

De kwalificatie van bitcoins

Tycho de Graaf¹

In deze bijdrage wordt ingegaan op de juridische kwalificatie van bitcoins. Daartoe wordt eerst uitgelegd hoe de techniek werkt. Daarna wordt de technische werkelijkheid juridisch weerspiegeld. Gefocust wordt daarbij op de privésleutel, de *wallet* waarin die sleutel is opgeborgen en de drager waarop de wallet staat. Alleen daarmee kan namelijk in technische zin over de bitcoins worden beschikt. Onderzocht wordt of het bitcoinsysteem vanuit verbintenisrechtelijk perspectief aangemerkt kan worden als een meerpartijenovereenkomst en vervolgens of bitcoins als waardepapieren kunnen worden gezien. Daarbij is het doel tot een juridische kwalificatie te komen die in overeenstemming is met de technische werkelijkheid en daarmee duidelijkheid te krijgen over de vraag hoe bitcoins moeten worden overgedragen, bezwaard, beslagen en geëxecuteerd.

1. Inleiding

Onduidelijk is hoe bitcoins vanuit juridisch perspectief moeten worden gekwalificeerd. Het antwoord op die vraag is onder andere relevant om te bepalen hoe bitcoins moeten worden overgedragen, bezwaard, beslagen en geëxecuteerd. In deze bijdrage probeer ik bitcoins te kwalificeren vanuit verbintenis- en goederenrechtelijk perspectief.² Daartoe leg ik eerst, voor zover relevant, vanuit technisch perspectief uit wat bitcoins zijn en hoe ze worden overgedragen. Vervolgens bespreek ik hoe het bitcoin-netwerk vanuit verbintenisrechtelijk perspectief kan worden gekwalificeerd, om vanuit daar de stap te zetten naar een uitgebreidere goederenrechtelijke kwalificatie. In dat kader neem ik aan dat de bitcoin geen geld is,³ en onderzoek ik met name of bitcoins als waardepapieren kunnen worden gezien. Deze bijdrage is betrekkelijk lang. Dat komt door het in elkaar grijpen van techniek, verbintenis- en goederenrecht, alsmede de noodzaak om vereisten en veronderstellingen ten aanzien van handtekeningen, schriftelijkheid en het geven en nemen van waardepapieren te duiden en te overwinnen. Dat komt ook doordat ik telkens tegenwerpingen bespreek die tegen het door mij te berde gebrachte kunnen worden ingebracht. Het doel van deze uitgebreide behandeling is dat alles aan het einde van deze bijdrage in elkaar grijpt, meer specifiek dat de bitcoin op een overtuigende wijze is gekwalificeerd en kort de gevolgen van een zodanige kwalificatie onder ogen zijn gezien.

2. Wat zijn bitcoins, hoe worden ze overgemaakt en waar staan ze?

Bitcoin is een cryptocurrency. Bitcoin-eenheden zijn bitcoins, millibits en satoshi's.⁴ Bitcoin transacties zijn:

- 1) gedecentraliseerd opgeslagen op diverse computers (*nodes*), die onderling en zonder centrale tussenpersoon (*disintermediated*) door gebruikmaking van het internet in een netwerk met elkaar verbonden zijn en aan verschillende personen toebehoren;
- 2) in een grootboek, dat publiek toegankelijk is, waaraan transacties alleen kunnen worden toegevoegd als minimaal 51% van de nodes het ermee eens zijn dat de transactie juist is (*consensus*) en dat voor het overige niet kan worden gewijzigd (*secure public ledger with a single source of truth*); en
- 3) dat voortdurend zonder tussenpersoon wordt gesynchroniseerd met gebruikmaking van een *peer-to-peer* protocol (denk aan bittorrent) zodat iedereen over hetzelfde grootboek beschikt.⁵

Om bitcoins en bitcoin-transacties beter te begrijpen, is het nuttig uiteen te zetten hoe bitcoin-transacties werken, bijvoorbeeld als A één bitcoin heeft en die wil overmaken naar B. Dat gebeurt in drie stappen: 1. B genereert drie reeksen van tekens waarmee hij als het ware een bitcoin-rekening opent en waarna B zijn toegangscode tot die rekening veilig opbergt, 2. A maakt een bitcoin over naar de bitcoin-rekening van B, waarna B die bitcoin ongeverifieerd op zijn rekening ontvangt en 3. die transactie wordt door andere deelnemers aan het bitcoin-netwerk geverifieerd en, als de transactie klopt, aan het gedecentraliseerde grootboek toegevoegd. De werkelijkheid is complexer, zoals nu zal blijken.

2.1. Aanmaken van sleutels, adres en wallet

Het overmaken begint ermee dat B moet beschikken over een bitcoin-adres (denk aan een bankrekeningnummer) waarnaar A de bitcoin kan overmaken. B maakt als volgt zo'n bitcoin-adres aan. Met gebruikmaking van wallet software (die draait op B's eigen computer of smartphone, of op een server van een derde) genereert B drie reeksen van niet-zelfgekozen tekens:

- 1) een privésleutel, die nodig is om de bitcoins over te kunnen maken die op het bijbehorende bitcoin-adres (zie hierna) staan (min of meer vergelijkbaar met een lang, ingewikkeld en niet te onthouden wachtwoord voor internetbankieren);
- 2) een uit de privésleutel afgeleide publieke sleutel, een (nog steeds) lange reeks tekens; en
- 3) een uit de publieke sleutel afgeleid, 58 tekens tellend bitcoin-adres, een verkorte versie van de publieke sleutel die nodig is om bitcoins op te kunnen ontvangen (denk aan een bankrekeningnummer) en dat vaak ook wordt weergegeven als QR-code die kan worden gescand in plaats van dat het adres moet worden gecopy-paste of overgetypt.⁶

Na het genereren van die reeksen tekens, bergt B zijn aldus gegeneerde privésleutel op in een zogeheten *wallet*. Er zijn twee verschillende vormen van wallets: hot/live wallets en cold wallets.⁷ Een *hot wallet* is software die draait op hardware die met het internet verbonden is en waardoor bitcoins meteen van het ene naar het andere bitcoin-adres kunnen worden overgemaakt. Die hardware kan toebehoren aan de gebruiker (B's eigen computer of smartphone) of aan een derde (B's leverancier). Als de hardware toebehoort aan B's leverancier is de privésleutel versleuteld opgeslagen door die leverancier en kan B die sleutel bij die leverancier opvragen, bijvoorbeeld door op diens omgeving in te loggen met gebruikmaking van zijn gebruikersnaam en wachtwoord (of meer).⁸ Zo'n wallet heet ook wel een web/online wallet. Als de hardware toe-

Om bitcoins en bitcoin-transacties beter te begrijpen, is het nuttig uiteen te zetten hoe bitcoin-transacties werken

behoort aan de gebruiker is de privésleutel versleuteld opgeslagen in software op diens computer (een desktop wallet)⁹ of een app op diens smartphone (een mobile wallet).¹⁰ Dat is in de regel dezelfde software/app als waarmee de hiervoor genoemde reeksen (privésleutel, publieke sleutel en bitcoin-adres) zijn gegenereerd.

Een *cold wallet* is niet met het internet verbonden en daarom veiliger dan een hot wallet, zij het minder gebruiksvriendelijk. Om bitcoins van het ene naar het andere bitcoin-adres over te maken, moet de privésleutel immers eerst 'uit' de wallet worden gehaald en worden 'gestopt' in software die op hardware draait die (wel) met het internet verbonden is. De simpelste vorm van een cold wallet is een paper wallet.¹¹ Dat is een stuk papier waarop zichtbaar de publieke sleutel en het bitcoin-adres staan afgedrukt en, meestal achter een kraslaag of een sticker, de privésleutel. Ingewikkelder is een hardware wallet.¹² Dat is een fysiek device dat eruit ziet als een USB-stick en uitsluitend bestemd is om privésleutels in op te slaan. In dat device zijn privésleutels versleuteld opgeslagen en de toegang daartoe is beveiligd met een code.

2.2. Ongeverifieerd overmaken van A naar B

Het overmaken kan beginnen zodra B de privésleutel, de publieke sleutel en het bitcoin-adres heeft aangemaakt en de privésleutel heeft opgeborgen in een wallet.¹³ Dan geeft B aan A het bitcoin-adres waarop hij de bitcoin wil ontvangen. Dat kan bijvoorbeeld doordat B op zijn smart-

Auteur

1. Mr. T.J. de Graaf is universitair docent burgerlijk recht aan de Universiteit Leiden. Hij dankt prof. mr. W.H. van Boom voor zijn commentaar op een eerdere versie.

Noten

2. Omwille van de overzichtelijkheid ga ik ervan uit dat Nederlands recht op alle relevante rechtsposities en -verhoudingen van toepassing is.
3. Bitcoins worden niet gerekend tot gangbaar geld in de zin van art. 6:112 BW en een betaling in bitcoins moet worden gezien als een inbetalinggeving in de zin van art. 6:45 BW waarvoor de toestemming van de schuldeiser is vereist. Zie W.A.K. Rank, 'Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten', in: R.A. Wolf e.a., *Bitcoins. Civiele en fiscale aspecten in beeld*, Deventer: Kluwer 2015, p. 26-39; R. Koolhoven, 'Over geldvoorwerpschulden en

de betaling met Bitcoins', in: R.J.C. Flach e.a. (red.), *Dwingend privaatrecht op maat*, Den Haag: Boom Juridische uitgevers 2015, p. 85-100; Mijnsen, *Verbindenissen tot betaling van een geldsom* (Mon. BW nr. B39) 2017; en I. Sluiter, 'Over Bitcoin, Blockchain en Bestuursrecht', *JBplus* 2018/3. Zie ook B. Bierens, 'Veranderend betaalgedrag vanuit een juridisch perspectief. Kan het contant geld al worden afgeschaft?', *NJB* 2018/942, afl. 19, p. 1348, die meent dat bitcoin op een elektronisch equivalent van contant geld lijkt en de overdracht van bitcoins gelijkenis vertoont met een girale betaling. Zie voor het Belgische recht J.-L. Verhelst, 'Zijn cryptomunten? Een analyse van Bitcoin', in: M.E. Storme & F. Helsen (red.), *Innovatie en disruptie in het economische recht*, Antwerpen: Intersentia 2017, p. 23-78.- 4. Een millibit is één duizendste van een bitcoin, zie [bit. Een satoshi is één miljoenste van een bitcoin en daarmee de kleinste denominatie van een bitcoin, net als dat een cent de kleinste denominatie van een euro is, zie \[https://en.bitcoin.it/wiki/Satoshi_\\(unit\\)\]\(https://en.bitcoin.it/wiki/Satoshi_\(unit\)\).](https://en.bitcoin.it/wiki/Milli-</div><div data-bbox=)
- 5. Zie voor een simpele uitleg van bitcoin <https://medium.freecodecamp.org/explain-bitcoin-like-im-five-73b4257ac833>. De werkelijkheid is complexer, zie <https://en.wikipedia.org/wiki/Bitcoin> en T.F.E. Tjong Tjin Tai, 'Juridische aspecten van blockchain en smart contracts', *TPR* 2017/2, p. 565-577.
- 6. A.M. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, Sebastopol, CA, USA: O'Reilly 2017, p. 55-70.
- 7. <https://www.coindesk.com/information/how-to-store-your-bitcoins/> en <https://www.buybitcoinworldwide.com/wallets/#types-of-wallets>.
- 8. Aangezien er een risico is dat bitcoins worden ontvreemd als de leverancier wordt

gehacked, nemen leveranciers vaak extra maatregelen, zoals het opslaan van privésleutels op servers die niet met het internet verbonden zijn en waarvandaan de privésleutels worden gehaald zodra de klant erom vraagt, zie bijv. www.coinbase.com/security.- 9. Bijv. Electrum, <https://electrum.org/>.
- 10. Bijv. Edge, <https://edge.app>, of BRD, <https://brd.com>.
- 11. Bijv. Wallet Generator, <https://walletgenerator.net>, of Bitcoin Paper Waller, <https://bitcoinpaperwallet.com>.
- 12. Bijv. een Trezor, <https://trezor.io>, of Ledger, www.ledger.com/products/ledger-nano-s?r=2c06&path=/products/ledger-nano-s&tracker=walletsintro.
- 13. Zie voor een beschrijving van het overmaken van bitcoins A.M. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, Sebastopol, CA, U ZSA: O'Reilly 2017, p. 8-14.



phone zijn bitcoin wallet app opent en de QR-code van zijn bitcoin-adres laat zien aan A. A kan die QR-code vervolgens scannen met zijn bitcoin wallet app en de camera op zijn smartphone. Daarmee maakt A zijn app duidelijk naar welk bitcoin-adres hij bitcoins wil overmaken, te weten het bitcoin-adres van B. A selecteert vervolgens in zijn app het bitcoin-adres van waaruit hij bitcoins wil overmaken (zijn eigen rekening dus), de hoeveelheid bitcoins die hij wil overmaken (in dit geval één), en de transactiekosten (in bitcoin) die hij daarvoor wil betalen. Daarbij geldt dat hoe hoger de in het vooruitzicht gestelde transactiekosten zijn, hoe sneller de transactie zal worden verwerkt. Vervolgens bevestigt A de transactie door ondertekening van die transactie met zijn (in zijn app opgeborgen) privésleutel. Met behulp van die ondertekening kan later worden vastgesteld (waarover hieronder meer) of A kan beschikken over de bitcoins op het aan die privésleutel verbonden bitcoin-adres en of op dat adres minimaal één bitcoin staat. Die controle wordt uitgevoerd om te voorkomen dat bitcoins twee keer worden uitgegeven.

Binnen een paar seconden na het ondertekenen van de transactie door A, wordt die transactie peer-to-peer over de nodes in het bitcoin-netwerk verspreid en zien de verbonden nodes stuk voor stuk voor het eerst het net door B gegenereerde bitcoin-adres en de betreffende transactie. In de tussentijd 'luistert' de app van B voortdurend of er transacties in het netwerk openbaar worden gemaakt die matchen met het bitcoin-adres dat is opgeslagen in B's app. Zodra B's app een match heeft geconstateerd, geeft die app aan dat B ongeverifieerd (*unconfirmed*) één bitcoin heeft ontvangen.

2.3. Verificatie van transacties door miners en controle door nodes

De volgende stap is dat de ongeverifieerde transactie wordt goedgekeurd en als block aan de blockchain wordt toegevoegd en daarmee in het gedecentraliseerde grootboek wordt opgenomen.¹⁴ Dat gebeurt in twee stappen door twee verschillende soorten partijen: miners en nodes, die op hun computers ieder verschillende software hebben geïnstalleerd waarmee ze aan het bitcoin-

netwerk deelnemen en hun respectievelijke taken vervullen.¹⁵

Als eerste stap vindt er een *speed competition* plaats. Dat is een wedstrijd waarbij computers (zogenoemde *miners*) volledig automatisch drie dingen doen: ze verzamelen verschillende transacties in een *block* (een *candidate block*), verifiëren of de daarin opgenomen transacties juist zijn (denk bij het overmaken van giraal geld aan *clearing*) en lossen, om misbruik te voorkomen, een op dat block betrekking hebbende ingewikkelde en unieke cryptografische puzzel op (het *proof of work*).¹⁶ Degene die als eerste de puzzel oplost, wint het recht voor te stellen om het aldus geminede block aan de blockchain toe te voegen.¹⁷ Hij heet daarom *proposer*.

Als tweede stap vindt er een *quality competition* plaats. Daarin gaan de nodes controleren of de proposer zijn werk goed heeft gedaan, dus terecht heeft vastgesteld welke in het candidate block opgenomen transacties juist zijn en of de oplossing van de cryptografische puzzel klopt. Die controle is vrij eenvoudig. Als minimaal 51% van de nodes het ermee eens is dat de proposer zijn werk goed heeft gedaan wordt zogeheten *consensus* bereikt, geldt de transactie als bevestigd (*confirmed*) en wordt het candidate block als block aan de blockchain toegevoegd. In ruil voor al zijn werk krijgt de proposer een beloning die wordt overgemaakt naar het door de proposer opgegeven bitcoin-adres. Die beloning bestaat uit een *block reward* en transactiekosten. Het block reward bestaat uit nieuwe bitcoins die door het bitcoin-netwerk worden gecreëerd en is op dit moment 12,5 bitcoins.¹⁸ Zo'n block reward is de enige manier waarop nieuwe bitcoins kunnen worden gedolven (*mined*), zeg maar in het leven worden geroepen. De transactiekosten bestaan uit het door de overmaker vooraf opgegeven aantal bitcoins en worden door hem betaald.

Echter, als minimaal 51% van de nodes vindt dat de proposer zijn werk niet goed heeft gedaan, dan wordt het candidate block afgekeurd, wordt de transactie niet bevestigd en begint een nieuwe speed competition. In dat geval krijgt de proposer niet alleen geen beloning (geen block reward en geen transactiekosten), maar wordt hij ook 'gestraft' doordat hij tevergeefs al die moeite heeft gestopt in het oplossen van die cryptografische puzzel. Die puzzel is dus zo ingewikkeld om misbruik te ontmoedigen.

Terug naar A en B. Als de transactie wordt bevestigd, geeft de app van A aan dat één bitcoin is overgemaakt naar het bitcoin-adres van B en de app van B dat B confirmed één bitcoin heeft ontvangen. Dat kan wel even duren.¹⁹ Over die ene bitcoin kan B vervolgens weer

beschikken met gebruikmaking van de privésleutel die hoort bij zijn bitcoin-adres.

2.4. Anonimiteit

Voor het aanmaken van een bitcoin-adres en het overmaken van bitcoins hoeven A en B geen persoons- of andere identificerende gegevens in te voeren. Zij kunnen anoniem blijven, als ze ten minste verder geen gegevens achterlaten waarmee kan worden achterhaald vanaf welke computer of smartphone zij handelen.²⁰ Voor het overmaken van bitcoins is alleen benodigd: het bitcoin-adres en de daarbij behorende privésleutel met behulp waarvan over de bitcoins op dat adres kan worden beschikt. Anders dan bij het overmaken van geld van de ene naar de andere bankrekening, is het niet relevant wie achter het betreffende bitcoin-adres schuilt gaat. Het ondertekenen van de transactie met de privésleutel dient er alleen maar toe in technische zin vast te stellen dat de ondertekenaar over de bitcoins mag beschikken die op het daaraan gekoppel-

Degene die zijn privésleutel kwijtraakt, kan niet meer beschikken over de bitcoins op het daarbij behorende bitcoin-adres

de bitcoin-adres staan. Het ondertekenen van de transactie dient er niet (ook) toe om de ondertekenaar als persoon te authenticeren: dus niet om vast te stellen dat de ondertekenaar is, wie hij zegt te zijn.

De keerzijde is dat degene die zijn privésleutel kwijtraakt, niet meer kan beschikken over de bitcoins op het daarbij behorende bitcoin-adres. Degene die zijn wachtwoord voor internetbankieren kwijt is, kan daarentegen uiteindelijk wel weer over het geld op zijn bankrekening beschikken. Dat kan hij bijvoorbeeld doen door langs te gaan bij een bankkantoor, zich te identificeren met zijn paspoort, zijn gezicht te tonen en zijn handtekening te zetten.

2.5. Technische samenvatting

Bezien vanuit de techniek kan het voorgaande als volgt worden samengevat:

14. Hoe die verificatie precies technisch is en welke transactiekosten daarvoor betaald moeten worden, is beschreven in A.M. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, Sebastopol, CA, USA: O'Reilly 2017, p. 212-267.

15. Zie in algemene zin D. Drescher, *Blockchain Basics. A Non-Technical Introduction in 25 Steps*, Apress: New York, 'Step 18 Verifying and Adding Transactions', p. 153-

164. Een miner downloadt mining software zoals CGMiner <https://en.bitcoin.it/wiki/CGMiner> of BFGMiner <http://bfgminer.org>, een node BitcoinCore <https://bitcoincore.org>.

16. Zie www.investopedia.com/tech/how-does-bitcoin-mining-work/ en A.M. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, Sebastopol, CA, USA: O'Reilly 2017, p. 28-29 (algemene beschrijving) en p. 213-240 (gedetailleerde

beschrijving).

17. In de praktijk werken miners samen in zogeheten mining pools en delen zij de eventuele winst die zij ontvangen (het block reward, zie hierna) als hun pool wint. Zie voor een overzicht van mining pools en hun 'marktaandeel' www.blockchain.com/pools.

18. Het block reward wordt ongeveer elke vier jaar gehalveerd. Zie voor het volgende moment <http://bitcoinclock.com>.

19. Zie voor een uitleg over hoe lang een

bitcoin transactie duurt <https://coincentral.com/how-long-do-bitcoin-transfers-take/>.

20. Ze kunnen voorkomen dat ze identificerende gegevens achterlaten door andere gebruik te maken van een Virtual Private Network (VPN) dienst, zoals NordVPN <https://nordvpn.com>, TorGuard <https://torguard.net> of private internet access www.privateinternetaccess.com/. Op dezelfde manier kunnen ook miners en nodes anoniem blijven.

- 1) een wallet bevat een privésleutel waarmee over bitcoins kan worden beschikt (en de wallet bevat dus niet de bitcoins zelf);
- 2) transacties in bitcoins worden opgeslagen op de blockchain (en dus niet in wallets);
- 3) transacties worden geverifieerd door miners die allemaal als eerste transacties willen verifiëren en een cryptografische puzzel willen oplossen;
- 4) het werk van de winnende miner (proposer) wordt gecontroleerd door nodes (aan het netwerk deelnemende computers die ieder het gedecentraliseerde grootboek hebben gedownload en verspreiden);
- 5) door de proposer goedgekeurde transacties worden als block aan de blockchain toegevoegd als minimaal 51% van de nodes het er overeen eens is dat de proposer zijn werk goed heeft gedaan;
- 6) in dat geval krijgt de proposer bitcoins (nieuwe bitcoins van het systeem en bestaande bitcoins van de overmaker (=transactiekosten));
- 7) deelnemers kunnen anoniem blijven; en
- 8) er is geen centrale instantie die verifieert of toezicht houdt.

3. Verbintenisrechtelijke analyse: de bitcoin-meerpartijovereenkomst

Hoe moet dit systeem verbintenisrechtelijk worden gekwalificeerd? Het bitcoin-systeem is mijns inziens aan te merken als een meerpartijovereenkomst.²¹ De allereerste deelname van een gebruiker, miner of node (tezamen: deelnemers) aan het bitcoin-netwerk valt in dat licht aan te merken als het aanvaarden van een impliciet derdenbeding (artikel 6:253 lid 1 BW). Dat derdenbeding is opgenomen in die meerpartijovereenkomst en is bedongen ten gunste van iedere gebruiker, miner en node die aan het bitcoin-netwerk wil deelnemen. Door aanvaarding van het op hem gerichte derdenbeding, wordt de betreffende gebruiker, miner of node partij bij de meerpartijovereenkomst (artikel 6:254 lid 1 BW). Die aanvaarding geschiedt door een verklaring (artikel 6:253 lid 3 BW) die besloten ligt in de deelname aan het netwerk (artikel 3:37 lid 1 BW) en die gericht is tot een andere deelnemer die dan al partij is bij de overeenkomst (artikel 6:253 lid 3 BW), te weten de eerste deelnemer met wie de kersverse toetredster voor het eerst peer-to-peer contact heeft. De meerpartijovereenkomst waarbij de kersverse toetredster partij is geworden, is een raamovereenkomst die niet alleen de algemene rechten en verplichtingen van partijen behelst, maar ook de rechten en verplichtingen ten aanzien van iedere afzonderlijke transactie. De inhoud van die rechten en verplichtingen is afhankelijk van de hoedanigheid van de betreffende deelnemer en valt daarom het makkelijkst

De bitcoin-meerpartijovereenkomst is geen klassieke, schriftelijke overeenkomst met allerlei contractsbepalingen

uit te leggen aan de hand van een voorbeeld, dat ik hierna zal behandelen.²²

Voordat ik dat doe, is het belangrijk te benadrukken dat de bitcoin-meerpartijovereenkomst geen klassieke, schriftelijke overeenkomst is met allerlei contractsbepalingen. Die meerpartijovereenkomst is een overeenkomst waarvan de inhoud wordt bepaald door de hiervoor beschreven techniek, meer in het bijzonder de werking van de bitcoin-software. Die software en de daarop betrekking hebbende documentatie is open-source en voor iedereen beschikbaar.²³ Door (de broncode van) die software te analyseren en die documentatie te lezen weet iedere deelnemer aan het bitcoin-netwerk, afhankelijk van de hoedanigheid waarin hij aan het bitcoin-netwerk deelneemt, wat hij moet doen of, met andere woorden, welke verplichtingen hij ten opzichte van zijn soortgenoten en andere soorten deelnemers heeft. Aangezien die verplichtingen niet met zoveel woorden in de meerpartijovereenkomst zijn opgenomen, maar uit de techniek volgen, zal ik van veel bedingen zeggen, dat ze impliciet zijn overeengekomen.

Verder is het goed stil te staan bij het einde van de meerpartijovereenkomst. Dat is op het moment dat die miner of node niet meer deelneemt aan het bitcoin-netwerk. Dan eindigt alleen het gedeelte van de meerpartijovereenkomst dat op hem van toepassing is en blijft de rest van de meerpartijovereenkomst gewoon bestaan. De miner of node die niet meer deelneemt, treedt dan als het ware uit de overeenkomst (als tegenovergestelde van toetreden tot de overeenkomst). De meerpartijovereenkomst is dus een overeenkomst waarbij derden op elk moment kunnen toe- of uittreden en ten aanzien waarvan dus steeds crediteurs- en debiteursvervanging plaatsvindt (waarover later meer).

Laten we nu, zoals gezegd, de inhoud van de rechten en verplichtingen illustreren aan de hand van een voorbeeld. Neem weer gebruiker A die één bitcoin wil overmaken naar B. A voert de vereiste transactiegegevens in zijn app in, ondertekent die transactie met zijn privésleutel en stuurt die het bitcoin-netwerk in. Door het eerste contact met het bitcoin-netwerk aanvaardt hij het tot hem gericht derdenbeding en wordt hij zodoende partij bij de meerpartijovereenkomst. Iedere miner die dan al deelneemt aan het bitcoin-netwerk is al partij geworden door zijn eerst contact met dat netwerk, net als iedere node dat is geworden door zijn eerste contact.

Iedere miner heeft zich ertoe verbonden mee te doen aan iedere speed competition die wordt geïnitieerd door gebruikers die transacties wensen te verrichten. In dat kader is de betreffende miner gehouden diensten te verrichten (te weten: transacties opnemen in een block, transacties verifiëren en cryptografische puzzels oplossen), tegen betaling (van het block reward en de transactiekosten) aan de winnende proposer wiens candidate block aan de blockchain wordt toegevoegd, op *no cure no pay* basis dus.

Iedere node heeft zich er op zijn beurt toe verbonden het door iedere proposer verrichte werk te controleren, en dus vast te stellen of die proposer terecht heeft vastgesteld of de in het candidate block opgenomen transacties van de gebruikers juist zijn en of de oplossing van de cryptografische puzzel klopt. Van die verplichting is de

node gekweten op het moment dan meer dan 51% van de nodes eensgezind de controle heeft uitgevoerd. Voor die controle door de nodes hoeft overigens niet rechtstreeks te worden betaald en dat is juridisch gezien ook niet nodig. Overigens zou wel een vorm van indirecte betaling kunnen worden geconstrueerd. Nodes die zelf transacties verrichten hebben er immers baat bij dat ook hun transacties worden gecontroleerd. En nodes die zelf *minen* hebben er baat bij de proposers te controleren. Immers, als zij vaststellen dat een proposer zijn werk niet goed heeft gedaan, begint de speed competition weer opnieuw en maakt iedere miner weer kans proposer te worden. Als hij vervolgens proposer wordt en blijkt dat hij zijn werk wel goed heeft gedaan, ontvangt hij het block reward en de transactiekosten.

De hiervoor beschreven rechten van de gebruiker ten opzichte van de miners en nodes om hun verificatie- respectievelijk controlewerkzaamheden te verrichten, zijn vorderingen en noem ik hierna gemakshalve *bitcoin-vorderingen*.²⁴ Die vorderingen moeten worden geëffectueerd om ervoor te zorgen dat bitcoins van het ene naar het andere bitcoin-adres worden overgemaakt. Tot dusver de technische uitleg en verbintenismatige kwalificatie, die ik nodig heb om bitcoins ook goederenrechtelijk te kunnen kwalificeren.

4. Goederenrechtelijke analyse

Nu is uitgelegd hoe de techniek werkt en welke overeenkomsten met welke inhoud tussen welke deelnemers tot stand komen, is het tijd te bezien hoe bitcoins vanuit goederenrechtelijk perspectief kunnen worden gekwalificeerd. Anderen gingen mij daarin voor. Van den Berg, Van der Velden & Vergouwen menen dat bitcoins 'stukjes software' zijn, die als vermogensrechten naar buitenlands recht gekwalificeerd moeten worden omdat de software in de VS is uitgegeven onder de MIT open source-licentie.²⁵

Het juridisch weerspiegelen van de technische werkelijkheid is nodig omdat code in blockchain-gevallen (vaak) law is

Rank meent het volgende: een bitcoin heeft meer weg van een zaak dan een vermogensrecht, maar kan slechts in het vermogensrechtelijke systeem worden ingepast door het te beschouwen als een (absoluut) vermogensrecht, hoewel dat wringt omdat rechten op een bitcoin op die manier met een bitcoin worden vereenzelvigd, terwijl het om verschillende dingen gaat.²⁶ Dammers vindt de bitcoin eerder een absoluut dan een relatief vermogensrecht.²⁷ Mijnsen concludeert dat een bitcoin moeilijk onder de categorie vermogensrecht van artikel 3:6 BW te brengen valt en dat, als een bitcoin al een goed is, een bitcoin niet overdraagbaar is omdat een bitcoin niet valt onder de in artikel 3:83 lid 3 BW genoemde rechten.²⁸ Daarentegen kwalificeert Tweehuysen bitcoin wel als een (absoluut) vermogensrecht.²⁹ J.L. Snijders & Tonino menen dat het bitcoin-stelsel grote gelijkenissen vertoont met het bartering-systeem³⁰ en dat (de door Geiregat gecoïnde en ook door hen gebruikte term) bitcoin-kapitaalcracht (mede) om die reden, net als het recht van het bartering-lid op bartering-eenheden, een vermogensrecht is in de zin van artikel 3:6 BW.³¹

Ook in de rechtspraak worden verschillende opvattingen gehuldigd. Daar worden bitcoins aangemerkt als ruilmiddel³² en op één lijn gesteld met goederen met een dagprijs in de zin van artikel 7:36 BW.³³ Ether, een andere cryptocurrency, wordt aangeduid als een goed.³⁴

21. Vergelijk S. Geiregat, 'Eigendom op bitcoins', *Rechtskundig Weekblad* 2017-18, nr. 27, p. 1043-1049 en voor een bewerkte, Engelstalige versie van dat artikel S. Geiregat, 'Cryptocurrencies are (smart) contracts', *Computer Law & Security Review*, 29 juni 2018, p. 1-6, <https://doi.org/10.1016/j.clsr.2018.05.030>, die naar Belgisch recht het bitcoin-netwerk als een meerpartijenovereenkomst beschouwt en de daaruit voortvloeiende rechten ziet als verwachtingen van degene die een bitcoin wallet heeft dat de overige deelnemers bitcoins als betaalmiddel aanvaarden wanneer diegene wil voldoen aan een betalingsverplichting jegens een van die overige deelnemers.

22. Deelnemers kunnen overigens in verschillende hoedanigheden aan het bitcoin-netwerk deelnemen. Miners zijn bijvoorbeeld ook vaak nodes.

23. Zie <https://github.com/bitcoin/bitcoin> respectievelijk <https://bitcoin.org/en/developer-documentation>.

24. Vergelijk M. Weij & M.C. Landerbarthold, 'Ruis in de ether en de juridische kwalificatie(s) van cryptovaluta. Noot bij Rechtbank Midden-Nederland 7 december 2017, ECLI:NL:RBMNE:2017:6646', *Tijdschrift voor Internetrecht* 2018-2, p. 67, die menen dat 'je een cryptovaluta in het kader van art. 3:6 BW eerder zou kunnen zien als een vordering die de "eigenaar" ervan heeft op de volledige crypto-valuta-gemeenschap in de Blockchain', hoewel niet duidelijk wordt welke inhoud die vordering volgens hen heeft. Vergelijk ook T.F.E. Tjong Tjin Tai, 'De blockchain als alternatief voor de notariële praktijk', in: F.W.J.M. Schols & B.C.M. Waaijer (red.), *Financiële zorgplicht van de notaris (preadviezen KNB)*, Den Haag: Sdu 2018, p. 123, die schrijft: 'Misschien is het wel mogelijk om de controlemogelijkheden of potentiële aanspraak op een tegoed in bitcoin te beschouwen als een vorderingsrecht, waar men bij de partij die de aanspraak heeft derdenbeslag zou kunnen leggen.'

25. M.F.M. van den Berg, J.W.P.M. van der Velden & C.W.M. Vergouwen, 'De Bitcoin-verzekering. Een kans voor de financiële sector om klantbelang centraal te stellen in innovatieve productontwikkeling', *MvV* 2014-5, p. 131.

26. W.A.K. Rank, 'Bitcoins: civielrechtelijke en toezichtrechtelijke aspecten' in: R.A. Wolf e.a., *Bitcoins. Civiele en fiscale aspecten in beeld*, Deventer: Kluwer 2015, p. 36-37.

27. W.F. Dammers, 'Bitcoins: een vreemde zaak? Noot bij Hof Arnhem-Leeuwarden 1 mei 2016, ECLI:NL:GHARL:2016:4219', *Tijdschrift voor Internetrecht* 2016-3, p. 112.

28. Mijnsen, *Verbintenissen tot betaling van een geldsom (Mon. BW nr. B39)*, 2017/1.6.

29. V. Tweehuysen, 'Goederenrechtelijk puzzelen met bitcoins', *AA* 2018-juli/augustus, p. 602-610.

30. Waarover HR 5 november 1993, ECLI:NL:HR:1993:ZC1128, *NJ* 1994/640

(Bartering), m.nt. H.J. Snijders.

31. J.L. Snijders & Y.C. Tonino, 'Goederenrechtelijke status van bitcoin (kapitaalcracht)', *Tijdschrift Financiering, Zekerheden en Insolventierechtpraktijk* 2018-6, p. 46-55, die op p. 50 bitcoin kapitaalcracht definiëren als 'de positie die de bitcoin-gebruiker... heeft, vanwege de verwachting dat hij die bitcoin-transacties kan doen in ruil voor een bepaalde tegenprestatie van de ontvangende bitcoin-gebruiker...'.
32. Rb. Overijssel 14 mei 2015, ECLI:NL:RBOVE:2014:2667, *JOR* 2014/266, m.nt. B. Bierens.
33. Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219, het hoger beroep van Rb. Overijssel 14 mei 2015, ECLI:NL:RBOVE:2014:2667, *JOR* 2014/266, m.nt. B. Bierens.
34. Rb. Midden-Nederland (vzr.) 7 december 2017, ECLI:NL:RBMNE:2017:6646.

En bitcoin wordt geacht 'kenmerken van een vermogensrecht' te vertonen, waardoor een vordering tot betaling in bitcoin beschouwd wordt als een vordering die in het kader van het faillissementsrecht voor verificatie in aanmerking komt.³⁵

In het buitenland is men eveneens driftig bezig bitcoins goederenrechtelijk te kwalificeren. Ten aanzien van het Belgische recht meent Vanwynsberghe dat bij mining de miner als gevolg van zaaksvorming het eigendomsrecht op de nieuw ontstane bitcoins verkrijgt en dat alleen paper wallets waardepapieren zijn, maar concludeert vervolgens dat bitcoin een onlichamelijk goed is dat tussen de privaatrechtelijke mazen van het net valt.³⁶ Ten aanzien van het Duitse recht concluderen Engelhardt & Klein, mede op grond van de numerus clausus (het gesloten stelsel van goederenrechtelijke rechten), dat de overdracht van bitcoins uitsluitend op verbintenisrechtelijk vlak plaatsvindt, een 'Realakt' is en geen verandering in de goederenrechtelijke posities tot gevolg heeft.³⁷ En in Rusland is, naar verluidt, wetgeving in voorbereiding op grond waarvan rechten ten aanzien van cryptocurrencies als goederenrechtelijke rechten worden aangemerkt.³⁸

Ieder van deze benaderingen heeft voor- en nadelen. Gelet op de omvang van deze bijdrage zal ik echter, anders dan te doen gebruikelijk, niet die voor- en nadelen daarvan bespreken en mijn eigen mening daarover vormen. In plaats daarvan ga ik vanuit de eerder gegeven technische uitleg en verbintenisrechtelijke kwalificatie op zoek naar een goederenrechtelijke kwalificatie die het beste past bij de wijze waarop het bitcoin-netwerk technisch functioneert. Het juridisch weerspiegelen van die technische werkelijkheid is nodig omdat code in blockchain-gevallen (vaak) law is.³⁹

Gelet op het voorgaande, moet een goederenrechtelijke kwalificatie aan de volgende, door de techniek bepaalde, drie eisen voldoen:

- 1) anonimiteit omdat het bitcoin-netwerk alleen waarde hecht aan het feit *dat* de transactie met de bij het bitcoin-adres behorende privésleutel wordt ondertekend, niet *wie* ondertekent;
- 2) eenvoudige crediteursvervangingsom dezelfde reden; en
- 3) eenvoudige debiteursvervangingsomdat miners en nodes op ieder moment kunnen toe- of uittreden tot respectievelijk uit de bitcoin-meerpartijenovereenkomst.

Bij de kwalificatie moet worden bedacht dat het feitelijk gezien een doodlopende weg is om te focussen op de goederenrechtelijke kwalificatie van (de registratie van) een bitcoin en bitcoin-transacties in het bitcoin-grootboek zoals opgeslagen in het blockchain-bestand. Dat bestand is immers decentraal opgeslagen op alle nodes overal ter wereld en dat zijn er op dit moment zo'n 10.000.⁴⁰ Daardoor is er geen uniek bestand en is het vervreemden, bezwaren, beslaan van en verhalen op alle of de meerderheid van die bestanden in ieder geval praktisch vrijwel onmogelijk. Dat is met opzet zo. Het bitcoin-netwerk is gebouwd om ervoor te zorgen dat een 'aanval' op één of meerdere nodes geen effect sorteert. Eveneens doodlopende kwalificatiewegen zijn wegen die voor het

vervreemden, bezwaren, beslaan of verhalen van/op bitcoins een handtekening vereisen, bijvoorbeeld omdat voor overdracht een akte vereist is.⁴¹ Een handtekening zoals bedoeld in ons Burgerlijk Wetboek en Wetboek van Burgerlijke Rechtsvordering dient er immers toe⁴² om degene die hem zet (de ondertekenaar) in staat te stellen zich te identificeren (duidelijk te maken wie hij is) en degene die het aldus ondertekende ontvangt om desgewenst, met gebruikmaking van de aldus gezette handtekening, de ondertekenaar te authenticeren (het betrouwbaar kunnen aantonen dat de ondertekenaar degene is die hij zegt of pretendeert te zijn). Dat proces van identificeren (door de gebruiker) en authenticeren (door miners en nodes) kan niet plaatsvinden in het bitcoin-netwerk. Het bitcoin-netwerk is immers gebouwd om anoniem transacties te verrichten.

Uitgaande van de bestaande feitelijke en juridische werkelijkheid, moet naar mijn idee worden gefocust op de privésleutel, de wallet waarin die sleutel is opgeborgen en de drager waarop de wallet staat. Alleen daarmee kan immers in technische zin over de bitcoins worden

Als een bitcoin gedolven is, worden op het zelfde moment de vorderingen ten opzichte van de miners en nodes aan toonder gesteld

beschikt. Vanuit juridisch perspectief is mijn eerste gedachte te onderzoeken of die drager als een waardepapier, en wel een toonderpapier, kan worden gekwalificeerd.⁴³ Toonderpapieren lenen zich immers bij uitstek voor anonimiteit en eenvoudige crediteursvervangingsom die reden onderzoek ik hierna of bitcoins goederenrechtelijk gezien als toonderpapieren kunnen worden gekwalificeerd en daarmee aan de drie gestelde eisen (anonimiteit, eenvoudige crediteursvervangingsom eenvoudige debiteursvervangingsom) kan worden voldaan.

4.1. De fysieke verschijningsvorm van de wallet als belichaming van de bitcoin-vorderingen

Bitcoins worden, zoals gezegd, door een miner als block reward gedolven/gecreëerd op het moment dat (i) minimaal 51% van de nodes erkent dat de in het candidate block opgenomen transacties op de juiste wijze zijn geverifieerd en de bijbehorende cryptografische puzzel goed is opgelost en (ii) de block reward bitcoins zijn bijgeschreven op het door de miner opgegeven bitcoin-adres. Aannemende dat de miner bij gebruikmaking van het bitcoin-netwerk niet zelf (on)bewust persoons- of andere identificerende gegevens heeft achtergelaten, kan dat delven niet aan een (rechts)persoon worden gekoppeld en is dus in technische zin sprake van een anoniem creëren.

Door het aldus aan toonder stellen wordt die levering ineens ook juridisch een fluitje van een satoshi

Over die bitcoins op dat bitcoin-adres kan de miner vervolgens alleen beschikken met gebruikmaking van de bij dat bitcoin-adres behorende privésleutel. Om een bitcoin te kunnen overmaken, maakt de houder van die privésleutel aanspraak op de hiervoor beschreven vorderingen ten opzichte van de miners en nodes om hun verificatie- respectievelijk controlewerkzaamheden te verrichten. Bij het uitvoeren van hun werkzaamheden checken miners en nodes, zoals gezegd, alleen of de privésleutel gekoppeld is aan het bitcoin-adres, en niet wie daarachter schuil gaat. Het maakt, met andere woorden, voor de miners en nodes niet uit of de privésleutel wordt gepresenteerd door, in dit geval, degene die de bitcoins gedolven heeft, iemand aan wie hij zijn privésleutel heeft gegeven of iemand die die sleutel gestolen heeft. Om die technische werkelijkheid ook juridisch te weerspiegelen moeten die vorderingen ten opzichte van de miners en nodes zo snel mogelijk aan toonder worden gesteld. Voor de volledig automatisch handelende miners en nodes heeft immers degene die die privésleutel als eerste toont, en niemand anders, recht de bitcoins over te maken (naar een bitcoin-adres van een ander of naar een ander bitcoin-adres van zichzelf).

Gelet op de manier waarop de techniek werkt, denk ik dat, juridisch gezien, als een bitcoin gedolven is, op hetzelfde moment (of een juridische Planck seconde⁴⁴ later) de vorderingen ten opzichte van de miners en nodes aan

toonder worden gesteld, en wel aan de toonder van de privésleutel die hoort bij het bitcoin-adres waar die bitcoin op staat. Die vrijheid om de bitcoin-vorderingen⁴⁵ aan toonder te stellen bestaat. Nederland kent een open stelsel van waardepapierenrecht: partijen zijn vrij om hun vorderingen aan toonder te stellen, of partijen dat willen is een kwestie van uitleg en zelfs als niet aan specifieke vormvereisten voor het (meest) in aanmerking komende waardepapier is voldaan, is de wettelijke regeling met betrekking tot dat waardepapier weliswaar niet van toepassing, maar het algemene waardepapierenrecht wel.⁴⁶ Door de wijze waarop het overmaken van het ene naar het andere bitcoin-adres technisch gezien werkt, dient er mijns inziens vanuit te worden gegaan dat partijen in de bitcoin-meerpartijenovereenkomst zijn overeengekomen dat bij ieder delven van bitcoins de bitcoin-vorderingen ten aanzien van die bitcoins meteen aan toonder worden gesteld, en wel aan de toonder van de (drager van de) privésleutel die gekoppeld is aan het bitcoin-adres waarop het block reward wordt bijgeschreven. Aldus wordt een toonderpapier gecreëerd. Hetzelfde geldt mutatis mutandis op het moment dat eenmaal gedolven bitcoins van het bitcoin-adres van de winnende miner worden overgemaakt naar een ander bitcoin-adres, alsmede voor ieder daaropvolgend overmaken. Zodra overgemaakte bitcoins confirmed op een ander bitcoin-adres zijn bijgeschreven, worden dus tegelijkertijd de bitcoin-vorderingen ten aanzien van die bitcoins aan toonder gesteld, en wel aan de toonder van de (drager van de) bij dat adres behorende privésleutel.

Dat toonderpapier is als volgt vormgegeven. De privésleutel waarmee over de gedolven of anderszins bijgeschreven bitcoins kan worden beschikt, is, zoals we zagen, opgeslagen in een wallet. De wallet is op zijn beurt een fysieke drager (paper wallet) of opgeslagen op een fysieke drager (overige wallets). Als de wallet is opgeslagen op een fysieke drager, dan is dat in de vorm van een bestand met

35. Rb. Amsterdam 14 februari 2018, ECLI:NL:RBAMS:2018:869, JOR 2018/154, m.nt. B. Bierens (*Koinz Trading*).

36. M. Vanwynsberghe, 'Bitcoin heeft het op de grenzen van het goederenrecht gemunt', *Rechtskundig Weekblad* 2014/15-37, p. 1442.

37. C. Engelhardt & S. Klein, 'Bitcoins – Geschäfte mit Geld, das keines ist. Technische Grundlagen und zivilrechtliche Betrachtung', *MMR* 2014-355.

38. Zie A. Seveliev, 'Some risks of tokenization and blockchainization of private law', *Computer Law & Security Review* 2018-34, p. 863-869.

39. Zie daarover T.J. de Graaf, 'Van oud naar nieuw: van internet naar smart contracts en van mensen naar code (I) en (II)', *WPNR* 7199 16 juni 2018, p. 494-501 en *WPNR* 7200 23 juni 2018, p. 525-530 en P. Filippi & A. Wright, *Blockchain and the Law. The Rule of Code*, Cambridge, Massachusetts: Harvard University Press

2018, die in dat verband over *lex cryptographica* spreken.

40. Voor een overzicht van deelnemende nodes en de landen waarin ze staan <https://bitnodes.earn.com>.

41. Akten zijn 'ondertekende geschriften, bestemd om tot bewijs te dienen', aldus art. 156 lid 1 Rv.

42. Zie voor een uiteenzetting van de functies van handtekeningen, en overigens ook geschriften, in het kader van de gelijkstellingsvraag van elektronische met schriftelijke handtekeningen S.M. Huydecoper & R.E. van Esch, *Geschriften en handtekeningen: een achterhaald concept?*, ITeR-reeks nr. 7, Alphen aan den Rijn/Diegem: Samsom Bedrijfsinformatie 1997, p. 71-162 en zie verder over de gelijkstelling van elektronische met schriftelijke stukken T.J. de Graaf, 'De lappendeken van de gelijkstelling van elektronisch met schriftelijk in het licht van vormvereisten en bewijskracht', *MvV* 2018/7-8, p. 243-248.

43. Zie voor een vergelijkbaar onderzoek, maar dan naar het gelijkstellen van elektronisch geld met waardepapieren R.E. van Esch, *Pecunia electronica non olet. Van gelijke behandeling van elektronisch geld met waardepapieren* (oratie Leiden), Deventer: Kluwer 2001, waarover de boekbespreking van G.J. van der Ziel R.E. van Esch, 'Pecunia electronica non olet. Van gelijke behandeling van elektronisch geld met waardepapieren', *RM Themis* 2004-1, p. 38-40. Zie voor een vergelijkbaar onderzoek naar het gelijkstellen van elektronische wissels en cheques met papieren wissels en cheques R.E. van Esch, 'De elektronische wissel en de elektronische cheque', in: R.E. van Esch, J.W. Winter & G.J. van der Ziel, *Afscheid van papier. Handelsrecht en moderne technologie (preadvis van de Vereniging 'Handelsrecht')*, Deventer: W.E.J. Tjeenk Willink 2001, p. 17-54. In beide onderzoeken wordt gelijkstelling bepleit.

44. In de juridische literatuur wordt vaak gesproken over een juridische seconde, maar in het licht van technologische ontwikkelingen lijkt het beter te spreken over een Planck seconde omdat dat volgens veel natuurkundigen de kortst mogelijke tijdsinterval is, zie https://en.wikipedia.org/wiki/Planck_time.

45. Ter herinnering: bitcoin-vorderingen zijn de vorderingen van de gebruiker ten opzichte van de miners en nodes om hun verificatie- respectievelijk controlewerkzaamheden te verrichten, welke werkzaamheden moeten worden uitgevoerd teneinde bitcoins van het ene naar het andere bitcoin-adres te kunnen overmaken.

46. R. Zwitser, *Order- en toonderpapieren (Monografieën BW nr. A28)*, Deventer: Wolters Kluwer 2017, nrs. 4 en 5, onder verwijzing, voor wat betreft het open stelsel, naar HR 19 april 2002, ECLI:NL:HR:2002:AE1683, *NJ* 2002/456 (Zürich/Lebosch).

privésleutel dat op een schijf staat, in de regel *flash geheugen*, of op een *solid state drive* of *hard disk*. Als het een schijf betreft, zit die op zijn beurt in een *dedicated device*, zoals een hardware wallet (het USB-stick achtige device), of een *non-dedicated device* waar in de regel ook iets anders op staat (zoals een smartphone of computer). Doordat de bitcoin-vorderingen aan toonder zijn gesteld (en wel aan de toonder van de privésleutel die aan het betreffende bitcoin-adres is gekoppeld), die privé sleutel in een wallet zit en die wallet (uiteindelijk) een fysieke verschijningsvorm heeft, zijn de bitcoin-vorderingen dus (uiteindelijk) belichaamd in een fysieke drager. Die fysieke drager zal ik hierna aanduiden met het neutrale begrip *waardedragers*.⁴⁷ Of het woord 'papier' bij dit alles roet in het eten gooit en hoe dat toonderpapier door de een aan de ander kan worden gegeven respectievelijk genomen zonder dat er bij de gever iets achterblijft, bespreek ik hierna onder de tegenwerpingen.

Anonimiteit en crediteursvervangings

Eerst maak ik de juridische kwalificatie af, van bitcoin-vorderingen als in de waardedragers belichaamde vorderingen. Is eenmaal aldus gekwalificeerd, dan is het betrekkelijk eenvoudig te voldoen aan de eisen van anonimiteit en

Voor een rechter lijkt het geen probleem te concluderen dat het aan toonder stellen van de bitcoin-vorderingen gelijk te stellen is met het in het leven roepen van een papieren waardepapier

eenvoudige crediteursvervangings. Het bitcoin-netwerk functioneert naar zijn aard op anonieme basis en het aan toonder stellen van de bitcoin-vorderingen ondermijnt dat niet. Het aan toonder stellen immers geen vermelding van persoons- of andere identificerende gegevens. Een waardepapier hoeft bijvoorbeeld niet ondertekend te zijn, wil het een waardepapier zijn. De wet veronderstelt in artikel 3:93 BW slechts dat er papier wordt gebruikt en ondertekening is geen vereiste voor het ontstaan van een waardepapier of de levering van de daarin belichaamde bitcoin-vorderingen.⁴⁸ En door het aldus aan toonder stellen wordt die levering ineens ook juridisch een fluitje van een satoshi.⁴⁹ Dan kunnen die vorderingen immers geleverd worden door bezitsverschaffing van de waardedragers ex artikel 3:93 jo. 3:90 BW, een eenvoudige manier van crediteursvervangings.

Debiteursvervangings

Ik keer terug naar de eis van eenvoudige debiteursvervangings. Er moet een constructie worden bedacht om het ook juridisch mogelijk te maken dat de miners en nodes die uit

de bitcoin-meerpartijenovereenkomst *uittreden*, vervangen worden door miners en nodes die tot die overeenkomst *toetreden*. Dat is een uitdaging. Het aan toonder stellen van vorderingen leidt slechts tot een eenvoudige manier van crediteursvervangings, maar biedt geen mogelijkheden ook de debiteur(en) eenvoudig te vervangen. De meest voor de hand liggende mogelijkheid om de tegenover de bitcoin-vorderingen staande verplichtingen (ofwel schulden) over te doen gaan, is schuldoverneming van die verplichtingen ex artikel 6:155 BW. Dat geschiedt door middel van een vormvrije overeenkomst waarbij een derde de schuld van de debiteur overneemt, en de crediteur daarin vormvrij toestemt. Deze oplossing ligt echter niet voor de hand omdat het niet per se de schuld is van de ene uittredende miner of node (om aan de bitcoin-vorderingen van de gebruikers te voldoen) die één-op-één door een andere toetredende miner respectievelijk node wordt overgenomen.

Het ligt meer voor de hand dat in de meerpartijenovereenkomst, impliciet en reeds nu voor alsdan, is overeengekomen dat iedere miner en node mag uittreden uit die overeenkomst en dat op dat moment de gebruikers afstand doen van hun bitcoin-vorderingen ten opzichte van die uittredende miner of node (artikel 6:160 BW). De 'nieuwe' miners en nodes die, door aanvaarding van de tot hen gerichte derdenbedingen, partij worden bij de meerpartijenovereenkomst gaan, in die opvatting, op hun beurt en ieder voor zich, een zelfstandige schuld aan ten opzichte van de gebruikers. Ook die opvatting is niet overtuigend. Als miners en nodes zich zo makkelijk aan hun verplichtingen kunnen onttrekken door simpelweg de verbinding met het bitcoin-netwerk te verbreken en ze daardoor meteen gekweten zijn van hun tegenover de bitcoin-vorderingen staande verplichtingen, is dan (bij nader inzien) überhaupt wel sprake van rechtens afdwingbare verplichtingen, waarvan de daartegenover staande rechten als vorderingen op naam kunnen worden gekwalificeerd en ten aanzien waarvan crediteursvervangings kan plaatsvinden door bezitsverschaffing van de waardedragers.⁵⁰

Een mogelijkheid om de aangedragen verbintenissen goederenrechtelijke kwalificatie wel rond te krijgen, is om de hulp van het ondernemingsrecht in te roepen. Het bitcoin-netwerk kan namelijk ook gezien worden als een meerpartijenovereenkomst waaraan gebruikers, een miners-rechtspersoon en een nodes-rechtspersoon deelnemen. De twee rechtspersonen nemen ieder voor zich een zelfstandige verplichting op zich om de werkzaamheden te verrichten die door miners respectievelijk nodes verricht moet worden. Aan de 'achterkant' van die rechtspersonen werken verschillende (rechts)personen, die steeds starten en stoppen met werken. Dat gebeurt op dezelfde manier als bij een rechtspersoon waarvan het personeels- en onderaannemersbestand, waarmee de rechtspersoon haar werkzaamheden voor haar klanten verricht, fluctueert omdat nieuwe arbeids-/onderaannemingsovereenkomsten worden aangegaan respectievelijk beëindigd. Welke rechtspersoon hier het meest geschikt voor is en hoe de externe en interne verhoudingen van die rechtspersoon in elkaar steken, valt buiten het bestek van deze bijdrage.

Wat wel binnen dat bestek valt, is een bespreking van twee belangrijke tegenwerpingen ten aanzien van de voorgestelde waardedragersconstructie: ten eerste, het

elektronische waardepapier is geen waardepapier omdat het niet van papier is en ten tweede, een elektronisch waardepapier is geen waardepapier omdat het niet kan worden gegeven en genomen. Die tegenwerpingen bespreek ik nu.

4.2. Tegenwerping 1: een waardepapier is van papier

Een waardepapier veronderstelt dat er papier wordt gebruikt; hoe wordt aan dat vereiste voldaan bij de aangedragen waardedragerechterlijke kwalificatie? Over het algemeen wordt immers aangenomen dat waardepapieren niet elektronisch kunnen bestaan omdat het op waardepapieren van toepassing zijnde leveringsartikel (artikel 3:93 BW) veronderstelt dat sprake is van een papier dat in de macht moet worden gebracht van de verkrijger.⁵¹ Artikel 6:227a lid 1 BW bepaalt echter dat als uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, daaraan ook is voldaan als aan een aantal in dat artikel gestelde vereisten is voldaan.⁵² Aan die vereisten wordt voldaan, zoals hierna zal blijken.

De inhoud van een bitcoin-transactie is voor partijen raadpleegbaar (artikel 6:227a lid 1 onder a BW). Zoals een papieren waardepapier kan worden gelezen teneinde vast te stellen wat de inhoud van de daaruit voortvloeiende rechten en verplichtingen is, zo kan iedereen (dus ook iedere partij) de blockchain raadplegen en daarop nagaan hoeveel bitcoins op welk bitcoin-adres staan.⁵³ De overige, hiervoor omschreven rechten en verplichtingen van de gebruikers, miners en nodes – zeg maar de algemene voorwaarden – vloeien voort uit de techniek, meer in het bijzonder de werking van de bitcoin-software in het bitcoin-netwerk. Zoals gezegd is die software en de daarop betrekking hebbende documentatie open-source en voor iedereen beschikbaar, en vloeien daar de rechten en verplichtingen van partijen uit voort. Sterker nog, de rechten en verplichtingen van iedere deelnemer zijn veel preciezer vastgelegd dan in een papieren waardepapier. De inhoud van de rechten en verplichtingen in een papieren waardepapier is immers vervat in tekst, over de interpre-

tatie waarvan geschillen kunnen ontstaan. De inhoud van de rechten en verplichtingen met betrekking tot bitcoins wordt daarentegen bepaald door code waarvan op voorhand kan worden vastgesteld hoe die zal worden uitgevoerd. Zoals gezegd, bij blockchain is code (meestal) law.

Ook de authenticiteit van de overeenkomst is in voldoende mate gewaarborgd (artikel 6:227a lid 1 onder b BW). Die eis is in de wet opgenomen omdat papier partijen beschermt tegen onopgemerkte manipulatie van de daarop vastgelegde gegevens, terwijl elektronisch bestanden makkelijker onopgemerkt kunnen worden gemanipuleerd (tenminste, als ze daartegen niet zijn beveiligd).⁵⁴ De bitcoin blockchain is echter juist zo ingericht dat als transacties eenmaal zijn vastgelegd in een blok op de blockchain, ze niet kunnen worden gewijzigd. De authenticiteit van de daarin opgenomen transacties is dus gewaarborgd. Sterker nog, met gebruikmaking van hedendaagse scan-, photoshop- en printtechnieken is het vervaardigen van een gemanipuleerde kopie en het vervolgens vernietigen van het papieren origineel vele malen eenvoudiger dan het manipuleren en vernietigen van een transactie die in de blockchain is opgeslagen.

Het moment van totstandkoming van de overeenkomst kan eveneens met voldoende zekerheid worden vastgesteld (artikel 6:227a lid 1 onder c BW). Het moment waarop een bitcoin op een bitcoin-adres wordt bijgeschreven, wordt immers tot op de seconde nauwkeurig in de blockchain vastgelegd. Bij papier is het moment van totstandkoming daarentegen vaak veel onzekerder.

De laatste eis is dat 'de identiteit van de partijen met voldoende zekerheid kan worden vastgelegd' (artikel 6:227a lid 1 onder d BW). Dat is een lastige eis omdat het bitcoin-netwerk, vanwege de gewenste anonimiteit, nu juist niet de identiteit van partijen registreert. Ondanks dat de wettekst doet vermoeden dat de eisen a t/m d cumulatief zijn, kan hier de parlementaire geschiedenis als een konijn uit de hoge hoed worden getoverd. Volgens de wetgever geven de eisen a t/m d enkel aan dat de gelijkstelling van elektronisch met papier in ieder geval plaatsvindt als aan alle eisen wordt voldaan, maar is het

47. Vergelijk het begrip 'duurzame gegevensdrager' uit onder andere art. 2 sub 10 en overweging 23 van de Richtlijn consumentenrechten 2011/83/EU, geïmplementeerd in art. 6:230g lid 1 onder h BW en waarover HvJ EU 5 juli 2012, ECLI:EU:C:2012:419, NJ 2012/542, m.nt. Mok en *Computerrecht* 2012/184, m.nt. Van Esch (*Content Services/Bundesarbeitskammer*) en HvJ EU 25 januari 2017, ECLI:EU:C:2017:38, TvC 2017-4, p. 178-182, m.nt. M.Y. Schaub (*BAWAG/Verein für Konsumenteninformation*).

48. Mr. M. Polak's Handboek voor het Nederlandse Handels- en faillissementsrecht, Derde deel, *Wissel- en Chequerecht*, door F.G. Scheltema, bewerkt door W.R. Meijer, Alphen aan den Rijn: Samson H.D. Tjeenk Willink 1993, p. 25 alsmede R. Zwitser, *Order- en toonderpapieren* (Monogra-

fiën BW nr. A28), Deventer: Wolters Kluwer 2017, nr. 1, die beiden onder andere verwijzen naar het feit dat een boekenbonnetoonderpapier is en in de regel ook niet ondertekend is. Zie ook G. van Empel & J.B. Huizink, *Betaling, waardepapier en documentair krediet*, Deventer: Kluwer 2002, nr. 24, die erkennen dat de wet nergens een handtekening eist voor het aan toonderstellen van een vordering, maar dat waardepapieren meestal wel ondertekend zijn. Anders: A. van Oven, *Handelsrecht*, Zwolle: W.E.J. Tjeenk Willink 1981, p. 206, die stelt dat een waardepapier een akte moet zijn en mitsdien door de schuldenaar moet zijn ondertekend.

49. Een satoshi is, zoals gezegd, de kleinste denominatie van een bitcoin, net als dat een cent de kleinste denominatie van een euro is, zie <https://en.bitcoin.it/wiki/>

Satoshi_(unit). Voor een wiskundige gelijkstelling zou wellicht over 10.000 satoshi's gesproken moeten worden om, net als bij een cent, op 1/100ste deel uit te komen.

50. Dezelfde vraag kan worden gesteld als we het uit het wisselrecht afkomstige concept van wisselschuldenaren zouden mogen veralgemeniseren en ten aanzien van de aan toonder gestelde bitcoin-vorderingen zouden mogen toepassen. Dat concept houdt in dat degene die zijn handtekening op het waardepapier zet, ten opzichte van de uiteindelijke houder daarvan voor betaling van de in de wissel belichaamde vordering aansprakelijk wordt, zie art. 142 lid 1, art. 129 lid 1 en art. 130 WvK en R. Zwitser, *Order- en toonderpapieren* (Monografieën BW nr. A28), Deventer: Wolters Kluwer 2017, nrs. 3 en 45, die ook opmerkt dat dat concept niet voor alle waardepapie-

ren geldt.

51. R. Zwitser, *Order- en toonderpapieren* (Monografieën BW nr. A28), Deventer: Wolters Kluwer 2017, nr. 1. Zie voor het elektronisch cognossement H.P.A.J. Martius, *Elektronisch handelsrecht* (diss.), 2008, NTHR-reeks deel 8, p. 194-204; en M.A.W. van Maanen & M.H. Claringbould, 'Aspecten van pandrecht op cognossementen', NTHR 2017-1, p. 10.

52. Art. 6:227a BW is onze implementatie van art. 9 lid 1 Richtlijn elektronische handel 2000/31/EG.

53. Bijvoorbeeld op www.blockchain.com/explorer.

54. R.E. van Esch, *Juridische aspecten van elektronische handel. Serie praktijkhandleidingen*, Deventer: Kluwer 2007, tweede herziene druk, p. 147.

Door genoeg te nemen met het verkrijgen van de privésleutel tot het bitcoin-adres van de vervreemder in plaats van het veel veiliger laten overmaken van de bitcoins naar een bitcoin-adres van de verkrijger, neemt die verkrijger welbewust het risico dat de vervreemder hem te slim af zal zijn

volgens de wetgever 'niet ondenkbaar dat de rechter daaraan in een concreet geval tot de conclusie komt dat gelijkstelling op zijn plaats is, ook al is niet aan alle vier genoemde voorwaarden voldaan'.⁵⁵ Voor een rechter lijkt het me geen probleem te concluderen dat het aan toonder stellen van de bitcoin-vorderingen gelijk te stellen is met het in het leven roepen van een papieren waardepapier. Immers, het bitcoin-netwerk voldoet beter dan papier aan de eisen a t/m c, partijen nemen van meet af aan willens en wetens deel aan een systeem dat mede gericht is op anonimiteit en hebben er dus kennelijk geen behoefte aan elkaars identiteit te weten te komen.

4.3. Tegenwerping 2: een elektronisch waardepapier kan niet worden gegeven en genomen

Lastiger wordt het wanneer gekeken wordt naar hetgeen volgt na de uitgifteovereenkomst, de overeenkomst waarin partijen overeenstemming bereiken over het uitgeven van het waardepapier. Daarna volgt immers het zogeheten corporele element dat bestaat uit het geven en nemen van het waardepapier. Dat corporele element blijkt het duidelijkst uit de handeling die volgens artikel 3:93 BW nodig is voor de levering van de in het waardepapier belichaamde vorderingen. Die leveringshandeling veronderstelt dat het waardepapier door de vervreemder aan de verkrijger wordt gegeven en er niets bij de vervreemder achterblijft. Toen ik eerder schreef over elektronische waardepapieren, was ik van mening dat er niet elektronisch gegeven en genomen kon worden: 'Rechten aan toonder en order die in een waardepapier zijn belichaamd, ontstaan doordat schuldenaar en schuldeiser met elkaar afspreken dat zij een recht aan toonder of order willen laten luiden (de consensus), gevolgd door het geven en nemen van het papier (de overgave ofwel het corporele element). (...) De Richtlijn elektronische handel brengt mee dat de consensus langs elektronische weg tot stand moet kunnen worden gebracht. De Richtlijn brengt ook mee dat de consensus niet zonder rechtsgevolg mag blijven. Ik kan mij echter niet voorstellen hoe het corporele element op elektronische wijze moet worden verwezenlijkt. Papier kan niet elektronisch worden gegeven en genomen. Een recht aan toonder of order dat in een waardepapier is belichaamd kan mijns inziens niet uitsluitend elektronisch ontstaan – de elektronische consensus moet door het fysieke geven en nemen van het papier worden gevolgd. Ik vraag mij af of de EG-wetgever dit voldoende heeft onderkend.'⁵⁶

Ten aanzien van bitcoins ben ik (inmiddels)⁵⁷ optimistischer. Het bij levering geven en nemen van de waardedragers die de bitcoin-vorderingen belichaamt, moet

naar mijn idee als volgt wordt gezien. Het geven van die waardedragers is het makkelijkst voor te stellen bij de paper wallet. Die wallet is van papier en dus is er, voor wat betreft het geven en nemen, geen enkel verschil met andere, meer klassieke papieren waardepapieren. Ook bij de hardware wallet kan de waardedragers makkelijk worden gegeven en genomen op zodanige wijze dat bij de vervreemder niets achterblijft. Bij de vervreemder van zo'n USB-stick-achtig device blijft bij de vervreemder immers ook niets achter, nadat hij het aan de verkrijger heeft gegeven.

Echter, als op het device ook iets anders staat, zoals op een smartphone of een computer (een non-dedicated device dus), ligt het niet voor de hand dat het hele device aan de verkrijger gegeven wordt. In dat geval kan de privésleutel bijvoorbeeld worden gecopypast en naar de verkrijger worden gemaïld. Doordat de vervreemder de privésleutel mailt naar de verkrijger, dematerialiseert de waardedragers. Op het moment dat de verkrijger de privésleutel in zijn wallet op een andere waardedragers opslaat, materialiseert de waardedragers weer. Natuurlijk blijft de privésleutel in dat geval ook achter bij de vervreemder, en is er in strikte zin geen sprake meer van een klassiek geven en nemen zoals we dat bij een papieren waardepapier gewend zijn. De miners en nodes zal het een zorg zijn: zij kijken enkel en alleen naar degene die een transactie als eerste met de privésleutel ondertekent, of hij nu rechtmatig houder van die sleutel is of niet. Voor de verkrijger van de aldus verstuurd privésleutel ontstaat daardoor het risico dat de vervreemder zelf een kopie van die sleutel achterhoudt en die sleutel eerder gebruikt om de op dat bitcoin-adres geregistreerde bitcoins weg te sluizen, dan dat de verkrijger de bitcoins naar een ander bitcoin-adres overmaakt. Maar hoe erg is dat? Laat ik, om die vraag te beantwoorden, de elektronische situatie vergelijken met een papieren situatie waarin de verkrijger in een soortgelijke vorm van onzekerheid verkeert.

Neem de situatie dat er één toonderpapier is uitgegeven. Dan kan de vervreemder zijn toonderpapier ook hebben gekopieerd voordat hij het origineel aan de verkrijger heeft gegeven. Doordat de hedendaagse kopieertechnieken zo goed zijn, zal de debiteur aan wie de malafide vervreemder het gekopieerde waardepapier vervolgens presenteert het verschil tussen origineel en kopie niet kunnen ontwaren en aan zijn in het waardepapier opgenomen verplichtingen voldoen. Natuurlijk is dat niet de bedoeling, maar het is net zo min de bedoeling dat degene die aan een ander een privésleutel verstrekt met betrekking tot een bitcoin-adres, een kopie daarvan

achterhoudt. Het doet me denken aan de *Oracle/UsedSoft*-zaak, waarin het HvJ EU bepaalde dat de eerste verkrijger van een softwarelicentie bij doorverkoop daarvan 'zijn eigen kopie op het moment van wederverkoop daarvan onbruikbaar [moet, toevoeging TG] maken om geen inbreuk te maken op het exclusieve recht van de auteur van het computerprogramma (...)'.⁵⁸ Dat is weliswaar een andere situatie, maar de kern blijft hetzelfde: als (de rechten op) bestanden worden doorverkocht met het oogmerk dat de verkrijger er exclusief over moet kunnen beschikken, is de vervreemder logischerwijs gehouden zijn kopieën van die bestanden te verwijderen. Het zou, met andere woorden, betoogd kunnen worden dat er weinig verschil is tussen enerzijds het verbod om vóór overdracht van een papieren waardepapier een kopie te maken en anderzijds het gebod om ná overdracht van een privésleutel opgeslagen op een non-dedicated device kopieën daarvan te verwijderen. Doordat er tussen die twee situaties (te) weinig verschil is, is er onvoldoende reden om, door het enkele verplaatsen van die privésleutel van de ene naar de andere wallet, het waardepapierrechtelijk karakter in vlammen te laten opgaan en aldus de waardenpapierrechtelijke rechten te onthouden aan de verkrijger en te concluderen dat er geen rechtsgeldige levering (en daarmee overdracht) heeft plaatsgevonden.

Wie het dematerialiseren en vervolgens weer materialiseren van de waardedragers een brug te ver vindt – en daar kan ik me iets bij voorstellen – kan wellicht door een tweede argument ervan worden overtuigd dat de waardedragers van de verkrijger ook een waardepapier is als de privésleutel wordt verplaatst zonder het geven en nemen van de waardedragers. Dat argument luidt als volgt. De wet voorziet erin dat verschillende exemplaren van een papieren waardepapier worden uitgegeven, zie artikel 163 en 226 WvK en artikel 8:413 BW.⁵⁹ In zo'n soort situatie is een houder van zo'n toonderpapier er ook niet zeker van dat een andere houder zijn *exemplaar* niet eerder zal presenteren, en die andere houder daarmee zijn vorderingsrecht eerder zal uitoefenen dan hij en waardoor zijn exemplaar in feite waardeloos wordt. In soortgelijke zin kan worden betoogd dat in de bitcoin-meerpartijenovereenkomst impliciet is overeengekomen dat de verkrijger van een bitcoin-vordering niet alleen tegelijkertijd een toonderpapier verkrijgt in de vorm van zijn waardedragers, maar ook een volmacht voor het uitgeven van meerdere waardedragers. Op het moment dat hij vervolgens zijn privésleutel aan een opvolgend verkrijger mailt en laatstgenoemde die sleutel opbergt in zijn wallet zonder daarbij het non-dedicated device van de vervreemder te verkrijgen, moet dat gezien worden als het, met gebruikmaking van die volmacht, geven en nemen van een nieuw exemplaar van de waardedragers. Die nieuwe waardedragers ontstaat op het moment dat de verkrijger de privésleutel in zijn wallet op een waardepapier opslaat. Op die manier hoeft een bestaande waar-

dedrager niet gedematerialiseerd en vervolgens in een andere waardedragers gematerialiseerd te worden, en is de verkrijger zich wel van meet af aan bewust van het risico dat de vervreemder ook een exemplaar heeft van de privésleutel waarmee hij, eerder dan de verkrijger, de bitcoins op het bijbehorende bitcoin-adres kan overmaken naar een ander bitcoin-adres.

Bovenstaande twee redeneringen winnen aan overtuigingskracht als we ons realiseren dat de verkrijger het risico niet hoeft te nemen dat de vervreemder hem te slim af is. Als hij er zeker van wil zijn dat de vervreemder niet een kopie van de privésleutel achterhoudt en hem daarmee te slim af kan zijn, kan hij met de vervreemder overeenkomen dat die de afgesproken hoeveelheid bitcoins overmaakt naar een bitcoin-adres van de verkrijger. Op het moment dat de transactie op die manier wordt vormgegeven en die transactie vervolgens in een block aan de blockchain is toegevoegd, is de verkrijger er zeker van dat de vervreemder niet meer over die bitcoins kan beschikken. Door genoeg te nemen met het verkrijgen van de privésleutel tot het bitcoin-adres van de vervreemder in plaats van het veel veiliger laten overmaken van de bitcoins naar een bitcoin-adres van de verkrijger, neemt die verkrijger welbewust het risico dat de vervreemder hem te slim af zal zijn. Door deze vorm van risico-aanvaarding in aanwezigheid van een beter alternatief, is het minder bezwaarlijk het waardepapierrechtelijk karakter te handhaven als het verstreken van de privésleutel niet gepaard gaat met de bezitsverschaffing van het non-dedicated device. De tegenovergestelde opvatting, het ontnemen van het waardepapierrechtelijk karakter aan de waardedragers van de verkrijger en het concluderen dat er geen rechtsgeldige levering (en daarmee overdracht) heeft plaatsgevonden, zou vooral (of zelfs: alleen) de vervreemder in de kaart spelen, terwijl beide partijen een rechtsgeldige, zij het risicovolle levering beoogden.

4.4. Gevolgen

Wat brengt ons deze goederenrechtelijke gelijkstelling van de waardedragers (waarin de bitcoin-vorderingen zijn belichaamd) met een waardepapier (te weten een toonderpapier)? Het brengt ons tot een juridisch kwalificatie die in overeenstemming is met de technische werkelijkheid. Het brengt ons ook betrekkelijk schone juridische eenvoud, die ik vanwege de lengte van deze bijdrage slechts kort kan tonen. Niet alleen kunnen die vorderingen makkelijk worden geleverd door bezitsverschaffing van de waardedragers. Ook een vuistpand kan eenvoudig worden gevestigd door die waardedragers in de macht van de pandhouder te brengen, aldus artikel 3:236 lid 1 BW. Voor dat alles is geen akte, handtekening, notaris of belastingdienst nodig. Het beslag- en executierecht wordt er eveneens eenvoudiger op. Het beslag op de in het waardepapier belichaamde vorderingen wordt namelijk gelegd door

55. Kamerstukken II 2001/02, 28197, 3, p. 53 (MvA).

56. T.J. de Graaf, 'Elektronische waardepapieren', in: R.E. van Esch & J.E.J. Prins (red.), *Recht en elektronische handel*, Serie

Recht en Praktijk nr. 68, Deventer: Kluwer 2002, p. 165-166.

57. Te mijner verdediging: toen ik het voorgaande schreef, bestonden bitcoins nog niet.

58. HvJ EU 3 juli 2012, C-128/11,

ECLI:EU:C:2012:407, NJ 2013/118, m.nt. P.B. Hugenholtz, r.o. 70.

59. R. Zwitser, *Order- en toonderpapieren* (Monografieën BW nr. A28), Deventer:

Wolters Kluwer 2017, nr. 16. In de praktijk komt dat volgens Zwitser vooral voor bij wissels en cognossemerten.

beslag te leggen op de waardedragers.⁶⁰ De bepalingen omtrent het beslag op zaken zijn in dat geval 'van overeenkomstige toepassing, tenzij uit de betreffende bepaling in verband met de aard van het recht anders volgt', aldus artikel 474a lid 1 Rv voor executoriaal beslag en artikel 702 lid 1 Rv voor conservatoir beslag.

5. Conclusie

Ik rond af. Vanuit verbintenisrechtelijk oogpunt kwalificeert het bitcoin-netwerk mijns inziens als een meerpartijenovereenkomst, waartoe de verschillende deelnemers (gebruikers, miners en nodes) toetreden doordat de betreffende deelnemer voor het eerst aan het netwerk deelneemt en daarmee het in die overeenkomst te zijnen gunste opgenomen derdenbeding aanvaardt. Op grond van die overeenkomst oefent een gebruiker die bitcoins overmaakt eigenlijk zijn vorderingsrechten uit, ten opzichte van de miners om die transactie te verifiëren en ten opzichte van nodes om het werk van de winnende miner te controleren, waarna de transactie (als die is goedgekeurd) in een block aan de blockchain wordt toegevoegd. De bitcoin-vorderingen kunnen alleen worden geëffectueerd met gebruikmaking van de privésleutel die hoort bij het bitcoin-adres van waaruit bitcoins worden overgemaakt.

Ter uitvoering van de daartoe strekkende, voorafgaande partijafpraak in de meerpartijenovereenkomst, worden de bitcoin-vorderingen ten aanzien van bitcoins die op een bitcoin-adres worden bijgeschreven, op hetzelfde moment als dat ze worden bijgeschreven, vanuit goederenrechtelijk perspectief aan toonder gesteld, en wel aan de toonder van de waardedragers waarop de privésleu-

tel staat die aan dat bitcoin-adres is gekoppeld. Die waardedragers belichaamt daarmee die bitcoin-vorderingen. Die bitcoin-vorderingen kunnen worden geleverd, bezwaard, beslagen en geëxecuteerd door bezitsverschaffing van de waardedragers. Degene die de waardedragers houdt, kan de daarin belichaamde bitcoin-vorderingen effectueren door gebruikmaking van de daarop opgeslagen privésleutel en daarmee de bitcoins van het daarbij behorende bitcoin-adres overmaken naar een ander bitcoin-adres.

Mocht de beoogd verkrijger van bitcoins willen voorkomen dat de vervreemder een kopie van de privésleutel achterhoudt en daarmee die bitcoins eerder wegsluist dan dat de beoogd verkrijger ze naar zijn bitcoin-adres kan overmaken, dan kan hij met de vervreemder overeenkomen dat die vervreemder niet de waardedragers aan hem geeft, maar de bitcoins overmaakt naar een bitcoin-adres van de verkrijger. Over de bitcoins op het bitcoin-adres van de verkrijger kan de vervreemder immers niet beschikken, omdat hij de daaraan gekoppelde privésleutel niet heeft. Dat de waardedragers doorgaans niet van papier is, is geen probleem. Dat privésleutels die op sommige waardedragers zijn opgeslagen worden verstrekt zonder tegelijkertijd die waardedragers zelf te geven, is evenmin een probleem. •

⁶⁰. Zie T.J. de Graaf & H.B. Krans, 'Verhaal op bitcoins door gedwongen medewerking van de schuldenaar', *WPNR* 7217 1 december 2018, p. 940-945 voor een overzicht over hoe een schuldeiser zijn tot betaling

van een geldsom veroordeelde schuldenaar kan dwingen zijn bitcoin-privésleutel prijs te geven zodat verhaal kan worden genomen op de bitcoins van die schuldenaar.