risico's zijn voor kleine investeringen en betalingen mogelijk niet problematisch: voor dergelijke gevallen kunnen smart contracts succes hebben. Dat zou op zich al significante effecten kunnen hebben voor het betalingsverkeer bij internationale (consumenten)transacties.

Willen we eigenlijk wel een systeem dat nooit terug te draaien is?

Al met al is de toekomst van smart contracts vooralsnog onzeker, maar wel hoogst interessant. De geconstateerde problemen vergen behoorlijke inspanning om op te lossen, maar zijn niet per se onoverkomelijk. Een deel van de juridische bezwaren kunnen door aanpassing van regelgeving deels worden omzeild. Niettemin blijven er enige intrinsieke complicaties bestaan. De ontwikkelingen van de afgelopen decennia hebben echter laten zien dat men niet voorbarig moet denken dat iets niet zal aanslaan of niet mogelijk is. *Smart contracts* zijn zeker iets om in de gaten te blijven houden. •

64. Vergelijk HR 2 september 2016, ECLI:NL:HR:2016:2012 waar de effectenin-stelling mede aansprakelijk is voor het zonder vergunning verlenen van advies door een tussenpersoon.

65. Overigens zullen zij vermoedelijk hun belangen onderbrengen in zelfstandige rechtspersonen.

66. In het bijzonder http://vessenes.com/we-need-some-best-practices-for-smart-contracts/, die wijst op de onderwerpen 'birth, death, change of owner, license/terms and copyright functions (…) pause and unexpected bug facilities. The terms and conditions of the contract should clearly spell out what happens in those cases and require the users to agree ahead of time to the plan in the code. (…) who can delete, terminate, pause or deprecate this contract?" Dit zijn allemaal onderwerpen waar in het contractenrecht over vele eeuwen oplossingen voor zijn ontwikkeld. Hij verwijst verder naar K. Delmolino, M. Arnett, A. Kosba, A. Miller & E. Shi, 'Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab' op http://fc16.ifca.ai/bitcoin/papers/DAKMS16.pdf.

67. http://vessenes.com/advice-for-dao-2-0s/, par. 'Upgradability and Custody'.

68. C. Busch & S. Reinhold, 'Standardisation of Online Dispute Resolution Services: Towards a More Technological Approach', *European Journal of Consumer and Market Law,* vol. 4 2015, nr. 1-2, p. 50-58.

69. C. Busch & S. Reinhold, 'Standardisation of Online Dispute Resolution Services: Towards a More Technological Approach', *European Journal of Consumer and Market Law*, vol. 4 2015, nr. 1-2, p. 50-58.