UNIVERSITEIT VAN TILBURG

Blockchain en het recht

Een verkenning van de reguleringsbehoefte

Maurice Schellekens
Eric Tjong Tjin Tai
Wesley Kaufmann
Femke Schemkes
Ronald Leenes

Tilburg University
Postbus 90153
5000 LE Tilburg
Nederland
<M.H.M.Schellekens@uvt.nl>
<T.F.E.TjongTjinTai@uvt.nl>

Juni 2019

TILT – Tilburg Institute for Law, Technology, and Society
P.O. Box 90153 • 5000 LE Tilburg • Tilburg • Phone +31 13 466 91 11
www.tilburguniversity.edu/tilt

Colophon

Auteurs
Maurice Schellekens
Eric Tjong-Tjin-Tai
Wesley Kaufmann
Femke Schemkes
Ronald Leenes

Uitgever
Tilburg University
TILT – Tilburg Institute for Law, Technology, and Society
en TIP – Tilburg Institute for Private law
In samenwerking met Tilburg School of Governance
Postbus 90153
5000 LE Tilburg
Nederland

In opdracht van
WODC, Ministerie van Veiligheid en Justitie
Turfmarkt 147
2511 DP Den haag
Nederland

Datum
Juni 2019

Inhoudsopgave

Colophon 2
Samenvatting 6
Summary 12
1. Introductie 17
1.1. Achtergrond 17
1.2. Onderzoeksvraag 17
1.3. Methode 17
1.4. Structuur van het rapport 18
2. Technische uitleg van blockchain 19
2.1 Introductie 19
2.2 Terminologie en rollen 22
2.3 Overige onderscheidingen 24
Enkele implicaties van consensusmechanismen 24
Toepassingen 24
Samengestelde transacties 25
Governance 26
2.4 Eigenschappen 27
3. Algemeen juridisch deel 29
3.1 Inleiding 29
3.2 Privaatrechtelijke aspecten 30
3.2.1 Algemeen 30
3.2.2 Wat is een blockchain in het privaatrecht? 30
3.2.3 Interne governance 34
3.2.4 Juridische betekenis van handelingen op de blockchain 35
3.2.5 Bewijskracht 36
3.2.6 Goederenrecht en de blockchain 37
3.2.7 Contractenrecht 41
3.2.8 Smart contracts als bijzondere toepassing 45
3.2.9 Aansprakelijkheid 50
3.2.10 Handhaving en regulering 55
3.2.11 Identiteit 57
3.2.12 Toepasselijk recht en jurisdictie 57
3.2.13 Gevolgen voor (juridische) beroepen? 62
3.3 Algemene Verordening Gegevensbescherming 64
3.3.1 Verantwoordelijke en verwerker 64
3.3.2 De territoriale werkingssfeer 68
3.3.3 Persoonsgegevens 69

3.3.4 Data minimalisatie en het recht op vergetelheid 70
3.4 Bestuursrecht en geautomatiseerde besluiten 73
3.4.1 Geautomatiseerd besluiten in het bestuursrecht 73
3.4.2 Elektronisch bestuurlijk verkeer 75
4. Use-cases 77
4.1 Inleiding 77
4.2 Use-case 1: Scheepsregistratie op de blockchain? 77
Het scheepsregister en de kadastrale registratie 77
Actoren bij de huidige scheepsregistratie 78
Korte beschrijving van de blockchain aanpak 79
4.3 Use-case 2: geautomatiseerde compliance en administratieve lastendruk – schatkistbankieren en onderwijshuisvesting 85
4.3.1 Korte beschrijving van de use-case 85
4.3.2 Kansen en risico's 87
4.3.3 Juridische knelpunten 90
4.4 Use-case 3: Het vervoer van afvalstoffen op grond van de EVOA 92
4.4.1 Korte beschrijving van de use-case, inclusief kansen en risico's 92
4.4.2 De use-case onder het huidige wettelijk kader 93
4.4.3 Aandachtspunten 94
4.5 Use-case 4: Het delen van privacygevoelige gegevens door de overheid -- het CAK 95
4.5.1 Korte beschrijving van de use-case 95
4.5.2 Kansen en risico's onder het huidige wettelijk kader 96
4.5.3 Aandachtspunten 98
5. Synthese 100
5.1 Introductie 100
5.2 Reguleringsvragen 100
5.2.1 Een kader 100
5.2.2 Aanvaardbaarheid van blockchain techniek 101
5.3 Handhaafbaarheid 111
5.3.1 Handhaving tegen wie? 111
5.3.2 Moeilijkheden in het adresseren van degene tegen wie gehandhaafd wordt 111
5.3.3 Het doorzetten van handhavingsmaatregelen 112
6. Conclusie 114
Bibliografie 119
Kamerstukken 133
Rapporten 133
Lijst met geraadpleegde organisaties 134
Begeleidingscommissie 135

Over de auteurs 136
Betrokken onderzoekers vanuit het departement TILT 136
Betrokken onderzoekers vanuit het departement Private Law 136
Betrokken onderzoeker vanuit Tilburg School of Governance 136

Samenvatting

Introductie

Blockchain is een techniek waarvan veel verwacht wordt en waaraan vele kwaliteiten worden toegedicht. Blockchain maakt het mogelijk dat partijen die elkaar niet kennen en allicht niet vertrouwen veilig met elkaar handel kunnen drijven. Vele traditionele intermediaren, zogenaamde trusted third partes zouden overbodig worden. Blockchain leidt zo tot efficiëntiewinst en kostenbesparing omdat velerlei functies geautomatiseerd kunnen worden. Blockchain zou nieuwe samenwerkingsvormen mogelijk maken en blockchain is het internet van waarde.

Het is een techniek die afgaande op bovenstaande verwachtingen, bestaande verhoudingen binnen de samenleving behoorlijk kan veranderen. Daarbij kunnen waarden en belangen onder druk komen te staan. Dat roept de vraag op wat de aanvaardbaarheid is van blockchain in de verschillende gedaantes die het kan aannemen. Dit rapport legt een kader aan waarmee de kansen en risico's die met de techniek gepaard gaan afgewogen kunnen worden en dat de wetgever een eerste handvat biedt om de geschiktheid van het huidige wettelijke kader te beoordelen.

Blockchaintechniek

Een blockchain is in wezen een databank waarvan vele exemplaren onder verschillende beheerders worden bijgehouden. Er wordt onderscheid gemaakt tussen zogenaamde permissionless en permissioned blockchains. Tot een permissionless blockchain kan een ieder vrijelijk als beheerder toetreden. De coordinatie binnen de blockchain, bijvoorbeeld ter uitvoering van een betaling met cryptocurrency, berust in beginsel niet op vooraf gemaakte afspraken of overeenkomsten, maar op een systeem van crypto-economische prikkels. In een permissioned blockchain kunnen alleen toegelaten beheerders actief zijn. Er kan een centrale instantie zijn die de toegang regelt of dit kan overgelaten zijn aan de zittende beheerders gezamenlijk. De coordinatie binnen een permissioned blockchain kan gebaseerd zijn op een systeem van crypto-economische prikkels, maar dat hoeft niet. Het kan ook gebaseerd zijn op onderlinge afspraken.

In dit rapport worden aan blockchains vier eigenschappen toegeschreven: ze zijn onveranderlijk, een blockchain is in beginsel blind, een blockchain is redundant en een blockchain is in technische zin transparant.

De onveranderlijkheid geldt in wezen alleen voor blockchains gebaseerd op een systeem van crypto-economische prikkels. De onveranderlijkheid betekent in wezen dat een individuele beheerder niet kan veranderen wat als de inhoud van de blockchain wordt gezien. Als een individuele beheerder oude gegevens in zijn exemplaar van de blockchain zou veranderen, dan wordt zijn exemplaar niet meer gezien als een geldig exemplaar van de blockchain. De beheerder diskwalificeert zichzelf als het ware. Indien een aantal beheerders zich samenpakken kan de inhoud van de blockchain wel worden veranderd, maar dit is niet eenvoudig en daarmee van gering praktisch belang. Een blockchain gebaseerd op afspraken kan wel voorzien in een mogelijkheid om oude gegevens te veranderen.

Blindheid van de blockchain betekent in wezen dat er geen garantie is dat gegevens die in een blockchain worden opgenomen correct zijn. Er kan bij opname van nieuwe gegevens wel gecontroleerd worden of de nieuwe gegevens consistent zijn met oude gegevens in de blockchain, maar dit is slechts een beperkte controle. Nieuw op te nemen gegevens kunnen eventueel gecontroleerd worden aan de hand van gegevens buiten de blockchain (ingebracht via een zogenaamd oracle), maar het is onduidelijk hoe betrouwbaar die gegevens zijn. Om kort te gaan, gegevens kloppen niet, enkel omdat ze in een blockchain zijn opgenomen.

Redundantie duidt op het feit dat er meerdere exemplaren van een blockchain bestaan. Redundantie kan voordelen bieden in termen van veiligheid, maar het kan ook een last zijn. Alles wat binnen een blockchain gerealiseerd wordt vergt coordinatie. Als de blockchain niet op afspraken berust ontstaat er afhankelijkheid van wat de techniek wel coordineert en wat niet.

Een blockchain is in technische zin transparant. Om te kunnen vaststellen welk exemplaar of versie van een blockchain geldig is moeten blockchains in hun geheel geinspecteerd kunnen worden. Voor veel toepassingen is echter niet handig dat alle gegevens in beginsel beschikbaar moeten zijn voor inspectie.

Een smart contract is code die op een blockchain wordt geplaatst en uitgevoerd wordt door beheerders van de blockchain. Een smart contract hoeft geen overeenkomst in juridische zin op te leveren. Het is in beginsel gewoon code. De code kan nadat zij eenmaal op een blockchain is geplaatst niet meer veranderd worden, ook niet door degene die de code op de blockchain plaatste.

Algemene juridische aspecten

Voor de juridische analyse heeft het onderzoek dat aan dit rapport ten grondslag ligt een aantal algemene juridische aspecten geanalyseerd.

Partijen die op de blockchain een overeenkomst willen sluiten kunnen daartoe gebruik maken van een smart contract. Geclaimd voordeel van een smart contract is dat het de gehele overeenkomst tussen partijen zou vastleggen en uitvoeren. Uitvoering van de overeenkomst is daarmee automatisch en gegarandeerd. Dat zou een belangrijke bron van conflicten rond overeenkomsten wegnemen, zodat het niet nodig en zelfs onwenselijk zou zijn om rechterlijke tussenkomst te zoeken.

Een smart contract is zelf niet een overeenkomst maar kan worden beschouwd als bewijs van totstandkoming van een juridische overeenkomst. De inhoud van die overeenkomst wordt bepaald volgens juridische regels. De programmacode van het smart contract zal belangrijk zijn om de inhoud van de overeenkomst vast te stellen, maar is daarbij niet doorslaggevend. Ook de bedoeling van partijen speelt een rol. Het kan lastig zijn om alle gewone regels van een overeenkomst in een smart contract vast te leggen op een begrijpelijke manier. Als de regels van een smart contract in strijd zijn met wat uit de juridische overeenkomst volgt, kan een partij in principe de rechter vragen om de uitvoering van het smart contract te corrigeren. Het is mogelijk dat dit niet effectief is te handhaven.

Smart contracts hebben diverse nadelen en risico’s. Smart contracts eisen meestal betaling vooraf wat tot renteverlies en valuta-risico’s leidt. Zij kunnen de gewone regels van het contractenrecht maar in beperkte mate uitvoeren: dat kan betekenen dat bescherming die een partij rechtens heeft (zoals bij overmacht) niet geffectueerd kan worden. Bij het gebruik van menselijke ‘oracles’ voor de beoordeling van omstandigheden wordt het smart contract weer afhankelijk van menselijke tussenkomst en verloopt dan niet automatisch. Smart contracts zijn niet te begrijpen of controleren zonder specialistische kennis, en het inhuren van zulke kennis is kostbaar, terwijl het riskant is om erop te vertrouwen dat het contract doet wat de ontwikkelaar zegt. Smart contracts wijken daarnaast wezenlijk af van de gewone manier waarop mensen een contract opvatten: als een onderdeel van een intermenselijke relatie, die niet tot in detail vooraf regelt hoe er met verschillende omstandigheden moet worden omgegaan.

Smart contracts kunnen in bepaalde omstandigheden voordelen bieden ondanks de risico’s. Dit lijkt met name het geval bij overeenkomsten met anonieme partijen in het buitenland, of als onderdeel

van een grotere gewone overeenkomst (waarbij het smart contract wordt gebruikt als uitvoering van een deel van die overeenkomst).

Een ander belangrijk algemeen onderwerp is de Algemene Verordening Gegevensbescherming. Voor het garanderen van een adequate verwerking van persoonsgegevens onder de AVG, speelt de verwerkingsverantwoordelijke een belangrijke rol. Vanwege het P2P karakter van blockchains kan het het lastig zijn uit te maken wie de verantwoordelijke(n) is (of zijn), met name indien toepassingen in de core code van de blockchain zijn opgenomen (zoals bijvoorbeeld native crypto-currencys). Zelfs indien een verantwoordelijke aangewezen kan worden, is het moeilijk voor deze persoon om de verantwoordelijkheid adequaat vorm te geven. Om iets te bereiken binnen een blockchain (bijvoorbeeld het wissen van gegevens) is coordinatie tussen de beheerders vereist. De coordinatie nodig voor het voldoen aan de rechten van betrokkenen wordt niet door de techniek ondersteund en soms zelfs tegengewerkt (opnieuw het wissen van gegevens). Het is de lastige taak van de verantwoordelijke(n) om die coordinatie op enigerlei wijze te realiseren.

Een ander heikel punt onder de AVG is het wissen van persoonsgegevens bijvoorbeeld in het kader van data minimalisatie en het recht op vergetelheid. In blockchains gebaseerd op een systeem van crypto-economische prikkels is dit in praktische termen niet mogelijk. Onduidelijk is op dit moment of deze spanning opgelost wordt door te kiezen voor een ander type blockchain dan wel relativering van wat ‘wissen’ betekent onder de AVG.

Use-cases

Ten behoeve van dit rapport is een viertal use-cases onderzocht.

Het scheepsregister

Het gebruik van een permissionless public blockchain voor het scheepsregister leidt tot een verschuiving van kosten en tijd (van initiële registratie naar latere transacties) en heeft een lagere betrouwbaarheid van de Nederlandse scheepsregistratie tot gevolg. Daarnaast zijn er risico’s voor fraude, privacy, en misbruik voor witwassen e.d. Voor Nederland, wegens de hier bestaande kwalitatief hoogwaardige scheepsregistratie, is een permissionless public blockchain daarom geen zinvolle optie. Andere blockchainvarianten zijn mogelijk maar hebben niet de voordelen van een permissionless public blockchain. Afhankelijk van de gekozen opzet zullen ook wettelijke regels in meerdere of mindere mate moeten worden aangepast.

Schatkistbankieren ten behoeve vean de nieuwbouw van scholen

In deze use-case is met name gekeken naar het nut van blockchain als middel om verantwoording af te leggen. De Auditdienst Rijk heeft onder andere als taak te controleren of het financiële beheer van het Rijk voldoet aan normen van doelmatigheid, rechtmatigheid, ordelijkheid en controleerbaarheid. Een blockchain die schatkistbankieren ten behoeve van de nieuwbouw van een schoolgebouw structureert zal controles door de Auditdienst Rijk allicht vereenvoudigen. Er zijn echter twee kanttekeningen te plaatsen. In de eerste plaats is vereenvoudigde controle ook zonder een blockchain te realiseren. In de tweede plaats dekt een blockchain implementatie niet alle dimensies die de Auditdienst zou willen controleren af. Een blockchain maakt de Auditdienst Rijk dus niet overbodig.

Het vervoer van afvalstoffen binnen de EU

De Europese Verordening Overbrenging Afvalstoffen (EVOA Verordening) staat niet in de weg aan het digitaal uitvoeren van de relevante processen. In dit opzicht zou implementatie in een blockchain mogelijk zijn. De onmogelijkheid van het verwijderen van op de blockchain geplaatste

persoonsgegevens is echter een punt van aandacht. Bovendien blijven fysieke controles nodig. Transporten die nooit ingevoerd zijn in de blockchain kent de blockchain niet. Als ingevoerde gegevens niet overeenstemmen met de werkelijkheid, kan de blockchain zelf dit niet constateren. Het is niet duidelijk wat de meerwaarde van een blockchain implementatie is ten opzichte van een traditioneel automatiseringsproces.

Het delen van privacygevoelige gegevens door de overheid -- het CAK

Deze use-case betreft gecompliceerde facturatieprocessen in het kader van de Wet Maatschappelijke Ondersteuning. In deze use-case kan automatisering van de werkprocessen een belangrijke vooruitgang betekenen. De meerwaarde van blockchain is niet duidelijk. Een blockchain implementatie heeft belangrijke nadelen in de sfeer van gegevensbescherming: gegevens kunnen niet of moeilijk gewist of gecorrigeerd worden. Om de vertrouwelijkheid van persoonsgegevens te waarborgen worden gegevens off chain opgeslagen. De vraag is of daarmee niet mogelijke voordelen van het gebruik van een blockchain weer weggenomen worden.

Synthese

Juridisch kader

Het in beeld brengen van de verschillende juridische aspecten van blockchains vergt een structuur die als ordenend principe kan functioneren. Daartoe is hier gekozen voor criteria van aanvaardbaarheid van normatieve technologie. Blockchain is normatieve technologie. Door haar opzet beoogt zij de verhoudingen tussen betrokken partijen opnieuw te definiëren. Bovendien is het gekozen schema van criteria voldoende algemeen om een breed beeld te gegeven van juridische aspecten. Hier komen de vier belangrijkste criteria aan bod.

Mensenrechten en morele waarden/beschermingsfunctie van het recht

Welke mensenrechten en morele waarden komen door het gebruik van blockchain onder druk? Sommige komen vrij expliciet onder druk in andere gevallen is het meer een impliciet proces. Gegeven het brede toepassingsgebied van blockchains kunnen mensenrechten en morele waarden onder druk komen. De belangrijkste die in dit onderzoek naar voren zijn gekomen zijn de hierna genoemde.

Tot de expliciet onder druk komende mensenrechten vallen onder andere privacy en gegevensbescherming, zoals hierboven reeds bleek.

Autonomie staat onder druk. Informatieplichten ten aanzien van gebruikers zijn onduidelijk en blockchaintoepassingen laten weinig ruimte voor het accommoderen van de autonomie van de gebruiker en eventuele andere betrokkenen (het vatten van processen in code en casu quo onveranderlijkheid). De geautomatiseerde afloop van processen gebaseerd op een beperkte set data (blindheid van de blockchain) houdt een risico in van ongelijke behandeling en discriminatie.

Ook kan blockchain impliciet tot ondermijning van rechtsnormen leiden. De blockchain/smart contracts kanaliseren gedrag en de toepasselijke rechtsnorm verdwijnt uit zicht. De code gaat in de gedachten van de betrokkenen de rol overnemen van het recht.

Hier is wel reden om de vinger aan de pols te houden.

Legitimiteit

Er wordt vaak geclaimd dat een blockchain vertrouwen overbodig zou maken. Daarbij wordt over het hoofd gezien dat in de code voor de blockchain of voor het smart contract vele keuzes besloten

liggen. In plaats van te geloven dat vertrouwen overbodig is geworden, doet men er beter aan zich af te vragen wat de legitimiteit is van de machtsuitoefening door middel van code. De legitimiteit heeft een formeel aspect (bestuurshandelen vergt een wettelijke basis, private partijen zijn in beginsel vrij te handelen), maar ook een waarborg aspect: er moeten voldoende waarborgen ingebouwd zijn om de eenvoudige gebruiker niet te overleveren aan de willekeur van de bouwer van de techniek. Er dient voor gewaakt te worden dat blockchains in naam van innovatie- of efficiëntiebevordering aan waarborgen en legitimiteit afdoen.

Democratie en transparantie van het stellen van regels

Blockchains hebben implicaties voor veel mensen die niet betrokken zijn geweest bij de ontwikkeling van de code die die implicaties bewerkstelligen. Dat doet de vraag rijzen naar de democratische legitimatie van blockchain: inhoeverre worden degenen die geraakt worden door blockchain betrokken in het vormgeven van een blockchain of blockchaintoepassing? De belangrijkste permissionless blockchains hebben een governance structuur waarin weliswaar een ieder kan participeren, maar de beslissingsmacht toch ligt bij miners en core code ontwikkelaars. Zeker als de maatschappelijke impact van blockchains toeneemt, is een effectieve governance een belangrijk aandachtspunt.

Proportionaliteit

Blockchain wordt ingezet voor uiteenlopende doeleinden. Het bereiken van efficiëntiewinst (betere dienstverlening, lagere kosten) is blijkens de use-cases een dominante beweegreden. Tegelijkertijd kunnen mensenrechten en morele waarden door de inzet van blockchains onder druk komen. Is een blockchain in dit speelveld een redelijk middel om het doel (efficiëntiewinst) te bereiken?

In de eerste plaats moet de claim dat een blockchain tot efficiëntiewinst leidt gemitigeerd worden. Een blockchain lost het probleem van de authenticiteit van gegevens die de blockchain ingaan niet op. Het waarborgen van authenticiteit vergt communicatie met de ‘buitenwereld’ (bijvoorbeeld traditionele intermediairs) en daar gaat efficiëntie verloren. Alleen kijken naar de werkzaamheden van de node-beheerders is een te eng perspectief en geeft geen volledig beeld van de (in)efficiëntie.

De claim dat blockchain problemen rond gefragmenteerde werkprocessen oplost, zoals bij het scheepsregister, is discutabel. Alle benodigde data kan weliswaar voor iedere relevante partij op de blockchain beschikbaar zijn, maar daarmee is nog geen workflow gerealiseerd. Inpassing en beoordeling van de data in een werkproces vergt een aparte laag in software die bovenop de blockchain gelegd zal moeten worden. Aangezien die (nog) niet bestaat rijst wederom de vraag of een klassieke ICT-implementatie van het werkproces niet efficiënter is of kan zijn.

Er is reden kritisch te zijn over de efficiëntiewinst die met blockchain projecten te behalen is, terwijl met name blockchains die op basis van crypto-economische prikkels functioneren daar belangrijke nadelen tegenover stellen: problemen rond de onveranderlijkheid van data, twijfels over de schaalbaarheid en bij blockchains die met proof-of-work werken, duurzaamheidsbezwaren.

Concluderend kan gezegd worden dat dit rapport kritisch is over blockchains. Dat neemt niet weg dat waar blockchain kansen biedt die aangegrepen moeten worden. Blockchain blijkt evenwel niet het geneesmiddel tegen alle kwalen te zijn en met name permissionless blockchains hebben bijwerkingen. Het is belangrijk bij het overwegen van nieuwe blockchain projecten om eerst een goede probleemanalyse te maken en nauwkeurig te bezien of een blockchain voor de geidentificeerde problemen een oplossing biedt. Als dit het geval is dan biedt het in hoofdstuk 5 uitgewerkte kader een eerste handvat om juridische randvoorwaarden in kaart te brengen en er zo een maatschappelijk verantwoorde innovatie van te maken.

Summary

Introduction

Blockchain is a technique from which much is expected and to which many qualities are attributed. Blockchain makes it possible that parties who do not know each other and probably do not trust each other can trade safely with each other. Many traditional intermediaries, so-called trusted third parties would become superfluous. Blockchain thus leads to efficiency gains and cost savings because many functions can be automated. Blockchain would enable new forms of collaboration and blockchain is of value to the internet.

It is a technique that, based on the above expectations, can considerably change existing relationships within society. Values and interests can come under pressure. This raises the question of the acceptability of blockchain in the different forms it can take. This report establishes a framework with which the opportunities and risks associated with the technology can be weighed and that the legislator offers a first tool to assess the suitability of the current legal framework.

Blockchain technology

A blockchain is essentially a database of which many copies are kept under different managers. A distinction is made between so-called permissionless and permissioned blockchains. Everyone can freely join a permissionless blockchain as a manager. Coordination within the blockchain, for example for the execution of a payment with cryptocurrency, is in principle not based on agreements or contracts made in advance, but on a system of crypto-economic incentives. In a permissioned blockchain, only authorized managers can be active. There may be a central body that controls access or this may be left to the incumbent managers together. Coordination within a permissioned blockchain can be based on a system of crypto-economic incentives, but that is not necessary. It can also be based on mutual agreements.

In this report, four properties are attributed to block chains: they are immutable, a blockchain is in principle blind, a blockchain is redundant and a blockchain is technically transparent.

The immutability essentially only applies to blockchains based on a system of crypto-economic incentives. The immutability essentially means that an individual manager cannot change what is seen as the content of the blockchain. If an individual manager changes old data in his copy of the blockchain, his copy would no longer be seen as a valid copy of the blockchain. The manager disqualifies himself as it were. If a number of managers work together, the content of the blockchain can be changed, but this is not easy and therefore of little practical importance. A blockchain based on agreements can provide for the possibility of changing old data.

Blindness of the blockchain essentially means that there is no guarantee that data included in a blockchain is correct. When recording new data, it can be checked whether the new data is consistent with old data in the blockchain, but this is only a limited check. New data to be recorded can possibly be checked on the basis of data outside the blockchain (entered via a so-called oracle), but it is unclear how reliable that data is. In short, data is not correct just because they are included in a blockchain.

Redundancy indicates that there are multiple copies of a blockchain. Redundancy can offer benefits in terms of safety, but it can also be a burden. Everything that is realized within a blockchain requires coordination. If the blockchain is not based on agreements, dependence will arise on what the technology does and does not coordinate.

A blockchain is transparent in a technical sense. In order to determine which copy or version of a blockchain is valid, it must be possible to inspect blockchains in their entirety. For many applications, however, it is not convenient that all data must in principle be available for inspection.

A smart contract is code that is placed on a blockchain and executed by managers of the blockchain. A smart contract does not have to provide a legal agreement. In principle it is just code. Once it has been placed on a blockchain, the code can no longer be changed, not even by the person who placed the code on the blockchain.

General legal aspects

The research underlying this report has analyzed a number of general legal aspects.

Parties that want to conclude an agreement on the blockchain can use a smart contract for this. The claimed advantage of a smart contract is that it would record and implement the entire agreement between the parties. Execution of the agreement is therefore automatic and guaranteed. That would remove an important source of conflicts about agreements, so that it would not be necessary and even undesirable to seek judicial intervention.

A smart contract is not itself an agreement but can be considered as proof of the conclusion of a legal agreement. The content of that agreement is determined according to legal rules. The program code of the smart contract will be important to determine the content of the agreement, but it is not decisive. The intention of the parties also plays a role. It can be difficult to lay down all the usual rules of an agreement in a smart contract in an understandable way. If the rules of a smart contract conflict with what follows from the legal agreement, a party can in principle ask the court to correct the implementation of the smart contract. It is possible that such attempt at legal enforcement is not effective.

Smart contracts have various disadvantages and risks. Smart contracts usually require payment in advance, which leads to interest loss and currency risks. They can only implement the normal rules of contract law to a limited extent: that may mean that protection that a party has in law (such as in the case of force majeure) cannot be obtained. When using human "oracles" for the assessment of circumstances, the smart contract becomes dependent on human intervention again and does not execute automatically. Smart contracts cannot be understood or controlled without specialist knowledge, and hiring such knowledge is costly, while it is risky to trust that the contract does what the developer says it does. Smart contracts also deviate substantially from the normal way in which people view a contract: as a part of an interpersonal relationship, which does not regulate in detail how to deal with different circumstances.

Smart contracts can offer benefits in certain circumstances despite the risks. This seems to be the case in particular with agreements with anonymous parties abroad, or as part of a larger ordinary agreement (where the smart contract is used as a part of that agreement).

Another important general topic is the General Data Protection Regulation. The controller plays an important role in guaranteeing adequate processing of personal data under the GDPR. Due to the P2P character of blockchains, it can be difficult to determine who the cotroller(s) is (or are), especially if applications are included in the core code (such as native crypto currencies). Even if a controller can be designated, it is difficult for this person to adequately shape the responsibility. To achieve something within a blockchain (such as deleting data), coordination between managers is required. The coordination needed to meet the rights of data subjects is not supported by the technology and sometimes even counteracts compliance with the GDPR. It is the difficult task of the controller(s) to achieve this coordination in any way.

Another tricky issue under the GDPR is the erasure of personal data in the context of data minimization and the right to be forgotten, for example. In blockchains based on a system of crypto-economic incentives, this is not possible in practical terms. It is currently unclear whether this tension will be resolved by opting for a different type of blockchain or putting into perspective what 'erasure' means under the GDPR.

Use-cases

Four use-cases were investigated for the purpose of this report.

The ship registration

The use of a permissionless public blockchain for the ship register leads to a shift in costs and time (from initial registration to later transactions) and results in a lower reliability of Dutch ship registration. In addition, there are risks of fraud, privacy, and abuse for money laundering, etc. For the Netherlands, because of the high-quality ship registration that exists here, a permissionless public blockchain is therefore not a useful option. Other blockchain variants are possible but do not have the benefits of a permissionless public blockchain. Depending on the chosen structure, legal rules will also have to be adjusted to a greater or lesser extent.

Treasury banking for the benefit of the new construction of schools

In this use-case, particular attention was paid to the usefulness of blockchain as a means of accountability. One of the tasks of the Auditdienst Rijk (national audit service) is to check whether the financial management of the Central Government meets standards of efficiency, legality, orderliness and verifiability. A blockchain that structures treasury banking for the construction of a new school building will probably simplify controls by the Auditdienst Rijk. However, two comments can be made. In the first place, simplified control can also be realized without a blockchain. Secondly, a blockchain implementation does not cover all dimensions that the Auditdienst Rijk wants to control. A blockchain does not make the Auditdienst Rijk superfluous.

The transport of waste within the EU

The European Regulation on on shipments of waste does not stand in the way of the digital execution of the relevant processes. In this respect, implementation in a blockchain would be possible. However, the impossibility of deleting personal data placed on the blockchain is a point of concern. In addition, physical checks remain necessary. Shipments that have never been entered in the blockchain the blockchain does not know about. If data entered does not correspond to reality, the blockchain itself cannot determine this. It is not clear what the added value of a blockchain implementation is compared to a traditional automation process.

The sharing of privacy-sensitive data by the government - the CAK

This use-case concerns complicated invoicing processes within the framework of the Social Support Act. In this use-case, automation of work processes can mean significant progress. The added value of blockchain is not clear. A blockchain implementation has important disadvantages in the field of data protection: data cannot be erased and it is difficult to correct data. To guarantee the confidentiality of personal data, data is stored off-chain. The question is whether this will remove the potential benefits of using a blockchain.

Synthesis

Legal framework

Charting the various legal aspects of blockchains requires a structure that can function as an ordering principle. To this end, criteria for acceptability of normative technology have been chosen. Blockchain is normative technology. Its purpose is to redefine the relationships between the parties involved. Moreover, the chosen scheme of criteria is sufficiently general to give a broad picture of legal aspects. Here the four most important criteria are discussed.

Human rights and moral values / protection function of law

Which human rights and moral values come under pressure through the use of blockchain? Some come under pressure quite explicitly, in other cases it is more an implicit process. The most important ones that emerged in this study are the ones listed below.

The human rights that explicitly come under pressure include privacy and data protection, as already shown above.

Autonomy is under pressure. Information obligations towards users are unclear and blockchain applications leave little room for accommodating the autonomy of the user. The automated execution of processes based on a limited set of data (blindness of the blockchain) entails a risk of unequal treatment and discrimination.

Blockchain can also implicitly lead to the undermining of legal standards. The blockchain / smart contracts channel behavior and the applicable legal standard disappears from view. The code will take over the role of the law in the minds of those involved. Here is reason to keep your finger on the pulse.

Legitimacy

It is often claimed that a blockchain would make trust superfluous. However, it is often overlooked that the code for the blockchain or for the smart contract contains many choices. Instead of believing that trust has become superfluous, it is better to ask yourself what the legitimacy of exercising power through code is. The legitimacy has a formal aspect (administrative action requires a legal basis, private parties are, in principle, free to act), but also a guarantee aspect: sufficient safeguards must be built in to prevent the simple user from surrendering to the arbitrariness of the builder of the technology. Care should be taken to ensure that block chains do not compromise guarantees and legitimacy in the name of promoting innovation or efficiency.Democracy and transparency of rules

Blockchains have implications for many people who have not been involved in the development of the code that those implications bring about. This raises the question of the democratic legitimacy of blockchain: to what extent are those affected by blockchain involved in shaping a blockchain or blockchain application? The most important permissionless block chains have a governance structure in which everyone can participate, but the decision-making power nevertheless lies with miners and core code developers. Especially, if the social impact of block chains increases, effective governance is an important point for attention.

Proportionality

Blockchain is used for a variety of purposes. Achieving efficiency gains (better services, lower costs) is, according to the use-cases, a dominant motive. At the same time, human rights and moral values can come under pressure through the use of blockchains. Is a blockchain a reasonable means of achieving the goal (efficiency gain)?

In the first place, the claim that a blockchain leads to efficiency gains must be mitigated. A blockchain does not solve the problem of the authenticity of data entering the blockchain. Guaranteeing authenticity requires communication with the "outside world" (for example traditional

intermediaries) and efficiency is lost there. Just looking at the work of the nodes is too narrow a perspective and does not give a complete picture of the (in) efficiency.

The claim that blockchain solves problems with fragmented work processes, such as with the ship register, is debatable. All required data may be available on the blockchain for every relevant party, but this has not yield a workflow. Integration and assessment of the data in a work process requires a separate layer in software that will have to be placed on top of the blockchain. As this does not (yet) exist, the question arises again whether a traditional IT implementation of the work process is or cannot be more efficient.

In particular blockchains that function on the basis of crypto-economic incentives have important disadvantages: problems with the unchangeability of data, doubts about scalability and blockchains who work with proof-of-work, sustainability concerns.

In conclusion, it can be said that this report is critical of block chains. That does not mean that where blockchain offers opportunities they not be seized. Blockchain, however, does not appear to be the cure for all ailments, and permissionless blockchains in particular have side effects. When considering new blockchain projects, it is important to first make a good problem analysis and carefully examine whether a blockchain offers a solution for the identified problems. If this is the case, the framework elaborated in Chapter 5 provides a first tool for mapping out legal preconditions and thus turning it into a socially responsible innovation.

1. Introductie

1.1. Achtergrond

Blockchain is een fenomeen dat zich in recente jaren op een grote publieke belangstelling mag verheugen. Het is een innovatieve techniek die een aanvulling kan vormen op het internet om het mogelijk te maken partijen die elkaar niet kennen of (volledig) vertrouwen met elkaar zaken te laten doen. Blockchain technieken pretenderen een vertrouwensprobleem op te lossen. Het open karakter van de blockchain zou bovendien kunnen bijdragen aan transparantie, controleerbaarheid en legitimiteit van allerlei maatschappelijke processen. Tevens zou blockchain vele intermediairs die als een *trusted third party* functioneren overbodig kunnen maken en daarmee een grote efficiëntieslag mogelijk kunnen maken.
Geïnspireerd door de veronderstelde eigenschappen van de techniek beginnen reguliere bedrijven en overheidsinstellingen zich te oriënteren op wat blockchain voor hun processen zou kunnen betekenen en eerste, veelal verkennende blockchainprojecten worden uitgevoerd. Indien bovenstaande verwachtingen van de techniek bewaarheid worden, kunnen bestaande verhoudingen binnen de samenleving behoorlijk veranderen. Daarbij kunnen waarden en belangen onder druk komen te staan. Dat roept de vraag op wat de juridische aanvaardbaarheid is van blockchain in de verschillende gedaantes die het kan aannemen. De aanvaardbaarheid vermindert waar de toepassing van blockchain techniek ertoe leidt dat door de wet beschermde waarden en belangen onder druk komen te staan. Aanvaardbaarheid kan weer toenemen waar een techniek een duidelijk nut heeft of waar door het maken van andere keuzes de druk op beschermde waarden en belangen afneemt.
Dit onderzoek beoogt een kader te ontwikkelen voor de aanvaardbaarheid van blockchain vanuit juridisch perspectief. Dit kader biedt een biedt de mogelijkheid om de kansen en risico's die blockchains bieden met elkaar in verband te brengen en zo het inzicht te vergroten in de mogelijkheden voor het benutten van de kansen die blockchain technologie burgers, bedrijven en overheden biedt en voor het beheersen van risico's en aandachtspunten in het licht van toekomstige wetgeving.

1.2. Onderzoeksvraag

De vraagstelling die centraal staat is: Wat zijn vanuit en perspectief van juridische aanvaardbaarheid de kansen en risico's verbonden aan blockchaintechniek?

1.3. Methode

Alvorens in te gaan op een analyse van het juridisch raamwerk waarbinnen blockchain technieken moeten opereren en welke kansen en risico's de technologie oplevert is enig begrip vereist van de verzameling technieken en technologieën die blockchain maken wat het is.

Blockchain is niet één enkele techniek, maar eerder een diverse verzamelingen van technieken en toepassingen die onderling nogal verschillen en niet zo heel veel gezamenlijke kenmerken vertonen. Eén kenmerk wordt zeker door welhaast elk van de verschillende vormen gedeeld, namelijk dat de achterliggende technologie ingewikkeld is.

Aan blockchain worden in de media allerlei eigenschappen toegeschreven en die niet zelden als absolute waarden gepresenteerd. Een uitgebreide beschrijving van de techniek stelt de lezer van dit rapport in staat de techniek beter op zijn waarde te schatten. Een goed begrip van de techniek maakt het mogelijk de juridische analyse scherper neer te zetten.

Blockchain is een breed fenomeen. Het is vrijwel onmogelijk om het in al zijn aspecten te vatten. Er worden velerlei toepassingsmogelijkheden aan blockchains toegeschreven. De uitwerking van die toepassingen is in verreweg de meeste gevallen niet erg volwassen en in veel gevallen is er in praktische zin weinig werkelijk gerealiseerd en bespiegelingen over die toepassingen hebben een hoog theoretisch gehalte. Om dit onderzoek uitvoerbaar te maken en houden is gekozen om een viertal use-cases als uitgangspunt te nemen voor de analyse. Deze use-cases betreffen merendeels projecten die als doel hebben een daadwerkelijke toepassing van blockchain technologie te realiseren. Vaak worden toepassingen beschreven in de financiële sector.[1] In dit rapport is er juist voor gekozen andersoortige toepassingen centraal te stellen.

1.4. Structuur van het rapport

Dit rapport bestaat uit 4 hoofdstukken. In hoofdstuk 2 wordt blockchaintechniek en verschillende technische varianten van blockchains beschreven. Tevens wordt aandacht besteed aan de achtergrond en herkomst van blockchain technologie en aan huidige toepassingsmogelijkheden vanuit een technisch perspectief. In hoofdstuk 3 een aantal juridische aspecten geanalyseerd die van belang zijn voor de in hoofdstuk 4 gepresenteerde use-cases, maar die zich niet lenen voor integrale behandeling binnen de use-cases. Hoofstuk 4 behandelt de use-cases die ten behoeve van dit rapport zijn onderzocht. Hoofdstuk 5 presenteert de bevindingen van de analyse van de use-cases in het licht van de centrale vraagstelling, wat betekent dit alles voor de wetgever? Het rapport wordt afgesloten met conclusies.

Schellekens is de hoofdauteur van het rapport. Paragraaf 3.2 is geschreven door Tjong Tjin Tai. De scheepsregsitratie use-case is gescheven door Schemkes en Tjong Tjin Tai. De use-case over schatkistbankieren is geschreven door Kaufmann. Leenes heeft een bijdrage geleverd aan hoofdstuk 2.

De auteurs zijn dank verschuldigd aan de experts die ten behoeve van dit onderzoek geïnterviewd zijn. Een lijst met de organisaties waar de geïnterviewden werkzaam zijn is als bijlage bij dit rapport opgenomen.

[1] Zie bijvoorbeeld J.J. Oerlemans, B.H.M. Custers, R.L.D. Pool en R. Cornelisse, Cybercrime en witwassen Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware, 319 Onderzoek en beleid.

2. Technische uitleg van blockchain

2.1 Introductie

Een blockchain is een databank die op meerdere plaatsen onder evenzovele beheerders wordt bijgehouden.[2] Nieuw toe te voegen data worden in een blok verzameld en 'en bloc' toegevoegd achteraan de bestaande databank, de blockchain. Het nieuwste blok bevat een digitale vingerafdruk (hash) van het laatste blok in de bestaande keten.

Een blockchain streeft ernaar de gegevens in de blockchain onveranderlijk vast te leggen. De achtergrond van het streven naar onveranderlijkheid is dat partijen voor wie de vastgelegde gegevens van belang zijn niet meer blind hoeven te vertrouwen op de beheerders van de databanken of derden die de beheerder zouden kunnen bewegen vastgelegde gegevens te veranderen of wissen.[3] Het elimineren van de noodzaak om te vertrouwen zou een nieuwe impuls geven aan het internet dat technisch gezien een zeker vertrouwen tussen gebruikers veronderstelt.

Onveranderlijkheid
Een claim van onveranderlijkheid is een stevige claim. Het is daarom van belang iets dieper in te gaan op de wijze waarop onveranderlijkheid wordt bewerkstelligd (of misschien beter, benaderd).

Een eerste element voor het benaderen van onveranderlijkheid hebben we al gezien: een blockchain wordt niet op één plek onder één beheerder bijgehouden. Er zijn meerdere volledige kopieën van een blockchain, bijgehouden door meerdere beheerders. Dit vermindert in sterke mate de afhankelijkheid van een of enkele beheerders. Individuele beheerders hebben betrekkelijk geringe invloed binnen het netwerk van nodes (knooppunten in het netwerk). Dit geeft tevens een eerste beperking van de onveranderlijkheid. Slechts wanneer een groot aantal beheerders samenspant kan de onveranderlijkheid van de geregistreerde data alsnog onder druk komen te staan.

Een tweede element is dat er economische prikkels worden ingebouwd om de beheerders te bewegen zich aan de spelregels, het protocol, te houden. Dit zijn positieve en negatieve prikkels. Daarin speelt de zogenaamde cryptocurrency, zoals bijvoorbeeld bitcoin, een rol. Beheerders die zich aan het protocol houden kunnen een beloning in de vorm van cryptocurrency verdienen. Een negatieve prikkel is dat een beheerder moet investeren voor hij in staat wordt gesteld cryptocurrency te verdienen. Een beheerder die zich niet aan het protocol houdt kan zijn investering als verloren beschouwen. De investering kan verschillende vormen aannemen. Het kan bijvoorbeeld een investering in elektriciteit en rekenkracht zijn (dit is het geval bij een systeem gebaseerd op zogenaamd Proof-of-Work) of bijvoorbeeld een investering in cryptocurrency (dit is het geval bij een systeem gebaseerd op zogenaamd Proof-of-Stake). Dit geeft echter ook weer een beperking aan. Indien prikkels hun werking verliezen (bijvoorbeeld omdat de waarde van de cryptocurrency daalt) dan kunnen de beheerders uitstappen. Dat kan het einde van de blockchain betekenen.

Dit alles is gevat in een softwaresysteem dat het moeilijker maakt voor beheerders om van het protocol af te wijken.

Het bovenstaande brengt echter ook weer een nieuw probleem met zich mee. Als er meerdere kopieën van een blockchain bestaan onder verschillende beheerders is er een risico dat de versies van de blockchain van elkaar gaan afwijken. Binnen de context van het elimineren van vertrouwen is dit probleem lastig op te lossen. Het aanduiden van een enkele beheerder als master die door de

[2] Technische begrippen, zoals 'beheerder', die in deze paragraaf worden gehanteerd worden uitgelegd in paragraaf 2.2.
[3] Nakamoto 2008, p.1.

anderen steeds gevolgd moet worden doet het voordeel van decentralisatie en daarmee geassocieerde, geclaimde eliminatie van vertrouwen teniet.

De oplossing voor het versieprobleem ligt in de door het protocol bepaalde regel dat de langste keten van geldige blokken de geldige keten is. Wat is nu een geldig blok? Dit wordt bepaald door uitvoering van het zogenaamde consensusmechanisme. In de bitcoin blockchain werkt dit als volgt:[4] De beheerders verzamelen alle transacties (i.e. nieuw aan de blockchain toe te voegen gegevens) gedurende een periode van circa 10 minuten en voegen deze samen tot hun zogenaamde kandidaatblok. Na ommekomst van de periode van 10 minuten beginnen alle beheerders een cryptografische puzzel op te lossen, gebaseerd op hun eigen kandidaatblok. De beheerder die er als eerste in slaagt zijn puzzel op te lossen stuurt zijn kandidaatblok samen met zijn Proof-of-Work (dat is het verifieerbare bewijs dat hij inderdaad zijn puzzel heeft opgelost) rond binnen het netwerk. De andere beheerders verifiëren dat het Proof-of-Work klopt en als dat het geval is geldt het blok van de winnende beheerder als geldig blok. Met andere woorden, de winnende beheerder heeft de langste, bestaande keten met een blok verlengd en daarmee is zijn keten nu de langste keten en dus de geldige keten. Iedere beheerder heeft in zijn blok een betaling aan zichzelf uitgeschreven, uit te betalen in nieuwe bitcoins. Alleen de winnaar van de puzzel ontvangt de betaling; immers alleen zijn blok wordt in de geldige keten opgenomen. Zodra het nieuwe blok aan de keten is toegevoegd start onmiddellijk een nieuwe competitie voor het volgende kandidaatblok. De duur van circa tien minuten is in wezen de tijd die nodig is om met krachtige computers de puzzel op te lossen.

> *Gedetailleerde uitleg van Proof-of work*
> Het basisidee van een blockchain is dat er blokken gegevens zijn die aan elkaar geschakeld zijn. In het geval van Bitcoin worden transacties die in een periode van circa 10 minuten plaatsvinden (ongeveer 2500) samengevoegd tot een *blok*. De volgende transacties komen in het volgende *blok* dat aan het begin een verwijzing bevat naar het vorige blok, en zo verder. Wanneer de reeks blokken van begin tot eind worden doorlopen is een volledig overzicht van alle transacties die plaats hebben gevonden beschikbaar.
> Om te garanderen dat er niet geknoeid is met de gegevens in een blok, bevat deze een 'controlegetal', een *hashcode*. De hashcode is een tekenreeks die wordt verkregen door de gegevens in het block door een functie te halen. Gebruikmakend van een welbekende hashfunctie, MD5, levert "Deze zin dient ter voorbeeld van hashfuncties." de volgende MD5-hash op: "**2948a9d076a01719fa67fef6a009790e**". Wanneer we een enkele letter veranderen is de hash volledig anders: "deze zin dient ter voorbeeld van hashfuncties." levert bijvoorbeeld "**c73a3318a1d7cd0d55ab712c19f84766**" op. Iedere wijziging in het blok is dus te detecteren. De hashcodes zijn onomkeerbaar. Het zal duidelijk zijn dat het niet mogelijk is om de korte tekenreeks van de hashcode om te toveren tot de voorbeeldzin, laat staan dat een echt blok dat uit duizenden tekens kan bestaan kan worden gecreëerd uit een tekenreeks van 32 tekens.
> Blokken bevatten ook een zogenaamd *Proof-of-Work*. In technische zin is de Proof-of-Work de tekenreeks die maakt dat de hashcode van het huidige blok (berekend uit de hashcode van het vorige blok, de transacties in het huidige blok en de Proof-of-Work) begint met een van tevoren vastgesteld aantal nullen (zie figuur 1). Dit vergt erg veel rekenkracht aangezien een grote hoeveelheid potentiële Proof-of-Work kandidaten moet worden gegenereerd en op basis daarvan hashcodes moeten worden berekend net zo lang tot een hashcode ontstaat die voldoet aan de eisen. De Proof-of-Work is een bewijs dat een substantiële investering heeft plaatsgevonden in het oplossen van een cryptografische puzzel. Alleen degene (node) die als eerste een Proof of Work heeft geleverd voor een blok mag dat blok aan de keten toevoegen.[5] Andere nodes controleren de hashcode van het nieuwe blok en voegen alleen geverifieerde blokken toe aan hun (lokale) keten. Doordat alle nodes deze procedure

[4] Antonopoulos 2017, Hoofdstuk 2.
[5] Voor het begrip ‘node’, zie wederom paragraaf 2.2.

doorlopen zijn er vele identieke geldige ketens. Deze procedure is dus een consensusmechanisme waarmee de geldigheid van de hele dataset wordt bepaald. De geldige keten in een blockchain is gedefinieerd als de langste aaneengesloten keten van blokken waarvoor Proof-of-Work bestaat.

Het aldus ingerichte stelsel levert de volgende resultaten:
Het netwerk convergeert naar één set gegevens. Dit gebeurt zonder decentralisatie aan te tasten: iedere tien minuten wint – naar verwachting – een andere beheerder. De beheerders investeren, nl. elektriciteit en rekenkracht in het oplossen van de puzzels (negatieve prikkel). De winnende beheerder verdient (mine-t) cryptocurrency (positieve prikkel). De blockchain is onveranderlijk in de volgende zin: een beheerder die gegevens in een oud blok verandert in zijn versie van de blockchain onderbreekt zijn keten. Het Proof-of-Work van het veranderde blok zal immers niet meer kloppen en dus verliest het blok zijn geldigheid. Ook de digitale vingerafdruk van dit blok in het opvolgende blok klopt niet meer. Daarmee is zijn keten onderbroken en niet meer de langste en zal door de rest van het netwerk genegeerd worden. De beheerders kunnen immers alleen bitcoins verdienen door een geldig blok toe te voegen aan de langste keten. Zij hebben er geen belang bij te investeren in een kortere keten.

Gedetailleerdere uitleg onveranderlijkheid
Indien een beheerder in een oud block gegevens verandert, dan correspondeert de hashcode van dat blok niet meer met die in het volgende blok en zal de keten van onze beheerder zijn onderbroken. De keten van onze beheerder is dan niet meer de langste en zal door de andere nodes genegeerd worden. Onze beheerder kan proberen dit te herstellen door nieuw Proof-of-Work te genereren voor alle blokken vanaf het blok waarin hij iets veranderd heeft tot en met het nieuwste blok. Maar de rest van het netwerk, gaat gewoon door nieuwe blokken toe te voegen aan hun lange keten. De kans voor onze beheerder om vanuit zijn achterstandspositie de rest van het netwerk in te halen en een nieuwe langste keten te genereren is miniem, dat kost simpelweg te veel rekenkracht. Dat is anders indien onze beheerder meer rekenkracht heeft dan de rest van het netwerk. Dat geeft dan meteen een randvoorwaarde aan voor de onveranderlijkheid van de bitcoin blockchain. Een beheerder of een consortium van beheerders die meer dan de helft van de rekenkracht bezitten kunnen de blockchain manipuleren en oude gegevens wijzigen al vergt dat wel een behoorlijke investering.

Blockchains worden onderscheiden in *permissionless* en *permissioned* blockchains en in publieke en private blockchains.

Een permissionless blockchain is een blockchain waarin een ieder miner kan worden.[6]
Bij een permissioned blockchain is het aan het hiërarchische oordeel van een centrale instantie of een collectiviteit (zoals de groep van alle miners) onderworpen wie als miner actief kunnen zijn. Hier kunnen alleen toegelaten miners deelnemen aan het consensusmechanisme.[7] In een permissioned blockchain is er vaak een centrale instantie die substantiële controle over de blockchain heeft.

Een permissioned blockchain kan met identieke protocollen werken als een permissionless blockchain. Het is echter ook mogelijk dat wordt volstaan met eenvoudiger consensusmechanismen. Een voorbeeld van een eenvoudiger consensusmechanisme is *round robin*: om beurten krijgen nodes de gelegenheid hun blok aan de keten toe te voegen.[8] Een dergelijke permissioned

[6] A permissionless blockchain is a blockchain, in which there are no restrictions on identities of transaction processors (i.e., users that are eligible to create blocks of transactions). Bron: BitFury Group 2015, p. 10.
[7] A permissioned blockchain is a blockchain, in which transaction processing is performed by a predefined list of subjects with known identities. Bron: BitFury Group 2015, p. 10.
[8] BitFury Group 2015, p. 12-13.

blockchain hoeft ook geen cryptocurrency te hebben. Afspraken om oude blokken te wijzigen kunnen eenvoudiger geaccommodeerd worden.[9] [10]

Bij een publieke blockchain kan iedereen lezen wat er op de blockchain staat. Bij een private blockchain kunnen alleen toegelaten gebruikers lezen wat er op de blockchain staat. Een permissionless blockchain is publiek.

Blockchains hebben velerlei toepassingen. De oer-permissionless-blockchain – de bitcoin blockchain – dient als betaalmechanisme met als inherente eigenschap dat voorkomen wordt dat bitcoins dubbel uitgegeven kunnen worden. Door alle transacties die met bitcoin plaatsvinden te registreren kan eenvoudig op het dubbel uitgeven van bitcoins gecontroleerd worden.

Een blockchain is een databank die op meerdere plaatsen onder evenzovele beheerders wordt bijgehouden.

Indien de kopieën of versies van verschillende beheerders uiteenlopen is een regel nodig om te bepalen wat de geldige versie is. Deze regel is dat de langste keten van geldige blokken de geldige keten is.

Een blockchain streeft ernaar de gegevens in de blockchain onveranderlijk vast te leggen.

In een permissionless en sommige permissioned blockchains zijn crypto- economische prikkels ingebouwd om de beheerders te bewegen zich aan de spelregels, het protocol, te houden en de onveranderlijkheid van gegevens niet aan te tasten.

Na deze korte introductie over de bitcoin blockchain kunnen de verschillende actoren binnen een blockchain geduid worden. We hebben dit overzicht nodig om de use-cases in meer detail te kunnen analyseren.

2.2 Terminologie en rollen

Wat is een blockchain?
In de introductie is bondig beschreven hoe de Bitcoin blockchain werkt. Bitcoin is de oorspronkelijke blockchain, maar in de loop der tijd zijn er vele varianten gemaakt op basis van een of meer uitgangspunten achter Bitcoin. Door deze variatie is het niet mogelijk een eenduidige definitie van 'de' blockchain te geven. De kenmerken die naar ons idee essentieel zijn om tot de familie van blockchain technologieën te behoren zijn:

- Data worden opgeslagen in blokken;
- Blokken gegevens zijn logisch aan elkaar gekoppeld door verwijzers (hashcodes).
- Er zijn meerdere kopieën (of versies) van de blokken gegevens (gedistribueerd model) onder beheer van verschillende beheerders.
- De geldigheid van een blok wordt bepaald door code.
- De langste keten van geldige blokken is de geldige keten.

Dat betekent dat we sommige kenmerken van de Bitcoin blockchain niet tot de kernelementen van een blockchain rekenen:

- Hoe precies gedefinieerd wordt wat een geldig blok is (voor Bitcoin is dat Proof-of-Work).

[9] Bitfury Group 2015, p. 12-14.
[10] Linnemann 2016.

- Dat de beheerders van de nodes in de blockchain (in de conceptie van de ontwerper) uitsluitend gedreven worden door economische prikkels.

Definities termen en rollen:

Blockchain:
: dit begrip wordt in dit rapport gebruikt om te verwijzen naar een database die middels software en/of hardware gedistribueerd wordt opgeslagen in de vorm van gekoppelde blokken, waarbij in beginsel de langste versie als de 'geldige' versie wordt gekwalificeerd.

Node:
: een computer met een softwareapplicatie die een versie van de 'volledige' transactiegeschiedenis van een blockchain beheert en/of een bijdrage levert aan het consensusmechanisme.[11]

Node-beheerder:
: dit begrip verwijst naar een *miner* en/of naar een *full node*-beheerder.

Miner:
: een persoon die bijdraagt aan de boekhouding op de door het protocol voorgeschreven wijze, bijvoorbeeld door middel van het oplossen van cryptografische puzzels. In sommige systemen wordt een vergelijkbare rol aangeduid met de term *validator*.

Full node:
: een computer met een softwareapplicatie die een versie van de 'volledige' transactiegeschiedenis van een blockchain downloadt en opslaat. Full nodes controleren of transacties en blokken voldoen aan de regels die in het betreffende blockchain protocol zijn vastgesteld en dragen aldus eveneens bij aan het consensusmechanisme.

Full node-beheerder:
: een natuurlijk persoon of een rechtspersoon die een full node beheert. Omdat de volledige versie op een veelheid van locaties wordt beheerd, zijn er ook veel full node-beheerders.

Core developer:
: een natuurlijk persoon die core blockchain protocollen ontwikkelt, zoals code betreffende consensus, validatie van blokken of transacties, de virtual machine (die Bitcoin Script bytecodes, of gecompileerde smart contracts uitvoert), en smart contract programmeertalen.

Ontwikkelaar van een smart contract:
: een natuurlijk persoon die smart contract code ontwikkelt op basis van de programmeertalen die door de core developers zijn ontworpen. De ontwikkelaar van een smart contract kan deze code mogelijk ook in opdracht van de aanbieder van het smart contract op de blockchain zetten.

Aanbieder van een smart contract:
: een natuurlijke persoon of een rechtspersoon die een individueel smart contract aanbiedt op een smart contract platform.

Gebruiker:
: een natuurlijk persoon of een rechtspersoon (niet zijnde developer, full node-beheerder of miner) die een blockchain raadpleegt of (transactie)gegevens aanbiedt voor opname in de blockchain. Een voorbeeld is iemand die een betaling met Bitcoin wil verrichten en daartoe de benodigde transactiedata aan een node aanbiedt. Een ander voorbeeld is een notaris die ten behoeve van een cliënt een akte op een kadaster-blockchain plaatst.

Een deelnemer:
: een natuurlijk persoon of een rechtspersoon die een versie van de blockchain beheert (full node) en/of gebruiker is van een blockchain. Gezien de verwarring die dit begrip teweeg kan brengen wordt deze term zo min mogelijk gebruikt in dit rapport.

Oracle:

[11] Antonopoulos 2017, Hoofdstuk 8.

een applicatie (software agent) die off-chain gegevens, aangeleverd door een derde partij of een andere applicatie, zoals een sensor, on-chain zet ten behoeve van de uitvoering van een smart contract.

Exchange:

een exchange is een digitale marktplaats waar vragers en aanbieders van cryptomunten elkaar ontmoeten en cryptomunten verhandeld kunnen worden tegen andere cryptomunten of fiat valuta.

Wallet:

software en/of hardware waarmee een 'bezitter' van cryptocurrency de betreffende publieke en private sleutel(s) beheert. Met behulp van de wallet kunnen betalingen met cryptocurrency ingeleid worden en kunnen betalingen in cryptocurrency ontvangen worden. De wallet kan informatie geven over (recente) transacties. Een wallet kan ook meerdere sleutelparen bevatten. Multisig toepassingen zijn ook mogelijk (meerdere private keys zijn dan nodig voor een enkele transactie).

2.3 Overige onderscheidingen

Enkele implicaties van consensusmechanismen

Schaalbaarheid

Veel blockchains werken met proof-of-work. Om de onveranderlijkheid te bewerkstelligen moet er voor ieder block een proof-of-work bestaan. Dat betekent uiteraard dat een nieuw blok pas toegevoegd kan worden als de generatie van het proof-of-work voltooid is. In de bitcoin blockchain kost dit ongeveer 10 minuten per blok. Bovendien hebben blokken een beperkte blokgrootte. Een en ander leidt dit tot twijfels over de schaalbaarheid, i.e. het aantal transacties dat de bitcoinblockchain per minuut aankan. Er is een risico dat de blockchain verstopt raakt bij toenemende populariteit.

Duurzaamheid

Om onveranderlijkheid te bewerkstelligen moet een consensus mechanisme uitgevoerd worden. Dit levert de benodigde controle getallen voor individuele blokken (hashcode in combinatie met proof-of-work) die garanderen dat de informatie in het betreffende blok integer is. Bovendien zorgt het consensusmechanisme ervoor dat ieder blok (eigenlijk keten van blokken) op vele plaatsen beschikbaar is zodat ook de integriteit van de ketens is gegarandeerd. In veel blockchains berust het consensusmechanisme op proof-of-work. Blockchain is een redundant systeem waarin alle miners proberen proof-of-work voor hun block te leveren (minen). Juist omdat ze allen minen, kost het veel rekenkracht en dus elektriciteit en is een blockchain met proof-of-work vanuit duurzaamheidsperspectief bijzonder nadelig.[1]

Toepassingen

Het moge duidelijk zijn dat de toepassingsmogelijkheden voor gedistribueerde databases waarvan blockchain slechts een variant is, schier oneindig zijn. Hieronder wordt een in de technische literatuur aangehouden onderscheiding in toepassingen aangehouden.

Distributed ledger

Indien een blockchain puur als een *distributed ledger* wordt gebruikt, dan dient zij om data over feiten zoals transacties vast te leggen. Het is van belang om te beseffen dat opname in een blockchain niet kan garanderen dat de gegevens zelf juist zijn. De blockchain kan er hooguit voor zorgen dat eenmaal opgeslagen gegevens niet meer gewijzigd kunnen worden. Daarbij gelden uiteraard de beperkingen van onveranderlijkheid zoals hierboven besproken.

Smart contracts

Vanuit technisch perspectief, is een smart contract code die een gebruiker op de blockchain kan plaatsen. De Ethereum blockchain ondersteunt de mogelijkheid om smart contracts te maken. Het biedt een platform en programmeertaal om smart contracts op te stellen en uit te voeren. Het concept van smart contracts wordt hier verder dan ook beschreven in de context van Ethereum, ook al is de mogelijkheid om smart contracts te maken niet beperkt tot de Ethereum blockchain. Voorbeelden van projecten die platforms voor smart contracts ontwikkelen of aanbieden, behalve Ethereum, zijn onder andere EOS, Tezos en het op bitcoin gebaseerde Rootstock.
Een Ethereum gebruiker kan een smart contract scheppen en daarin de instructies opnemen die hem goeddunken, maar zodra het smart contract eenmaal in de blockchain is opgenomen, wordt de uitvoering van het smart contract geregeld door het platform en de instructies/voorwaarden (code) in het smart contract. De gebruiker die het smart contract op de blockchain heeft gezet kan daar geen invloed meer op uit oefenen.[12]
Een smart contract kan onder geprogrammeerde voorwaarden tokens overdragen. Via een oracle kan het feiten van buiten de blockchain (geprogrammeerd) in aanmerking nemen. Zo kan men een smart contract zo programmeren dat het een bepaalde dienst verricht, zoals het openen van een IoT hoteldeur, indien aan bepaalde voorwaarden, zoals betaling, is voldaan. Het smart contract controleert automatisch of aan de voorwaarden is voldaan.[13]
Het smart contract, i.e. de code wordt uitgevoerd door alle nodes in het netwerk. Degene die het contract ‘vraagt’ de deur te openen (voor hemzelf of voor een ander) zal een transaction fee moeten betalen die ten goede komt aan de node-beheerders, die immers rekencapaciteit ter beschikking moeten stellen om de code van het contract uit te voeren. Dit kan betekenen dat er een zekere uitdaging in zit om een businessmodel rond smart contracts te ontwikkelen. Veel internetgebruikers zijn immers gewend dat allerlei diensten gratis – in de zin van zonder directe financiële tegenprestatie – worden verleend.
Zoals uit het hiervoor gegeven voorbeeld van een IoT hoteldeur blijkt, kan een smart contract functioneren op een manier die enigszins doet denken aan de uitvoering van een overeenkomst. Dat is ook de achtergrond van de term ‘smart contract’. De term ‘smart contract’ is voor het eerst gebruikt door Nick Szabo in 1996.[14] De term bestond al ruim voor de eerste blockchain ontstond. Of een smart contract ook in juridische zin een overeenkomst kan zijn is een vraag die paragraaf 3.2.8 behandeld wordt.

Tokens

Tokens
Een token is een uniek element. De uniciteit moet begrepen worden in de zin dat een bitcoin niet dubbel uitgegeven kan worden. Welke betekenis een token heeft hangt af van de context waarin het gebruikt wordt (bijvoorbeeld een loyalty card, een munt, etc.) In blockchain context bestaan zogenaamde native tokens. Dit zijn de cryptocurrencies zoals bitcoin en ether die nodig zijn om het consensus mechanisme te laten werken. Daarnaast kunnen ook tokens op applicatieniveau gedefinieerd worden. Deze laatste worden hier verder niet behandeld.[15]

Samengestelde transacties

In de informatica, worden verschillende decentrale systemen naar toepassing onderscheiden. Sommige categorieën vinden hun oorsprong in de periode voorafgaande aan Nakamoto’s blockchainpaper. De toepassingen die hierna genoemd worden zien op ingewikkelder structuren dan

[12] Om aan de bezwaren die aan de onveranderlijkheid van smart contracts tegemoet te komen, is de functie ‘delegatecall’ ontwikkeld. Iedere aanroep van een ongewenst smartcontract wordt dan doorgeleid naar een ander contract. (Grincalaitis 2018).
[13] Buterin 2014.
[14] Szabo 1996.
[15] Zie https://www.ethereum.org/token .

eenvoudige smart contracts. De decentrale toepassingen krijgen allicht een impuls door de komst van blockchains.

Een eerste mogelijkheid bestaat uit Decentralised Applications (DApps). Dit is een applicatie die ontstaat door een aantal smart contracts aan elkaar te koppelen. Vervolgens worden Decentralised Organisations onderscheiden. Dit zijn in wezen door mensen geleide organisaties waarbij de interacties tussen de betrokkenen en het beheer van de eigendommen van de organisatie verlopen via een in software vastgelegd protocol dat gehandhaafd wordt in een blockchain.[16]
Nog een stap verder gaan zogenaamde Decentralised Autonomous Organisations (hierna DAO). Een DAO is een organisatie die geleid wordt door regels vastgelegd in smart contracts.[17]

Het bovenstaande geeft onderscheidingen weer die in de literatuur worden gemaakt. Het zijn meer typeringen van toepassingen dan dat er harde scheidslijnen te trekken zijn. Ook is onduidelijk of toepassingen als DAOs in de praktijk een hoge vlucht zullen nemen.

Smart contract: Code die een gebruiker op de blockchain plaatst. Een andere gebruiker kan deze code 'bezoeken'. De code wordt dan uitgevoerd door nodes. De code is onveranderlijk op dezelfde wijze als data in een blockchain onveranderlijk zijn.
Token: Een token is een uniek element. De uniciteit moet begrepen worden in de zin dat een bitcoin niet dubbel uitgegeven kan worden.
Decentralised application: Een applicatie die ontstaat door twee of meer smart contracts te koppelen.
Decentralised Autonomous Organisation (DAO): Een DAO is een organisatie die geleid wordt door regels vastgelegd in smart contracts.

Governance

Het ontwerp van een blockchain is niet voor de eeuwigheid. Er bestaat in de praktijk behoefte om een blockchain aan te passen, bijvoorbeeld aan veranderende behoeften in de tijd. Met andere woorden, er is behoefte aan een governance structuur die besluitvorming over aanpassingen in goede banen leidt. Uiteraard is in iedere blockchain een eigen praktijk rond governance gegroeid. De governance kan meer impliciet zijn en berusten op machtsverhoudingen, maar kan ook meer expliciet gemaakt zijn. Waar dat laatste het geval is, kan de structuur al dan niet ten dele ingebed zijn in het protocol. Bij de beschrijving van governance structuren in permissionless blockchains, maakt Finck onderscheid tussen twee hoofdtypen van governance: on chain en off chain governance.

On chain governance ligt in handen van de houders van cryptocurrencys. Hun invloed is evenredig aan de hoeveelheid cryptocurrency die ze houden. Beheerders van nodes en softwareontwikkelaars moeten door de currencyhouders geaccepteerde aanpassingen doorvoeren en hebben als zodanig geen formele invloed. Snelheid en efficiëntie worden genoemd als voordelen van on-chain governance, maar er zijn vragen in termen van representativiteit van belanghebbende actoren (bijvoorbeeld indien het aantal participerende currency-houders klein is) en vragen rond de bescherming van minderheidsbelangen (bijvoorbeeld omdat de telling van stemmen een te grote invloed heeft).

Bitcoin en Ethereum werken met off-chain governance. Daarin worden meer stakeholders betrokken bij de besluitvorming. Eenieder kan een Bitcoin Improvement Proposal (hierna BIP) resp. Ethereum

[16] Vitalik Buterin , DAOs, DACs, DAs and More: An Incomplete Terminology Guide, May 6, 2014. Beschikbaar op: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (6 mei 2019).
[17] Prusty, Narayan (27 Apr 2017). Building Blockchain Projects. Birmingham, UK: Packt. p. 9.

Improvement Proposal in discussie brengen binnen de bredere bitcoin resp. Ethereum gemeenschap. Er is een functionaris – bijv. de BIP editor – die nieuwe voorstellen in de openbare GitHub repository plaatst. Uiteindelijk beslissen de ontwikkelaars welke voorstellen geaccepteerd worden. Dan is het nog aan miners die gezamenlijk tenminste de helft van de rekenkracht bezitten om de aanpassing door te voeren.

2.4 Eigenschappen

In de voorgaande paragrafen is een beschrijving van de werking van blockchains gegeven. Op basis van de beschrijving van de werking kunnen een aantal eigenschappen van blockchains onderscheiden worden. Het gaat om de volgende

- onveranderlijkheid
- blindheid
- redundantie en decentralisatie
- transparantie

Hierna worden deze eigenschappen nader geduid en wordt een reflectie gegeven over de kansen en risico's die deze eigenschappen in abstracto bieden bij inzet van een blockchain in een praktische context.

Onveranderlijkheid

Deze eigenschap heeft betrekking op informatie (data of code) opgenomen in een blockchain. We beginnen met de onveranderlijkheid van data. Gegevens die eenmaal zijn opgenomen in een blockchain die bouwt op crypto-economische prikkels kunnen niet eenvoudig veranderd worden. Dit is in wezen een positieve eigenschap. Een databank wordt over het algemeen bijgehouden om gegevens te bewaren. De integriteit van de gegevens is een nastrevenswaardig belang. Dit is bijvoorbeeld van belang voor blockchains omdat zij toegepast worden om tokens die een waarde vertegenwoordigen over te dragen (vgl. de uitdrukking het internet van waarde) of omdat ze worden gebruikt om een juridische status vast te leggen (bijv. Kadaster). Er kunnen echter ook omstandigheden zijn waarin het gewenst is gegevens weer uit een blockchain te verwijderen of te wijzigen. Gegevens kunnen incorrect blijken of ze verliezen hun bruikbaarheid na verloop van tijd. Dan kan het gewenst zijn de gegevens te verwijderen om zo correctheid van gegevens te bewerkstelligen, opslagcapaciteit te besparen of de snelheid van het systeem te vergroten.
Net als data die eenmaal in een blockchain zijn opgenomen kan ook een smart contract niet meer uit de blockchain verwijderd worden. Dit is een positieve eigenschap in de zin dat het van belang is dat code die gebruikt wordt om een transactie af te wikkelen, niet halverwege veranderd wordt. Niettemin, is het ook gewenst code die niet adequaat functioneert of niet meer past in veranderde gebruiksbehoeften weer te kunnen verwijderen.
Concluderend kan gezegd worden dat de onveranderlijkheid van een blockchain helpt om integriteit te borgen, maar ook in de weg kan staan. Soms is veranderlijkheid gewenst.

Blindheid

Als een registratie niet functioneert dan komt dat vaak omdat er gegevens ontbreken, incorrect zijn, niet tijdig zijn aangeleverd, door een onbevoegde partij zijn aangeleverd etc. (zie scheepsregister use-case, ILT use-case, CAK use-case). Er vindt controle plaats van relevante gegevens alvorens ze worden verwerkt in de keten. Deze verificatie en/of authenticatie vindt vaak plaats door daartoe aangewezen en geautoriseerde partijen. De bitcoin blockchain bevat geen mechanismen om verificatie/authenticatie van gegevens die de blockchain binnenkomen uit te voeren. De bitcoin blockchain kan daarom geen transacties tegenhouden die door een onbevoegde partij worden verricht. In de praktijk, bestaat behoefte aan een garantie van authenticiteit van gegevens voor verdere verwerking. De procedure voor het vaststellen van welke gegevens in de blockchain worden opgenomen is uitsluitend gericht op andere zaken: de procedure zorgt ervoor dat de verschillende kopieën/versies van de blockchain gelijklopen (dezelfde gegevens registreren), dat geen beheerder een overwegende invloed krijgt, dat er beloningen voor beheerders zijn die hen motiveren actief te

blijven als miner etc.. De blockchain kan garanderen dat de gegevens in de blockchain integer zijn, maar kan niet garanderen dat ze juist zijn; het is 'garbage in, garbage out'.
Bovendien is de uitvoering van een transactie op een blockchain een geautomatiseerd proces dat geen menselijke tussenkomst vergt.[18] Menselijke tussenkomst functioneert ook niet als waarborg van de authenticiteit van opgenomen gegevens.

Een mogelijke tegenwerping is dat de bitcoin blockchain controleert op double spending. Er vinden dus wel degelijk controles plaats en bovendien zonder menselijke tussenkomst. De controle op double spending is echter de uitzondering die de regel bevestigt. Deze controle kan uitgevoerd worden omdat de gegevens die voor het uitvoeren van de controle nodig zijn in de blockchain zelf aanwezig zijn. Er zijn veel andere zaken waar de bitcoin blockchain niet op controleert en ook niet kan controleren. Een voorbeeld is: is degene die een bitcoin transactie aanbiedt wel bevoegd om gebruik te maken van de betreffende private sleutel? Om dit te weten is kennis van buiten de blockchain nodig.

Misschien zou men ook nog kunnen tegenwerpen dat het onredelijk is om van de blockchaintechniek te verlangen dat zij authenticiteit garandeert. Dat kan een normale centrale databank immers ook niet. Een centrale databank kan inderdaad ook niet controleren of ingevoerde gegevens correct zijn, maar er wordt gewoonlijk ook niet geclaimd dat een gewone databank de noodzaak om te vertrouwen elimineert. Die claim wordt juist wel ten aanzien van blockchains gemaakt.

Smart contract code is ook blind
Ook een smart contract opgenomen in een blockchain heeft geen grip heeft op wat er buiten de blockchain gebeurt. Uiteraard kan een smart contract via een oracle rekening houden met informatie van buiten de blockchain. Hierbij zijn twee kanttekeningen te maken. In de eerste plaats, bevestigt dit dat een smart contract in de regel blind is. Een smart contract kan alleen iets zien als het raadplegen van een desbetreffend oracle expliciet ingeprogrammeerd is. In de tweede plaats moet een smart contract ook maar vertrouwen op de authenticiteit van het oracle. Een voorbeeld kan dit illustreren. Een IoT-hoteldeur gaat niet meer open als een smart contract geconstateerd heeft dat de verblijfsperiode van de betreffende hotelgast is verstreken. Dit impliceert dat de blockchain erop vertrouwt dat er niet gemanipuleerd is met de hoteldeur. De IoT hoteldeur is een oracle waarop het smart contract moet vertrouwen.

Redundantie en decentralisatie

Er bestaan meerdere kopieën van de databank.[19] Door redundantie staat of valt het functioneren van een blockchain niet met het functioneren van een enkele node in het netwerk. De redundantie geeft ook een zekere bescherming tegen een van buiten komende dreiging, zoals een natuurramp, of een cyber aanval. In zoverre is dit een positieve eigenschap.
Redundantie en decentralisatie creëren echter ook coördinatieproblemen. Sommige coördinatieproblemen worden langs technische weg opgelost, bijvoorbeeld hoe zorg je ervoor dat de verschillende versies van de blockchain dezelfde data registreren? Andere coördinatieproblemen worden echter niet opgelost: hoe verwijder je data uit alle kopieën? Bovendien beperken coordinatieproblemen zich niet tot operationele kwesties (zoals het verwijderen van data uit alle kopieën), maar strekken zich ook uit tot de meer strategische kwesties van aanpassing van het protocol om op de lange duur bij de tijd te blijven.

[18] Een miner of full node is niet actief betrokken bij de uitvoering van het consensus mechanisme of formele verificatie van transacties. Uiteraard kan een beheerder van een node als hij dat wil ingrijpen op alles wat er op zijn systeem gebeurt. Ingrepen die echter niet passen binnen het protocol leiden er toe dat de beheerder zichzelf diskwalificeert en worden daarmee sterk ontmoedigd.
[19] Een kanttekening is het volgende: Miners concurreren met elkaar. Dat stimuleert hen steeds snellere computerapparatuur te kopen met allicht ook een hoger elektriciteitsverbruik. De toenemende kosten leiden tot concentratie onder miners. Dat vermindert de redundantie.

Transparantie

De geldige keten is de langste keten met geldige blokken. Om dit te kunnen constateren moeten full nodes transparant zijn over de keten. In een publieke blockchain kan iedereen de data op de blockchain lezen. In een private blockchain kunnen alleen de toegelaten deelnemers de blockchain lezen (maar dit kan ook nog een grote groep zijn). Voor veel toepassingen is het echter niet handig dat iedereen alles kan lezen.
Een manier om dat op te lossen is ervoor te zorgen dat iedereen nog wel de data kan zien, maar daar geen informatie aan kan ontlenen. Voorbeelden zijn versleuteling van on-chain data, het werken met pseudoniemen, off-chain opslag met on-chain alleen een digitale vingerafdruk van de off-chain opgeslagen informatie etc. De off-chain opgeslagen informatie moet dan uiteraard ook weer adequaat beveiligd worden. Dit alles voegt echter complexiteit toe.
Een andere oplossing is werken met leesrechten. Eenieder kan alleen de data lezen waartoe hij leesrechten heeft. De gebruikers met beperkte leesrechten zullen dan de keten niet meer kunnen verifiëren; ze kunnen hem immers niet meer helemaal lezen. Zij zullen dan moeten vertrouwen op tussenpersonen die de keten wel kunnen auditen. Nu zou men misschien nog kunnen leven met het idee dat niet iedereen data kan auditen (veel gewone gebruikers zullen dit immers nooit doen), maar lastiger is dat ook deze oplossing complex is. De leesrechten zullen immers door iedere full node op dezelfde manier toegepast moeten worden.
Een ander punt is dat transparantie van data nog niet gelijk staat aan het adequaat informeren. Het hiervoor genoemde voorbeeld van de IoT hoteldeur kan dit illustreren: voor de hotelgast is niet alleen van belang dat de IoT hoteldeur doet wat zij verondersteld is te doen, maar ook is van belang dat de code van het smart contract doet wat het smart contract hoort te doen. Dat is vast te stellen door de code van het smart contract zoals dat op de blockchain staat te inspecteren. Dat veronderstelt echter wel dat de waarde van de transactie de tijdsinvestering in inspectie rechtvaardigt. De hotelgast kan de inspectie van de code uiteraard ook uitbesteden aan een EDP-auditor. Dat introduceert echter weer een nieuwe tussenpersoon, die moet worden vertrouwd.

Op basis van hun werking kunnen een aantal eigenschappen van blockchains worden onderscheiden en gerelativeerd. Het gaat om de volgende:
• onveranderlijkheid
• blindheid
• redundantie en decentralisatie
• transparantie

3. Algemeen juridisch deel

3.1 Inleiding

Hoewel juridische kwesties bij de specifieke use-cases aan de orde komen, zijn er diverse algemene vragen die ten behoeve van de overzichtelijkheid beter in het algemene deel aan de orde kunnen worden gesteld voor alle use-cases tezamen. Te denken valt aan vragen van IPR (jurisdictie en toepasselijk recht), de juridische betekenis (geldigheid, bewijskracht), aansprakelijkheid. Deze vragen kunnen bij de huidige stand van zaken mogelijk nog niet eenduidig worden beantwoord. In dat geval zal worden getracht verschillende alternatieven te schetsen of mogelijk suggesties voor toekomstige regelgeving te doen. Het is niet ondenkbaar dat de rol van accountants en notarissen verandert onder invloed van blockchain. Of, en hoe dit gebeurt, is uiteraard een toekomstige omstandigheid waarover geen harde informatie bestaat.[20] Het onderzoek schetst een beknopt verwachtingspatroon voor zover kenbaar uit bestaande literatuur. Verwachtingen die nauw samenhangen met smart contracts worden bij de derde use-case behandeld.

[20] Zie ten aanzien van notarissen Tjong Tjin Tai 2018a.

3.2 Privaatrechtelijke aspecten

3.2.1 Algemeen[21]

Blockchaintechnologie roept verschillende vragen op voor het privaatrecht. Het privaatrecht heeft betrekking op de regels die tussen burgers onderling gelden, zoals de vraag of je een contract moet nakomen, of iemand schadevergoeding aan een ander moet betalen omdat hij eigendom van die ander heeft beschadigd. In het privaatrecht is het uitgangspunt dat mensen vrij zijn om te doen wat ze willen. Er zijn maar weinig beperkingen. Blockchaintechnologie is daarom in principe toegelaten, de vraag is vooral of gebeurtenissen en handelingen op en rond blockchains gevolgen hebben in het privaatrecht. Om dit te beoordelen werkt het privaatrecht met regels die uitgaan van bepaalde privaatrechtelijke concepten zoals 'overeenkomst' of 'contract', 'goederen' en dergelijke. De taak van juristen is om bij gebeurtenissen in de wereld te beoordelen of sprake is van zo'n concept, bijvoorbeeld of een gesprek tussen twee mensen is uitgemond in een overeenkomst. Dit proces heeft 'kwalificatie'. De belangrijkste vragen rond blockchain hebben ermee te maken hoe onderdelen en aspecten van blockchain moeten worden gekwalificeerd, en wat daar de gevolgen van zijn.

3.2.2 Wat is een blockchain in het privaatrecht?

Een blockchain is een verschijnsel dat gebruik maakt van Internet (of eventueel andere netwerkverbindingen), waarbij diverse computers (nodes) samenwerken. Die nodes worden gecontroleerd door mensen:[22] node-beheerders. Computers zelf worden in het recht beschouwd als dode dingen, werktuigen die door mensen worden gebruikt. Voor de kwalificatie van een blockchain draait het er daarom om hoe de relatie tussen de node-beheerders moet worden gekarakteriseerd (gekwalificeerd). Juristen noemen de juridische relatie tussen mensen ook wel een 'rechtsverhouding'. Om het plaatje compleet te maken is het nodig verschillende mogelijkheden te onderzoeken.

De eerste stap is of er tussen de node-beheerders een *overeenkomst* bestaat. 'Overeenkomst' is de juridische naam voor wat niet-juristen vaak contract noemen. Met 'contract' wordt meestal bedoeld een papier (of elektronische variant daarvan) waarin partijen hun afspraken hebben neergelegd en dat zij hebben ondertekend: dit bewijst dat er een overeenkomst is gesloten. Maar het is ook mogelijk om een mondelinge overeenkomst te sluiten, daarom spreken juristen liever van 'overeenkomst'. Om te bepalen of er een overeenkomst is, moeten we eerst vaststellen of er juridische verplichtingen bestaan tussen node-beheerders onderling en tussen node-beheerders en gebruikers.

a. Een blockchain leidt op zichzelf niet tot verplichtingen

Van belang is dat er in een blockchain geen verplichting is van node-beheerders om iets te doen. De gedachte achter een blockchain is dat er een prikkel is om transacties te verwerken, waardoor genoeg nodes zullen werken om de blockchain draaiende te houden. Er is ook geen verplichting om de node actief te houden, om downtime te vermijden o.i.d. Node-beheerders mogen, als zij dat willen, een vervalste blockchain op hun node draaien, transacties en *proof of work* weigeren. Dat zou wel betekenen dat zij het protocol niet volgen. Maar er is geen directe sanctie; de gedachte achter een blockchain is dat iemand die het protocol niet opvolgt vanzelf buiten de blockchain blijft staan omdat de andere node-beheerders de verwerkingen van die node niet accepteren. Er is dus een feitelijke dwang om mee te doen, maar geen juridische verplichting. Net zoals het niet verplicht

[21] Om de tekst begrijpelijk te houden voor niet-juristen wordt niet op alle nuances en details ingegaan en is soms gekozen voor gewone taal in plaats van de precieze juridisch terminologie.
[22] Om precies te zijn: dit kunnen natuurlijke personen (mensen) of rechtspersonen (ondernemingen en dergelijke) zijn.

is om in een gesprek dezelfde taal te spreken als de andere deelnemers, maar dat wel nodig is als je daadwerkelijk mee wil praten.

Er is dus geen verplichting om actief bij te dragen aan de blockchain. Dit kan indirect ook worden afgeleid uit de hack van The DAO (zie par 3.2.3), waarbij de meerderheid van de Ethereum-deelnemers er feitelijk voor heeft gekozen om af te wijken van het eerdere protocol: dit werd niet opgevat als een schending van een juridische of andere verplichting. Voor bijzondere blockchains zou dit anders kunnen zijn. Een voorbeeld is een blockchain die onderdeel is van een overeenkomst om bepaalde administratieve processen tussen een paar bedrijven draaiend te houden.

Hieruit volgt ook dat er geen verplichting is van node-beheerders jegens gebruikers om transacties te verwerken.[23] De principiële techniek van blockchain berust erop dat node-beheerders niet afhankelijk zijn van vertrouwen op een juridische verplichting van node-beheerders om zich correct te gedragen; de blockchain zou automatisch leiden tot betrouwbaar gedrag van de blockchain als geheel, ongeacht wat individuele node-beheerders doen. Daarnaast mag iedere node-beheerders op ieder moment stoppen met deelname aan de blockchain. Als alle node-beheerders stoppen, houdt de blockchain op te bestaan. Gebruikers hebben geen concrete aanspraken op node-beheerders om de blockchain overeind te houden.

Wel kan het zo zijn dat betrokkenen bij een blockchain verplicht zijn om elkaar niet nodeloos in de weg te zitten, of juridisch gesproken: onrechtmatig te handelen. Dit volgt uit art. 6:162 BW en de daaruit voortvloeiende verplichting om rekening te houden met belangen van anderen.[24] Een voorbeeld is de relatie tussen beheerders van naburige nodes. De nodes beïnvloeden elkaar zo direct dat het mogelijk is dat er op de beheerders van naburige nodes verplichtingen rusten zonder overeenkomst Men kan denken aan opzettelijk vervalsen van berichten, het selectief doorlaten van transacties e.d. dat tot gevolg heeft dat de beheerder van een andere node extra rekencapaciteit moet inzetten of minder kans heeft om succesvol te ‘minen’. Zie over aansprakelijkheid par. 2.9.

b. Aansluiting bij een permissionless blockchain: geen overeenkomst

Als node-beheerders aansluiten bij een permissionless blockchain, sluiten zij dan een overeenkomst? Dit lijkt niet het geval te zijn. Een overeenkomst houdt in dat partijen tegenover elkaar verplichtingen op zich nemen. Zoals hierboven onder (a) is besproken, leidt een blockchain op zichzelf niet tot verplichtingen.

Die conclusie vindt bevestiging in een andere argumentatie. Om een node aan te sluiten bij een permissionless blockchain is geen toestemming nodig. Weliswaar kan een node-beheerder een node zo instellen dat deze geen berichten van een bepaalde andere node accepteert (technisch gezien is dit mogelijk), maar het blockchain protocol gaat er bij een permissioned blockchain per definitie vanuit dat node-beheerders andere node-beheerders zonder meer toelaten. Het gaat dan te ver om het niet weigeren van een nieuwe node-beheerder te beschouwen als een bewuste beslissing (een rechtshandeling) om een overeenkomst aan te gaan. Bovendien is er geen sprake van wederkerigheid van prestaties die de deelnemers jegens elkaar zouden moeten leveren (zoals art. 6:261 BW eist).

Dat het aansluiten bij een permissionless blockchain niet als het sluiten van een overeenkomst kan worden opgevat, betekent niet dat er nooit een overeenkomst bestaat tussen node-beheerders. Een simpel voorbeeld is als node-beheerders een smart contract afsluiten. Dan is er tussen hen een overeenkomst, die echter los staat van het aangesloten zijn bij een blockchain. Interessanter is de mogelijkheid dat de node-beheerders een overeenkomst sluiten over het in stand houden van een blockchain. Twee varianten zijn relevant.

---

[23] Law en Teo 2017, p. 246-247. Geiregat 2017 en 2018 (ook De Graaf 2019) betoogt het tegendeel, maar dit lijkt te berusten op een miskenning van de aard van het blockchainprotocol, dat in het algemeen nodes vrij laat om wel of niet deel te nemen aan de blockchain en mee te doen met het verifiëren en genereren van een *proof of work*. Zijn opvatting zou ertoe leiden dat deelnemers verplicht zouden zijn om te blijven meewerken aan de blockchain; in de overige literatuur is nog nooit zo’n verplichting aangenomen voor gewone blockchains die niet voortkomen uit een voorafgaande overeenkomst.

[24] Vgl. HR 15 november 1957, NJ 1958/67 (Baris/Riezenkamp) voor de precontractuele verhouding.

c. Voorafgaande overeenkomst

Het is mogelijk dat partijen vooraf een overeenkomst sluiten die (mede) inhoudt dat zij zullen gaan samenwerken in een toekomstige, nog te realiseren blockchain. Deze overeenkomst bepaalt dan de details van hun onderlinge verhouding. De blockchain is dan gewoon een onderdeel van de overeenkomst, en partijen moeten zich gedragen volgens de regels van de overeenkomst. Dan geldt het gewone overeenkomstenrecht.

De overeenkomst zou kunnen neerkomen op een joint venture of een maatschap, of een andere rechtspersoon als een vereniging, coöperatie en dergelijke. Hiervoor gelden de gewone regels van het rechtspersonenrecht.

Het protocol van de blockchain is in zo'n geval onderdeel van de gehele overeenkomst tussen de node-beheerders: het is in zekere zin een uitvoeringskwestie, zoals een blauwdruk een onderdeel is van de uitvoering van een aannemingsovereenkomst. Zo'n overeenkomst zal waarschijnlijk vaak betrekking hebben op een permissioned blockchain, als partijen zo'n blockchain opzetten om een bepaalde vorm van samenwerking te bewerkstelligen: zij willen dan waarschijnlijk zelf bepalen wie bij de blockchain mogen aansluiten. Maar het is ook mogelijk dat partijen een overeenkomst sluiten om een permissionless blockchain op te richten, bijvoorbeeld omdat zij denken winst te behalen juist doordat veel derden aansluiten bij de blockchain.[25]

d. Aansluiting bij een bestaande permissioned blockchain

Een tweede mogelijkheid is dat bij bepaalde typen blockchains het aansluiten bij de blockchain wél als een overeenkomst moet worden gekwalificeerd, ook al geldt dat niet bij alle blockchains. Dat is het geval bij permissioned blockchain.

Bij een permissioned blockchain is de toelating tot de blockchain namelijk gereguleerd. Deze toelating kan op verschillende manieren zijn geregeld. Eén mogelijkheid is dat er een voorafgaande controle plaatsvindt door een of meer specifieke node-beheerders[26] of door een controlerende instantie. Een andere mogelijkheid is dat toelating berust op aanvaarding door de gezamenlijke node-beheerders (door stemming of door gebruikmaking van een consensus-mechanisme in de blockchain).

Het lijkt aannemelijk dat de node-beheerders bij de toelating van nieuwe node-beheerders juridisch gezien rechtshandelingen verrichten en een (gezamenlijke) overeenkomst aangaan met de nieuwe node-beheerders. De bedoeling zal immers zijn dat de nieuwe node-beheerder het recht heeft om aan te sluiten bij de blockchain, terwijl de andere node-beheerders waarschijnlijk daar ook iets voor verwachten. Het aanmelden bij en toelaten tot de blockchain is dan een handeling met juridische betekenis.[27]

De aanmelding en toelating tot een permissioned blockchain lijken op de toetreding tot een maatschap. Het is mogelijk dat een permissioned blockchain daadwerkelijk als maatschap moet worden gekwalificeerd (art. 7A:1655 BW).[28] Voor een maatschap is vereist dat het gaat om een overeenkomst tot samenwerking gericht op het behalen van vermogensrechtelijke voordeel ten behoeve van alle vennoten, door middel van inbreng door alle vennoten.[29] De inbreng van de node-beheerders bestaat uit het leveren van rekenkracht, en de opbrengsten worden verdeeld volgens de

[25] Dit is in essentie wat er gebeurt bij een Initial Coin Offering (ICO).

[26] Het is mogelijk dat de nodes automatisch onder bepaalde voorwaarden accepteren; dat wordt juridisch gezien toegerekend aan de node-beheerders.

[27] Het is dan een (wederkerige) rechtshandeling (art. 6:213 juncto 6:261 BW), omdat partijen dan over en weer verplichtingen op zich nemen. Het ligt niet voor de hand dat bij de toelating alleen eenzijdig verplichtingen worden aanvaard. Hierbij is vereist dat de node-beheerders bij de aanmelding en toelating de wil hebben om rechtsgevolgen te bewerkstelligen (art. 3:33 BW).

[28] De Filippi & Wright 2018, p. 142 stellen zelfs dat in de U.S.A. en veel Europese landen 'decentralized organisations formed for the purpose of making a profit likely would be deemed a "general partnership" and consequently lack the ability to shield members' assets if the organization injures a third pary or is unable to pay its creditors." Zie over kwalificatie en gevolgen van verschillende samenwerkingsvormen Tjong Tjin Tai e.a. 2009.

[29] Asser/Maeijer & Van Olffen 7-VII 2017/28.

regels van het protocol.[30] Toch is het niet helemaal zeker of een blockchain als maatschap kan worden aangemerkt: art. 7A:1670-1672 BW geven aan dat er beperkingen zijn aan de wijze waarop de winst uit de maatschap mag worden verdeeld, en deze wettelijke bepalingen impliceren ook dat de wetgever bij een maatschap dacht aan samenwerkingsverbanden zoals een advocatenmaatschap, waarbij alle winst jaarlijks wordt verdeeld in plaats van dat automatische verdeling plaatsvindt per transactie of 'proof of work' volgens de regels van een protocol. Dit blijkt ook uit art. 7A:1676 BW dat bij gebreke van andere bedingen aan alle maten de bevoegdheid tot beheersdaden toekent. Dit valt slecht te verenigen met de normale opzet van een blockchain, in het bijzonder als de blockchain veel nodes en node-beheerders heeft.

Als de aansluiting bij een permissioned blockchain geen toetreding tot een maatschap is, gaat het om een zogenaamde 'onbenoemde' overeenkomst, dat wil zeggen een overeenkomst waar geen bijzondere regeling in het wetboek voor is. De verplichtingen en rechten van de partijen volgen dan gewoon uit de overeenkomst. Omdat in dit geval de overeenkomst niet schriftelijk is vastgelegd in een contract (anders gaat het om geval (a) hierboven), zal de inhoud van de overeenkomst grotendeels worden bepaald door het protocol,[31] dat immers door de node-beheerders is aanvaard toen zij aan de blockchain deelnamen. Het feit dat het om een blockchain gaat leidt op zichzelf niet tot juridische verplichtingen voor de node-beheerders (zie hierboven onder a.), maar het is mogelijk dat het protocol daarnaast andere regels bevat die wel tot rechten en verplichtingen leiden.

Als een permissioned blockchain inhoudt dat de node-beheerders gezamenlijk een overeenkomst hebben gesloten, is het ook mogelijk dat andere gebruikers die geen node-beheerder zijn rechten kunnen ontlenen aan de blockchain en daarom aanspraken hebben op de node-beheerders. Of dit daadwerkelijk zo is, zal afhangen van de concrete afspraken rond de permissioned blockchain en kan daarom niet in het algemeen worden beantwoord. Meestal zal dan nodig zijn dat een gebruiker zelf een overeenkomst heeft gesloten met de node-beheerders, waar dan ook een verplichting van de gebruiker tegenover moet staan.[32]

(e) Een permissionless blockchain is een feitelijke samenwerking, geen juridische samenwerkingsvorm

Zoals besproken onder (a) leidt een permissionless blockchain niet tot een overeenkomst (al kunnen de node-deelnemers natuurlijk wel een overeenkomst sluiten).
Zo'n blockchain is dan feitelijke samenwerking die geen juridische samenwerking inhoudt.[33]
Omdat de gezamenlijke node-beheerders geen overeenkomst hebben gesloten, kan het ook geen maatschap zijn (wat een soort overeenkomst is) en ook geen rechtspersoon[34] (waar ook een overeenkomst voor nodig is). Nieuwe node-beheerders die aansluiten, of buitenstaanders die als cliënt gebruikmaken van de blockchain, kunnen dan ook geen overeenkomst sluiten met de blockchain: die blockchain is immers juridisch gesproken niets, geen partij waar een overeenkomst mee kan worden gesloten.

Een permissionless blockchain leidt op zichzelf niet tot een overeenkomst tussen node-beheerders, en is een feitelijke samenwerkingsvorm.

[30] Hierbij is wel vereist dat er vermogensrechtelijk voordeel is voor de node-beheerders, wat niet noodzakelijk bij iedere blockchain het geval hoeft te zijn. Zie bijvoorbeeld openbare registers: daarbij is niet direct voordeel voor de node-beheerders zelf aan de orde. Echter als de node-beheerders geen voordeel hebben bij deelname, is de vraag wat dan hun motief is.
[31] Naast mogelijk andere vooraf gegeven informatie.
[32] Het is mogelijk dat in sommige gevallen een gebruiker er gerechtvaardigd op mag vertrouwen dat de permissioned blockchain goed functioneert zonder dat de gebruiker een overeenkomst heeft gesloten.
[33] Echter De Filippi & Wright 2018, p. 142 suggereren dat als de blockchain is gevormd met als doel het maken van winst er sprake is van een 'general partnership'. Zij lijken geen uitzondering te maken voor een permisionless blockchain.
[34] Een blockchain kan natuurlijk wel zijn opgezet door een rechtspersoon, maar is niet zelf een rechtspersoon (zoals ook een fabriek eigendom kan zijn van een rechtspersoon maar de fabriek daarmee niet zelf een rechtspersoon is).

Een permissioned blockchain impliceert dat er een overeenkomst is tussen node-beheerders en eventuele andere partijen.
Een permissionless blockchain leidt op zichzelf niet tot rechten en verplichtingen tussen node-beheerders onderling en node-beheerders en gebruikers, tenzij zij zelf verdere afspraken maken.

3.2.3 Interne governance

Zoals uit par. 3.2.2 blijkt is het mogelijk dat een blockchain onderdeel uitmaakt van een overeenkomst. In dat geval zal de overeenkomst bepalen of er een bepaalde governance-structuur geldt binnen de blockchain-samenwerking.

Als er geen overeenkomst is, is er geen juridische governance-structuur. Wel kan er een feitelijke machtsverhouding bestaan die als een impliciete governance-structuur kan worden aangemerkt.[35] Afhankelijk van de concrete opzet van de blockchain kunnen node-beheerders, core developers, en/of groepen deelnemers een dominante rol innemen waarmee zij in feite de toekomstige ontwikkeling van de blockchain kunnen bepalen.[36] Zo is er bij bitcoin een bepaalde governance-structuur aan te wijzen.[37] Zo'n feitelijke machtsverhouding is geen juridische governancevorm (omdat zij niet berust op juridische verplichtingen), maar kan wel juridische gevolgen hebben voor bijv. aansprakelijkheid en handhaving (par. 3.2.9 en 3.2.10).

Een voorbeeld van de werking van zo'n impliciete governance-structuur is de afwikkeling van de hack van The DAO in 2016.[38] The DAO was een subsysteem op de Ethereum blockchain, bedoeld voor investeringsvoorstellen. Iedere Ethereum-gebruiker kon aansluiten bij een voorstel door een klein bedrag aan zo'n voorstel (dat de vorm van een smart contract had) over te maken.[39] De code van het desbetreffende smart contract leidde er echter tersluiks toe dat als een gebruiker zo'n betaling had verricht, zijn hele account werd leeg getrokken. Waarschijnlijk betrof dit geen vergissing maar was dit opzettelijk aangebracht om investeerders op te lichten: de ontwikkelaars van dit smart contract hebben zich nooit bekend gemaakt en hebben ook nooit aangegeven dat dit leegtrekken onbedoeld was. Uiteindelijk werd op initiatief van de Ethereum-developers een zogenaamde *hard fork* voorgesteld.[40] en heeft de meerderheid van de Ethereum-nodebeheerders ingestemd met deze *hard fork*. Het gevolg hiervan is dat het leegtrekken van de accounts is teruggedraaid en de oorspronkelijke eigenaren weer hun cryptocurrency (Ether) terug hadden. Dit laat zien dat het niet onmogelijk is om transacties op een blockchain ongedaan te maken.[41]

Een bijzondere vorm van impliciete governance is als de (meerderheid van de) nodes worden gecontroleerd door één partij of een samenwerkende groep, zonder dat dit bekend is. Die partij of groep kan dan in feite beslissen wat er op de blockchain gebeurt.[42] Een blockchain kan ook zo zijn ontworpen dat maar een beperkt aantal nodes beslist, wat weer kan leiden tot kwetsbaarheid van de blockchain. Een voorbeeld is de NEO blockchain die werkte met zeven consensus node-beheerders, en niet meer werkte toen één van die nodes offline ging tijdens het vormen van de consensus.[43]

[35] Werbach 2018a, p. 133-148.
[36] Zie in detail Finck 2019, p. 182-110.
[37] De Filippi & Loveluck 2016.
[38] Hierover o.a. Werbach 2018a, p. 67-69, Finck 2019, p. 187-189.
[39] Zo'n voorstel is een smart contract, een programma dat zelf een tegoed heeft in de cryptocurrency.
[40] Dit komt kort gezegd neer op een verandering van de code van de blockchain op zo'n manier dat transacties werden teruggedraaid. Dit werkt echter alleen voor de nodes die deze verandering accepteren: zij splitsen dan af van de onveranderde blockchain. Die afsplitsing kan niet worden afgedwongen; de nodes die niet meegaan blijven werken op de 'oude' blockchain. Er is dan dus een splitsing of scheuring, een 'fork' in blockchain-termen.
[41] Een deel van de community was het er overigens niet mee eens en is doorgegaan met de blockchain van vóór de fork (deze versie heet Ethereum classic).
[42] Men spreekt wel van een '51 %-attack'. Zie ook Werbach 2018a, p. 119-123 over verschillende vormen van invloed.
[43] https://www.coindesk.com/when-blockchains-go-down-why-crypto-outages-are-on-the-rise

Een permissionless blockchain heeft geen juridische governance-structuur, maar kan wel een feitelijke vorm van governance hebben.
Een permissioned blockchain heeft een juridische governance-structuur vanwege het permissioned karakter van de blockchain.

3.2.4 Juridische betekenis van handelingen op de blockchain

a. Algemeen

Gebeurtenissen op de blockchain worden in het algemeen behandeld volgens de gewone regels van het privaatrecht.[44] Zij kunnen dus juridisch gevolgen hebben, net zoals in de offline wereld. Als een blockchain gebruiker met daden duidelijk maakt dat hij een aanbod accepteert, komt daarmee een overeenkomst tot stand, ongeacht of het om daden op de blockchain gaat of om fysieke zichtbare daden (zoals handopsteken bij een veiling). Preciezer: gebeurtenissen op een blockchain kunnen juridische betekenis krijgen doordat zij kunnen worden opgevat als verklaringen (art. 3:35 BW),[45] of doordat het gebeurtenissen zijn die anderen (onrechtmatig) benadelen (art. 6:162 BW). Hiervoor gelden de gewone regels.

Het is niet verboden om op een blockchain handelingen te verrichten. Alles wat op de blockchain gebeurt is daarom in principe 'geldig', dat wil zeggen dat iets alleen verboden is als het in strijd is met een specifieke regel. Een illegale transactie met of op een blockchain kan wel nietig zijn, maar dat is vanwege het illegale karakter, niet omdat het een blockchain betreft.

In bepaalde gevallen zijn er wel extra eisen. In het privaatrecht betreft dit met name zogenaamde vormvoorschriften en informatieverplichtingen.

Handelingen op een blockchain zijn in principe (rechts)geldig.

b. Vormvoorschriften

In sommige gevallen stelt het recht dat er formaliteiten (vormvoorschriften) moeten worden nageleefd.[46] Dit geldt ook als er een blockchain bij betrokken is. Het voert te ver hier alle mogelijke formaliteiten te behandelen.[47]

Een bijzondere soort vormvoorschrift is de eis van schriftelijkheid: deze moet wel apart worden behandeld. Voor bepaalde overeenkomsten en andere soorten handelingen eist de wet dat deze *schriftelijk* wordt gesloten of verricht. Als dat niet gebeurt, is de overeenkomst of rechtshandeling ongeldig.[48] Tegenwoordig bepalen art. 156a Rv en art. 6:227a BW dat ook op elektronische wijze aan het schriftelijkheidsvereiste kan worden voldaan, als er aan verschillende vereisten is voldaan.[49] Aan de eisen van deze wetsartikelen kan ook op een blockchain worden voldaan: het is daarom bijvoorbeeld mogelijk een verjaring te stuiten door middel van het doen van een mededeling aan de wederpartij via de blockchain (als die mededeling ten minste is ondertekend en ook daadwerkelijk aankomt bij de wederpartij).[50] Een uitzondering is er voor gevallen waarin "de wet de tussenkomst voorschrijft van de rechter, een overheidsorgaan of een beroepsbeoefenaar die

[44] Evenzo VBW 2017, p. 22-23.
[45] Om precies te zijn: dit is zo als de wederpartij die gedraging "overeenkomstig de zin die hij daaraan onder de gegeven omstandigheden redelijkerwijze mocht toekennen, heeft opgevat als een door die ander tot hem gerichte verklaring van een bepaalde strekking" (art. 3:35 BW). Of een gebeurtenis daadwerkelijk wordt opgevat van een verklaring zal dus van allerlei omstandigheden kunnen afhangen.
[46] Evenzo voor Duits recht: VBW 2017, p. 23-24.
[47] Een voorbeeld is de overhandiging van een koopakte van onroerende zaak aan de consument-koper (art. 7:2 lid 2 BW).
[48] De juridische term is 'nietig'. Zie Huydecoper en Van Esch 1997, met betrekking tot de elektronische handtekening.
[49] Er zijn nog enkele andere wettelijke regels die schriftelijkheid lijken te eisen, maar uit onderzoek blijkt dat uiteindelijk elektronische rechtshandelingen bijna altijd toegestaan zijn (De Graaf 2018a).
[50] Een mogelijk probleem is alleen dat art. 6:227a lid 1 sub d BW eist dat de identiteit van partijen bekend is: als de partijen op een blockchain alleen anoniem bekend zijn, kan dit een obstakel zijn.

een publieke taak uitoefent".[51] In dergelijke gevallen is een elektronische overeenkomst niet toegestaan en kan deze dus ook niet op de blockchain worden gesloten.

Vormvoorschriften vormen bijna nooit een obstakel voor overeenkomsten op een blockchain.

3.2.5 Bewijskracht

De blockchain heeft geen bijzondere bewijskracht. Nederland kent een vrij stelsel van bewijslevering (art. 152 Rv). Bewijs kan worden geleverd met alle middelen,[52] en de rechter is vrij in de waardering van het bewijsmateriaal, waarbij wel geldt dat hij zijn oordeel toereikend moet motiveren.[53]

Transacties die bij de blockchain zijn ingediend zijn ondertekend met een *private key*.[54] Dit is een elektronische handtekening in de zin van art. 3:15a BW en eIDAS-Verordening 910/2014. Meestal wordt bij blockchains gebruik gemaakt van een private-public key paar op basis van het RSA-algoritme. Dit is een zogenaamde geavanceerde elektronische handtekening (art. 26 eIDAS-Verordening).[55] Zo'n transactie kan dan tellen als een elektronische akte die dezelfde bewijskracht heeft als een gewone schriftelijke akte (art. 156a Rv).

Een rechter zal als vermoeden moeten aannemen dat de ondertekening met de private key bewijst dat de transactie is gegenereerd door de 'eigenaar' van de sleutel.[56] Het gevolg is dat de elektronische akte dan zogenaamde dwingende bewijskracht heeft tussen partijen voor wat in de akte staat.[57] Maar het is mogelijk om tegenbewijs te leveren tegen deze 'dwingende' bewijskracht (art. 151 lid 2 Rv). Een voorbeeld is dat de eigenaar bewijst dat de sleutel was gekopieerd door een hacker die vervolgens met deze sleutel een valse verklaring ondertekende.

Overigens geldt dat negatieve gevolgen van onbevoegd gebruik (zoals ongewenste overboekingen) meestal voor rekening van de 'eigenaar' blijven, omdat de eigenaar zijn sleutel voldoende moet beveiligen.[58] Maar dat staat los van de vraag of het gebruik van de sleutel bewijst dat een verklaring is gedaan door de eigenaar.

Daarnaast moet niet alles wat op de blockchain is geregistreerd als 'waar' worden aangenomen: een blockchain is niet beter dan de kwaliteit van wat erin wordt gestopt.[59] De toegevoegde waarde is vooral dat in beginsel wel vaststaat dat de transactie *op een bepaald moment* is ingediend met gebruikmaking van de sleutel (timestamping). Een blockchain zou daarmee een vergelijkbare functie kunnen vervullen als vroeger de registratie van akten bij de Belastingdienst op grond van de Registratiewet.[60] Een beperking is dat transacties en registraties op een blockchain niet absoluut onveranderlijk zijn.[61] Ook hier moet tegenbewijs mogelijk blijven.

Registraties op een blockchain kunnen worden aangevoerd als bewijs voor feiten, en leveren net zoals andere vormen van bewijs niet meer op dan een vermoeden van juistheid, waar tegenbewijs tegen kan worden geleverd.

---

[51] Art. 6:227a lid 2 BW. Voorbeelden zijn de eis van notariële akte (bijv. art. 2:64 BW), de eis van goedkeuring door de overheid van een rechtshandeling tot verkrijging van een goed waarover een gerechtelijke procedure aanhangig is als de verkrijger o.a. een rechter of advocaat is (art. 3:43 BW).
[52] Asser Procesrecht/Asser 3, Bewijs, 2017, nr. 52.
[53] Asser Procesrecht/Asser, Bewijs, nr. 257.
[54] Dit geldt althans voor implementaties gelijkend op bitcoin; bij specifieke permissioned blockchain zou dit mogelijk niet zo zijn! Zoals blijkt is dit wel relevant voor de bewijskracht hiervan.
[55] Zo'n handtekening mag niet als regel worden achtergesteld bij een gewone handtekening, maar er geldt niet dat zo'n handtekening zonder meer gelijkgesteld is aan een gewone handtekening (art. 25 lid 1 eIDAS-Verordening).
[56] Of door iemand die door de eigenaar in staat is gesteld om van die sleutel gebruik te maken, en daarmee is gemachtigd om in zijn naam te handelen.
[57] Art. 156 lid 1 en 3 Rv, art. 156a Rv, art. 157 lid 2 Rv.
[58] HR 19 november 1993, NJ 1994/622 (COVA).
[59] Vgl. Werbach 2018a, p. 104.
[60] Berlee 2018a.
[61] De Filippi & Wright 2018, p. 113: 'Blockchains are not immutable'. Zij wijzen op kwaadaardige aanvallen. Evenzo Werbach 2018a, p. 103.

Blockchaintechnologie kan toegevoegde waarde hebben door de mogelijkheid van registratie van het tijdstip van transacties.

3.2.6 Goederenrecht en de blockchain

Blockchaintechnologie roept verschillende vragen op die betrekking hebben op het goederenrecht: of er kan worden gesproken over eigendom, of cryptocurrencies geld zijn[62] e.d. De oorspronkelijke blockchain, die onderdeel is van het bitcoinsysteem, berust op een virtuele munt, wat ook wel 'cryptocurrency' wordt genoemd. Deze 'munt' heeft in de maatschappij daadwerkelijk economische waarde. Het is echter ook mogelijk om zo'n 'munt' te hebben alleen om een blockchain te laten werken, zonder dat het de bedoeling is dat die 'munt' economische waarde heeft. Om die reden wordt inmiddels ook wel gesproken over 'tokens' (par. 2.5). Een token die niet is bedoeld om economische waarde te hebben maar alleen om de blockchain te laten functioneren noemt men ook wel een *utility token*.

(a) Zijn tokens geld?

Bitcoin of andere cryptocurrencies zijn juridisch gezien geen geld.[63] Natuurlijk is bitcoin wel een ruilmiddel dat door veel mensen wordt geaccepteerd, maar dat betekent niet dat het geld is: hetzelfde kan immers worden gezegd van iets als goud. Geld in de zin van het privaatrecht moet 'gangbaar' zijn in het land waarin de betaling plaatsvindt (art. 6:112 BW). De reden dat bitcoin geen geld is vooral dat het niet gangbaar is, dat wil zeggen, zeer breed geaccepteerd is als betaalmiddel.[64] Tot nog toe is bitcoin nagenoeg niet te gebruiken bij reguliere fysieke winkels of online winkels, op enkele zeldzame uitzonderingen na. Voor andere cryptocurrency geldt dit nog sterker.

Een ruimere definitie van geld is er in art. 1.1 Wet op het financieel toezicht, dat bepaalt wat kan tellen als 'electronisch geld':[65] "geldswaarde die elektronisch of magnetisch is opgeslagen, die een vordering op de uitgever vertegenwoordigt, die is uitgegeven in ruil voor ontvangen geld om betalingstransacties te verrichten als bedoeld in artikel 4, punt 5, van de richtlijn betaaldiensten,[66] en waarmee betalingen kunnen worden verricht aan een andere persoon dan de uitgever." Cryptocurrencies op een blockchain voldoen hier niet aan: zij zijn niet verkregen van een uitgever in ruil voor geld, en vertegenwoordigen geen vordering op een uitgever (er is zelfs geen daadwerkelijke uitgevende instantie).[67]

Het is wel mogelijk om af te spreken dat een 'betaling' wordt gedaan met bitcoin of een andere cryptocurrency. Juridisch gezien gaat het dan om een ruil, of een aanvullende afspraak om een betaling in geld te laten voldoen door een andere prestatie. Zo kan er ook 'betaald' worden door

[62] Strikt genomen betreft de kwalificatie als 'geld' niet het goederenrecht, maar voor niet-juristen is dit waarschijnlijk de meest logische plaats om deze vraag te behandelen.
[63] Dat wil zeggen, geen geld in de zin van art. 6:112 BW of art. 1.1 Wft. Zie Rank 2015, Mijnssen 2017, p. 4-6, Baukema 2013, verder Tweehuysen 2018, met verdere verwijzingen in nt. 9. Vgl. over de classificatie Bayern 2014, Allen 2017, Vandezande 2018 (met negatieve conclusie op p. 163), en ten aanzien van de Uniform Commercial Code: Schroeder 2016.
[64] Rank 2015, p. 181 geeft verder als eisen aan dat het zou moeten gaan om geld dat tevens een fysieke verschijningsvorm heeft en gerelateerd moet zijn "aan een door een nationale of internationale overheid gecreëerde en bestendigde rekeneenheid". Het is niet geheel zeker of dit ook daadwerkelijk noodzakelijke eisen zijn.
[65] Zie de (tweede) Richtlijn elektronisch geld (2009/110/EG), hierover Mijnssen 2017, par. 1.5, en uitvoerig over de Europese regels Vandezande 2018, hfdst. IV, ook Goossens en Verslype 2019, p. 65.
[66] Richtlijn 2007/64/EG.
[67] Rank 2015, p. 181, Mijnssen 2017, p. 4-6. Anders: Weij en Landerbarthold 2018 (en De Graaf 2019), die stellen dat er een vordering is op de cryptogemeenschap. Zoals in par. 3.2.2 betoogd is zo'n 'gemeenschap' geen rechtspersoon of maatschap en kan er juridisch dan ook geen vordering daarop bestaan; bovendien is er geen verplichting van de nodes om verder te gaan met het ondersteunen van de blockchain.

levering van een bijzondere postzegel, iTunes-tegoed, edelstenen.[68] Het is daarom niet nodig om cryptocurrencies als geld aan te merken.

Uit strafrechtelijk en fiscaal oogpunt is het evenmin noodzakelijk om cryptocurrencies als 'geld' aan te merken. Het interfereren met cryptocurrencies ('stelen') kan al worden bestraft op grond van het geldende strafrecht. Het zal immers meestal gebeuren door het zonder bevoegdheid toe-eigenen van en gebruiken van de private key, wat neerkomt op computervredebreuk (art. 138ab Sr), of aftappen van data (art. 139c Sr) en bezitten van afgetapte data (art. 139e Sr).

Een tegoed in bitcoin kan door de Belastingdienst als vermogen worden belast, net zoals andere soorten claims.[69] De kwalificatie 'geld' of niet kan wel relevant zijn voor de vraag of transacties met bitcoin BTW-plichtig kunnen zijn.[70]

Er kunnen wel andere redenen zijn om de regels te wijzigen en cryptocurrencies als geld te kwalificeren.[71] Het valt buiten het bestek van dit onderzoek.

Cryptocurrencies (en andere tokens) zijn geen geld, en er is geen dringende reden om cryptocurrencies als geld aan te merken.

(b) Blockchain en goederenrecht[72]

Als tokens geen geld zijn, blijft mogelijk dat tokens (en registraties op een blockchain) moeten worden beschouwd als goederen, dat wil zeggen dat iemand eigenaar kan zijn van tokens of een inschrijving op een blockchain.[73]

Een blockchain is in essentie niet meer dan een grote gedistribueerde database waar informatie op staat. Deze informatie kan een tegoed representeren in de bijbehorende cryptocurrency, maar kan ook andere informatie bevatten (zoals registratie van feiten of akten) of zelfs een overeenkomst inhouden (smart contract). Goederenrechtelijk heeft dit alles echter geen zelfstandige status. Een tegoed in een cryptocurrency is op dit moment niet in te passen in het stelsel van zaken en vermogensrechten. Weliswaar lijkt het nog het meest op een vermogensrecht (art. 3:6 BW), maar het is geen *recht.*[74] Vermogensrechten worden meestal onderverdeeld in absolute vermogensrechten (die jegens eenieder gelden) en relatieve vermogensrechten (die jegens een concrete schuldenaar gelden).[75] Tokens of tegoed op een blockchain vallen onder geen van deze twee categorieën. Het is niet een door de wet erkend absoluut, jegens eenieder geldend recht (zoals een intellectueel-eigendomsrecht): daarvoor is een concrete wettelijke regeling nodig, en er is geen regeling waar tokens onder vallen.[76] Het is ook niet een persoonlijk, jegens een concrete ander (de schuldenaar) geldend te maken recht (vorderingsrecht).[77] Er is immers geen concrete wederpartij die iets verplicht is te doen.[78] De aanspraak die de 'eigenaar' van bitcoin heeft houdt alleen in dat hij zijn tegoed kan gebruiken om een transactie (overboeking naar een andere account) in het netwerk in te brengen, in de hoop dat deze overboeking door de blockchain wordt aanvaard.[79] Alleen als de blockchain onderdeel is van een overeenkomst, is dit anders: dan gelden de gewone regels van het overeenkomstenrecht (par. 3.2.2).

---

[68] Overigens blijkt hieruit ook dat bitcoin en andere cryptocurrencies in de praktijk ongeschikt kunnen zijn voor transacties vanwege grote koersfluctuaties. Schade door niet-levering van bitcoins kan dan oplopen, zie voor een praktijkgeval Hof Arnhem-Leeuwarden 31 mei 2016, ECLI:NL:GHARL:2016:4219.

[69] De Reus & van Nijnatten 2018, Putman 2017, Knuist 2014. Vgl. Bal 2015.

[70] Veldhuijzen, Van de Berg, Van Goor 2015, Wolf 2015, Goossens en Verslype 2019, p. 68-69, mede verwijzend naar HvJ 22 oktober 2015, C-264/14.

[71] Zie Allen 2017 voor enkele tegenargumenten.

[72] Uitvoerig: Tweehuysen 2018.

[73] De Graaf 2019 vat de discussie in de literatuur samen en geeft een eigen opinie.

[74] Rank 2015, par. 5.2.

[75] Asser/Bartels & Van Mierlo 3-IV 2013/1.

[76] Naar common law verdedigen Law & Teo 2017, p. 253 de erkenning van zo'n recht.

[77] Bayern 2014, p. 31-33. Dit betreft de zogenaamde actieve zijde van een verbintenis.

[78] Tweehuysen 2018, p. 606. Zie ook hierboven, par. 3.2.2. Geiregat (2017 en 2018) en De Graaf (2019) stellen dat er wel een concrete wederpartij is op wie verplichtingen rusten.

[79] Snijders & Tonino 2018.

Toch is het mogelijk dat bitcoin (en andere tokens) wel een vermogensrecht uitmaken. Het systeem van het goederenrecht voldoende open is om vermogensrechten te erkennen die niet exact in de categorieën van art. 3:6 BW passen;[80] dan zou het recht op bitcoin een absoluut vermogensrecht kunnen zijn.[81] Een argument hiervoor is dat een aanspraak op bitcoin duidelijk economische waarde heeft. De opzet van bitcoin lijkt het op een ruilsysteem, en een aanspraak in zo'n systeem zou kunnen vallen onder een ruime interpretatie van het begrip 'vermogensrecht'.[82]

Het is niet zeker of zo'n argumentatie zal worden bevestigd door de Hoge Raad als daar een zaak over komt in cassatie. Tot dat het geval is, blijft de goederenrechtelijke status van bitcoin (en andere tokens) onzeker.

Voor de zekerheid kan dan beter worden uitgegaan van het wettelijk systeem, waarin bitcoin geen vermogensrecht of ander goed is. In de praktijk is het meestal ook niet nodig dat bitcoin als vermogensrecht wordt erkend.[83] Het is bijvoorbeeld nu al mogelijk om contracten te sluiten over bitcoin, beslag te leggen op bitcoin, en bitcoin executoriaal te verkopen (par. 3.2.10). Toch valt het te overwegen om de goederenrechtelijke status van bitcoin (en andere tokens) uitdrukkelijk in de wet te regelen. Het zou voor de praktische uitvoerbaarheid wenselijk zijn als dit in internationaal verband gecoördineerd wordt, in het bijzonder in de Europese Unie, nu dit ook gevolgen kan hebben op financiële toezichtwetgeving en fiscale regels. Vanwege de handelswaarde die bitcoin en vergelijkbare tokens hebben, zou het dan zinvol zijn om zulke tokens als goed te erkennen.[84]

Voor andere toestanden of registraties[85] op de blockchain geldt hetzelfde: zulke registraties zijn geen goed.[86] Een registratie in een register (zoals het kadaster) is zelf geen goed; het is hooguit bewijs van eigendom, of noodzakelijk voor de verkrijging van eigendom.[87] Dat dergelijke registraties waarde kunnen hebben voor de betrokkene maakt niet dat deze registraties zelf vermogensrechten worden.[88]

In de literatuur is tot op heden geen dringende reden aangegeven om de huidige stand van zaken te wijzigen en registraties op een blockchain als goed te kwalificeren.

Tokens en andere registraties op een blockchain zijn volgens de huidige stand van het recht geen goederen. Het is niet nodig, maar wel zinvol om de wet aan te passen en de goederenrechtelijke status van tokens nader te regelen.

(c) Tokens en financieel toezicht

Ook als tokens geen geld of goederen zijn, is het mogelijk dat er financiële toezichtsregels op van toepassing zijn. Hoewel dit onderwerp strikt genomen buiten het privaatrecht valt, wordt hier kort aandacht aan besteed.[89]

Financieel toezicht beoogt de stabiliteit en efficiënte werking van financiële markten te waarborgen. Het toezicht beoogt onder meer fraude te voorkomen en strekt ook tot bescherming van consumenten tegen machtsmisbruik en onwetendheid. Er wordt toezicht gehouden op de verhandeling van geld en waardepapieren (die geld of andere objecten met waarde, zoals aandelen

[80] Zie hierover de regeringscommissaris W. Snijders die een belangrijke rol speelde bij de totstandkoming van het BW, waarin het goederenrecht is geregeld (Snijders 2005).
[81] Rank 2015, p. 183 r.k., 184 l.k.
[82] Snijders & Tonino 2018, verwijzend naar HR 5 november 1993, NJ 1994/640. Die uitspraak geeft echter niet evident een onderbouwing voor hun standpunt. Zie over de juridische status van ruilsystemen ook Zwitser 1995.
[83] Goodwill is bijvoorbeeld ook geen goed, maar toch is het mogelijk om daar overeenkomsten over te sluiten.
[84] Voor utility tokens zou dit niet nodig zijn.
[85] Bijvoorbeeld een 'elektronische akte' die op de blockchain wordt gezet.
[86] Bij de huidige stand van zaken is data ook geen goed.
[87] Vgl. art. 3:89 lid 1 BW voor levering van onroerende zaken, waar onder meer inschrijving van de leveringsakte in de openbare registers is vereist.
[88] Vauplane 2018 wijst overigens op nieuwe Franse wetgeving (Ordonnance no. 2017-1674 van 8 December 2017) waarbij betekenis toekomt aan beheer van registraties voor effecten: dit beheer kan als bewijs dienen en daardoor indirect goederenrechtelijk effect hebben.
[89] Zie ook Hofert 2018 over Duitse en Amerikaanse regelgeving.

in een vennootschap, vertegenwoordigen). Verder valt onder het financieel toezicht ook de markt voor beleggingsdiensten en andere financiële diensten.

Aangezien tokens, in het bijzonder bitcoin, in de praktijk handelswaarde hebben, kan de uitgifte van en omgang met zulke tokens ertoe leiden dat regels van financieel toezicht van toepassing zijn.[90] Ten dele is dit onproblematisch. De uitgifte van tokens bij een zogenaamde Initial Coin Offering kan inhoudelijk neerkomen op uitgifte van waardepapieren, zodat het gerechtvaardigd is dat hier de regels met betrekking tot uitgifte van waardepapieren en effecten van toepassing zijn.[91] Vanwege de gevolgen op het financiële systeem is deze toepasselijkheid gerechtvaardigd. Voor andere soorten tokens of activiteiten is dit minder duidelijk, wat kan leiden tot terughoudendheid in de fintech- en blockchainbranche, en tot gevolg kan hebben dat maatschappelijk wenselijke initiatieven worden ontmoedigd.

Op dit moment is zowel van de zijde van toezichthouders als van de zijde van de fintech-industrie en andere geïnteresseerden in blockchaintechnologie sprake van onduidelijkheid. Dit gebied heeft bijzondere aandacht van de AFM en DNB. De noodzaak van verbeterde regelgeving is onderstreept in een eind 2018 verschenen rapport.[92] Het rapport geeft vrij precies aan dat op hoofdlijnen inmiddels enige verduidelijking is aangebracht, en wijst concreet openstaande problemen aan. In het bijzonder is duidelijk dat cryptocurrencies met financieringsdoel vallen onder effectenwetgeving. Cryptocurrencies met (wat het rapport noemt) alleen een gebruiks- of transactiefunctie,[93] waaronder ook bitcoin valt, vallen niet onder effectenwetgeving,[94] maar ook op dat gebied is er behoefte aan consumentenbescherming. De noodzaak aan regelgeving is met name groot doordat er internationaal geen uniforme aanpak is.

De conclusie, dat verduidelijking van regelgeving nodig is, kan worden onderschreven. Ook als de hoofdlijnen wel zijn verduidelijkt, zoals dat een utility token niet onder de Wft valt, blijft een probleem dat het niet altijd duidelijk is of de AFM een bepaald token als utility token zal opvatten.[95] Dit ontmoedigt nieuwe initiatieven.

In bredere zin geldt dat onduidelijk is in hoeverre de handelswaarde van tokens doorwerkt in publiekrechtelijke regels. Zo telt bitcoin wel als vermogen in de zin van vermogensbelasting, maar is nog niet duidelijk in hoeverre cryptocurrencies ook kunnen worden beschouwd als vermogen ten behoeve van de bepaling van liquiditeit en solvabiliteit.[96]

Verder is er toezicht op financiële transacties om criminele activiteiten tegen te gaan. Het betreft dan vooral het voorkomen van witwassen en financiering van o.a. terroristische activiteiten. Hiervoor gelden regels die onder meer grenzen stellen aan en een meldplicht opleggen voor het aannemen van grote bedragen contant geld.[97] De verhandeling van cryptocurrencies kan ook worden gebruikt voor witwaspraktijken, zodat het wenselijk is dat regels tegen witwassen zich ook tot cryptocurrencies uitstrekken. Aanpassing hiervan vindt op moment van schrijven plaats.[98]

---

[90] Het gaat dan met name om de zogenaamde MiFiD II (Markets in Financial Instruments Directive) 2014/65/EU van 15 mei 2014, de Wet financieel toezicht (Wft), en verdere uitvoeringsregels.
[91] Zie Nannings 2018, Goossens en Verslype 2019, p. 80-81.
[92] DNB en AFM, *Crypto's. Aanbevelingen voor een regelgevend kader*. Kamerstukken II 2018-2019, 32 013, nr. 201, bijlage.
[93] 'Gebruikscrypto's' zijn wat hier utility tokens worden genoemd. Transactiecrypto's zijn cryptocurrencies die "als middel voor algemene transacties of waardeverplaatsing" dienen, waaronder bitcoin. Zie het rapport *Crypto's*, p. 9.
[94] Dit werd eerder ook al verdedigd door Nannings 2018, p. 81-83. In diverse Amerikaanse staten zijn daarom wetten ingevoerd die een uitzondering geven op basis van een duidelijke definitie van utility tokens, zie Wyoming (House Bill 70, aanvaard: Wyoming Enrolled Act No. 27, https://www.wyoleg.gov/Legislation/2018/HB0070) en Montana (House Bill 0584, https://leg.mt.gov/bills/2019/HB0599/HB0584_1.pdf).
[95] De AFM geeft geen algemene regels: "De AFM beoordeelt per geval of de Wft van toepassing is en zal hier scherp toezicht op houden. Aanbieders moeten vooraf analyseren in hoeverre raakvlakken met het financieel toezicht bestaan voordat zij hun ICO lanceren". (https://www.afm.nl/nl-nl/consumenten/themas/waarschuwing/fintech/ico, geraadpleegd 7 juni 2019).
[96] Dit punt is opgeworpen in de gehouden interviews. Zie bijv. de Solvabiliteitsrichtlijn II 2009/138.
[97] Zie de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).
[98] Dit is gebeurd met de vijfde anti-witwasrichtlijn 2018/843 (Anti-Money Laundering directive, AMLD 5) die per 9 juli 2018 de vorige vierde, richtlijn 2015/849 heeft gewijzigd. De richtlijn moet uiterlijk 10 januari 2020 zijn

De uitgifte van tokens kan vallen onder regels van financieel toezicht. Het verdient aanbeveling om de regelgeving en de uitoefening van toezicht (verder) te verduidelijken.

3.2.7 Contractenrecht

a. Algemeen

Rond en met behulp van een blockchain kunnen diverse overeenkomsten (contracten) worden gesloten. In het algemeen gelden hiervoor de gewone regels (par. 3.2.4). In par. 3.2.2 is besproken of de deelname aan een blockchain op zichzelf leidt tot een overeenkomst. Hier gaat het over gevallen waarbij de blockchain gebruikt wordt als instrument voor het sluiten en/of uitvoeren van een overeenkomst. Het gaat hierbij om twee verschillende groepen gevallen.

Ten eerste kan het gaan om overeenkomsten die tot stand komen door communicatie via een blockchain (waarbij de voorwaarden van de overeenkomst op de blockchain kunnen worden vastgelegd in een elektronische akte). De blockchain wordt dan gebruikt als een techniek voor het sluiten van contracten, net zoals dit kan met e-mail en websites. Het is ook mogelijk dat een deel van de overeenkomst wordt uitgevoerd met behulp van de blockchain. Bij een dergelijke opzet zijn er verschillende regels om op te letten. Deze worden in deze paragraaf behandeld.

Ten tweede is het mogelijk dat geprobeerd wordt om een overeenkomst niet alleen met behulp van de blockchain te sluiten en vast te leggen, maar ook de uitvoering van de overeenkomst zoveel mogelijk via de blockchain te laten verlopen. Dit is in wezen wat de bedoeling is van smart contracts. Omdat daarbij extra problemen ontstaan die er niet zijn bij de eerste soort overeenkomsten, worden smart contracts in een afzonderlijke paragraaf (3.2.8) behandeld.

b. De algemene regels voor overeenkomsten op een blockchain

Voor overeenkomsten die met behulp van een blockchain worden gesloten en/of uitgevoerd gelden in het algemeen de gewone regels van het contractenrecht. Hieronder vallen de regels met betrekking tot eventuele formaliteiten (zie par. 3.2.4.b).

Voor het sluiten van overeenkomsten, de uitleg van overeenkomsten, en de inhoud van overeenkomsten gelden ook op een blockchain geen bijzondere regels, behalve de regels die hierna worden behandeld. In het algemeen is het mogelijk om een blockchain zo op te zetten dat daarbij algemene voorwaarden van toepassing zijn: het is dan nodig dat deelnemers en/of gebruikers van de blockchain alleen toegang verkrijgen als zij deze voorwaarden hebben geaccepteerd. Daarnaast gelden de gewone regels voor geldige aanvaarding van algemene voorwaarden.[99] Aanvaarding door te ‘klikken’ op een knop op een website is mogelijk.[100]

c. Dienst van de informatiemaatschappij

Een bijzondere groep regels volgt uit het begrip ‘dienst van de informatiemaatschappij’, art. 3:15d BW. Hieronder vallen alleen diensten die worden verricht op individueel verzoek: televisie valt hier bijvoorbeeld niet onder, video-on-demand wel.[101] Het lijkt er niet op dat het werk dat nodes doen (het instandhouden van een blockchain door te minen) hier onder valt: dat werk vindt immers niet plaats op individueel verzoek. Weliswaar zal een gebruiker een transactie aanbieden in de hoop dat deze wordt verwerkt, maar de regels van een blockchain eisen niet dat die transactie daadwerkelijk wordt uitgevoerd. Het lijkt meer op de wijze waarop Internet werkt: het IP-protocol vereist dat servers de data die zij ontvangen verder doorgeven, maar daaruit volgt niet dat een individuele gebruiker (in wiens belang het is dat die data wordt doorgegeven) een overeenkomst met elke server heeft of dat

geïmplementeerd. De consultatie voor de Implementatiewet wijziging vierde anti-witwasrichtlijn (die cryptocurrencies betrekking heeft) is afgesloten op 15 januari 2019 (https://www.internetconsultatie.nl/wijzigingamld4). Overigens is ook andere implementatiewetgeving in verband met de AMLD 5 aanhangig, zoals het wetsvoorstel voor het zogenaamde UBO-register (Kamerstukken 35 179).

[99] Zoals de mogelijkheid deze daadwerkelijk te raadplegen en duurzaam op te slaan (art. 6:234 lid 2 BW). Zie verder art. 6:227a-227c, 232-234 BW.

[100] HvJ 21 mei 2015, C-322/14 (El Majdoub/CarsOnTheWeb).

[101] Drijber 2001, blz. 124, A.R. Lodder in: Lodder & Kaspersen 2002, blz. 72.

elke server jegens elke gebruiker een dienst van de informatiemaatschappij verleent in de zin van art. 3:15d BW.[102]

Als er echter een overeenkomst met behulp van een blockchain tot stand komt en/of wordt uitgevoerd, zal meestal wel sprake van zo'n dienst van de informatiemaatschappij.[103] Op de dienstverlener rusten dan diverse informatieverplichtingen.[104] Het gaat met name om art. 3:15d en 15e BW. Dit kan voor dienstverleners bij een blockchain lastig zijn. Ten eerste zal dan bij het gebruik van de blockchain moeten worden geregeld dat er een manier is om een potentiële afnemer van de dienst de benodigde informatie te verschaffen. Dit is technisch te realiseren, maar er zal wel een voorziening voor moeten worden getroffen (het is niet noodzakelijk onderdeel van een blockchain). Ten tweede eist art. 3:15d lid 1 BW dat er informatie wordt gegeven over onder andere identiteit, adres van vestiging, communicatiemiddelen, registratiegegevens.[105] Bij blockchains wordt vaak gewerkt met anonieme of pseudonieme partijen die hun echte naam en adres niet bekend maken (par. 3.2.11). Als een partij zijn identiteit niet wil prijsgeven, schendt hij deze verplichtingen. Men kan verdedigen dat dit niet erg is, omdat het in de blockchainwereld niet nodig is dat je weet wie je wederpartij is. Onder de huidige regelgeving is de praktijk van pseudonieme aanbieders op een blockchain echter niet toegestaan.

De Autoriteit Consument en Markt is belast met de handhaving van deze bepalingen voorzover het om bedrijven gaat,[106] en kan dwangsommen en boetes opleggen (art. 2.9 Wet handhaving consumentenbescherming). Als het gaat om financiële diensten of activiteiten is ook de Autoriteit Financiële Markten bevoegd tot handhaving (art. 3.1 Wet handhaving consumentenbescherming). Het is niet duidelijk of het niet-naleven van deze informatieverplichtingen ook leidt tot nietigheid van de overeenkomst of aansprakelijkheid jegens de wederpartij.[107]

d. Regels voor elektronische overeenkomsten e.d.

Naast de regels die gelden voor 'diensten van de informatiemaatschappij' zijn er ook regels die specifiek gelden bij het sluiten van elektronische overeenkomsten, overeenkomsten op afstand en dergelijke. Deze zijn gebaseerd op Europese richtlijnen.[108] Het gaat in het bijzonder om de volgende regels.

- Precontractuele informatieplichten: algemeen (art. 6:227b BW), voor dienstverleners (art. 6:230a-230f BW), voor B2C overeenkomsten in het algemeen (art. 6:230l-n BW), B2C overeenkomsten buiten een verkoopruimte (art. 6:230t BW), B2C overeenkomsten op afstand (art. 6:230v BW).
- Verbodsregels, zoals art. 6:230u BW dat een handelaar verbiedt een aanbod te doen om een overeenkomst buiten een verkoopruimte te sluiten als hij weet of moet vermoeden dat dit leidt tot verplichtingen voor de consument die niet in overeenstemming zijn met diens draagkracht. Daarnaast zijn van belang de regels die oneerlijke handelspraktijken verbieden

[102] Anders zou Internet niet kunnen werken: alle servers zouden dan alle gebruikers moeten informeren op de hier beschreven wijze. Hierom lijkt het ook niet wenselijk dat het werk van node-beheerders wordt beschouwd als een dienst van de informatiemaatschappij: dan zouden alle node-beheerders alle gebruikers van bitcoin moeten informeren voglens art. 3:15d BW voordat zij transacties zouden mogen verwerken. Daar zit niemand op te wachten, het minst van al de gebruikers die vaak juist anoniem willen blijven en geen gerichte communicatie van alle node-beheerders willen ontvangen.

[103] Dit zou bijvoorbeeld anders kunnen zijn als de blockchain alleen als tijdelijk communicatiemiddel wordt gebruikt, zoals e-mail, en de overeenkomst voor het overige puur fysiek wordt uitgevoerd.

[104] Art. 3:15d BW, ook art. 6:230b-230e BW.

[105] Ten dele zijn deze eisen ook in art. 3:15e BW opgenomen.

[106] Zie art. 2.2 Wet handhaving consumentenbescherming en onderdeel a van de Bijlage bij deze wet. Dit geldt voorzover het gaat om bedrijven tegenover consumenten (art. 8.1 en 8.2 lid 1 en 2 Wet handhaving consumentenbescherming).

[107] De wetgever liet dit open, mede omdat nietigheid niet altijd passend of mogelijk was. Zie Kamerstukken II, 2002/03, 28 197, nr. 5, blz. 15. Zie Groene Serie Vermogensrecht (Tjong Tjin Tai), art. 3:15d, aant. 5 (2010) mede verwijzend naar Drion 2000 en Sander 2001, blz. 80-81.

[108] Te weten de Dienstenrichtlijn 2006/123/EG en de Richtlijn Consumentenrechten 2011/83/EU, en de Richtlijn oneerlijke handelspraktijken 2005/29/EG.

(art. 6:193a-193j BW). Deze strekken onder meer ertoe dat de verstrekte informatie volledig is en niet misleidend of onjuist.
- Regels voor de wijze van aangaan, bewijs van en herstel van een overeenkomst (art. 6:227a en 227c BW). Op de regel voor herstel wordt hierna, onder e, nader ingegaan.
- Een 'ontbindingsrecht' van de consument bij B2C overeenkomsten buiten de verkoopruimte (art. 6:230o-230s BW), d.w.z. herroeping en niet ontbinding wegens wanprestatie, evenzo bij B2C overeenkomsten op afstand en buiten de verkoopruimte inzake financiële producten en diensten (art. 6:230x-z BW). Hierna, onder e, wordt hier nader op ingegaan.

Een consument kan in een procedure zich op deze regels beroepen. Verder is de Autoriteit Consument en Markt belast met de handhaving van art. 6:227a-c en 230g-z BW voorzover het bedrijven betreft,[109] en kan dwangsommen en boetes opleggen (art. 2.9 Wet handhaving consumentenbescherming). Als het gaat om financiële diensten of activiteiten is ook de Autoriteit Financiële Markten bevoegd tot handhaving (art. 3.1 Wet handhaving consumentenbescherming).

Deze regels brengen in het algemeen extra werk met zich voor aanbieders van overeenkomsten, maar zijn niet onmogelijk om aan te voldoen bij gebruik van blockchains. Een deel van de precontractuele informatieverplichtingen heeft betrekking op gegevens over identiteit en adres:[110] hiervoor gelden dezelfde bezwaren als hierboven zijn besproken voor art. 3:15d en 15e BW.

Een bijzondere regel die in de weg zou kunnen staan aan consumentenkoop via smart contracts is de regel dat een consument hoogstens verplicht is tot vooruitbetaling van de helft van de koopprijs (art. 7:26 lid 2, slot, BW). Bij smart contracts is het normaal gesproken de bedoeling dat de gehele contractssom wordt 'betaald', d.w.z. vastgezet in het smart contract, die het bedrag dan bij nakoming uitbetaald aan de wederpartij. Dit komt neer op vooruitbetaling in de zin van art. 7:26 lid 2 BW. In de praktijk hebben consumenten er overigens geen probleem mee om het gehele bedrag vooruit te betalen, wat de primaire optie is van veel websites.[111]

e. Herstel en herroeping/ontbinding

Een bijzonder aandachtspunt is dat diverse van de hierboven genoemde regels eisen dat een wederpartij de mogelijkheid heeft om niet gewilde handelingen vóór een elektronische overeenkomst te herstellen[112] of om een overeenkomst op afstand of buiten de verkoopruimte binnen een zekere termijn te 'ontbinden' (dat wil zeggen, herroepen) zonder opgave van redenen.[113] Deze regels botsen op het 'immutable', onwrikbare, karakter van transacties op een blockchain. De implementatie van de vastlegging of uitvoering van de overeenkomst zal de mogelijkheid moeten bieden voor wijzigingen volgens deze regels. Technisch gezien is dit mogelijk, maar het heeft wel tot gevolg dat er in zoverre afbreuk wordt gedaan aan het 'immutable' aspect van blockchaintechnologie.

Als een partij niet de technische mogelijkheid biedt tot herstel of 'ontbinding' op de blockchain zal hij verplicht blijven om de overeenkomst ongedaan te maken. Zonodig zal dit buiten de blockchain of de specifieke overeenkomst om moeten gebeuren, zoals door het verrichten van een terugbetaling op de blockchain of in gewone valuta op een gewone bankrekening. Als dit mogelijk is, is er geen sprake van strijd met het 'immutable' karakter van een blockchain (zoals een

[109] Zie art. 2.2 Wet handhaving consumentenbescherming en onderdeel a van de Bijlage bij deze wet. Dit geldt voorzover het gaat om bedrijven tegenover consumenten (art. 8.1, 8.2, derde en vierde lid, en 8.2a Wet handhaving consumentenbescherming).
[110] Zie art. 6:227b lid 1, 230b sub 1-5 en 12-13, art. 230d sub 2, art. 230l lid b, art. 230m lid 1 sub b-d BW.
[111] Het is overigens mogelijk bij individuele afspraak hiervan af te wijken; afwijking bij algemene voorwaarden is vernietigbaar. Zie Groene Serie Bijzondere Overeenkomsten (M.M. van Rossum), art. 7:26, aant. 4.
[112] Art. 6:227c lid 1 BW eist dat "Degene die een dienst van de informatiemaatschappij als bedoeld in artikel 15d lid 3 van Boek 3 verleent, stelt de wederpartij passende, doeltreffende en toegankelijke middelen ter beschikking waarmee de wederpartij voor de aanvaarding van de overeenkomst van door hem niet gewilde handelingen op de hoogte kan geraken en waarmee hij deze kan herstellen." Deze bepaling is een implementatie van art. 11 lid 2 E-commerce Richtlijn 2000/31/EG en mag dus niet door de Nederlandse wetgever worden gewijzigd.
[113] Art. 6:230o BW (met uitzonderingen in art. 6:230p BW), en voor financiële diensten art. 6:230x BW.

terugbetaling van een overboeking bij een gewone bankrekening ook niet betekent dat de oorspronkelijke betaling wordt geschrapt, alleen dat de gevolgen worden gecompenseerd).

Dat het mogelijk is om buiten de blockchain om alsnog de gevolgen van een niet-gewilde overeenkomst terug te draaien betekent echter niet per se dat is voldaan aan de eis van art. 6:227c lid 1 BW: het is immers nodig dat er "passende, doeltreffende en toegankelijke middelen" ter beschikking worden gesteld om de niet-gewilde overeenkomst te herstellen (d.w.z. ongedaan te maken). Als de overeenkomst eenvoudig is af te sluiten en uit te voeren via de blockchain, lijkt het niet passend of doeltreffend als een partij vervolgens alleen via e-mail kan communiceren over het herstel van een ongewilde overeenkomst, en maar moet hopen dat deze overeenkomst vervolgens daadwerkelijk handmatig wordt teruggedraaid. Voor de mogelijkheid van 'ontbinding' ligt dit anders: daarvoor hoeft niet per se een mogelijkheid te zijn ingebouwd.

f. Redelijkheid en billijkheid, en verplichtingen om wijzigingen mogelijk te maken

Het voorgaande punt is breder dan alleen de twee in de wet uitdrukkelijk genoemde gevallen. Een bijzonderheid van blockchaintechnologie is dat transacties op de blockchain voorafgegeven spelregels moeten volgen: het protocol. Bij gewone regels is het mogelijk dat er discussie is of een handeling de regels schendt, en kunnen partijen bovendien discussiëren of er werkelijk sprake is van schending: een partij kan uitleggen dat de formele schending in werkelijkheid geen probleem is of hoort te zijn (de geest versus de letter van de wet). Bij een blockchain zou het systeem de regels moeten handhaven en zou het onmogelijk moeten zijn dat transacties de regels schenden.[114] In zoverre zouden alle gebeurtenissen op de blockchain per definitie geldig moeten zijn volgens de regels van de blockchain. Zoals echter blijkt uit de The DAO-hack (zie par. 3.2.3) valt een systeem niet helemaal samen met de expliciet opgeschreven regels. In een samenwerkingsverband als een blockchain moeten de deelnemers zich redelijk opstellen tegenover elkaar; de wet noemt dit 'redelijkheid en billijkheid' (art. 6:2 en 248 BW). De redelijkheid en billijkheid kunnen met zich brengen dat partijen hun gedrag mede moeten laten bepalen door elkaars belangen en verwachtingen, die niet uitputtend worden geregeld door de expliciete regels van de blockchain.[115] Hierdoor is het mogelijk dat een handeling die volgens de blockchain-regels geldig is, volgens het recht toch als ongeldig moet worden beschouwd en moet worden teruggedraaid of ongedaan worden gemaakt.

Het contractenrecht laat toe dat er contracten met behulp van een blockchain worden gesloten en/of uitgevoerd. Er gelden enkele extra eisen, die berusten op Europese regels.
Er gelden verschillende informatieverplichtingen. Deze kunnen ook op een blockchain worden uitgevoerd. Een drempel is dat enkele verplichtingen eisen dat de identiteit en het adres en andere gegevens van een commercieel handelende partij worden bekend gemaakt: dat is problematisch als zo'n partij anoniem wil blijven.
Er gelden verschillende regels over de manier waarop zo'n overeenkomst tot stand komt en kan worden gewijzigd, hersteld, of 'ontbonden'. Het is technisch mogelijk hieraan te voldoen, maar dit vergt wel een extra inspanning bij de implementatie van de blockchain, of handmatige actie van een partij buiten de blockchain om wanneer zulke gevallen zich voordoen.
Algemeen geldt dat in specifieke gevallen het contractenrecht kan eisen dat de uitkomst van de regels van de blockchain wordt aangepast aan wat in de gegeven omstandigheden redelijk is. De contractspartijen zijn dan verplicht hieraan medewerking te verlenen.

[114] Het is wel mogelijk dat een ongeldige transactie dat een of meer nodes een ongeldige transactie aanvaarden (doordat zij bijvoorbeeld expres hebben afgesproken de blockchain te manipuleren), maar de essentie van blockchaintechnologie is dat dit niet door het gehele systeem aanvaard zal worden.
[115] Vgl. HR 19 oktober 2007, ECLI:NL:HR:2007:BA7024, NJ 2007/565 (Vodafone).

3.2.8 Smart contracts als bijzondere toepassing

Bij smart contracts zijn de bevindingen over het contractenrecht in het algemeen (par. 3.2.7) van toepassing, maar het is nodig om enkele additionele opmerkingen te maken.

Korte beschrijving

Smart contracts zijn programma's die op een blockchain worden uitgevoerd, en die beogen om automatisch een (onderdeel van een) contract uit te voeren.[116] Hiervoor is een bepaald type blockchainomgeving voor nodig, waarin gebruikers betalingen kunnen uitvoeren met de cryptocurrency van het platform, en programma's kunnen laten uitvoeren die automatisch betalingen uitvoeren of andere acties verrichten.

Het algemene idee van smart contracts is al ouder dan blockchain.[117] Blockchaintechnologie heeft het echter gemakkelijker gemaakt om smart contracts praktisch te realiseren, op basis van crypto-currency zoals bitcoin.[118] In plaats van alleen eenvoudige overboekingen kan in een smart contract worden opgenomen dat een betaling pas wordt verricht als er aan een al dan niet gecompliceerd samenstel van voorwaarden is voldaan, terwijl het contract tevens kan communiceren met de buitenwereld. Daardoor kan bijvoorbeeld een contract verzorgen dat de kamer van een hotel pas toegankelijk wordt als de huur is voldaan, of dat een bestelling betaald wordt als het pakketje is afgeleverd door de pakketbezorger. Om signalen van de buitenwereld te ontvangen is een interface nodig: men noemt dit een 'oracle'.[119]

Het bekendste voorbeeld van een smart contract platform is Ethereum (Ethereum.org). Dit berust op een alternatieve cryptocurrency, genaamd Ether. Smart contracts worden op dit platform geprogrammeerd in een script-taal geheten Solidity.

In de praktijk kan dit als volgt werken. Een partij biedt een smart contract aan op de blockchain,[120] waarna een andere partij dit smart contract kan aanvaarden. Dat kan bijvoorbeeld gebeuren doordat die partij een betaling doet aan het smart contract.[121] Een voorbeeld: een verkoper van goederen op een handelsplatform kan bijvoorbeeld voor de afwikkeling van de koop een smart contract op Ethereum aanbieden, waarbij de betaling aan de verkoper pas wordt gedaan als het smart contract bericht krijgt van de pakketbezorger dat het pakje daadwerkelijk is afgeleverd. De koper moet dan wel vooraf het hele bedrag aan het smart contract betalen. Als het pakje niet binnen twee weken wordt afgeleverd, krijgt de koper automatisch het geld teruggestort. Hiermee is voor de verkoper verzekerd dat hij zijn geld ontvangt, en voor de koper dat hij een pakket ontvangt.[122]

In het bovenstaande voorbeeld wordt het smart contract gebruikt als manier om een voorafgaande koopovereenkomst uit te voeren. Het is echter mogelijk dat er geen eerdere overeenkomst is, maar dat er alleen een smart contract is. Bijvoorbeeld: een partij biedt een smart contract aan om investeringen te doen in een onderneming. Geïnteresseerde partijen doen

---

[116] Algemeen over smart contracts: Reyes 2017, Werbach & Cornell 2017, Raskin 2017, Savelyev 2016, Perugini & Dal Checco 2015, Paech 2017, Mik 2017, Sklaroff 2017, Casey & Niblett 2017, Giancaspro 2017, De Filippi & Wright 2018, Tjong Tjin Tai 2017a, 2017c, 2018b, Werbach 2018a, p. 63-67, Fries en Paal 2019, Finck 2019, p. 24-28, Fries & Paul 2019, Szostek 2019, hfdst. V, Allen 2018.

[117] Szabo 1997, N. Szabo, 'The Idea of Smart Contracts', at szabo.best.vwh.net/smart_contracts_idea.html, Peyton Jones, Eber & Seward 2000, Surden 2012.

[118] Over de technische aspecten: Alharby & Van Moorsel 2017.

[119] Bijv. Werbach 2018a, 213-214. Dit kan een sensor zijn, maar ook een menselijke tussenpersoon. Zie Tjong Tjin Tai 2018b voor een uitvoeriger discussie over de wisselende rollen van oracles, ook Finck 2019, p. 25.

[120] De programmacode is dan op de blockchain geplaatst met een bepaald identificatienummer, waardoor naar dat smart contract kan worden verwezen.

[121] Het smart contract heeft een identificatienummer (id) waar betalingen aan kunnen worden gedaan: die betaling wordt geregistreerd op de blockchain. Die betaling is dan in beheer bij het smart contract; vervolgens bepaalt de programmacode van het smart contract wat er met die betaling gebeurt. Bijv. wordt het tijdelijk bewaard totdat duidelijk is aan wie het doorbetaald of terugbetaald moet worden, of wordt het direct doorbetaald aan de aanbieder van het smart contract.

[122] Hiermee zijn niet alle problemen uitgesloten; het is bijvoorbeeld mogelijk dat het pakje niet het gevraagde product bevat.

investeringen door betalingen te doen aan dat smart contract, en volgens de regels van het smart contract wordt bepaald wanneer zij dividenduitkeringen ontvangen. In zo'n geval kan er wel een geldige overeenkomst tussen partijen zijn, maar zullen de afspraken tussen partijen vooral moeten worden afgeleid uit de programmacode van het smart contract (er is immers geen ander document waarin afspraken zijn vastgelegd). Er wordt verdedigd dat partijen dan gebonden zijn aan de programmacode, dus dat de overeenkomst wordt bepaald door het smart contract.

De meerwaarde van smart contracts lijkt te zijn gelegen in twee aspecten.

- De uitvoering van het contract is 'gegarandeerd' zonder dat tussenkomst van mensen of de rechter nodig is: de betaling kan bijvoorbeeld door het contract zelf worden verricht in de gebruikte cryptocurrency, en als er technische voorzieningen voor zijn getroffen kunnen ook andere uitvoeringshandelingen (zoals de toegang tot een hotelkamer) zonder menselijke tussenkomst worden verricht. Een smart contract is 'self-executing', zelfuitvoerend.
- Als gevolg van het zelfuitvoerende karakter van smart contracts wordt geclaimd dat smart contracts de juridische contractspraktijk geheel of voor een groot deel zouden kunnen vervangen.[123]

In de praktijk lijken smart contracts niet zo ver te gaan. Zij worden vooral gebruikt om *onderdelen* van een contractuele relatie uit te voeren, niet om de gehele contractuele relatie te vangen.[124] Het smart contract is dan ingebed in een groter framework contract dat een gewone juridische overeenkomst is. Het gebruik van geprogrammeerde contracten is al vóór de opkomst van bitcoin verwezenlijkt voor financiële (optie)contracten.[125] In wezen valt een deel van de bancaire automatisering te begrijpen als eenvoudig 'smart contract': denk aan automatische incasso of overboeking. Dit is dan ook niet zo bijzonder; ook snoepautomaten en pinautomaten zijn vormen van automatische uitvoering van een overeenkomst, zij het dat zij zonder blockchaintechnologie functioneren.

Geldigheid en bijzondere regels[126]

Smart contracts zijn op zichzelf toegestaan onder het BW.[127] Door een smart contract te 'accepteren' volgens de regels van het smart contract platform kunnen partijen een overeenkomst sluiten in de zin van art. 6:213 BW.[128] Het smart contract (dat wil zeggen, de programmacode daarvan) levert bewijs van de inhoud van de (juridische) overeenkomst. Dat het contract is geformuleerd in de programmeertaal is geen bezwaar.[129] Verder is het uiteraard mogelijk dat naast de programmacode extra informatie is gegeven die betekenis heeft voor de inhoud van de overeenkomst.

Om vast te stellen wat de juridische verplichtingen en rechten van partijen zijn is het nodig de inhoud van de overeenkomst vast te stellen. Dit wordt ook wel genoemd: uitleg van de overeenkomst. Ook als die overeenkomst is ontstaan door aanvaarding van een smart contract, zal de uitleg volgens de gewone uitlegregels moeten plaatsvinden. Daarbij tellen zowel de tekst als de bedoeling van partijen.[130] Bij een smart contract is er geen gewone tekst zoals bij een contract in

---

[123] Verstraete 2018 betoogt dat smart contracts ook erop vertrouwen dat de Staat ervoor zorgt dat er een werkend privaatrechtelijk regime is.

[124] Dit is in interviews naar voren gebracht en vindt ook steun in de literatuur.

[125] Peyton-Jones c.s. 2000.

[126] Over de juridische status van smart contracts volgens Nederlands recht: Tjong Tjin Tai 2017a, Van Eersel & Van den Bergh 2017, Schmaal & Van Genuchten 2017, Naves 2018, De Graaf 2018a, Stam 2018, De Vries 2019, Neppelenbroek 2019, p. 282-290.

[127] Het is dan ook niet nodig om voor de geldigheid van smart contracts een wettelijke regeling te treffen. Zo'n regeling is er wel in Italië (Decreto-Legge 14 dicembre 2018, n. 135). Die regeling (art. 8-ter) houdt (kort gezegd) niet meer in dan dat wordt bevestigd dat het sluiten van een overeenkomst in de vorm van een smart contract gelijk staat met het sluiten van een schriftelijke overeenkomst.

[128] Tjong Tjin Tai 2017c, nr. 35, Naves 2018, p. 63, Van Eersel & Van den Bergh 2017 p. 45, De Vries 2019, p. 76. De acceptatie van het smart contract volgens de regels van de smart contract omgeving kan juridisch worden beschouwd als aanvaarding van een aanbod om een overeenkomst te sluiten (vgl. par. 3.2.4.a). Vgl. voor *common law* Werbach & Cornel 2017, p. 341-343, O'Shields 2017, p. 185-187, en voor de PECL en DCFR M. Kõlvart, M. Poola, & A. Rull 2016.

[129] Vgl. De Filippi & Wright 2018, p. 79 voor de U.S.A.

[130] Schmaal en Van Genuchten 2017.

gewone taal. De tekst is in zo'n geval vooral de code van het smart contract.[131] Daarnaast kunnen er ook andere documenten zijn die onderdeel zijn van de overeenkomst, bijvoorbeeld algemene voorwaarden van het platform o.i.d. Het is dus niet per se zo dat er alleen een smart contract in programmacode is.

Voor de uitleg is de tekst (in dit geval de code) niet allesbepalend: het is altijd mogelijk dat partijen naast het smart contract iets anders hebben afgesproken, dat uit e-mailwisseling blijkt dat partijen iets anders bedoelden dan in het smart contract (de programmacode) staat. Maar als er weinig andere aanwijzingen zijn, zal het smart contract praktisch gezien de basis vormen voor de uitleg. Dat partijen misschien niet zelf in staat zijn het smart contract te begrijpen, is daar geen obstakel voor. Hetzelfde geldt voor gewone contracten: deze kunnen zijn opgesteld in juridisch jargon met details die voor niet-juristen moeilijk te begrijpen zijn. Vanwege de bijzondere aard van een smart contract (waarmee partijen kennelijk bedoelen de uitvoering van hun overeenkomst vooral door de code te laten plaatsvinden) is verdedigbaar dat de rechter voor de uitleg vooral zal letten op de tekst van het smart contract (de programmacode).[132] Dit zou bijvoorbeeld betekenen dat als een bepaalde voorwaarde niet is opgenomen in het smart contract maar wel is besproken tussen partijen, de rechter toch zal beslissen dat de overeenkomst zo moet worden uitgelegd dat die voorwaarde er geen onderdeel van uitmaakt, omdat partijen bewust de code van het smart contract hebben aanvaard.[133] Maar als wordt bewezen dat partijen toch bedoelden die voorwaarde op te nemen, zal die bedoeling tellen.[134] Uiteindelijk gaat het om vaststelling van de inhoud van de juridische overeenkomst, en de code van het smart contract is daar slechts één factor bij. Als het smart contract dan tot andere uitkomsten leidt dan uit de juridische overeenkomst volgt, geldt de juridische overeenkomst. De uitkomst van het smart contract moet dan worden gecorrigeerd.[135] Een partij kan daarvoor naar de rechter gaan, al kan het lastig zijn om een eventuele uitspraak daadwerkelijk te laten uitvoeren (par. 3.2.10).

De uitleg van smart contracts kan verder problematisch zijn doordat programmacode niet is gemaakt als medium om de bedoeling van menselijke partijen weer te geven.[136] Om te helpen bij de uitleg te helpen zou de ontwikkelaar van het contract commentaar in de programmacode kunnen opnemen.

Sommige bedingen (zoals een rechtskeuze) kunnen niet of nauwelijks als gewone programmacode worden opgenomen. Het lijkt alleen mogelijk deze als commentaar in het programma op te nemen. Het is dan wel nodig dat partijen begrijpen dat zulk commentaar bindende bedingen kan bevatten.

Een bijzonder probleem is dat smart contracts kunnen verwijzen naar functies (deelprogramma's) uit algemene bibliotheken,[137] die zelf weer naar andere functies kunnen verwijzen. Zulke functies fungeren als algemene voorwaarden. Om dan de complete contractuele relatie te begrijpen is het nodig al deze functies te lezen (en dus het spoor van verwijzingen te volgen). De uitleg van het contract wordt dan nog lastiger als zulke functies tegenstrijdige bedingen bevatten (zoals tegenstrijdige rechtskeuzes).

Algemene analyse van smart contracts

[131] De Vries 2019, p. 77, wijst er overigens op dat er een verschil is tusen de werkelijk uitvoerbare code (byte-code), en het programma in een voor mensen leesbare programmeertaal (broncode) die daarna door een compiler wordt vertaald in byte-code. Hier nemen we aan dat het gaat om de broncode.
[132] Tjong Tjin Tai 2017c, nr. 36-37, ook Schmaal en Van Genuchten 2017.
[133] Dit zou met name het geval kunnen zijn als partijen zijn bijgestaan door technisch onderlegde adviseurs. Vgl. voor de relevantie van juridische bijstand bij contractsuitleg HR 19 januari 2007, NJ 2007/575, r.o. 3.7.3, HR 4 juni 2010, NJ 2010/312, r.o. 3.6.
[134] Vgl. Naves 2018, p. 65.
[135] Vgl. Finck 2019, p. 27.
[136] Giancaspro 2017, p. 832-833 behandelt diverse problemen voor deze uitleg. Allen 2018 gaat dieper in op de bredere context waarin contracten tot stand komen.
[137] De Filippi & Wright 2018, p. 138, vgl. Werbach 2018a, p. 206-208 en 212.

De geclaimde voordelen van smart contracts blijken bij nader onderzoek niet of niet zonder beperkingen aanwezig. Daarnaast zijn er enkele algemene beperkingen en risico's bij het gebruik van smart contracts.

- Smart contracts – in de op dit moment gangbare vorm - eisen dat de partij die tot betaling is verplicht al vooraf de betaling aan het smart contract doet, waarna het smart contract de betaling pas vrijgeeft aan de wederpartij als aan de betalingsvoorwaarden is voldaan. Dit lijkt op een bankgarantie[138] of kredietbrief.[139] Het nadeel van deze werkwijze is dat de schuldenaar dan niet langer de beschikking heeft over die betaling, ook als het contract uiteindelijk wordt ontbonden en hij het geld weer terugkrijgt. Dat is economisch gezien onvoordelig (het geld kan dan niet op andere wijze worden benut), en brengt valutarisico's met zich als de gebruikte cryptocurrency in de tussentijd van waarde verandert.
- Smart contracts kunnen niet de gehele complexiteit van de contractspraktijk vangen. Veel contractuele leerstukken zijn niet of moeilijk te implementeren in smart contracts.[140] Kwesties zoals de vraag of er sprake is van overmacht zijn niet goed te programmeren op de manier zoals partijen zouden verwachten.[141] Ook kunnen sommige contractsbepalingen als inspanningsverplichtingen[142] of garanties[143] niet of moeilijk in smart contracts geprogrammeerd worden. Dit geldt ook voor andere zogenaamde open normen, die geen precieze inhoud hebben (zoals een verplichting om een 'redelijk' voorstel te doen).[144] Het is wel mogelijk om in het smart contract op te nemen dat een externe partij (een oracle) wordt ingeschakeld om te beoordelen of er sprake is van overmacht, schending van een garantie of inspanningsverplichting.[145] Maar die partij functioneert dan in feite als arbiter, en daardoor is de uitvoering van het contract niet meer automatisch gegarandeerd. Het wordt dan mogelijk om die arbiter aansprakelijk te houden voor onjuiste beslissingen en op die wijze de uitvoering van het smart contract te blokkeren. Er wordt wel verdedigd dat AI oplossingen mogelijk zou maken,[146] maar de technische mogelijkheden van AI zijn op dit ogenblik nog niet zo ver. Slotsom is dat de uitvoering van een smart contract op diverse punten zal afwijken van wat volgens het geldende recht volgt uit de juridische overeenkomst.
- De hierboven besproken bezwaren zouden kunnen verminderen als er op langere termijn voldoende best practices ontstaan, voorbeeldcontracten die de juridische verfijning in voldoende mate benaderen.[147] Dit zou kunnen doordat er softwarebibliotheken ontstaan waarin veelvoorkomende stukjes van contracten zijn opgenomen: een gebruiker van een contract zou dan gewoon zo'n bibliotheek kunnen gebruiken.[148] Of dit haalbaar is, zou nader moeten worden onderzocht.[149]
- Smart contracts zijn niet of nauwelijks te begrijpen of controleren voor gebruikers die geen bijzondere IT-kennis hebben.[150] Daarentegen vallen gewone juridische overeenkomsten nog wel

[138] Tjong Tjin Tai 2015.
[139] McJohn & McJohn 2016.
[140] Giancaspro 2017, Janssen 2017, Tjong Tjin Tai 2017b en 2018b, Van der Roest 2017, Evadgian 2018, Werbach 2018a, p. 125, Finck 2019, p. 27.
[141] Zie Tjong Tjin Tai 2018b, 2017b.
[142] De Filippi & Wright 2018, p. 77.
[143] De Filippi & Wright 2018, p. 77.
[144] Werbach & Cornell 2017, p. 367 over overmacht, ook 372-373, Künnapas 2016, uitvoerig Tjong Tjin Tai 2018b. Optimistisch zijn Casey & Niblett 2017, p. 24, echter zonder inhoudelijke analyse.
[145] Mik 2017, p. 21-24.
[146] Casey & Niblett 2017, p. 24.
[147] Werbach & Cornell 2017, p. 374-375, Paech 2017, p. 1097.
[148] De Filippi & Wright 2018, p. 82. Dit lijkt enigszins op het gebruik van modelcontracten.
[149] Er wordt bijvoorbeeld voorbijgegaan aan de mogelijkheid dat de voorwaarden conflicteren of in combinatie anders uitwerken dan bedoeld, dat er versiebeheer nodig is als er verbeterde voorwaarden worden opgesteld. In essentie ontmoet men dan dezelfde problemen die systeembeheerders en ontwikkelaars tegenkomen bij het gebruik van softwarebibliotheken.
[150] De Filippi & Wright 2018, p. 141 suggereren dat slechts 'a small number of people are capable of auditing that code'. Overigens liet de hack van TheDAO ook zien dat dit zelfs voor relatief deskundige personen moeilijk kan zijn, omdat smart contract platforms enige bijzonderheden hebben die afwijken van gewone programma's, zoals het gegeven dat het in wezen gaat om parallele uitvoering.

enigszins te begrijpen. Daarom zullen gebruikers van smart contracts moeten vertrouwen op de mededelingen van de ontwikkelaar van het smart contract, wat grote risico's oplevert bij malafide ontwikkelaars.[151] Gebruikers kunnen als alternatief vertrouwen op deskundig advies of auditing van contracten, maar dat brengt kosten met zich waardoor er geen verbetering is ten opzichte van gewone juridische overeenkomsten. De risico's kunnen overigens kleiner zijn als het gaat om contracten die al vaak zijn gebruikt en/of afkomstig zijn van een goed bekend staande partij.
- Het perspectief van smart contracts wijkt wezenlijk af van gewone juridische overeenkomsten: een programma vereist dat voor alle mogelijkheden vooraf (ex ante) regels en oplossingen zijn geprogrammeerd. Hierdoor worden de kosten van het contracteren verschoven naar de aanvang: er moeten hoge kosten worden gemaakt om alles goed te regelen.[152] Juridische contracten daarentegen maken het mogelijk om in ingewikkelde gevallen ex post een oplossing te construeren door het vormen van nieuwe regels die in de gegeven omstandigheden rechtvaardig zijn.[153] Het gebruik van open normen, die niet goed zijn te implementeren in smart contracts, is een voorbeeld waarbij partijen zelf de voorkeur eraan geven niet alle toekomstige problemen uitputtend te regelen.[154]
- Uit sociologisch onderzoek is gebleken dat contractspartijen vaak veeleer denken vanuit de zakelijke relatie, waarbij het contract niet steeds naar de letter hun relatie regelt. Dit zogenaamde gegeven van *relational contracting*[155] staat op gespannen voet met de statische structuur van smart contracts.[156] Wijziging van de overeenkomst is in de praktijk vaak wenselijk (en ten dele verplicht, zie par. 3.2.7).[157] Diverse rechtsregels vereisen dat partijen ingeval van moeilijkheden, zoals bij niet-nakoming of het optreden van overmacht, met elkaar in overleg treden om de ontstane problemen adequaat te regelen of op te lossen.[158] Een dergelijke dynamiek is lastig vorm te geven in de procedurele programmeertalen (scripttalen) die bij smart contracts gangbaar zijn.[159]

Het gebruik van smart contracts lijkt daarom diverse nadelen te hebben. Toch is het voorstelbaar dat in bepaalde gevallen de contractspartijen het verlies aan bescherming van de gewone juridische regels voor lief nemen. Dit is met name te verwachten in gevallen waar sowieso de gewone rechtsgang niet of nauwelijks effectief is of te kostbaar,[160] zoals bij transacties met relatief geringe waarde, over grote afstand en/of met anonieme partijen. Dit kan zich voordoen bij internationale consumentenkoop via platformen als eBay of Aliexpress, en in de internationale handel.[161] Smart contracts hebben dan toegevoegde waarde doordat de nakoming van het contract in sterkere mate is verzekerd,[162] ook al zal het contract bij lastigere situaties niet geheel volgens normale verwachtingen uitwerken.

---

[151] Wikipedia (https://en.wikipedia.org/wiki/Ethereum) verwijst naar Bartoletti, et al. 2017, over de aanwezigheid van vele piramidespelen op Ethereum.
[152] Sklaroff 2017, p. 292, verwijzend naar Tapscott & Tapscott 2016, p. 103.
[153] Werbach & Cornell 2017, p. 361 and Mik 2017, p. 17
[154] Sklaroff 2017, p. 279-286, ook Sklaroff 2017, p. 293-295, Mik 2017, p. 19-20.
[155] Werbach & Cornell 2017, p. 367, ook Levy 2017, De Filippi & Wright 2018, p. 84.
[156] Smart contract behoeven overigens niet *immutable* te zijn; het is technisch mogelijk om wijzigingsmogelijkheden in te bouwen. Zie Marino & Juels 2016, vgl. hierover Sklaroff 2017, p. 291.
[157] Werbach & Cornell 2017, p. 367, O'Shields 2017, p. 187, Werbach 2018a, p. 126, 161-163.
[158] Zoals door het verzenden van ingebrekestelling. Zie ook Tjong Tjin Tai, 2017b.
[159] Overigens gaan Peyton Jones, Eber & Seward 2000 uit van functionele programmeertalen die op andere wijze werken.
[160] Eenmaa-Dimitrieva & Schmidt-Kessen 2017, Tjong Tjin Tai 2017b en 2017c.
[161] Het stelsel van cognossementen, kredietbrieven, wissels e.d. zou mogelijk efficiënter kunnen worden opgezet via smart contracts. Bovendien wordt in de internationale handel ook gewerkt met 'oracles' *avant la lettre*, deze worden aangeduid met namen als surveyor, certification agency, conformity assessment body (Tjong Tjin Tai 2018b).
[162] Immers als alleen de juridische regels gelden zou het praktisch onmogelijk zijn om de wederpartij te achterhalen, en kostbaar om een procedure aan te spannen en ten uitvoer te leggen. Een smart contract zou dan voor diverse probleemgevallen redelijke oplossingen kunnen bieden die dan automatisch worden afgedwongen, ook al is niet bekend wie de wederpartij is en ook als de overeenkomst misschien onder een rechtsstelsel valt dat andere regels hanteert.

Daarnaast kunnen smart contracts nuttig zijn ter vervanging van menselijke uitvoering van een (deel van een) contractuele relatie: dit kan efficiëntie-voordelen opleveren, terwijl ingeval van geschillen partijen toch nog naar de rechter zouden kunnen stappen.

Smart contracts zijn programma's op een blockchain die op de blockchain worden uitgevoerd en die beogen (delen van) een overeenkomst tussen partijen uit te voeren. Als voordelen worden genoemd dat smart contracts automatisch en daarmee gegarandeerd worden uitgevoerd, en dat zij gesloten kunnen worden zonder dat het nodig is juridisch advies in te winnen.
Smart contracts zijn op zichzelf geldig: het is niet verboden een overeenkomst te sluiten door middel van een smart contract. Het is dan ook niet nodig om de wet aan te passen voor smart contracts.
Een smart contract is zelf niet een overeenkomst maar kan worden beschouwd als bewijs van totstandkoming van een juridische overeenkomst. De inhoud van die overeenkomst wordt bepaald volgens juridische regels. De programmacode van het smart contract zal belangrijk zijn om de inhoud van de overeenkomst vast te stellen, maar is daarbij niet doorslaggevend. Ook de bedoeling van partijen speelt een rol. Het kan lastig zijn om alle gewone regels van een overeenkomst in een smart contract vast te leggen op een begrijpelijke manier. Als de regels van een smart contract in strijd zijn met wat uit de juridische overeenkomst volgt, kan een partij in principe de rechter vragen om de uitvoering van het smart contract te corrigeren. Het is mogelijk dat dit niet effectief is te handhaven.
Smart contracts hebben diverse nadelen en risico's. Smart contracts eisen meestal betaling vooraf wat tot renteverlies en valutarisico's leidt. Smart contracts kunnen de gewone regels van het contractenrecht maar in beperkte mate uitvoeren: als een partij dan geen effectieve rechtsbescherming heeft, raakt die partij bescherming kwijt (zoals bij overmacht) die zij wel heeft bij gewone overeenkomsten. Bij het gebruik van menselijke 'oracles' voor de beoordeling van omstandigheden wordt het smart contract weer afhankelijk van menselijke tussenkomst en verloopt dan niet automatisch. Smart contracts zijn niet te begrijpen of controleren zonder specialistische kennis, en het inhuren van zulke kennis is kostbaar, terwijl het riskant is om erop te vertrouwen dat het contract doet wat de ontwikkelaar zegt. Smart contracts wijken daarnaast wezenlijk af van de gewone manier waarop mensen een contract opvatten: als een onderdeel van een intermenselijke relatie, die niet tot in detail vooraf regelt hoe er met verschillende omstandigheden moet worden omgegaan.
Smart contracts kunnen in bepaalde omstandigheden voordelen bieden ondanks de risico's. Dit lijkt met name het geval bij overeenkomsten met anonieme partijen in het buitenland, of als onderdeel van een grotere gewone overeenkomst (waarbij het smart contract wordt gebruikt als uitvoering van een deel van die overeenkomst).

3.2.9 Aansprakelijkheid

Bij blockchaintechnologie zijn de mogelijkheden voor aansprakelijkheid lastig te bespreken doordat er veel verschillende betrokkenen zijn die verschillende posities innemen. Daarbij hangt veel af van de specifieke invulling van blockchaintechnologie die is gekozen. In het algemeen zijn de volgende hoofdlijnen aan te wijzen.[163] Wij concentreren ons hier op buiten-contractuele aansprakelijkheid. Voor contractuele aansprakelijkheid (aansprakelijkheid tussen contractspartijen) kunnen de gewone regels worden toegepast.

a. Gronden voor aansprakelijkheid

Er zijn verschillende mogelijkheden waarom iemand aansprakelijk zou kunnen zijn (gronden voor aansprakelijkheid). Enkele voorbeelden:

- Er staan onrechtmatige uitlatingen op de blockchain (zoals privacygevoelig materiaal) of inbreukmakend materiaal (bijvoorbeeld een foto waar auteursrecht op rust). Het plaatsen of laten staan van zulke materiaal kan dan een onrechtmatige daad uitmaken.

[163] Zie ook Tjong Tjin Tai 2017a en 2017c.

- Er zijn bitcoin 'gestolen' doordat een hacker toegang kreeg tot de private key, en daarmee een overboeking naar een door hem gecontroleerde account deed. Die overboeking is dan onrechtmatig jegens de eigenaar van het account. Is er in dit soort gevallen iemand aansprakelijk naast de hacker?[164]

Zoals uit deze voorbeelden blijkt is in veel gevallen duidelijk, door een vergelijking met gevallen waar geen blockchain bij betrokken is, of er sprake is van onrechtmatig handelen. Een paar bijzondere gevallen verdienen nadere aandacht.

In sommige gevallen kan het lastig zijn om vast te stellen of er sprake is van onrechtmatig handelen. Een voorbeeld: de hack van The DAO (par. 3.2.2) lijkt neer te komen op oplichting, maar een significant deel van de deelnemers van The DAO vond de hack niet oneerlijk, omdat alle gebruikers zelf het smart contract konden bestuderen op de effecten ervan. Een ander voorbeeld is de Parity hack, waarbij door een bug in de Parity wallet[165] tegoed kon worden ontvreemd door hackers. Een groep white hat hackers (goed bedoelende hackers) heeft toen de resterende tegoeden weggenomen om deze veilig te stellen, en heeft deze later ook daadwerkelijk weer teruggegeven aan de oorspronkelijke 'eigenaars'.[166] Is hun handelen nu rechtmatig?

Een bijzondere regeling is dat transacties of handelingen op de blockchain, afhankelijk van de precieze omstandigheden, kunnen worden gekwalificeerd als een *'dienst van de informatiemaatschappij'* in de zin van art. 3:15d BW (zie par. 3.2.7.c). Een deelnemer die zo'n dienst verleent is verplicht om diverse soorten informatie te verschaffen, zoals zijn identiteit en adres van vestiging, e.d. Deze regel is gebaseerd op art. 5 Richtlijn 2000/31/EG en mag dus niet door de Nederlandse wetgever worden geschrapt. Niet-naleving van deze verplichtingen is een economisch delict (art. 1 onder 4° van de Wet op de economische delicten), en daarmee ook een onrechtmatige daad omdat dit een schending van een wettelijke plicht uitmaakt (art. 6:162 BW). Het lijkt er op dit moment niet op dat een node-beheerder, door transacties te verwerken, een dienst van de informatiemaatschappij verleent. Daarvoor is zijn rol in de transactieverwerking te klein en onbepaald: het is het blockchainsysteem als geheel dat de transacties verwerkt, niet de node-beheerder die soms bij een geslaagde poging om te minen cryptocurrency verdient en het volgende block mag bepalen.

Schending van regels van de blockchain is op zichzelf geen onrechtmatige daad (zie par. 3.2.3). De aard van de blockchain is dat conformiteit met de regels wordt afgedwongen, maar niet dat node-beheerders of andere deelnemers hier juridisch toe verplicht zijn. Uiteraard is wel mogelijk dat een deelnemer zelf door concreet op een bepaalde manier te handelen onrechtmatig handelt. Een voorbeeld is dat een deelnemer met enkele andere node-beheerders samenspant om te zorgen dat de transacties van een andere deelnemer gedurende enige tijd worden geblokkeerd.[167]

Aansprakelijkheid kan verder soms worden gebaseerd op *medewerking aan wanprestatie*[168] of *medewerking aan onrechtmatige daad*.[169] De juridische regels hierover zijn betrekkelijk vaag, waardoor het onzeker is hoe deze moeten worden toegepast op een nieuwe ontwikkeling als blockchaintechnologie. Aansprakelijkheid op deze basis wordt in het algemeen zelden aangenomen en dan vooral bij beroepsbeoefenaren als advocaten en notarissen, aan wie strengere eisen worden gesteld (zie hierna, 'Poortwachters'). Bij blockchain lijkt vooral belangrijk het geval dat node-beheerders niet meewerken aan het terugdraaien van transacties. Bij grootschalige blockchainsystemen zoals bij bitcoin ligt niet voor de hand dat deelnemers in zo'n geval onrechtmatig handelen. Het systeem draait er immers in essentie juist om dat transacties niet regelmatig worden teruggedraaid. Daarnaast kan men zich afvragen of het omgekeerde zou kunnen

---

[164] Bij diefstal van een private key uit een wisselbeurs is uiteraard wel de beurs aansprakelijk als deze onvoldoende beveiliging had; dat is een gewone contractuele kwestie.

[165] Een 'digitale portemonnee' waarmee tegoeden in verschillende cryptocurrencies kunnen worden bewaard.

[166] https://cointelegraph.com/news/parity-hack-white-hat-group-drains-85-mln-as-company-fills-holes, https://motherboard.vice.com/en_us/article/qvp5b3/how-ethereum-coders-hacked-back-to-rescue-dollar208-million-in-ethereum

[167] Wat mogelijk is als het slachtoffer alleen via deze nodes communiceert met het gehele blockchain-netwerk.

[168] Zie o.a. Van Bochove 2013.

[169] Tjong Tjin Tai 2007, p. 210-15, Tjong Tjin Tai 2012.

gelden: is het onrechtmatig om wel mee te werken aan een fork waardoor transacties worden teruggedraaid (zoals ingeval van de hack van The DAO)? Ook hier ligt voor de hand dat geen sprake is van onrechtmatigheid: de mogelijkheid van een fork is 'ingebakken' in het systeem, zodat alle betrokkenen hier rekening mee hebben te houden. Voor permissioned blockchains is dit anders, omdat daar de regels van de toepasselijke overeenkomst gelden. Dan gaat het eenvoudigweg om het vaststellen van de inhoud van die overeenkomst.

Voor blockchains gelden de gewone regels voor aansprakelijkheid. Het volgen van of het schenden van de regels van de blockchain is in het algemeen niet onrechtmatig. Het meewerken of niet meewerken aan een *fork (wijziging van de blockchain)* lijkt ook niet zonder meer onrechtmatig te zijn.
Het is mogelijk dat dienstverlening met blockchains telt als een dienst voor de informatiemaatschappij, zodat er onrechtmatig wordt gehandeld als de regels voor zulke diensten niet worden nageleefd. Het verdient aanbeveling als wordt verduidelijkt of en wanneer sprake is van zo'n dienst.

b. Aansprakelijke partijen

Aansprakelijkheid hangt af van de rol die een partij heeft. De verschillende partijen die in aanmerking komen worden hierna nagelopen.[170] Finck spreekt van 'regulatory access points'.[171] Deze zijn breder dan partijen die in de feitelijke governance van de blockchain invloed hebben (par. 3.2.3). Het gaat hierbij ook om partijen als ISP's en banken die kunnen helpen een blockchain te beheersen (door deze uit te sluiten van regulier verkeer) zonder dat zij de richting van de blockchain zelf kunnen bepalen.

De *blockchain* zelf kan niet aansprakelijk gesteld worden, omdat een blockchain geen natuurlijk persoon of rechtspersoon is. Wel is het mogelijk dat de blockchain geheel onderdeel is van een rechtspersoon (par. 3.2.2): dan kan die rechtspersoon wel aansprakelijk zijn voor het onrechtmatig toebrengen van schade aan derden. Dat betekent niet per se dat iedere vorm van schade waarbij de blockchain is betrokken leidt tot aansprakelijkheid. In het algemeen zal waarschijnlijk vereist zijn dat de rechtspersoon die de blockchain controleerde wist of kon weten van het mogelijk ontstaan van schade en dat van die rechtspersoon in de gegeven omstandigheden kon worden verwacht hiertegen maatregelen te nemen.[172]

De gezamenlijke *node-beheerders als maatschap*. Als de gezamenlijke node-beheerders van de blockchain een maatschap zijn (waarover par. 3.2.2) zijn deze deelnemers allen aansprakelijk voor schulden van de maatschap. Als de aansprakelijkheid is gebaseerd op een overeenkomst die de maatschap is aangegaan is deze aansprakelijkheid in beginsel hoofdelijk,[173] als de aansprakelijkheid berust op onrechtmatige daad wordt verdedigd dat iedere deelnemer voor een gelijk deel van de schade aansprakelijk is (dus bij 1000 deelnemers slechts 1/1000 deel).[174]

Node-beheerders, gebruikers en andere deelnemers. In het algemeen is er geen aansprakelijkheid voor de deelname als node-beheerder aan een blockchainsysteem op zichzelf, aangenomen dat het geen systeem met illegaal oogmerk betreft.[175] De samenwerking in een blockchain geeft geen grond voor groepsaansprakelijkheid (art. 6:166 BW), omdat de blockchain geen activiteit is die gevaar voor schade doet ontstaan van zodanige aard dat dit reden zou moeten

[170] Zie ook VBW-studie 2017, p. 33-34
[171] Finck 2019, p. 45-58.
[172] Dit zijn gewone eisen voor het aannemen van aansprakelijkheid op grond van onrechtmatige daad.
[173] Dat wil zeggen: iedere deelnemer kan voor het gehele bedrag worden aangesproken. Zie art. 7:407 lid 2 BW, en verder Asser/Maeijer & Van Olffen 7-VII 2017/116b. Dit is anders als de tekortkoming niet aan de deelnemer kan worden toegerekend (art. 7:407 lid 2 BW).
[174] Asser/Maeijer & Van Olffen 7-VII 2017/118-119.
[175] Dit kan anders zijn bij een exchange op het darkweb, bijvoorbeeld het vroegere beruchte Silk Road.

zijn om niet aan de blockchain deel te nemen.[176] Een blockchain is op zichzelf in het algemeen ook geen rechtspersoon en ook geen maatschap (par. 3.2.2).

Gevolg hiervan is dat een deelnemer alleen aansprakelijk is voor eigen daden. Een voorbeeld is dat een gebruiker zonder toestemming een auteursrechtelijk beschermde foto op de blockchain zet. Dit is gewoon een onrechtmatige daad waarbij het niet bijzonder is dat deze met gebruikmaking van de blockchain gebeurt.

Een vraag is of node-beheerders in zo'n geval aansprakelijk kunnen zijn voor medewerking aan onrechtmatig handelen. Neem het voorbeeld van een gebruiker die een inbreukmakende foto op de blockchain plaatst. Hierbij geldt echter een bijzondere regel. Een blockchain kan mogelijk worden aangemerkt als een Internetdienstverlener of ISP[177] in de zin van art. 6:169c BW en art. 12-15 Richtlijn 2000/31/EG. Dergelijke dienstverleners (in het bijzonder 'hosting ISP's') zijn niet aansprakelijk voorzover zij louter passief zijn. Het ligt voor de hand dat iedere node-beheerder zelf zo'n dienstverlener is: immers hij draagt bij aan het goed laten werken van de blockchain, en maakt de inhoud van de blockchain beschikbaar voor anderen. Dus als de blockchain gewoon automatisch handelt volgens de regels, zijn node-beheerders aansprakelijk. Maar als een derde aangeeft dat er op de blockchain inbreukmakende informatie staat,[178] geldt dat de ISP verplicht is deze informatie te verwijderen of anders zelf aansprakelijk kan zijn (notice and take-down). Het gevolg kan zijn dat een deelnemer door een derde gedwongen wordt af te wijken van het protocol door een block te verwijderen dat volgens het protocol geldig is en op de blockchain zou moeten blijven![179]

Gebruikers. Een gebruiker van de blockchain (zoals een eigenaar van bitcoin die niet zelf een node opereert) is niet aansprakelijk voor het gebruik op zichzelf, aangezien dat niet onrechtmatig is. Wel is mogelijk dat hij op de blockchain onrechtmatig handelt, bijvoorbeeld door inbreukmakende informatie op de blockchain te zetten in een transactie, of door de blockchain voor onrechtmatige doeleinden te gebruiken, zoals witwassen van zwart geld. Een gebruiker is echter niet aansprakelijk voor wat er op de blockchain gebeurt buiten zijn eigen handelen: hij heeft daar immers geen invloed op.

Bepalende organen (o.a. core developers). Kan de aanwezigheid van een interne governancestructuur (par. 3.2.3) tot aansprakelijkheid van de beleidsbepalende partijen leiden? Als men kijkt naar art. 2:11 BW, dat het mogelijk maakt dat de formele bestuurders aansprakelijk zijn voor een vennootschap, geldt dat deze aansprakelijkheid niet geldt voor feitelijk beleidsbepalende personen.[180] Wel is het mogelijk dat een persoon het onrechtmatig handelen of wanprestatie van een rechtspersoon bewerkstelligt of toelaat: dan kan die persoon aansprakelijk zijn als hem een voldoende ernstig persoonlijk verwijt treft.[181] Een blockchain is in het algemeen geen rechtspersoon. Het lijkt daarom te verwachten dat beleidsbepalende of invloedrijke partijen bij de blockchain nog minder snel aansprakelijk zijn, alleen als aan de norm is voldaan dat zij zelf onrechtmatig handelen jegens een bepaald slachtoffer (en dus deze partij een persoonlijk verwijt treft). In wezen is dit de gewone norm voor onrechtmatige daad.

Poortwachters. Een bijzondere rol rond de blockchain zou kunnen zijn weggelegd voor poortwachters: partijen die in de positie zijn om (als groep) de toegang tot een bepaald systeem te bepalen. Voorbeelden zijn banken, notarissen, van wie de tussenkomst nodig is om toegang te verkrijgen tot het officiële betalingsverkeer of het rechtsverkeer, zoals overdracht van onroerend goed.[182] Bij blockchainsystemen kunnen er ook poortwachters aanwezig zijn.

---

[176] Nader Asser/Hartkamp & Sieburgh 6-IV 2015, nr. 127.
[177] Internet Service Provider.
[178] Bijvoorbeeld inbreuk op privacy of auteursrecht; het kan ook gaan om het inroepen van het 'right to be forgotten'.
[179] Het is echter de vraag of dit feitelijk mogelijk is omdat het terugdraaien niet door een individuele deelnemer kan gebeuren maar door het gehele netwerk moet gebeuren. Zie hierover par. 3.2.11.
[180] HR 14 maart 2008, NJ 2008/466 (mr. Aerts q.q.).
[181] Zie o.a. HR 18 februari 2000, NJ 2000/295 (Oosterhof), HR 8 december 2006, NJ 2006/659 (Ontvanger/Roelofsen). Er is veel jurisprudentie, die echter mede gericht is op de concrete casus. Van belang is dat het niet nodig is dat het gaat om een formele bestuurder; het kan ook voldoende zijn dat de persoon in feite de volledige zeggenschap had over een andere rechtspersoon (HR 14 november 1997, NJ 1998/270 (Henkel/JMG).
[182] Vgl. Werbach 2018, p. 27 en Werbach 2018a, p. 129, sprekend van edge services'.

Bijvoorbeeld zijn er bij bitcoin onofficiële poortwachters, te weten de bitcoin-exchanges.[183] Om bitcoin om te zetten in officiële valuta is het immers nodig om iemand bereid te vinden bitcoin te ruilen voor 'echt' geld. Exchanges vervullen die rol. Overheden zijn de laatste tijd begonnen om zich op deze exchanges te richten teneinde bitcoin deels te reguleren.[184] Afgezien van eventuele nieuwe specifieke wettelijke regels voor bepaalde poortwachters is het mogelijk dat een partij die zich in de positie van een poortwachter bevindt aansprakelijk wordt gesteld als hij meewerkt aan onwenselijke gebeurtenissen op de blockchain, deze niet tegenhoudt,[185] of althans niet waarschuwt. In de rechtspraak is dit aangenomen ten aanzien van banken die niet waarschuwen tegen een piramidespel.[186] Het is niet zeker of deze rechtspraak ook kan worden toegepast op niet-officiële poortwachters.

Onzekerheid over de aansprakelijkheid van eventuele poortwachters is overigens wel een risico, omdat dit ertoe kan leiden dat blockchains geen toegang krijgen tot de reguliere economie, doordat bijvoorbeeld banken weigeren te wisselen voor reguliere valuta.

Adviseurs en andere dienstverleners. Voorzover bij de blockchain beroepsbeoefenaren zijn betrokken, zoals adviseurs, advocaten, notarissen, softwareontwikkelaars, softwareauditors e.d., zijn deze volgens de gewone regels aansprakelijk bij fouten.[187] Er zijn op zichzelf geen bijzonderheden die aandacht behoeven. Wel is het zo dat op gereguleerde beroepen als advocaten en notarissen, en op financiële dienstverleners, zwaardere zorgplichten rusten dan op gewone beroepsbeoefenaren. Het gevolg daarvan is dat zij sneller aansprakelijk gesteld kunnen worden dan gewone partijen.

c. Analyse en aanbevelingen

Uit het voorgaande blijkt dat de bestaande aansprakelijkheidsregels kunnen leiden tot aansprakelijkheid bij diverse betrokkenen bij een blockchain. Het valt op dat de directbetrokkenen (in het bijzonder node-beheerders en core-developers) niet snel aansprakelijk zijn, terwijl meer zijdelings betrokken partijen (zoals banken) mogelijk wel aansprakelijk zijn. Verder is niet geheel duidelijk onder welke omstandigheden partijen precies aansprakelijk zullen zijn; er is nog geen rechtspraak die duidelijkheid geeft. Deze onduidelijkheid kan een beletsel zijn voor het adopteren van blockchain. Een mogelijke aanbeveling is daarom om nadere regels in te voeren. Hiervoor zijn verschillende mogelijkheden, bijvoorbeeld de volgende.

- Een vrijstelling als in art. 6:196c BW voor Internet Service Providers, waardoor intermediairs in beginsel niet aansprakelijk zijn voor medewerking aan een blockchain.
- Regels als art. art. 2:11 BW om feitelijk beleidsbepalende organen in de blockchain (die feitelijke governance uitoefenen) onder specifieke omstandigheden aansprakelijk te houden.
- Het kan wenselijk zijn, mede ten behoeve van handhaving, bepaalde partijen juist sneller aansprakelijk te houden (zie ook par. 3.2.10).

Uiteindelijk hangt de keuze van maatregelen af van rechtspolitieke keuzes. Zulke regels zullen vooral effectief zijn als zij in internationaal verband zijn geharmoniseerd of ten minste afgestemd (par. 3.2.10).

Betrokkenen bij een blockchain zijn in het algemeen niet snel aansprakelijk wegens betrokkenheid, tenzij zij zelf onrechtmatig handelen volgens de gewone regels. Wel kunnen bijzondere partijen, zoals bepaalde beroepsbeoefenaren, of (door de wet aangewezen) poortwachters sneller aansprakelijk zijn voor hun rol bij de blockchain.
De afwezigheid van duidelijk aansprakelijke partijen bij schade veroorzaakt door een blockchain kan onwenselijk zijn: een oplossing kan zijn gelegen in het verlagen van aansprakelijkheidsdrempels of

[183] Low & Teo 2017, p. 265 wijzen erop dat de relatie tussen klant en beurs niet erg duidelijk is.
[184] Vgl. Blemus 2017, ook Overwater & Custers 2018.
[185] De Filippi & Wright 2018, p. 70.
[186] HR 23 december 2005, NJ 2006/289 (Safe Haven) en HR 27 november 2015, NJ 2016/245 (ABN AMRO/St. Gedupeerde Beleggers vd B).
[187] Dit valt onder gewone beroepsaansprakelijkheid, vgl. Tjong Tjin Tai 2017a. Zie voor bijzondere regels voor notarissen Tjong Tjin Tai 2018a.

het verduidelijken van aansprakelijkheidsregels voor bepaalde groepen betrokkenen bij een blockchain. Ter facilitering van blockchain kan het ook wenselijk zijn te verduidelijken wanneer geen aansprakelijkheid bestaat.

3.2.10 Handhaving en regulering[188]

Handhaving verdient bijzondere aandacht bij blockchain. Het wordt namelijk betoogd dat het, als gevolg van het decentrale karakter van de (publieke) blockchain,[189] in feite niet mogelijk is voor overheden om in te grijpen in de werking van blockchain om conformiteit met rechtsregels af te dwingen. Immers zelfs als alle *nodes* in één land zouden worden uitgeschakeld, blijven er genoeg over in andere landen om het systeem draaiend te houden. Zelfs als alle nodes in bijvoorbeeld Europa en de U.S.A. plat zouden worden gelegd zijn er vele nodes in China en andere landen.

Deze claims zijn evenwel niet gebaseerd op een grondige analyse van de praktijk van rechtshandhaving. Ook als niet alle partijen aan te pakken zijn, is het mogelijk om deelname aan een blockchain te verbieden of aan strenge restricties te onderwerpen. Voor bona fide partijen zoals grote banken is dit een belangrijk beletsel.[190] Dergelijke maatregelen zouden erop neerkomen dat er informele of formele poortwachters ontstaan rond blockchainapplicaties. Zulke poortwachters bieden een concreet handvat voor handhaving.[191]

Dergelijke ontwikkelingen zouden gestimuleerd kunnen worden door duidelijke aansprakelijkheidsregels omtrent deelname aan de blockchain. Zoals bleek uit de analyse van de hack van The DAO is het wel degelijk mogelijk om een blockchain aan te passen: er is een governancestructuur, zij het impliciet,[192] en zo'n governancestructuur maakt het gemakkelijker om partijen aansprakelijk te stellen, wijzigingen af te dwingen, en dergelijke. Tot slot blijkt ook uit ontwikkelingen rond bitcoin dat overheden, als zij voldoende prioriteit geven aan een bepaalde partij, er in kunnen slagen om de uiteindelijke handelende individuen te vinden en te vervolgen, hun servers en tegoeden in beslag te nemen.[193] Zolang uiteindelijk mensen de controle uitoefenen over de nodes, is regulering mogelijk.[194] In de literatuur wordt inmiddels erkend dat regulering van blockchain ook wenselijk is, mede om de goede werking van blockchain te bevorderen.[195]

Dit alles neemt niet weg dat het decentrale, anonieme karakter van publieke blockchain het inderdaad voor individuen lastiger kan maken om een concrete wederpartij op de blockchain aan te spreken. Regulering van blockchain zal waarschijnlijk het effectiefst verlopen als deze is gericht op poortwachters.[196] Daarnaast zal internationale coöperatie de handhaving vergemakkelijken.[197] Wellicht zou de Nederlandse overheid zulke coöperatie moeten stimuleren, bijvoorbeeld door het aansturen op een wereldwijde regeling. Op dit moment zijn er slechts lokale wetgevingsinitiatieven.[198]

---

[188] Zie uitvoerig De Filippi & Wright 2018, hfdst. 11.
[189] Voor een permissioned blockchain is handhaving relatief eenvoudig aangezien een dergelijke blockchain een controlerend governance-mechanisme heeft, geïmpliceerd in de aanwezigheid van controle op de toelating en de daarmee geïmpliceerde overeenkomst (par. 3.2.1 en 3.2.2).
[190] Zo beginnen banken 2018 steeds huiveriger te worden van het zelfs indirect betrokken te zijn bij bitcoin-handel. Zie voor Nederland (https://www.sprout.nl/artikel/crypto/nederlandse-banken-weigeren-bitcoin-ondernemers), in de U.S.A. (https://www.theverge.com/2018/2/4/16971666/cryptocurrency-bitcoin-jpmorgan-chase-bank-of-america-citigroup-credit-card), in Zwitserland UBS (https://cointelegraph.com/news/ubs-chairman-cryptocurrencies-are-highly-speculative-investment-vehicles), Ierland (https://news.bitcoin.com/bitcoin-businesses-denied-banking-services-in-ireland/). Dit houdt (voor Nederland) verband met de onzekerheid of bitcoin afkomstig is van misdrijven en zou moeten worden gemeld in het kader van de Wwft.
[191] De Filippi & Wright 2018, p. 70, Finck 2019, p. 45-58, 182-210. Vgl. Walport 2015, p. 44. Zie ook par. 3.2.3.
[192] De Filippi & Loveluck 2016.
[193] Een voorbeeld is de vervolging van Silk Road.
[194] De Filippi & Wright 2018, p. 155, 175.
[195] Bijv. Werbach 2018a, o. 175-200. Ook uit de afgenomen interviews blijkt dat men in de blockchainindustrie in principe positief staat tegenover regulering en toezicht, mits dit op passende wijze plaatsvindt.
[196] De Filippi & Wright 2018, p. 52, 70, Finck 2019, p. 45-58.
[197] Finck 2019, p. 59-60.
[198] Zie het overzicht bij Finck 2019, p. 161-165.

Een bijzonder probleem is daarnaast dat een blockchain relatief autonoom functioneert: een individuele deelnemer heeft het in het algemeen niet in zijn macht om de blockchain te wijzigen, om informatie te wissen of transacties terug te draaien.[199] Hoewel de impliciete governance-structuur van een blockchain het gemakkelijker kan maken om de blockchain te wijzigen, kan dit in de praktijk – afhankelijk van allerlei omstandigheden, zoals de concrete opzet en het protocol van de blockchain – meer of minder gemakkelijk zijn. Men moet echter wel beseffen dat er technische mechanismen mogelijk zijn om handhaving te vergemakkelijken, ook als men niet alle concrete nodes van de blockchain fysiek kan achterhalen. Bijvoorbeeld zou er een wettelijke regel kunnen worden vastgesteld om lokale ISP's of node-beheerders te verplichten om de IP-adressen van niet-meewerkende node-beheerders te blokkeren en buiten de werking van het protocol te laten, waardoor deze voor wat betreft de 'legale' nodes niet meer kunnen bijdragen aan het vaststellen van nieuwe blokken. Een overheid die koste wat kost wil handhaven zou een wettelijke verplichting kunnen opnemen dat alle blockchaintoepassingen zo'n blokkademogelijkheid inbouwen,[200] en het strafbaar stellen om deel te nemen aan blockchaintoepassingen die hier niet aan voldoen.[201] Dit zou ook kunnen uitmonden in een vergunningensysteem of registratiesysteem voor blockchains en blockchaindeelnemers.[202] Dit zal geen 100%-handhaving opleveren,[203] aangezien deelnemers buiten de jurisdictie van de overheid hier mogelijk geen gevolg aan geven,[204] maar kan wel een belangrijke disincentive zijn.

In gevallen waar een wezenlijk Nederlands overheidsbelang aan de orde is bij een blockchain kan het wenselijk zijn dat wordt geëist dat de blockchain geheel in Nederland ligt, dat wil zeggen dat alle nodes in Nederland zijn gelegen.[205] Dat verkleint het risico van buitenlandse inmenging en maakt eenvoudige handhaving door de Nederlandse overheid mogelijk.

Hoewel handhaving op een blockchain lastig kan zijn (met name bij permissionless blockchains), zijn er verschillende reguleringsmogelijkheden om greep te krijgen op een blockchain: het aanwijzen of reguleren van poortwachters, internationale samenwerking, verlagen van drempels voor aansprakelijkheid voor betrokkenen bij blockchain, instellen van additionele eisen (of zelfs vergunningen of registratie-eisen) voor (medewerking aan) blockchains. Of het wenselijk is om dergelijke regels aan te nemen, valt buiten het bestek van dit onderzoek.

Wat betreft goederenrechtelijke vormen van handhaving (beslag en executie) geldt dat deze theoretisch lastig te plaatsen zijn en praktisch moeilijk uitvoerbaar kunnen blijken,[206] maar dat dit in sommige concrete gevallen wel praktisch te realiseren is.[207] Aannemelijk is dat de rechter de 'eigenaar' van een bitcointegoed kan verplichten om zijn privé-sleutel te gebruiken om een tegoed aan een bewaarder over te maken.[208] Op soortgelijke wijze kan voor andere blockchaintoepassingen een concrete deelnemer verplicht worden om een handeling op de blockchain te verrichten. Het

[199] De Filippi & Wright 2018, p. 49-52, 114-116.
[200] De Filippi & Wright 2018, p. 180 over de mogelijkheid om protocolwijzigingen e.d. af te dwingen van concrete miners.
[201] De Filippi & Wright 2018 p. 126 (ook 176), noemen ook de mogelijkheid van aansprakelijkheid voor het ondersteunen van 'illegale' diensten.
[202] De Filippi & Wright 2018, p. 183.
[203] De Filippi & Wright 2018, p. 126 wijzen erop dat het mogelijk blijft dat er voldoende andere deelnemers blijven die genoeg prikkels ontlenen aan fees om de blockchain draaiend te houden.
[204] De Filippi & Wright 2018, p. 145.
[205] Dit punt is naar voren gekomen uit de afgenomen interviews.
[206] Tweehuysen 2018, Bernardt en Van Vlastuin 2015, Van Ingen en Smits 2018, Biemans 2018, De Graaf en Krans 2018.
[207] Zie voor een voorbeeld http://www.bvd-advocaten.nl/blogs/beslaglegging-op-bitcoins-kan-dat: het beslag werd uitgevoerd doordat de deurwaarder computers met daarop wachtwoorden van de beslagene in beslag nam, en de beslagene (op straffe van dwangsom) werd verplicht om het bitcointegoed aan de deurwaarder over te maken (die dit tegoed bewaarde). De uitspraak waarnaar wordt verwezen is niet openbaar gemaakt.
[208] Vgl. HR 13 september 2013, NJ 2014/455 (Molenbeek), r.o. 3.9.9 ten aanzien van bewijsbeslag, en zie ook het in de vorige noot genoemde voorbeeld.

verdient aanbeveling om uitdrukkelijke regels vast te stellen om de juridische onzekerheid op dit punt weg te nemen. Verder verdient het aanbeveling dat nader onderzoek wordt verricht naar regels voor effectieve mogelijkheden voor verwezenlijking van beslag en tenuitvoerlegging van uitspraken.

Overigens is deze onduidelijkheid ook aanwezig op het (aan goederenrechtelijke handhaving verwante) gebied van faillissementsrecht.[209]

Beslag en uitvoering van rechterlijke uitspraken op blockchain is op dit moment mogelijk maar kan praktisch lastig uit te voeren zijn. Het verdient aanbeveling om de regels op dit punt te verhelderen en te verbeteren.

3.2.11 Identiteit

Een afzonderlijk punt van aandacht is de identiteit van gebruikers. De deelnemers (gebruikers en node-beheerders) aan de blockchain zijn bekend onder hun public key: zij zijn wat heet 'pseudoniem' (niet geheel anoniem, immers te identificeren aan hun public key, maar hun werkelijke identiteit is niet per se bekend). Hoewel het mogelijk is dat hun werkelijke identiteit bekend is, is dat niet noodzakelijk voor het functioneren van de blockchain. Dit roept een paar bijzondere vragen op.

Allereerst kan men zich afvragen of het juridisch mogelijk is om rechtshandelingen aan te gaan onder pseudoniem. Dit is inderdaad mogelijk. Het gaat er om dat de partij identificeerbaar is, en dat hoeft niet per se door het weten van de werkelijke identiteit. Als je een kop koffie op het station koopt zal je meestal ook geen identificatie geven, terwijl niet wordt betwist dat er een geldige overeenkomst tot stand komt. Ook de koop van een chocoladereep uit een automaat is een geldige rechtshandeling.

Het gebruik van pseudoniem kan wel problematisch zijn in gevallen waar het nodig is nader onderzoek te doen naar de werkelijke partij. Een voorbeeld is de notaris, die de wilsbekwaamheid van partijen en de afwezigheid van dwang moet onderzoeken.[210] Daarnaast eist financiële regelgeving (ter bescherming van de consument[211] en ter bestrijding van witwassen) dat banken en andere financiële instellingen weten wie hun klant is (know-your-customer principe).[212] Deze regels staan in de weg aan het gebruik van blockchaintechnologie in deze sectoren, tenzij partijen naast de public key ook hun werkelijke identiteit kenbaar en controleerbaar maken. Ook geldt dat de regels inzake 'diensten van de informatiemaatschappij' eisen dat zo'n dienstverlener zijn identiteit bekend maakt (par. 3.2.7c).

In dergelijke gevallen zijn deze regels ingesteld om bepaalde (algemene) belangen te waarborgen, zoals de bestrijding van terrorisme en fraude of de bescherming van consumenten. Deze regels kunnen daarom niet zomaar worden afgeschaft omdat zij bepaalde blockchaintoepassingen bemoeilijken. De keuze om deze regels aan te passen is uiteindelijk een (rechts)politieke, waarbij een rol speelt dat deze regels vaak gebaseerd zijn op Europese regelgeving en daarom niet door de Nederlandse wetgever kunnen worden gewijzigd.

De pseudonimiteit van deelnemers aan een blockchain is in het algemeen geen probleem, maar kan obstakels opleveren voor bepaalde gevallen waar is vereist dat de werkelijke identiteit van een deelnemer bekend is. De (Europese) wetgever zal moeten beoordelen of zulke regels moeten worden aangepast, gelet op de belangen die deze regels moeten waarborgen.

3.2.12 Toepasselijk recht en jurisdictie[213]

Een voor de praktijk belangrijke vraag is welke regels van welk land van toepassing zijn bij geschillen over blockchain. Het gaat dan om twee vragen: welke rechter is bevoegd (jurisdictie), en

[209] Beerepoot 2018, Van Ingen & Smits 2018b.
[210] Tjong Tjin Tai, 2018a (preadvies KNB), p. 106 en 118.
[211] Zie bijv. art. 4:23 Wft.
[212] VBW-studie 2017, p. 35. Zie o.a. de Wwft en de vijfde anti-witwasrichtlijn 2018/843 (Anti-Money Laundering directive, AMLD 5) die per 9 juli 2018 de vorige vierde, richtlijn 2015/849 wijzigt.
[213] Zie ook Garau Sobrino 2017, die dit probleem alleen aanstipt, Vauplane 2018 over securities. Raskin 2015 pleit voor een afwijkende benadering, waar bitcoin als 'property' zou moeten worden opgevat om jurisdictiegeschillen op te lossen. Dit is niet in overeenstemming met het geldende recht.

welk rechtsstelsel is van toepassing. Dit wordt geregeld door het rechtsgebied van Internationaal Privaatrecht (IPR). Vanwege de technische aard van dit deelgebied is de analyse in deze paragraaf helaas onvermijdelijk moeilijker leesbaar.[214] In de conclusie aan het slot wordt alles samengevat.

Voor de behandeling van IPR-vragen is het van belang helder te hebben voor welke rechtsverhouding de vraag beantwoord wordt. Bijvoorbeeld: een Duits bankenconsortium bouwt op basis van blockchain software van een Zwitserse aanbieder een systeem waarin effecten verhandeld kunnen worden via smart contracts. Dan kan bijvoorbeeld een Nederlander via een smart contract effecten verkopen aan een Belg. Uit dit eenvoudige voorbeeld kunnen al direct een aantal zaken geleerd worden. Ten eerste zijn sommige van deze vragen niet bijzonder voor blockchain, zoals in het voorbeeld de levering van software. In de tweede plaats is duidelijk dat de vraag niet steeds globaal voor de blockchain beantwoord kan worden. Op de verhouding tussen het bankenconsortium en de Nederlandse gebruiker van het handelssysteem kan ander recht van toepassing zijn dan op de verhouding tussen de Nederlander en de Belg die een smart contract sluiten met elkaar. In de derde plaats is te verwachten dat professionele partijen meestal uitdrukkelijk afspraken maken over toepasselijk recht en bevoegde rechter om eventuele onduidelijkheden voor te zijn.

Problemen in de context van toepasselijk recht en jurisdictie zullen zich dan ook vooral voordoen waar de default regels van Rome I Verordening 593/2008 of EEX-verordening 1215/2012 toegepast moeten worden en dan vooral waar deze regels plaatsaanduidingen bevatten. Deze problemen kunnen meer conceptueel of meer feitelijk van aard zijn. Een conceptueel probleem doet zich voor waar onduidelijk is hoe een plaatsaanduiding op een blockchain toegepast moet worden. Bijvoorbeeld: wat is “de plaats waar de verbintenis … uitgevoerd moet worden” in een blockchain?[215] Een meer feitelijk probleem doet zich voor indien een plaats feitelijk niet vast te stellen is: de “woonplaats van de gedaagde” is conceptueel helder maar feitelijk niet vast te stellen indien de beoogde gedaagde anoniem is.

Gelet op de verkennende aard van dit onderzoek is het niet mogelijk om de uitgangspunten en alle regels van IPR te behandelen en uit te leggen. Daarom zal hier slechts voor de belangrijkste soorten gevallen geschetst worden hoe het IPR ongeveer werkt, om te laten zien dat men de gewone IPR-regels probleemloos kan toepassen. In Nederland gelden, voorzover beide partijen woonachtig zijn in EU-lidstaten die onder de toepasselijke regelgeving vallen, de Verordening Rome I 593/2008 en art. 7 lid 1 EEX-Verordening 1215/2012 (herschikking). Als niet bekend is wat de nationaliteit en woonplaats van de wederpartij is, kunnen deze verordeningen niet worden toegepast en geldt het algemene Nederlandse IPR (boek 10 BW). Het is op zichzelf denkbaar dat wel valt vast te stellen dat de wederpartij in Europa woonachtig is[216] maar niet valt te bepalen in wel land hij precies woont.[217]

Rechterlijke bevoegdheid

Voorzover het gaat om een ‘Europees’ geval gelden wat jurisdictie betreft de volgende hoofdregels.

De rechter van woonplaats van de gedaagde is in beginsel bevoegd (art. 4 EEX-Vo). Bij een vordering op basis van *onrechtmatige daad* geldt daarnaast art. 7 punt 2 EEX-Vo 1215/2012 wat als alternatief aanknopingspunt geeft de plaats van ontstaan van schade, naast eventueel het centrum van de belangen van de geschade rechtspersoon.[218] Zie Shevill[219] en eDate.[220] en HvJ 17 oktober

[214] De analyse is toch opgenomen, omdat anders niet onderbouwd is hoe wij tot onze conclusies komen.
[215] Art. 7(1)(a) EEX-Verordening 1215/2012.
[216] Bijvoorbeeld door de gebruikte taal, gegevens van de gebruikte ISP, IP-adres e.d. Dit alles zal ook afhangen van de concrete blockchainapplicatie.
[217] Bijvoorbeeld omdat de gebruikte taal in diverse landen wordt gebruikt, e.d.
[218] HvJ 17 oktober 2017, C-194/16 (Bolagsupplysningen).
[219] HvJ 7 maart 1995, C-68/93 (Shevill e.a.).
[220] HvJ 25 oktober 2011, C-509/09 en C-161/10 (eDate Advertising), zie Tjong Tjin Tai 2017c, nr. 34. Zie ook HR 3 juni 2016, ECLI:NL:HR:2016:1054.

2017, C-194/16 (Bolagsupplysningen). ‘Schade’ houdt niet slechts in het schadebrengende feit, maar ook nadelige gevolgen daardoor kunnen bijvoorbeeld nadelige vermogensconsequenties worden gelocaliseerd in het land waar het slachtoffer een bankrekening heeft.[221] Het volstaat echter niet dat er alleen nadelige vermogensconsequenties zijn: als het schadebrengende feit in een andere lidstaat plaatsvond ligt het voor de hand dat de rechter van die andere lidstaat bevoegd is, en kan de rechter van de lidstaat waar de vermogensconsequenties zich voordoen alleen bevoegd zijn als er ook andere aanknopingspunten met die lidstaat zijn.[222] Als de daad op de blockchain plaatsvond, is er geen locatie voor het schadebrengende feit zelf. Het is niet geheel zeker of in zo’n geval dan vanzelf het land kan worden gekozen waar eiser/slachtoffer de nadelige gevolgen ondervindt, of dat er nog steeds additionele aanknopingspunten nodig zijn.

Voorzover het gaat om een *overeenkomst* is bepalend de plaats van uitvoering (art. 7 punt 1 EEX-Vo). Dit kan lastige vragen veroorzaken als de uitvoering geschiedt op de blockchain: bijvoorbeeld een partij betaalt de andere partij voor een wijziging op de blockchain.[223] In een dergelijk geval is er als aanknopingspunt altijd nog de woonplaats van de gedaagde (mits bekend en in Europa, zie anders hierna). Er is dus nooit een geval dat er geen bevoegde rechter is. Overigens is het zeer wel mogelijk dat de uitvoering ook ten dele in de fysieke wereld plaatsvindt (zoals bij een smart contract over de koop van een boek).

Voor een *niet-Europees geval* gelden voor de jurisdictie van de Nederlandse rechter art. 1-14 Wetboek van Burgerlijke Rechtsvordering.[224] Deze regels vertonen grote gelijkenis met de regels van de EEX-Verordening. De Nederlandse rechter is bevoegd indien gedaagde in Nederland woont (art. 2 Rv), als de (verbintenis uit de) overeenkomst in Nederland moet worden uitgevoerd (art. 6 sub a Rv), en bij onrechtmatige daad als het schadebrengende feit zich in Nederland heeft voorgedaan of kan voordoen (art. 6 sub e Rv).

Verder kunnen partijen uiteraard een keuze maken voor een bevoegde rechter. Aan de geldigheid van zo’n forumkeuze worden relatief strenge eisen gesteld, om te waarborgen dat partijen hier uitdrukkelijk voor kiezen.[225]

Bovendien geldt de vangnetbepaling van art. 9 sub b Rv: als een gerechtelijke procedure buiten Nederland onmogelijk blijkt, is de Nederlandse rechter bevoegd (forum necessitatis). Naar Nederlands IPR is het daarom niet mogelijk dat geen enkele rechter bevoegd is.

Toepasselijk recht

Ook hier behandelen we eerst Europese gevallen.

Bij verbintenissen uit *overeenkomst*, geeft de Verordening Rome I regels over het toepasselijke recht. Een professionele blockchain-aanbieder kan eisen dat node-beheerders en gebruikers akkoord gaan met algemene voorwaarden of een gebruiksovereenkomst voor de blockchain en daarin een rechtskeuzebeding opnemen. Rome I laat een door partijen overeengekomen rechtskeuze in ruime mate toe. De rechtskeuze zet doorgaans het dwingend en aanvullend recht van het land wiens recht toepasselijk zou zijn geweest zonder rechtskeuze opzij. De gemaakte rechtskeuze moet dan echter wel vallen binnen de raamwerkcondities die Rome I aan een vrije rechtskeuze stelt. Ten eerste moeten er aanknopingspunten in het gekozen land liggen. Ten tweede kan een rechter de rechtskeuze passeren wanneer overwegingen van openbare orde daartoe aanleiding geven. Ten derde gelden voor consumenten in diverse gevallen bijzondere beschermingsregels, waardoor vaak het rechtsstelsel van de consument van toepassing is, of

[221] HvJ 28 januari 2015, C-375/13, ECLI:EU:C:2015:37, NJ 2015/332 (Kolassa/Barclays Bank) voor een gedupeerde belegger.
[222] HR 15 september 2017, ECLI:NL:HR:2017:2358 (Universal Music), verwijzend naar de in die zaak gegeven prejudiciële beslissing HvJ 16 juni 2016, Zaak C-12/15, ECLI:EU:C:2016:449 (Universal Music/Schilling).
[223] Bij een smart contract is mogelijk dat een deel van de verplichtingen in de fysieke werkelijkheid worden uitgevoerd, zoals de levering van een pakket of de verhuur van een hotelkamer.
[224] Behoudens eventuele bijzondere verdragen.
[225] Art. 25 Herschikking EEX-Verordening 1215/2012, art. 8 Rv.

beschermende regels uit dat rechtsstelsel van toepassing blijven als er voor een ander rechtsstelsel is gekozen.[226]

Bij afwezigheid van een gemaakte rechtskeuze wordt het toepasselijk recht bepaald door de regels die Rome I daaromtrent geeft. Als er een eigenaar of facilitator is die de blockchain bij wijze van dienstverlening aanbiedt dan is het recht van het vestigingsland van de aanbieder[227] van toepassing (art. 4 lid 1 sub b Rome I). Probleem is dat de kenmerkende prestatie (verwerken van transacties) wordt geleverd door de 'gemeenschap', de node-beheerders. Deze lijken dus de aanbieder te zijn. Maar deze node-beheerders kwalificeren normaal gesproken niet als een rechtspersoon en zijn dus niet als geheel juridisch relevant voor het IPR: de verhoudingen zijn daar te los voor.[228]

Indien geen sprake is van dienstverlening dan is het recht van toepassing van het land waar de partij die de meest kenmerkende prestatie van de overeenkomst verricht haar gewone verblijfplaats heeft (art. 4 lid 2 Rome I). Indien op basis van het bovenstaande geen recht aangewezen kan worden, wordt voor bepaling van het toepasselijk recht bezien met welk land de overeenkomst de nauwste aanknopingspunten heeft (art. 4 lid 4 Rome I). Bij toepassing van art. 4 lid 2 of 4 Rome I kunnen velerlei potentiële aanknopingspunten in aanmerking komen: waar staan de servers? Waar wonen de betrokken gebruikers? Welke valuta worden gebruikt?[229] Dit geeft aanleiding tot onzekerheid.

Voor *onrechtmatige daad* geldt als hoofdregel dat het recht van het land waar de schade zich voordoet van toepassing is, ongeacht het land waar het schadebrengende feit zich voordeed of waar indirecte gevolgen zich voordoen (art. 4 lid 1 Rome II). Als beide partijen in hetzelfde land wonen is dat recht van toepassing (art. 4 lid 2 Rome II). Als een ander land een kennelijk nauwere band heeft met het geval is het recht van dat land van toepassing (art. 4 lid 3 Rome II). In het geval van activiteit op de blockchain zal de directe benadeling op de blockchain geen locatie aanwijzen nu de blockchain zelf geen locatie is, dus zal men terugvallen op verdere nadelige gevolgen, die zich in het algemeen zullen voordoen bij de woonplaats van de benadeelde.[230]

Indien derde landen betrokken zijn, wordt bepaling van het toepasselijke recht uiteraard ingewikkelder. Wat betreft Nederlands IPR kan het volgende worden opgemerkt.[231]

Wat betreft toepasselijk recht geldt, zoals gezegd, boek 10 BW. Voor overeenkomst en o.d. verklaren art. 10:153-159 BW in essentie de regels van Rome II van overeenkomstige toepassing. De hierboven gegeven analyse geldt dus ook voor niet-EU gevallen.

Onder deze regels kunnen partijen een keuze maken voor een toepasselijk rechtsstelsel. Aan de geldigheid van zo'n rechtskeuze worden relatief strenge eisen gesteld, om te waarborgen dat partijen hier uitdrukkelijk voor kiezen.[232]

Voor staatlozen geeft art. 10:16 BW aan dat, indien 'zijn' recht' van toepassing is, dan het recht van het land van zijn gewone verblijfplaats geldt.

Oproeping

Als laatste een korte opmerking over de oproeping van partijen. Bij blockchain kunnen er twee complicaties optreden: de woonplaats van de wederpartij is niet bekend, en de identiteit van de wederpartij is niet bekend. Het eerste is niet problematisch, het tweede wel.

[226] Art. 6 lid 1 en 2 Rome I. En zie voor bescherming ten aanzien van bevoegdheid art. 17-19 Herschikking EEX-Verordening 1215/2012.
[227] Dit is problematisch, aangezien niet duidelijk is wie de aanbieder is: dit komt terug bij .
[228] Zie ook Cafaggi en Clavel 2011 over IPR bij netwerken. Vgl. ook Polak 1993.
[229] Schuringa 2017, p. 373.
[230] Vgl. HvJ 7 maart 1995, C-68/93 (Shevill e.a.) en HvJ 25 oktober 2011, C-509/09 en C-161/10 (eDate Advertising).
[231] Het navolgende geldt behoudens eventuele bijzondere verdragen.
[232] Art.3 lid 1 Verordening Rome I 593/2008, art. 10:10 BW.

Als een eiser een wederpartij wil dagvaarden[233] gelden daarvoor de gewone regels qua termijn en wijze van oproeping.[234] Dat er een blockchain bij betrokken is maakt dit niet anders. Bij een in Nederland wonende partij geldt dat bij het woonadres wordt gedagvaard (art. 46 Rv). Bij een in het buitenland wonende partij geldt dat als bekend is op welk adres de partij woont, dat op dat adres kan worden betekend volgens de regels van art. 55 en 56 Rv, waarbij (afhankelijk van het aan de orde zijnde andere land) de Betekeningverordening II of het Haags Betekeningsverdrag moet worden gevolgd. Als niet bekend is wat het adres[235] is van de partij kan op grond van art. 54 lid 2 Rv bij zogenaamd openbaar exploot worden betekend.[236] Vervolgens kan een gewone procedure worden gevolgd; overigens kan het wel lastig zijn om een uitspraak te executeren als het adres van de wederpartij niet bekend is.

Verder is mogelijk dat de werkelijke identiteit van de wederpartij niet bekend is. In dat geval is volgens het huidige recht geen directe oplossing mogelijk. Art. 61 Rv biedt weliswaar de mogelijkheid om anonieme partijen te dagvaarden, maar dit geldt alleen in het specifieke geval van krakers van een bebouwde onroerende zaak. Op zichzelf valt overigens wel te verdedigen dat een deze bepaling bij analogie kan worden toegepast als er geen andere mogelijkheid is om de identiteit van de wederpartij te achterhalen en er alles aan is gedaan de wederpartij op de hoogte te stellen van de procedure:[237] eiser zou immers anders geen toegang tot de rechter hebben, wat op gespannen voet staat met art. 6 EVRM.[238] Het is onzeker of de rechter dit uiteindelijk zal toelaten.

De mogelijkheid om een anonieme wederpartij te dagvaarden lijkt slechts van theoretisch belang. Als het immers niet mogelijk is om de identiteit en/of woonplaats van de wederpartij te achterhalen, hoe kan dan een gunstige uitspraak ten uitvoer worden gelegd? Inderdaad kan dit lastig zijn als de aan de orde zijnde blockchain geen mogelijkheden voor tenuitvoerlegging van rechterlijke uitspraken heeft ingebouwd. Toch gaat het hierbij niet louter om een theoretische mogelijkheid. Het is bijvoorbeeld denkbaar dat tenuitvoerlegging slaagt door derdenbeslag, doordat de wederpartij een account heeft bij een Nederlandse bitcoinbeurs.[239] Een ander voordeel van zo'n verstekvonnis kan zijn dat het hierdoor mogelijk is om onmiddellijk executiemaatregelen te treffen zodra de identiteit van de wederpartij alsnog bekend is geworden: er hoeft dan niet te worden gewacht op een rechterlijke uitspraak.

Conclusies en aanbevelingen

IPR-regels geven concrete uitkomsten: er is altijd een bevoegde rechter en een toepasselijk recht. Het probleem met blockchain is dat de uitkomst van de IPR-regels niet altijd zeker is, en dat het mogelijk is dat er rond een blockchain, afhankelijk van het geschil en de betrokken partijen, verschillende bevoegde rechters en toepasselijke rechtsstelsels zijn. Dit is een gevolg van het gegeven dat IPR uitgaat van aanknopingspunten in de fysieke wereld, en 'virtuele' aanknopingspunten negeert omdat die niet bij een bepaalde lidstaat aansluiten: bij een geschil over blockchain is mogelijk dat de meeste aanknopingspunten virtueel zijn en daardoor relatief

[233] In sommige zaken kan de nieuwe (zogenaamde 'KEI')-wetgeving inzake Burgerlijke rechtsvordering van toepassing zijn. Omdat dit alleen bij de Hoge Raad en enkele rechtbanken in bepaalde zaken het geval is, zal deze mogelijkheid hier niet verder worden besproken. Deze wetgeving leidt niet tot wezenlijk andere resultaten; het belangrijkste verschil is dat er andere terminologie wordt gebruikt.

[234] Voor de wijze van betekening van de dagvaarding zie art. 45 e.v. Wetboek van Burgerlijke Rechtsvordering, en voor de termijn zie art. 114-117 Wetboek van Burgerlijke Rechtsvordering.

[235] Woonadres en/of werkelijk verblijf.

[236] Het maakt hierbij niet uit of er bekend is dat hij wel in een bepaald land (Nederland of een ander land) woont of verblijft, het draait erom dat er geen concreet woonadres of werkelijke verblijfplaats bekend is.

[237] Vgl. Rb Amsterdam 5 maart 2009, ECLI:NL:RBAMS:2009:BH7006, wat overigens krakers van een onbebouwde onroerende zaak betrof en dus dicht tegen het in art. 61 Rv geregelde geval lag.

[238] Het belang van de wederpartij om van de procedure op de hoogte te zijn zou dan op andere wijze moeten worden bereikt dan met een gewone dagvaarding, en zou bijvoorbeeld kunnen door middel van elektronische communicatie via de blockchain.

[239] Zie par. 3.2.10 over beslag op bitcoin.

ondergeschikte fysieke aanknopingspunten de doorslag geven, wat tot zeer uiteenlopende uitkomsten kan leiden. Dit is onbevredigend.[240]

Verder leidt het ontbreken van een locatie bij samenwerking op de blockchain ook tot afgeleide complicaties. Een voorbeeld is een samenwerking die daarna moet worden geformaliseerd in een traditionele rechtspersoon. Daarbij kan de vraag ontstaan in welk land de inbreng/funding is geschied: als die inbreng op de blockchain is verricht is er geen duidelijke locatie.[241]

Vanwege deze problemen verdient het aanbeveling dat er in internationaal verband regels worden opgesteld die de internationale dimensie van blockchaingeschillen in goede banen leiden. Te denken valt aan een alternatieve bevoegdheid van de rechter waar de core developers van de blockchain zijn gevestigd. Een andere (praktisch misschien moeilijk te verwezenlijken) mogelijkheid zou zijn de oprichting van een bijzonder internationaal gerechtshof voor blockchaingeschillen.[242]

Los van deze mogelijkheden kunnen core developers en node-beheerders problemen voorkomen door uitdrukkelijk een overeenkomst te (laten) sluiten waarbij een bevoegde rechter en toepasselijk recht worden aangewezen.[243] Ook gebruikers kunnen zelf (proberen)[244] afspraken te maken met andere partijen.

Bij blockchain kunnen de gewone regels van het internationaal privaatrecht worden toegepast om te bepalen welk rechtsstelsel van toepassing is en welke rechter bevoegd is om over het geschil te oordelen. Een probleem is dat de uitkomsten van die regels zeer uiteenlopend kunnen zijn, afhankelijk van relatief ondergeschikte omstandigheden. Dit komt doordat het belangrijkste element, de blockchain zelf, niet gerelateerd is aan een bepaalde staat. Dit kan alleen worden opgelost door internationale samenwerking om regels op te stellen over blockchain, mogelijk door oprichting van een internationaal gerechtshof voor blockchaingeschillen. Daarnaast kunnen problemen in de praktijk worden vermeden door bij een permissioned blockchain in een overeenkomst bedingen op te nemen waarbij een toepasselijk recht en een bevoegde rechter worden aangewezen (rechtskeuze en forumkeuze).

3.2.13 Gevolgen voor (juridische) beroepen?

Uit de analyse hierboven blijkt dat blockchaintechnologie diverse taken kan vervullen die tot op heden vooral door juristen en andere beroepsgroepen werden vervuld. Er wordt dan ook al sinds enkele jaren uitvoerig gediscussieerd over de vraag wat blockchain zal betekenen voor de toekomst van juridische beroepen en andere beroepen. Een uitvoerige analyse zou een apart onderzoek vereisen. Hier kunnen alleen enkele voorlopige inschattingen worden gegeven voor een paar beroepen.

Blockchaintechnologie heeft in zekere zin op ieder beroep invloed, net zoals de telefoon, e-mail en tekstverwerker de dagelijkse uitvoering van het werk sterk veranderd hebben. Maar daaruit volgt niet dat de wezenlijke functie van een beroep ook wordt gewijzigd door blockchain. Bijvoorbeeld accountancy gaat niet zozeer om het vastleggen van transacties maar om de controle op de financiële administratie. Accountants zullen in de toekomst misschien kennis van blockchain moeten hebben, zoals zij ook moeten begrijpen hoe een geautomatiseerde boekhouding werkt, maar zulke technische kennis verandert het beroep niet essentieel.

Voor bepaalde beroepen lijkt blockchaintechnologie echter wel kerntaken te vervangen. Zoals uit de analyse hierboven blijkt is blockchaintechnologie met name geschikt voor bepaalde taken:

- vertrouwensdiensten waarbij identiteit moet worden geverifieerd,

[240] Vauplane 2018, p. 102.
[241] In iets andere vorm gegeven in een interview.
[242] Dit kan ook laagdrempelig, zoals de manier waarop domeinnaamgeschillen worden beslecht door een vorm van e-arbitrage.
[243] Een voorbeeld is Ethereum. Zie https://www.ethereum.org/terms-of-use, par. 'Governing Law and Jurisdiction', waarin Zwitsers recht van toepassing wordt verklaard en het gerecht te Zug (Zwitserland) bevoegd wordt verklaard.
[244] Of dit daadwerkelijk mogelijk is hangt onder meer af van de opzet van de blockchain, de communicatiemogelijkheden en de bereidwilligheid van de andere partijen.

- automatische uitvoering van gestandaardiseerde taken, zoals verwerking van elektronische documenten,
- automatische uitvoering van (eenvoudige en complexe) betalingstransacties, en
- registratie ten behoeve van bewijs.

Zulke taken worden ook door juristen uitgevoerd. Een voorbeeld is het zogenaamde 'passeren van akten' door een notaris:[245] de notaris stelt bijvoorbeeld de leveringsakte van een huis op, ontvangt de partijen op zijn kantoor, controleert dat zij zijn wie zij zeggen (door controle van identiteitsbewijzen), leest de akte voor en legt deze uit, laat de partijen en getuigen ondertekenen, en zorgt voor de verdere afhandeling van de akte (zoals de inschrijving van de akte in het desbetreffende register, maar ook de financiële afwikkeling, en het archiveren van de akte). Deze taken kunnen voor een deel door blockchaintechnologie worden vervangen. Het kadaster zou in de vorm van een blockchain kunnen worden ingericht,[246] de leveringsakte is dan een transactie op de blockchain, het is niet nodig partijen fysiek op kantoor te zien, identiteitscontrole vindt plaats aan de hand van *private keys*, en de transactie blijft 'gearchiveerd' op de blockchain. De kernfunctie is dan technisch op de blockchain gezet en de notariële tussenkomst is in zoverre overbodig.

Maar de taken van een notaris zijn breder dan alleen het zuiver technische passeren van de akte.[247] De notaris moet onder meer letten op:

- de wilsvorming van partijen: begrijpen partijen echt wat zij doen[248] en willen zij dit zelf, of is er sprake van dwang?
- zijn partijen echt wie zij zeggen te zijn?[249] Zijn zij bevoegd om een bedrijf te vertegenwoordigen?
- de juistheid van de akte: is deze duidelijk, wordt hiermee bereikt wat de bedoeling is?[250]
- onrechtmatige benadeling van partijen, bijvoorbeeld door een carrouselfraude waarbij een onroerende zaak een paar keer achter elkaar snel wordt doorverkocht tegen een kunstmatig hoge verkoopprijs, om de schijn te wekken dat het veel waard is, of doordat een huis dat al verkocht is tegen de afspraak in aan een derde wordt geleverd,
- publieke belangen, zoals witwassen of financiering van terrorisme.[251]

Dit zijn taken ter bescherming van zwakkere partijen (die bijvoorbeeld minder handig zijn met technologie, geen hoge opleiding hebben genoten e.d.), derden (dus anderen die nadeel zouden ondervinden van transacties, bijvoorbeeld doordat er fraude wordt gepleegd), en publieke belangen (zoals het tegengaan van witwassen en financiering van terrorisme). Zulke taken zijn lastig tot onmogelijk te automatiseren met gewone blockchaintechnologie.[252] Het is niet voldoende om te zeggen dat partijen maar zelf verantwoordelijk moeten zijn voor de juistheid van de transactie: een onduidelijke of onjuiste akte kan ook buitenstaanders benaderen (bijvoorbeeld latere kopers die moeten weten welke afspraken er zijn tussen buren). De wetgever heeft er daarom bewust voor gekozen om vast te houden aan de verplichte rol van de notaris bij bepaalde transacties.

De wetgever kan ervoor kiezen om deze publieke belangen te laten vallen en de verplichte rol van de notaris te verkleinen. Of dit wenselijk is, is een rechtspolitieke keuze.

Een vergelijkbare analyse kan worden gemaakt voor ieder beroep. De uitkomst hiervan zal wisselen, afhankelijk van het beroep dat aan de orde is. Zie bijvoorbeeld ook par. 3.2.8 over de mogelijkheden

[245] Melis/Waaijer 2019, hfdst. 6-9.
[246] Dit heeft diverse nadelen, zie Use-case 1.
[247] In Tjong Tjin Tai 2018a is een gedetailleerde analyse te vinden.
[248] Het gaat er dan niet om dat zij precies alle voorwaarden van (bijvoorbeeld) een hypotheek snappen, maar wel begrijpen dat zij aansprakelijk zijn als de hypothecaire lening niet wordt terugbetaald.
[249] Controle met alleen een private key is onvoldoende betrouwbaar voor identiteitscontrole, aangezien een private key kan worden gestolen. Dit gebeurt bijvoorbeeld regelmatig met bitcoin.
[250] Dit is lastig te automatiseren doordat er veel verschillende en gecompliceerde situaties kunnen bestaan.
[251] De notaris moet bijvoorbeeld letten op de herkomst van gelden, onder meer ter uitvoering van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).
[252] Misschien zouden deze taken (deels) door geavanceerde algoritmen worden uitgevoerd. Dat valt echter buiten het bestek van dit onderzoek.

en beperkingen van smart contracts: dit is relevant voor de rol van juristen als adviseurs bij contracten. Als moet worden onderzocht of blockchaintechnologie een bepaald beroep kan vervangen, moet ook worden bekeken of de taken van het beroep breder zijn dan alleen de taken die een blockchain kan vervangen. Vaak moeten ook belangen van derden of publieke belangen worden gewaarborgd, en is het moeilijk om die belangen puur automatisch te beschermen. Daarnaast wordt bij blockchaintechnologie in het algemeen verwacht dat gebruikers in staat zijn zelf op te letten op risico's en zelf kunnen kiezen voor de gevolgen van hun handelingen. Zulk inzicht kan niet van iedere burger worden verwacht. Ook hierom kan hulp van beroepsbeoefenaren nodig blijven.

3.3 Algemene Verordening Gegevensbescherming

In de literatuur is meermalen gewezen op de potentieel problematische verhouding tussen de verwerking van persoonsgegevens in blockchains en de AVG.[253] Blockchain is een technologie die een aantal eigenschappen bezit die op gespannen voet zouden staan met de bescherming van persoonsgegevens zoals vereist door de AVG. MEP Jan Philipp Albrecht heeft zelfs te kennen gegeven dat volgens hem: [254]

> 'Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design. This does not mean that blockchain technology, in general, has to adapt to the GDPR, it just means that it probably can't be used for the processing of personal data.'

Dit is een nogal vergaand uitgangspunt. Hierna wordt een analyse van knelpunten gegeven.

3.3.1 Verantwoordelijke en verwerker

Deze paragraaf geeft aan wie als verantwoordelijke en verwerker kunnen worden aangewezen binnen een blockchaincontext. Daarbij wordt in het bijzonder bezien tot welke moeilijkheden het toepassen van deze concepten uit de AVG aanleiding kan geven in de vaak horizontale verhoudingen tussen actoren in een blockchain en hoe de belangen van betrokkenen daarbij onder druk kunnen komen te staan.

3.3.1.1 Algemeen

De AVG definieert de verantwoordelijke als degene die 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.[255] In een blockchain context kan vaak een centrale partij onderscheiden worden die verantwoordelijk is voor het aanbieden van een dienst. Deze partij zal vaak ook als verantwoordelijke in de zin van de AVG kunnen worden beschouwd (aangenomen dat de dienst het verwerken van persoonsgegevens omvat). Deze partij kiest het doel (de dienst) en de middelen (bijv. een smart contract). Bijvoorbeeld indien de staat een permissioned blockchain gebruikt kan zij zelf als verwerkingsverantwoordelijke aangemerkt worden.[256] Een ander voorbeeld is een online winkel die als smart contract op een blockchain wordt aangeboden. De winkelier is hier verantwoordelijk voor de verwerking van persoonsgegevens die in het kader van het winkelen worden verzameld. Of de onderliggende blockchain permissioned of permissionless is maakt hier niets uit. Net zoals de houder van een traditionele webshop verantwoordelijke is voor de verwerking van persoonsgegevens die in het kader van online winkelen worden verzameld. Daar is ook niet relevant hoe de governance over het onderliggende internet is geregeld. Een ander voorbeeld is een verzekeraar die via een smart contract (dat is gewoon code) een formulier aanbiedt om schades te claimen.[257] De verzekeraar is verantwoordelijk voor de verwerking van persoonsgegevens in de

[253] Mayer 2018.
[254] Mayer 2018.
[255] Art. 4 sub 7 AVG.
[256] Finck 2019, p. 101.
[257] Voorbeeld ontleend aan CNIL 2018.

ingevulde formulieren. Ook een oracle dat persoonsgegevens aanreikt aan een smart contract zal doorgaans als verantwoordelijke worden aangemerkt voor de levering van persoonsgegevens.
Wie een dienst aanbiedt zal doorgaans uit het dienstaanbod blijken. Bijvoorbeeld degene die zich in een smart contract als aanbieder van de dienst presenteert. Indien een dienst anoniem wordt aangeboden dan zal op een andere wijze achterhaald moeten worden wie de dienst aanbiedt. Wie het smart contract op de blockchain heeft geplaatst zou daarvoor een aanwijzing kunnen zijn.

Hoewel blockchain decentraliteit hoog in het vaandel heeft staan, is het toch vaak mogelijk een centrale partij aan te wijzen die als verwerkingsverantwoordelijke kan functioneren, zelfs in permissionless blockchains.

3.3.1.2 Bijzonder geval: permissionless blockchains

Echter, niet altijd zal een centrale dienstverlener aangewezen kunnen worden in een permissionless blockchain. Wie is bijvoorbeeld verantwoordelijk voor het verwerken van bitcoin transacties?

> De core developers zijn wel een centrale partij: zij hebben core-code die de dienst (bitcoin transacties) mogelijk maakt geschreven. Niettemin, liggen zij als verantwoordelijke(n) minder voor de hand. Als leveranciers van de software gaan er geen persoonsgegevens door hun computersystemen. Bovendien kunnen de core developers geen node-beheerders verplichten om hun software of updates daarvan te gebruiken. Zij bepalen niet doel of middelen.

Indien er geen smart contract is en de dienst bouwt op de core code, zijn de nodes en gebruikers de meest gerede kandidaten om als verantwoordelijken aangewezen te worden in een permissionless blockchain. Wie van hen als verantwoordelijken gelden, hangt in sterke mate af van de duiding van hun onderlinge verhouding. Hieronder worden drie perspectieven op hun onderlinge verhouding gegeven.

1. De gebruikers vormen een P2P netwerk. De node-beheerders zijn slechts steunverleners.

De gebruikers van bitcoins vormen met elkaar een peer-to-peer netwerk. De miners en full node-beheerders zijn niet meer dan technisch steunverleners die er als het ware tussenuit vallen en hooguit als verwerkers van persoonsgegevens aan bod komen (zie hieronder). De gebruikers zijn verantwoordelijken voor de persoonsgegevens, die zij op de blockchain schrijven.[258] De Franse CNIL omschrijft dit als “les participants, qui ont un droit d’écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs peuvent être considérés comme responsables de traitement.”[259] Voor een gebruiker die handelt in de uitoefening van beroep of bedrijf is dit helder. Een gebruiker die handelt als privépersoon kan volgens de CNIL een beroep doen op de huishoudexceptie.[260] Dan zou hij niet een verantwoordelijke voor de betreffende verwerkingen van persoonsgegevens zijn. Het is echter niet helemaal duidelijk of dit ook geldt als de privé gebruiker persoonsgegevens op een publieke blockchain schrijft.[261] Dan zal hij allicht toch als verantwoordelijke gelden.

2. De full node-beheerders bieden gezamenlijk een dienst aan

[258] Als overwegingen om hen als verantwoordelijken te zien, zou men kunnen aanvoeren dat zij er voor kiezen om een bepaalde blockchain en blockchaintoepassing (= middelen) te gebruiken en daarmee ook de verwerkingen van persoonsgegevens die daarmee gepaard gaan. Zij kunnen eventueel volledig afzien van het gebruik van een blockchain of blockchaintoepassing.
[259] CNIL 2018, p. 2.
[260] CNIL 2018, p. 3. De CNIL laat daarbij in het midden of dit ook geldt indien persoonsgegevens op een openbare blockchain worden geplaatst.
[261] Volgens het oude Lindqvist arrest van het Hof van Justitie, gewezen onder richtlijn 94/46/EC, valt internetpublicatie buiten de huishoudexceptie (bron: HvJ 6 november 2003, zaak C-101/01, Zweden tegen Bodil Lindqvist, r.o. 47). Zie ook Laan 2018, par. 3.2. Overweging 18 AVG lijkt daarentegen de grenzen van de huishoudexceptie weer ruimer te trekken: ‘Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten.’

Een ander perspectief is dat alle beheerders van full nodes gezamenlijk een dienst aanbieden waarmee bitcointransacties kunnen worden verricht. De gebruikers zijn dan de afnemers van deze dienst. De miners zijn technisch steunverleners. Juridisch zou het dan mooi zijn als de full node-beheerders ook gezamenlijk verantwoordelijk zijn voor de verwerkingen van persoonsgegevens. Daartoe is vereist dat zij 'gezamenlijk de doeleinden en middelen van de verwerking bepalen'.[262]
Aan dit perspectief wordt soms tegengeworpen dat node-beheerders in een permissionless blockchain niets gezamenlijk bepalen.[263] Dat de blockchain als geheel functioneert, is het gevolg van afzonderlijke feitelijke handelingen die niet berusten op een voorafgaande afspraak. Maar deze tegenwerping vat de werkelijkheid van een permissionless blockchain niet volledig, want de verwerkingen door een afzonderlijke full node hebben alleen betekenis omdat zij in een groter (feitelijk) geheel plaatsvinden. Het is ook kwestieus of voor het gezamenlijk bepalen van doel en middelen (als bedoeld in art. 26 AVG) een afspraak nodig is.[264] Net zoals bij de bepaling van een enkelvoudige verantwoordelijkheid ook meer naar de feitelijke situatie gekeken worden dan naar de formeel juridische, zou dit ook voor de bepaling van meervoudige verantwoordelijk kunnen en moeten gebeuren.[265][266]
De miners zijn allicht geen verantwoordelijken omdat zij slechts rekenwerk verrichten ten behoeve van consensus, net zoals een beheerder van een e-mail server niet verantwoordelijk is voor de persoonsgegevens in de payload van een e-mail bericht.[267]
Dat node-beheerders niet weten welke persoonsgegevens ter verwerking zullen worden aangeboden is eveneens geen beletsel. Zoekmachine Google is ook verantwoordelijke zonder te weten welke persoonsgegevens in door haar geïndexeerde websites worden gepubliceerd. In r.o. 34 van Costeja v Google Spain, geeft het Hof aan:

> "Overigens moet worden vastgesteld dat het niet enkel in strijd zou zijn met de duidelijke bewoordingen, maar tevens met de doelstelling van deze bepaling, die erin bestaat een doeltreffende en volledige bescherming van de betrokkenen te verzekeren via een ruime omschrijving van het begrip „verantwoordelijke", indien de exploitant van een zoekmachine van die omschrijving zou worden uitgesloten omdat hij geen controle uitoefent over de op webpagina's van derden gepubliceerde persoonsgegevens."

Tenslotte zij nog opgemerkt dat dit perspectief niet uitsluit dat naast de full node-beheerders ook de gebruiker als verantwoordelijke kan gelden, met name wanneer diensten gestapeld worden en de gebruiker zelf ook een dienstverlener is.[268]

3. Iedere node-beheerder is een afzonderlijke dienstverlener

Een full node-beheerder biedt een opslag- en verificatiedienst aan (bijvoorbeeld checken op double spending). Een miner verricht diensten gericht op consensus. Iedere full node-beheerder is uitsluitend verantwoordelijk voor zijn eigen verwerkingen van persoonsgegevens.[269] Een miner is als rekenaar voor consensus allicht geen verantwoordelijke. Ook hier geldt uiteraard dat het geen

[262] Art. 26 lid 1 AVG
[263] Bohme & Pesch 2017, p. 479.
[264] Als partijen eenmaal als gezamenlijke verantwoordelijken gelden, moeten zij uiteraard een onderlinge regeling treffen (art. 26 AVG). Maar voor de vraag of ze gezamenlijk verantwoordelijk zijn is geen overeenkomst vereist.
[265] Vergelijk in dit verband ook hoe de art 29. WP de term 'determine' benadert (weliswaar in de context van een enkelvoudige verantwoordelijke) in Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 februari 2010, p. 8. Zie ook Wirth en Kolain 2018, p. 5.
[266] De CNIL praat enigszins langs dit probleem waar zij zegt: "Lorsqu'un groupe de participants décide de mettre en oeuvre un traitement ayant une finalité commune, […] tous les participants pourraient être considérés comme ayant une responsabilité conjointe, conformément à l'article 26 du RGPD […]." CNIL 2018, p. 3.
[267] Overweging 47 Richtlijn 95/46/EG. Zie ook Martini & Weinzierl 2017, par. II (2)(a). Zie ook European Union blockchain observatory and forum 2018, p.18. Een relativering is dat de AVG op dit punt strikter kan blijken dan richtlijn 95/46/EG.
[268] Vergelijk de conclusie van AG Bobek, 19 december 2018, Zaak C‑40/17, Fashion ID en EUHvJ 5 juni 2018, zaak C‑210/16, Wirtschaftsakademie.
[269] Luis-Daniel Ibáñez, Kieron O'Hara, and Elena Simperl 2018, Section 3, p. 4. Laan 2018 classificeert dit als gedifferentieerde verantwoordelijkheid.

beletsel is dat node-beheerders niet weten welke persoonsgegevens ter verwerking zullen worden aangeboden.

In permissionless blockchains zijn diensten die uitsluitend bouwen op core code meervoudig duidbaar. Dat maakt het moeilijk om uit te maken wie volgens de AVG als verwerkingsverantwoordelijke heeft te gelden.

Ieder van deze drie perspectieven heeft nadelen.

1. De gebruikers vormen een P2P netwerk.

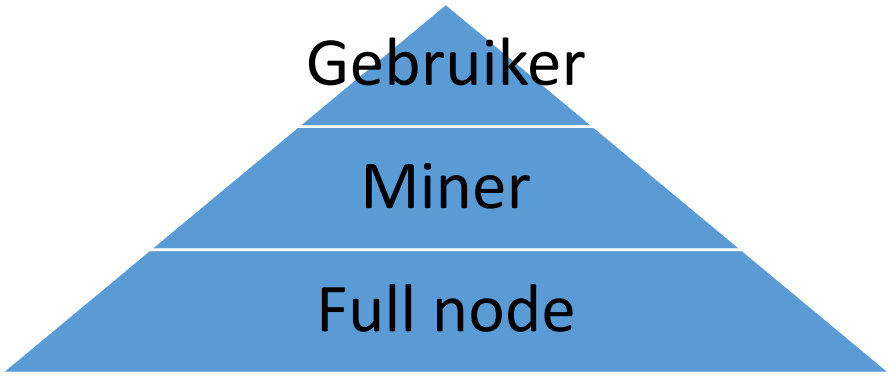
Indien privégebruikers een beroep kunnen doen op de huishoudexceptie is niet duidelijk wie als verantwoordelijke heeft te gelden. Schuift dit dan door naar de node-beheerders? Aangenomen dat de gebruikers verantwoordelijke zijn, dan zullen de full node-beheerders als verwerkers gelden (zie hieronder). De verantwoordelijke moet verwerkingsovereenkomsten sluiten met de node-beheerders.[270] In een permissionless blockchain is dat extreem lastig, want de node-beheerders en gebruikers zijn talrijk, hun samenstelling wisselt en bovendien hoeft hun identiteit niet bekend te zijn. Inde praktijk, worden doorgaans geen verwerkersovereenkomsten met node-beheerders gesloten.

2. De full node-beheerders bieden gezamenlijk een dienst aan

De node-beheerders moeten als verantwoordelijken een onderlinge regeling met elkaar aangaan om de verantwoordelijkheden onderling te verdelen.[271] De vraag is of daarvan veel terecht komt. In een permissionless blockchain kan ieder vrijelijk als node-beheerder toe en uittreden. Ook hoeft de identiteit van node-beheerders niet bekend te zijn. Onder die omstandigheden zullen de gezamenlijke verantwoordelijken niet of nauwelijks een onderlinge regeling kunnen treffen als bedoeld in art. 26 AVG.

3. Iedere full node-beheerder is afzonderlijk verantwoordelijk

Een verdeling waarbij iedere node-beheerder afzonderlijk verantwoordelijk is voor zijn eigen verwerkingen is onvoldoende transparant.[272] Het is onduidelijk voor de betrokkenen tot wie zij zich kunnen wenden met klachten.



Figuur 1 Iedere gebruiker heeft te maken met meerdere miners en per miner is er weer tenminste een full node-beheerder.

De rode draad door deze nadelen is dat in afwezigheid van een sterke governance structuur in de blockchain, de positie van verwerkingsverantwoordelijke moeilijk op een adequate manier vorm te geven is. De belangen van betrokkenen kunnen onder druk komen te staan. Moerel betwijfelt of in een permissionless blockchain zonder een noemenswaardige governance structuur überhaupt wel

[270] Art. 28 lid 3 AVG.
[271] Art. 26 lid 1 AVG. Anders dan Finck, wordt een onderlinge regeling hier niet gezien als een voorwaarde om van gezamenlijke verantwoordelijkheid te kunnen spreken.
[272] Laan 2018, par. 3.3.

een acceptabele inrichting van de verantwoordelijkheid kan plaatsvinden.[273] De CNIL raadt dan ook aan 'que le responsable de traitement soit identifié en amont. Par exemple, les participants peuvent créer une personne morale sous la forme d'une association ou d'un GIE. Elles peuvent également choisir d'identifier un participant qui prend les décisions pour le groupe et de le désigner comme responsable de traitement.'[274] Dat is de facto een advies om op te schuiven naar een permissioned blockchain.

In situatie waarin geen natuurlijke centrale partij aanwezig is die de rol van verwerkingsverantwoordelijke op zich kan nemen, doet zich het gebrek aan stevige governance in een permissionless blockchain sterk gevoelen. Het is de vraag of de verwerking van persoonsgegevens wel adequaat kan worden vormgegeven een permissionless blockchain. De AVG drukt partijen in de richting van een permissioned blockchain.

3.3.1.3 Verwerker

De verwerker is degene die 'ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'.[275] Blockchain specifiek is de vraag of een node-beheerder als verwerker kan gelden (uiteraard in situaties waarin hij niet reeds verantwoordelijke is, zie hierboven). Volgens de CNIL kan dit inderdaad het geval zijn, bijvoorbeeld indien een node-beheerder in opdracht van de verantwoordelijke verifieert of een transactie aan de eisen voldoet die daaraan technisch gesteld worden.[276] Een full node-beheerder die gegevens opslaat zou ook naar analogie met een ISP die webhosting aanbiedt ook als verwerker kunnen worden aangemerkt.[277] Gegeven de informele verhoudingen binnen een permissionless blockchain, is het echter de vraag of een node-beheerder handelt 'namens' de verantwoordelijke (als genoemd in art. 28 lid 1 AVG). Bovendien is, zoals reeds hiervoor opgemerkt, bij permissionless blockchains het aantal verwerkende node-beheerders vaak groot en wisselend en zijn ze ongeïdentificeerd. In zo'n situatie, is niet goed voorstelbaar dat een verantwoordelijke verwerkingsovereenkomsten sluit met alle verwerkende node-beheerders. Dat kan ertoe leiden dat de node-beheerders niet als verwerkers, maar als verantwoordelijken worden aangemerkt.[278] Daarmee lijkt inachthouding van de AVG formeel juridisch misschien wel afgedekt te zijn, maar de vraag is of een groot aantal kleine verantwoordelijken niet leidt tot intransparantie voor de betrokkenen en daarmee allicht tot onrechtmatigheid van de verwerkingen.

In permissionless blockchains is het adequaat aansturen van en contracteren met 'verwerkende' node-beheerders lastig. Een falen bergt het risico in zich dat de verwerking van persoonsgegevens niet transparant wordt bevonden.

3.3.2 De territoriale werkingssfeer

Zowel permisisionless als permissioned blockchains strekken zich vaak uit over de grenzen van Nederland en van de EU. Voor de territoriale toepasselijkheid van de AVG is de plaats van vestiging van de verantwoordelijke of verwerker het uitgangspunt, ongeacht waar de verwerkingen plaatsvinden. De AVG is van toepassing op alle verantwoordelijke of verwerkende beheerders van nodes, gebruikers of eigenaars van blockchains gevestigd binnen de EU. De AVG is ook van toepassing op de buiten de EU gevestigde beheerder van een node, gebruiker of eigenaar van een blockchain die verantwoordelijke of verwerker is, mits de verwerkingen betrokkenen in de EU betreffen en verband houden met a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.

[273] Moerel 2019, p. 844.
[274] CNIL 2018, p. 3.
[275] Art. 4 sub 8 AVG.
[276] CNIL 2018, p. 4.
[277] Art. 29 WP, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Example no. 16, p. 25. Onder richtlijn 95/46/EG, achtte de Oostenrijkse Datenschutzcommission een provider van webhosting diensten een verwerker. Bron: Datenschutzcommission 14 november 2003, K120.819/006-DSK/2003.
[278] Art. 29 WP, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, Example no. 16, p. 25.

In veel gevallen is duidelijk wie verantwoordelijke en verwerker is in een blockchain (zie de desbetreffende paragraaf), echter niet altijd. In het bijzonder bij toepassingen die in de core code zijn opgenomen (bijv. een cryptocurrency) kan grote onduidelijkheid bestaan over wie verantwoordelijke is. Toch is niet zonder meer te concluderen dat zich dit negatief op de territoriale werkingssfeer uitwerkt.[279] Bijvoorbeeld bij een bitcoin transactie van of aan een betrokkene in de EU, is een beheerder van een node buiten de EU vrijwel steeds betrokken, hetzij als verwerker, hetzij als verantwoordelijke (alleen of in gezamenlijkheid). Zoals ook opgemerkt wordt in de paragrafen over verantwoordelijke en verwerker is het echter kwestieus of alle verantwoordelijke of betrokken blockchain actoren hun verantwoordelijkheden wel nemen. Gegeven hun aantal is handhaving lastig, zeker indien zij zich buiten de EU bevinden.

De AVG is ook van toepassing op de buiten de EU gevestigde beheerder van een node, gebruiker of eigenaar van een blockchain die verantwoordelijke of verwerker is, mits de verwerkingen betrokkenen in de EU betreffen en verband houden met a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.
Het is de vraag of de AVG goed te handhaven is buiten de EU.

3.3.3 Persoonsgegevens

De AVG is van toepassing op de verwerking van persoonsgegevens. Onder persoonsgegeven wordt verstaan alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (art. 4(1) AVG).
Anonimisering kan een verwerking van gegevens aan de werking van de AVG onttrekken. Aan anonimisering worden strikte voorwaarden gesteld. Anonimisering is alleen anonimisering als het niet omkeerbaar is.[280] De vraag is of dit een bruikbaar perspectief biedt voor blockchain.
Voor de vraag naar persoonsgegeven dan wel anonieme gegevens, kan onderscheid gemaakt worden tussen transactiedata (i.e. inhoudsdata) en de publieke sleutel waarmee een gebruiker zich legitimeert in een blockchain.[281]
Versleutelde transactiedata kunnen ontsleuteld worden, bijvoorbeeld in het kader van KYC en AML-verplichtingen. Zij zijn niet onomkeerbaar en gelden als pseudoniem onder de AVG. Ook gehashte transactiegegevens gelden waarschijnlijk als pseudoniem. Met brute rekenkracht is het onder omstandigheden namelijk mogelijk de gegevens waarover de hash berekend is terug te halen.
Een andere mogelijkheid is om persoonsgegevens off chain op te slaan. On chain worden dan gegevens opgeslagen die het mogelijk maken de integriteit van de off chain opgeslagen gegevens te verifiëren. Bij deze oplossing moet er echter voor gewaakt worden dat niet alsnog de on chain opgeslagen gegevens als persoonsgegevens gelden. Er zijn wel gesofisticeerde oplossingen die beloven dit te ondervangen.[282]
De publieke sleutel waarmee een gebruiker zich legitimeert in de blockchain geldt als pseudoniem. Door de sleutel te combineren met andere informatie (bijvoorbeeld het IP-adres van waaruit de sleutel is gebruikt, of andere transacties verricht met dezelfde sleutel) kan alsnog een identiteit achterhaald worden. Ook hier behoeft het meer gesofisticeerde middelen om in de buurt van anonimiteit te komen, zoals: zero-knowledge proofs, state channels, ring signatures, of het toevoegen van ruis.

Persoonsgegevens verliezen door anonimiseren hun status als persoonsgegeven. De AVG stelt hoge eisen aan anonimisering. Het is niet gemakkelijk om aan de werking van de AVG te ontsnappen door het treffen van anonimiseringsmaatregelen.

[279] Mogelijk anders: Berberich & Steiner 2016, p. 423.
[280] Groep Gegevensbescherming Artikel 29, Advies 5/2014 over anonimiseringstechnieken, 0829/14/NL WP 216, p. 9. Laan & Rutjes 2017, p. 368.
[281] Finck 2018, p. 93.
[282] J. Eberhardt and S. Tai (2017). On or Off the Blockchain? Insights on Off-Chaining Computation and Data. ESOCC 2017: 6th European Conference on Service-Oriented and Cloud Computing.

Voor transactiedata, kan off chain opslag van persoonsgegevens een deel van de oplossing vormen. On chain wordt dan slechts een hash of cryptografische sleutel opgeslagen. Aan de hand daarvan kunnen de off-chain opgeslagen gegevens geverifieerd worden. Het is echter nog steeds mogelijk dat de gegevens die bij off chain opslag wel on chain worden opgeslagen (de hash, publieke sleutel) als persoonsgegeven gelden.
Een cryptografische sleutel (waarmee een gebruiker zich legitimeert) geldt als niet anoniem. Er zijn wel maatregelen die anonimiteit dichterbij brengen, zoals het toevoegen van ruis of zero-knowledge proofs.

3.3.4 Data minimalisatie en het recht op vergetelheid

Volgens art. 5(1)(c) AVG moeten persoonsgegevens 'toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt'. Dit is het principe van de minimale gegevensverwerking. Volgens overweging 39 AVG betekent dit vooreerst dat de opslagperiode van persoonsgegevens tot het minimum wordt beperkt.
Ten aanzien van blockchains roept dit de vraag op wanneer gegevens ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt in een blockchain. Voorts is de vraag hoe de opslagperiode van gegevens beperkt kan worden in een blockchain.
Het recht op vergetelheid is onder de gelding van de gegevensbescherming richtlijn erkend in de Google-Spain zaak. In de AVG, is het recht gecodificeerd en bij die gelegenheid ook versterkt.[283] Op grond van art. 17(1) AVG, heeft de betrokkenen het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen in een aantal genoemde omstandigheden. Deze omstandigheden omvatten onder andere de situatie dat de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt, en in bepaalde gevallen van het intrekken van toestemming voor de verwerking.
De vraag is ook hier onder welke omstandigheden een recht op wissing bestaat met betrekking tot in een blockchain opgeslagen gegevens en hoe in een blockchain voldaan kan worden aan een plicht tot wissing.

De tegenstelling is niet zo scherp als het lijkt

Zijn er omstandigheden waarin de opslagperiode van gegevens in een blockchain niet beperkt hoeft te worden, c.q., waarin gegevens niet gewist hoeven te worden?

Data minimalisatie
De Franse CNIL maakt voor data minimalisatie onderscheid tussen identificerende data en transactiedata.[284] Voor identificerende data, blijft de publieke sleutel nodig zolang de blockchain bestaat. Data minimalisatie vergt hier niet het wissen van persoonsgegevens.[285] Transactiedata – die persoonsgegevens zijn - moeten volgens de CNIL versleuteld of met behulp van een versleutelde hash opgeslagen worden.[286] Alleen, als uit een Privacy Impact Assessment blijkt dat de risico's voor betrokkenen gering zijn is eventueel ook open opslag mogelijk.[287]

Recht op wissing
Art. 23 AVG geeft de mogelijkheid om rechten van betrokkenen te beperken. Het recht op wissing kan beperkt worden door lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat. Bovendien moet de beperking in een

[283] EU HvJ 13 mei 2014, zaak C‑131/12, Google Spain SL en Google Inc. tegen Agencia Española de Protección de Datos (AEPD) en Mario Costeja González.
[284] Laatstgenoemde noemt de CNIL 'données complémentaires (ou « la charge utile »)'.
[285] CNIL 2018, p.7 en Bohme & Pesch 2017, p. 480.
[286] CNIL 2018, p.7.
[287] CNIL 2018, p. 7-8.

democratische samenleving een noodzakelijke en evenredige maatregel zijn ter waarborging van belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid.[288] In overweging 73 AVG, wordt het houden van openbare registers die nodig zijn om redenen van algemeen belang als voorbeeld genoemd. Dit kan een relevante uitzonderingsmogelijkheid vormen voor blockchains die openbare registers bevatten.[289] In dit verband, zij ook gewezen op de Manni-zaak van het HvJ van de EU (nog beslist onder de gegevensbeschermingsrichtlijn 95/46/EU).[290]

> Manni vroeg om schrapping, anonimisering of afscherming van hem betreffende gegevens uit het Italiaanse bedrijvenregister waarin hij genoemd wordt in verband met een oud faillissement. Een gegevens- en ratingbureau had deze gegevens uit het register betrokken. Het Hof woog de bescherming van belangen van derden ten aanzien van vennootschappen, de rechtszekerheid, de eerlijkheid van handelstransacties en het goede functioneren van de interne markt af tegen het fundamentele recht op gegevensbescherming.[291] Het kwam tot de conclusie dat er geen sprake was van een onevenredige inbreuk op het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens als neergelegd in de artikelen 7 en 8 van het Handvest, met name omdat slechts een beperkt aantal persoonsgegevens openbaar worden gemaakt.[292]

Blockchains die publieke registers bevatten zouden onder de AVG kunnen profiteren van een lidstaatrechtelijke bepaling als bedoeld in art. 23 AVG. Op basis van de Manni zaak is aan te nemen dat de wezenlijke inhoud van grondrechten en fundamentele vrijheden (als genoemd in art. 23 aanhef AVG) inderdaad onverlet kan blijven bij een lidstaatrechtelijke beperking van het recht op wissing ten behoeve van openbare registers, mits de openbaar te maken persoonsgegevens beperkt blijven.[293]

Er zijn situaties waarin persoonsgegevens nodig blijven en niet gewist hoeven te worden. Dit kan zich voordoen ten aanzien van persoonsgegevens in openbare registers.

Hoe te voldoen aan een plicht tot wissing?

De relativeringen beschreven in de vorige paragraaf kunnen niet wegnemen dat er gevallen zijn waarin wel degelijk persoonsgegevens verwijderd of tenminste ontoegankelijk gemaakt zouden moet worden.
Daarbij doen zich met name in permissionless blockchains twee problemen voor.
Ten eerste is het vanuit het perspectief van een adequate bescherming van persoonsgegevens niet voldoende dat slechts een full node de betreffende persoonsgegevens van zijn versie van de blockchain wist. De persoonsgegevens zouden dan nog via de overige full nodes beschikbaar zijn. In beginsel zouden alle full nodes daarom de gegevens moeten wissen. Vooral in permissionless blockchains ontbreekt het vaak aan een manier om alle beheerders van full nodes te bereiken.[294]
In de tweede plaats, zijn er blockchains die op basis van een crypto-economisch protocol werken. Dit protocol is erop uitgelegd om wijzigingen tegen te werken en hen duur en omslachtig te maken, als men binnen de regels van het protocol wil blijven opereren. Men zou in de bitcoin blockchain een aantal miners mee moeten krijgen dat tenminste de helft van de rekenkracht in het netwerk representeert.[295] Dan zou het nog een behoorlijke investering vergen van de miners. Theoretisch zou men ook buiten het protocol om kunnen gaan als alle beheerders van nodes het daarover eens

[288] Art. 23(1) aanhef & sub e. AVG.
[289] Martini & Weinzierl 2017
[290] HvJ 9 maart 2017, zaak C‑398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce tegen Salvatore Manni.
[291] C-398/15, r.o. 60.
[292] C-398/15, r.o. 57, 58.
[293] Vergelijk ook Moerel 2019, p. 846, Kunze et al.
[294] Martini & Weinzierl 2017, p.
[295] Nakamoto 2008, p. …

zijn (of tenminste zoveel als een eventueel aanwezige governance structuur zou vergen). Zo'n overeenstemming zal wel in de praktijk van een permissionless blockchain met 'overtuigde' beheerders van nodes niet zo gauw bereikt worden, omdat de integriteit van de blockchain dan in wezen komt te berusten op 'normale' afspraken tussen de beheerders van nodes en de (theoretische?) meerwaarde van de blockchain als een systeem dat uitsluitend bouwt op crypto-economische prikkels en onwijzigbaar is zo goed als wegvalt.
Bij meer praktisch ingestelde beheerders kan echter het inzicht postvatten dat een systeem dat wijzigingen tegenwerkt, veel praktische bezwaren heeft (zoals onder andere het voldoen aan een plicht tot wissing van persoonsgegevens). Een permissioned blockchain met normale afspraken tussen beheerders over de integriteit van opgeslagen gegevens werkt dan beter.

Oplossingsrichtingen

Gegeven dat er permissionless blockchains zijn die aan onwijzigbaarheid in hiervoor omschreven zin vasthouden, beveelt de Franse CNIL aan om niet persoonsgegevens onversleuteld of alleen gehasht op een blockchain op te slaan.[296] Het idee is dat dit de risico's voor de betrokkenen minimaliseert, ook als niet volledig gevolg gegeven kan worden aan rechten van betrokkenen, zoals het recht op wissing. Er zijn wel technieken die compliance met de eisen van de AVG dichterbij brengen, maar het behoeft nog nader onderzoek of de technische oplossingen daadwerkelijk aan de AVG voldoen.[297] Als technische benaderingen kunnen onder andere de volgende worden genoemd:

Off chain opslag

Een mogelijkheid is dat transactiegegevens off chain worden opgeslagen en dat in de blockchain een hash staat van de off chain opgeslagen gegevens.[298] De off chain opgeslagen gegevens kunnen dan gewist worden. De on-chain hash zou gewoon in de blockchain blijven staan maar zijn betekenis verliezen omdat datgene waarnaar hij verwijst niet meer bestaat. Een bezwaar hiertegen is dat allicht uit een hash de verwezen (persoons)gegevens weer herleid kunnen worden, vooral indien de verwezen data klein in omvang zijn. Dat risico kan weer verkleind worden door de hash te versleutelen. De Franse CNIL ziet dit als een aanbevolen oplossing in het licht van de eisen van privacy-by-design, privacy-by-default en data minimalisatie.[299]

Full nodes en pruning

Een full node slaat de gehele blockchain op. Echter niet iedere node hoeft een full node te zijn. Als slechts een beperkt aantal nodes full nodes zijn dan leidt dit tot een zekere minimale gegevensverwerking. Een beperking is uiteraard dat er doorgaans wel een aantal full nodes nodig zal blijven. Pruning is een mogelijkheid voor miners om hun validatie werk te doen zonder over een volledige kopie van de blockchain te hoeven beschikken. Een miner zou slechts over de laatste honderden blokken hoeven te beschikken. Dit bespaart niet alleen opslagruimte maar draagt ook bij aan data minimalisatie.

Zero-Knowledge bewijzen en homomorfe encryptie

Het uitvoeren van code in een blockchain vergt doorgaans dat de input data onversleuteld beschikbaar zijn voor de nodes die de code uitvoeren. Met zero-knowledge proofs en homomorphic encryption bestaan er mogelijkheden om bewerkingen uit te voeren zonder dat het computersysteem waarop de bewerking wordt uitgevoerd deze data te weten komt. Uiteraard vertraagt dit berekeningen en vergroot het de complexiteit.

Editable blockchain

Accenture heeft een techniek ontwikkeld om een blockchain editable te maken.[300] Dit schept uiteraard een achterdeur in de blockchain. Er zullen daarom goede afspraken gemaakt moeten

[296] CNIL 2018, p. 10.
[297] CNIL 2018, p. 11.
[298] Finck 2018, p. 107.
[299] CNIL, Premiers elements d' analyse de la CNIL. Blockchain, Septembre 2018, p. 8.
[300] https://www.accenture.com/nl-en/insight-editing-uneditable-blockchain

worden over de procedure voor het aanbrengen van edits en hoe transparantie over de edits betracht kan worden. Nadere technische analyse zou moeten uitwijzen of wat overblijft nog wel meer is dan alleen een blockchain in naam.

Er zijn wel technieken die compliance met de eisen van de AVG rond wissing dichterbij brengen, maar het is onduidelijk of zij daadwerkelijk aan de AVG voldoen.

3.4 Bestuursrecht en geautomatiseerde besluiten

3.4.1 Geautomatiseerd besluiten in het bestuursrecht

De overheid maakt gebruik van geautomatiseerde besluitvorming op velerlei terreinen, zoals voor het opleggen van aanslagen door de belastingdienst of voor het opleggen van verkeersboetes op basis van automatische nummerplaatherkenning. Voor het nemen van geautomatiseerde besluiten zouden smart contracts in een blockchain ingezet kunnen worden. Een argument om voor smart contracts te kiezen zou allicht efficiëntie kunnen zijn of de grotere transparantie die openbare blockchains bieden. Hieronder wordt de inzet van smart contracts geëvalueerd vanuit juridisch perspectief. Geautomatiseerde besluitvorming is zowel genormeerd in de AVG, als in de AWB.

De Algemene Verordening Gegevensbescherming

Voor het geautomatiseerd besluiten op basis van persoonsgegevens is art. 22(1) AVG van belang:

> De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

Besluitvorming die geautomatiseerd is maar waarin een mens tevens een niet-marginale inbreng heeft wordt niet getroffen door dit verbod. Lid 2 van art. 22 AVG laat bovendien toe dat lidstaten uitzonderingen maken op het verbod van zuiver geautomatiseerde besluitvorming. Zo is ook een geautomatiseerd besluit mogelijk indien dat besluit:

> b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene;

Nederland heeft een lidstaatrechtelijke bepaling als bedoeld in art. 22(2)(b) AVG opgenomen in art. 40 Uitvoeringswet AVG.

> 1. Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.

Gegeven wettelijke plicht c.q. algemeen belang, is daarmee een brede uitzondering geschapen voor alle besluiten die niet op profilering zijn gebaseerd. Profilering houdt in dat iemand op basis van een kenmerk van de groep waartoe hij behoort beoordeeld wordt. Hij hoeft het betreffende kenmerk niet zelf te hebben. Daarmee is een bijzonder risicovolle categorie van geautomatiseerde besluiten onder het verbod gebleven. Niettemin betwijfelde de afdeling advisering van de Raad van State, of art. 22(2)(b) AVG een algemene uitzondering (nl. voor alle besluitvorming strikt op basis van individuele kenmerken) toelaat.[301] Art. 22 AVG zou het oog hebben op specifieke wettelijke grondslagen, zoals bijvoorbeeld in sectorale wetgeving. Zolang de rechter hierover niet geoordeeld

[301] . Kamerstukken II 2017/18, 34851, 4, p. 45.

heeft blijft hier onzekerheid over bestaan. Vooralsnog kunnen bestuursorganen besluiten gebaseerd op individuele kenmerken geautomatiseerd nemen. Niettemin moeten wel maatregelen genomen worden ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene (art. 22(2)(b) AVG en art. 40 lid 2 UAVG). Zo dient de verantwoordelijke de betrokkene informatie te verschaffen over:[302] 'het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.' Andere relevante maatregelen zijn volgens art 40 lid 3 UAVG het borgen van het recht op menselijke tussenkomst,[303] het recht voor betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.

De Algemene Wet Bestuursrecht
Besluiten moeten voldoen aan de algemene beginselen van behoorlijk bestuur, zoals het zorgvuldigheids- en evenredigheidsbeginsel. Dat geldt uiteraard ook voor geautomatiseerd genomen besluiten. Op grond van de art. 4.7 en 4.8 AWB geldt bovendien een hoorplicht. De vraag is of aan geautomatiseerd genomen besluiten hogere eisen gesteld moeten worden omdat ze naar hun aard minder transparant zijn.
De Raad van State heeft geoordeeld over een besluit genomen met behulp van het AERIUS-systeem. Dit systeem wordt ingezet bij besluiten die over de uitstoot van stikstof gaan. Zij heeft aangegeven welke informatie over de besluitvorming medegedeeld moet worden en hoe dat moet gebeuren:

> "Ter voorkoming van deze ongelijkwaardige procespositie rust in dit geval op genoemde ministers en de staatssecretaris de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen."[304]

Van Eck heeft in haar proefschrift aangegeven dat geautomatiseerd genomen besluiten inderdaad vaak ondoorzichtig zijn en dat een algoritme niet altijd duidelijk maakt of een besluit in overeenstemming met de geldende regels is genomen.[305] In de literatuur is ook betoogd dat de uitzondering op de hoorplicht van art. 4.12 AWB (geen hoorplicht bij beschikking over financiële verplichting of aanspraak) niet op zou mogen gaan bij geautomatiseerde besluitvorming.[306] Art. 22(2) AVG vergt immers passende beschermingsmaatregelen. Juist besluiten van een financieel karakter lenen zich vaak goed voor automatisering.

Besluiten genomen met behulp van smart contracts

We zagen dat geautomatiseerde besluitvorming passende maatregelen vergt ter bescherming van de betrokkenen en ter waarborging van de zorgvuldigheid waarmee besluiten worden genomen. Procedurele maatregelen zijn het horen van de betrokkene of het betrekken van een mens in de besluitvorming. Deze maatregelen dienen om het beeld van de betrokkene en zijn situatie te corrigeren ten opzichte van wat uit beschikbare gegevens alleen volgt (of beter lijkt te volgen). Het horen van de betrokkene is bijvoorbeeld nuttig indien gegevens niet bij de betrokkene zijn ingewonnen. Bij geautomatiseerd besluiten in een blockchain lijkt ons aan deze maatregelen

[302] Art. 13(2)(f), 14(2)(g) en 15(1)(h) AVG
[303] Deze maatregelen lijken ontleend aan art. 22 lid 3 AVG.
[304] Raad van State 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o. 14.4.
[305] B.M.A. van Eck, Geautomatiseerde ketenbesluiten & Rechtsbescherming (diss. Tilburg), 2018, p. 21.
[306] Niels Jak & Steven Bastiaans (2018). De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid, NJB 40, p. 3018-3025.

evenzeer behoefte te bestaan als bij geautomatiseerd besluiten zonder blockchain. Er is vooralsnog geen reden om aan te nemen dat in een blockchain aan deze procedurele waarborgen minder behoefte zou bestaan en aldus een efficiëntiewinst zou zijn te behalen. Het gaat er immers om niet uitsluitend af te gaan op het beeld dat uit data spreekt.[307]

Dat geautomatiseerde besluitvorming plaatsvindt in een blockchain neemt niet het risico weg dat het beeld dat uit de data spreekt niet klopt.

We zagen ook dat ter verantwoording van een geautomatiseerd genomen besluit informatie verstrekt moet worden. De betrokkene moet in staat gesteld worden de onderliggende keuzes en gegevens te beoordelen en betwisten. In zijn AERIUS-beslissing, verlangt de Raad van State echter niet expliciet dat het algoritme of de code beschikbaar wordt gesteld. In een blockchain, is de code vaak wel beschikbaar. De core code is open source en smart contract code kan in beginsel door eenieder geïnspecteerd worden. De vraag is of daarmee de gemaakte keuzes volledig openbaar zijn gemaakt. Enerzijds zou men kunnen argumenteren dat het openbaar maken van de code uitgaat boven het enkele openbaren van de gemaakte keuzen. Het laat precies zien welke geautomatiseerde stappen genomen worden. Anderzijds is het de vraag of de code voldoende begrijpelijk is voor de betrokkene. Code is erg gedetailleerd waardoor het lastig kan zijn de essentie te distilleren. Een openbaarmaking van de gemaakte keuzes in natuurlijke taal kan veel begrijpelijker zijn en voorkomt dat de betrokkene een deskundige moet inschakelen om de code van het smart contract te duiden. In deze lijn past ook het onderscheid dat de minister van rechtsbescherming maakt tussen technische transparantie en uitlegbaarheid. [308] Een redenering dat een blockchain een efficiëntievoordeel levert omdat de lasten van het verstrekken van de AERIUS-beslissing genoemde informatie zouden wegvallen, lijkt daarmee kwestieus.

Dat de code van een smart contract dat gebruikt is voor geautomatiseerde besluitvorming openbaar is, wil niet noodzakelijkerwijze zeggen dat ook rechtens voldoende transparantie is betracht.

3.4.2 Elektronisch bestuurlijk verkeer

De AWB geeft regels voor elektronisch bestuurlijk verkeer. Een bestuursorgaan kan een bericht dat tot een of meer geadresseerden is gericht, elektronisch verzenden voor zover de geadresseerde kenbaar heeft gemaakt dat hij langs deze weg voldoende bereikbaar is (art. 2:14 lid 1 AWB). Omgekeerd, kan een bericht elektronisch naar een bestuursorgaan worden verzonden voor zover het bestuursorgaan kenbaar heeft gemaakt dat deze weg is geopend. (art. 2:15 lid 1 AWB). Het aanhangige voorstel voor een Wet digitale overheid[309] voorziet erin dat overheidsorganen verplicht kunnen worden bepaalde technische standaarden toe te passen in het elektronisch verkeer met burgers. Daarmee wordt een volgende stap gezet in de digitalisering van het verkeer tussen overheid en burger.
Voor ondertekening kan een elektronische handtekening gebruikt worden, die voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt (art. 2. 16 lid 1 AWB).

In beginsel staat de elektronische weg open en is het daarmee ook mogelijk een blockchain toe te passen in het verkeer tussen overheidsorgaan en burger.[310]

[307] Vergelijk in dit verband ook de opmerkingen gemaakt over de blindheid van een blockchain in hoofdstuk 1.
[308] Kamerstukken II 2018/19, 26643, 570.
[309] Kamerstukken II 2017/18, 34972, nr. 2 (Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)).
[310] Uiteraard moet aan de randvoorwaarde worden voldaan dat elektronisch berichtenverkeer aan de burger voldoende betrouwbaar en vertrouwelijk is, gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt (art. 2:14 lid 3 AWB).

De AWB laat elektronisch berichtenverkeer tussen overheidsorgaan en burger toe. Het feit dat een blockchain digitaal is is daarmee geen argument tegen gebruik van een blockchain.

4. Use-cases

4.1 Inleiding

Omdat blockchain technologie nog betrekkelijk nieuw is, zijn in dit onderzoek 4 use-cases betrokken. Deze use-cases moeten zicht geven op mogelijke problemen en knelpunten die zich in de praktijk voordoen. Daartoe is in de use-cases als volgt te werk gegaan. In een use-case staat een administratie centraal die nu op een traditionele manier gevoerd wordt en die in de toekomst of heden bij wijze van proef met blockchain verricht wordt. Een use-case beschrijft de traditionele administratie en de context waarin hij gevoerd wordt en met de actoren en rollen die daarin figureren. Vervolgens wordt de geplande of voorgenomen blockchain variant besproken, met aandacht voor relevante technische en organisatorische verschillen. De use-case geeft aan welke voordelen worden verwacht van de overgang op een blockchain gebaseerd systeem. Waar mogelijk en zinvol worden ook de voordelen afgezet tegen andere ICT-oplossingen. De use-case brengt ook de verwachte of geconstateerde risico's in beeld die met overgang op een blockchain gepaard gaan. Op basis van het voorgaande worden juridische knelpunten in beeld gebracht.

4.2 Use-case 1: Scheepsregistratie op de blockchain?

De use-case in steekwoorden

Probleem: een complex registratieproces
Relevante partijen: reder, inspectie ILT, klassenbureaus, kadaster, notaris.
Geclaimde bijdrage van blockchain: kostenbesparing en tijdsbesparing
Juridische implicaties: om een kosten- en tijdbesparende blockchain te realiseren zou de wet aangepast moeten worden. Een aantal waarborgen zouden dan komen te vervallen met lagere kwaliteit van de openbare registers als gevolg.
Balans: een blockchain kan alleen een tijds- en kostenbesparing realiseren ten koste van de betrouwbaarheid van de registratie. Blockchain brengt geen win-win situatie.

In Nederland kunnen schepen worden geregistreerd in het scheepsregister.[311] Dit heet 'teboekstellen'. Als het schip teboekgesteld is, is het een zogenaamd registergoed,[312] zolang dat niet zo is, is het een gewone roerende zaak en kan er bijvoorbeeld geen hypotheek op worden gevestigd.[313] Verder is teboekstelling in principe vereist voor het varen onder Nederlandse vlag.[314] Het proces van teboekstelling en wijziging van de registratie is ingewikkeld: daarom is het zinvol na te gaan of het gebruik van blockchaintechnologie tot verbetering kan leiden. Daarvoor is het nodig kort te beschrijven hoe de registratie van schepen in elkaar zit en verloopt.

Het scheepsregister en de kadastrale registratie

De Nederlandse scheepsregistratie bestaat eigenlijk uit twee onderdelen.

[311] Voor de meeste binnenschepen is dit verplicht (art. 8:785 BW), voor zeeschepen en schepen in aanbouw is het mogelijk maar niet verplicht (art. 8:194 e.v. en 8:784 e.v. BW). Voor zeeschepen kunnen verder internationele regels gelden; deze vallen buiten het bestek van dit onderzoek.
[312] Art. 8: 199 en 8:790 BW. Asser/Japikse *8-II** 2012/67.
[313] De scheepshypotheek blijkt in de praktijk vaak een noodzaak om tot de financiering van het schip te komen, Asser/Japikse *8-II** 2012/15 en 2012/16.
[314] Bij bedrijfsmatig gebruik van een zeeschip; dan is in principe een zeebrief vereist, die alleen (op enkele uitzonderingen na) wordt afgegeven als het schip geregistreerd is (art. 4 Zeebrievenwet).

Het *scheepsregister*, dat in beheer is bij het Kadaster, is een openbaar register in de zin van art. 3:16 BW.[315] Dit is een geordende verzameling[316] van documenten die betrekking hebben op bepaalde goederen (in dit geval schepen): brondocumenten, zoals notariële akten, beslagen, rechterlijke uitspraken en besluiten van overheden.[317]

Daarnaast is er de zogenaamde *kadastrale registratie*:[318] hierin worden de rechten geregistreerd met betrekking tot het schip, zoals wie eigenaar is, of er een hypotheekrecht op is gevestigd.[319] Men kan dit vergelijken met een bankrekening: het scheepsregister is zogezegd het overzicht van alle overboekingen, de kadastrale registratie geeft het saldo (de uitkomst). De kadastrale registratie geeft verder een zoekingang naar relevante aktes in het openbare register.[320] De meeste andere landen hebben niet een dergelijke kadastrale registratie.[321]

De Nederlandse registratie van schepen bestaat uit twee onderdelen: het scheepsregister, en de kadastrale registratie die de actuele toestand van het schip vermeldt.

Actoren bij de huidige scheepsregistratie

Bij de scheepsregistratie zijn verschillende actoren betrokken.[322] Belangrijk zijn met name:[323]

1. De reder: de eigenaar van het schip.
2. De Inspectie Leefomgeving en Transport (ILT): toezichthouder op naleving van internationale normen op het gebied van veiligheid, milieu en leef- en werkomstandigheden aan boord, en heeft uitvoerende taken zoals uitgifte van diverse documenten voor registratie.
3. Klassenbureaus: voeren verschillende registratie- en certificatieprocessen en keuringen uit.
4. Het Kadaster: stelt het schip teboek in het Nederlandse openbare scheepsregister en in de kadastrale registratie voor schepen, en controleert o.a. de inschrijfvereisten en de identiteit van partijen.
5. De notaris. Deze moet verplicht worden ingeschakeld bij overdracht of vestiging van rechten op een schip, maar is niet nodig bij de eerste teboekstelling.[324]

De aanwezigheid van verschillende partijen, en de daaruit resulterende complexiteit van het registratieproces, is bekritiseerd: veel processen zijn belegd bij verschillende registerpartijen, zijn van elkaar afhankelijk en niet goed op elkaar afgestemd.[325] Een voorbeeld ter illustratie.

> Voor de teboekstelling heeft de reder een zeebrief nodig, en hiervoor is weer een meetbrief nodig. Bij een buitenlands zeeschip moet bovendien een nationaliteitsverklaring worden aangevraagd. De reder moet verder beschikken over diverse (verzekerings-)certificaten en bemanningsdocumenten.

[315] Dit valt onder beheer van het Kadaster, zie art. 8 Kadasterwet, op grond waarvan het bestuur van het Kadaster nadere regels kan stellen over dit register.
[316] Tegenwoordig is dit (grotendeels) een elektronische database. *
[317] Op grond van art. 3:16 en 3:17 BW. Het is een verzameling van ingeschreven akten waaruit de rechtstoestand van het registergoed kan worden afgeleid, zie Pitlo/Reehuis, Heisterkamp, Van Maanen & De Jong 2012, nr 45 en Vos en Roes, *WPNR* 2018/7180.
[318] Zie art. 7 lid 1 sub b Kadasterwet, sprekend over 'de registratie voor schepen' (nadere geregeld in art. 85-89 Kadasterwet).
[319] Art. 85 lid 1 Kadasterwet.
[320] Wil men deze informatie achterhalen door enkel in het openbaar register te kijken, zal dit niet mogelijk zijn. Het openbaar register is een database van akten, zonder de verwijzing uit de kadastrale registratie is het praktisch onmogelijk de juiste akte(n) te vinden. Voor meer informatie zie Vos en Roes, *WPNR* 2018/7180.
[321] Vgl. art. 85 lid 1 Kadasterwet: de registratie voor schepen 'ontsluit' de openbare registers. Zie Louwman, *WPNR* 2018/7209, met verwijzing naar onderzoek van Fernando P. Mendez Gonzalez naar de organisatie van kadasters en landregisters in dertig Europese landen. Zie verder over het registerstelsel Asser/Bartels & Van Mierlo 3-IV 2013/487 e.v., Vos en Roes, *WPNR* 2018/7180
[322] Rapportage verbetering Nederlands Scheepsregister 2016, p. 1 e.v.
[323] Andere partijen zijn bijvoorbeeld het KiWa Register dat bemanningsdocumenten verzorgt en brancheverenigingen en de vakbonden.
[324] De notaris onderzoekt o.a. de beschikkingsbevoegheid van partijen en stelt de benodigde akte in de zin van art. 3:89 lid 1 jo lid 4 BW op.
[325] Rapportage verbetering Nederlands Scheepsregister 2016.

De zeebrief, het bemanningscertificaat en een aantal verzekeringscertificaten worden uitgegeven door de ILT.[326] Verschillende registratie- en certificatieprocessen van het ILT worden weer uitgevoerd door klassenbureaus, die tevens het eerste contactpunt zijn bij vragen en problemen van de reder. De meetbrief wordt verkregen met medewerking van de scheepswerf, klassenbureaus en de reder.[327]
Na verkrijging van deze stukken registreert het Kadaster het schip. Daarbij moeten het schip en de eigenaar geïdentificeerd worden. Bij de eerste teboekstelling controleert de scheepsinspecteur feitelijk het schip, de bewaarder van het kadaster controleert de stukken. Na goedkeuring schrijft de bewaarder van het Kadaster het schip in. De scheepsinspecteur brengt vervolgens het brandmerk (een registratienummer) aan op het schip.[328]

De uitwisseling van alle stukken en de veelheid aan onderling afhankelijke en parallelle processen leidt tot vertragingen.[329] Dit kan leiden tot aanzienlijke kosten voor reders.[330]

Korte beschrijving van de blockchain aanpak

Er wordt wel gesuggereerd dat een blockchain dit proces zou kunnen verbeteren. De scheepsregistratie lijkt een geschikte kandidaat voor implementatie op een blockchain: het is al een openbaar register,[331] werkt ook met datering van registratie (zoals *timestamping* op een blockchain),[332] en voegt alleen documenten toe zonder oude documenten te verwijderen.
Het is technisch gezien mogelijk om het scheepsregister als permissionless blockchain op te zetten. Iedereen mag dan documenten in het register plaatsen en er vindt geen verificatie plaats. Daarbij gelden wel enkele beperkingen.
- Een blockchain lost niet eventuele inefficiënties in de onderliggende processen op, en vergt bovendien dat die processen geautomatiseerd worden om aan te sluiten op de blockchain.
- Het is nodig om een standaard op te zetten voor de registraties op de blockchain: er moeten immers veel verschillende documenten worden geregistreerd die automatisch moeten worden verwerkt om de voordelen van een blockchain te realiseren. Uit onderzoek blijkt dat dit niet eenvoudig is, en misschien zelfs onmogelijk.[333] Het is waarschijnlijk wel mogelijk een automatische controle op te stellen voor de meeste standaardgevallen,[334] dat dan echter verhindert dat bijzondere gevallen goed worden geregistreerd. De Kadasterwet geeft zeer gedetailleerde regels over de in te schrijven gegevens,[335] en het Kadaster controleert nu of alle vereiste gegevens wel aanwezig zijn.[336]
- Een beperking is verder de identificatie van het schip:[337] dat moet noodzakelijk gebeuren door fysieke controle van een schip, en er moeten waarborgen zijn dat een schip niet twee keer kan

[326] Rapportage verbetering Nederlands Scheepsregister 2016, p. 1.
[327] Rapportage verbetering Nederlands Scheepsregister 2016, p. 42.
[328] Bij wijzigingen in het scheepsregister (na de eerste teboekstelling) zijn ook andere partijen betrokken, zoals de notaris en een eventuele financierder.
[329] Deze complexe inrichting zorgt ook voor versnippering in de informatievoorziening. Er is geen ‘one stop information shop’-principe: partijen weten soms niet bij wie ze moeten zijn voor welke informatie, of worden weer doorverwezen. Rapportage verbetering Nederlands Scheepsregister 2016, p. 3.
[330] Het stilliggen van een schip kan tot duizenden tot tienduizenden euro’s per dag kosten, Rapportage verbetering Nederlands Scheepsregister 2016, p. 3.
[331] In zoverre voegt blockchain dan echter niets toe Vos, *JBN* 2018/11-50.
[332] Art. 3:18 BW, zie nader Asser/Bartels & Van Mierlo 3-IV 2013/300.
[333] Zie ten aanzien van landregistratie Vos, *JBN* 2018/11-50: het gaat dan bijvoorbeeld om diverse rechten die tegelijkertijd op een object rusten (bundle of rights), of de nu nog bestaande mogelijkheid om handmatig in een vrij veld commentaar toe te voegen.
[334] Deze zou dan in het blockchainprotocol kunnen worden opgenomen.
[335] O.a. art. 24-40 Kadasterwet.
[336] Art. 3:19 en 20 BW, met enkele correctiemogelijkheden of aanvullende aantekeningen over ontbrekende gegevens (bijv. art. 23, 37 lid 4 en 43 Kadasterwet). Verder zorg het Kadaster dat niet-verplichte stukken niet worden ingeschreven (art. 44 lid 3 Kadasterwet, maar zie art. 46 Kadasterwet), waardoor het register ‘schoon’ blijft.
[337] Bij percelen is de identificatie nadrukkelijk aandachtspunt: het staat bijvoorbeeld hoog op de agenda van de Dutch Blockchain Coalition, Vos, *JBN* 2018/11-45.

worden geregistreerd.[338] Dit deel van het registratieproces blijft dus afhankelijk van menselijke tussenkomst.

Wijziging van wettelijke regels

De huidige wettelijke regels staan in de weg aan een implementatie van het scheepsregister op een permissionless blockchain. Om dit mogelijk te maken zullen ten minste de volgende regels moeten worden gewijzigd.

- Als het register op een permissionless blockchain staat, kan het Kadaster niet langer verantwoordelijk zijn voor het register, zodat de Kadasterwet moet worden gewijzigd, evenals het Burgerlijk Wetboek.[339] Dit is alleen anders als wordt gekozen voor een implementatie waarbij het Kadaster doorslaggevende invloed heeft op de blockchain.[340] Het is niet nodig de hoofdregel over de openbare registers in het BW te wijzigen: art. 3:16 BW is in algemene termen geformuleerd en laat een implementatie in de vorm van een blockchain toe.
- Ook andere regels inzake de scheepsregistratie moeten worden gewijzigd, zoals art. 9 lid 2 Kadasterwet (dat documenten niet alleen elektronisch maar ook van papier e.d. kunnen zijn), art. 10a-11c Kadasterwet (over de wijze waarop stukken moeten worden aangeboden, de bevoegdheid van het bestuur van het Kadaster om regels te stellen, en de wijze waarop de inschrijving plaatsvindt), art. 117 Kadasterwet (over de aansprakelijkheid van het Kadaster voor fouten: het moet duidelijk worden gemaakt dat het Kadaster dan geen invloed heeft op de juistheid van het register en dat fouten in het register daardoor kunnen doorwerken in de kadastrale registratie van schepen). Ook zullen regels die ervan uitgaan dat de bewaarder van het register inschrijvingen weigert moeten worden veranderd.[341] Verder moet de uitvoering van de kadastrale registratie van schepen worden gewijzigd (art. 85-89 Kadasterwet), zie hierna. Tot slot zal mogelijk de uitvoerende regelgeving over schepen moeten worden gewijzigd.[342]
- De eis van notariële tussenkomst bij overdracht van schepen (art. 3:89 lid 1 juncto lid 4 BW), vestiging van (beperkte) rechten op schepen (art. 3:98 BW), en vestiging van een hypotheek (art. 3:260 BW).
- Het is niet nodig de regels over beslag op schepen te wijzigen, nu die regels alleen spreken over inschrijving in de registers (art. 566-568, 573, 579 Rv), en de wet niet verbiedt dat een register in de vorm van een blockchain wordt geïmplementeerd.
- Er zal nader onderzoek nodig zijn voor eventuele aanpassing van de regels in het Burgerlijk Wetboek die uitgaan van een voldoende betrouwbaar openbaar register.[343] Een blockchain geeft immers wel zekerheid over het moment van aanbieding van stukken, maar geen controle op de inhoudelijke juistheid, terwijl de aanvullende zekerheid van de kadastrale registratie ook komt te vervallen. Het valt te verwachten dat er vaker pogingen worden ondernomen voor fraude of misbruik, en een blockchain biedt daar niet vanzelf bescherming tegen. Een voorbeeld is ‘diefstal’ van een private key van de eigenaar van een schip:[344] als een blockchain volledig vertrouwt op de elektronische ondertekening kan de ‘dief’ vervolgens het schip overdragen aan een derde (zonodig via andere partijen). Die derde kan dan te goeder trouw zijn. Het is niet zeker of het wenselijk is dat

[338] Dit is namelijk verboden: Art. 8:194 lid 2 en 8:784 lid 2 BW, Parl. Gesch. Verkeersmiddelen en vervoer 1992, p. 259 in Asser/Japikse *8-II** 2012/26.
[339] O.a. moet worden gewijzigd art. 2a sub a en c (taak tot bevordering rechtszekerheid en informatievoorziening aan de overheid), art. 3 (het houden van de registers), art. 3d (bevoedheid tot stellen regels voor de opgedragen taken, waaronder maatregelen voor beveiliging, beheer), art. 7 (belast met verrichten van inschrijvingen), art. 9 Kadasterwet. Ook moet worden gewijzigd art. 3:19 en 20 BW, dat de bewaarder van de registers de bevoegdheid geeft een inschrijving die niet aan de wettelijke vereisten voldoet te weigeren.
[340] Zie daarover hieronder bij de nadelen, punt 5.
[341] Bijv. art. 8:790 lid 2 BW over het niet inschrijven van een rechterlijke uitspraak voordat deze in kracht van gewijsde is gegaan.
[342] Bijvoorbeeld de Maatregel teboekgestelde schepen 1992.
[343] Zie bijv. art. 3:23-26 BW, ook art. 8:800 lid 2 BW.
[344] Zulke ‘diefstal’ komt bij bitcoin regelmatig voor.

de oorspronkelijke eigenaar of de nieuwe eigenaar moet worden beschermd.[345] Op dit moment is zulke fraude nagenoeg onmogelijk door de controle die de notaris uitvoert.

Een permissionless blockchain voor het scheepsregister vereist aanpassing van tal van wettelijke regels. De belangrijkste regels hebben betrekking op de verantwoordelijkheid van het kadaster, het afschaffen van controles op inhoud van het register (door notaris en Kadaster), en het bijhouden van de kadastrale registratie. Verder is mogelijk aanpassing nodig van regels die voortbouwen op de bestaande betrouwbare kadastrale registratie.

Voordelen

1. Kostenbesparing. Doordat iedere partij zelf gegevens kan toevoegen en de bewaarder van het kadaster niet meer nodig is voor het scheepsregister.[346] Ook zou notariële tussenkomst overbodig zijn (als de regelgeving wordt aangepast).
2. Tijdsbesparing: de controles door de bewaarder van het kadaster en de notaris zouden niet nodig zijn of geautomatiseerd kunnen plaatsvinden (zoals controle of de vervreemder daadwerkelijk als eigenaar van het schip geregistreerd staat).[347] Overigens is dit ten dele ook mogelijk door verdere automatisering van het kadaster, zonder gebruik van blockchain.[348]

Nadelen

1. Het belangrijkste nadeel is het vervallen van de kadastrale registratie. Bij een scheepsregister op een permissionless blockchain zullen belanghebbenden zelf een onderzoek moeten doen op het register om alle relevante documenten te achterhalen en te analyseren om de actuele toestand van een schip vast te stellen. In andere landen is dit geen nadeel omdat zij geen kadastrale registratie kennen en dit dus de bestaande werkwijze is. Voor Nederland zou dit echter een significante achteruitgang betekenen met aanzienlijke kosten en tijdsverlies tot gevolg: partijen die een transactie willen verrichten zullen dan immers alsnog kosten moeten maken en moeten wachten totdat de verificatie van het register en de documenten is voltooid. De controle kan bij de huidige stand der techniek niet geheel automatisch worden uitgevoerd (vanwege de hierna te noemen extra controles die nodig zijn).

Een alternatief zou zijn om de kadastrale registratie te handhaven (naast het scheepsregister op een blockchain). Maar dan zou er alsnog betaald moeten worden voor de registratie van schepen (alleen dan niet voor inschrijving in het register zelf, maar voor het bijwerken van de kadastrale registratie[349]), en zullen daarbij ook controles moeten worden uitgevoerd om de beoogde betrouwbaarheid van de kadastrale registratie te behouden. De beoogde kosten- en tijdsbesparing wordt dan niet of slechts in beperkte mate gerealiseerd.

2. Identiteitscontrole. Identificatie op een blockchain vindt plaats door middel van een elektronische handtekening, de *private key*. Voor scheepsregistratie moet de werkelijke identiteit van de betrokken (rechts)personen worden vastgesteld,[350] en deze volgt niet rechtstreeks uit de private key (vaak is zelfs niet bekend wie achter een private key zit). Bij een gewone blockchain is er geen voorziening om de echte identiteit van een gebruiker vast te stellen,[351] tenzij er Trusted Third Parties worden ingeschakeld, maar dan wordt in wezen de notaris opnieuw uitgevonden. Het is mogelijk dat identiteitscontrole door een niet-notariële TTP goedkoper is, en men zou ook de eis van vaststelling van identiteit kunnen afschaffen. Er is echter een publiek belang bij vaststelling van identiteit: dit is bijvoorbeeld nodig voor bestrijding van witwassen en financieren van terrorisme.[352] Daarom is nodig

[345] Dit valt onder art. 3:86 BW, maar misschien moet er bij een register op blockchain een andere afweging plaatsvinden.
[346] Het is mogelijk dat het Kadaster nog wel de kadastrale registratie zou moeten bijhouden, zie hierna.
[347] Vos, *JBN* 2018/11-50.
[348] Vos, *JBN* 2018/11-50.
[349] Op grond van art. 108 Kadasterwet.
[350] Art. 18 en 21 Kadasterwet.
[351] Vos, *JBN* 2018/11-45.
[352] Op basis van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)

dat een betrouwbare partij de identiteitscontrole uitvoert. Overigens is mogelijk dat in de toekomst betere technische voorzieningen worden ontwikkeld voor identificatie van personen.[353]
3. Controles tegen fraude, misbruik en vergissingen. Overdracht van een schip (en andere handelingen) moeten daadwerkelijk gewild zijn door de eigenaar. Een blockchain heeft echter geen controles op (bijvoorbeeld) gebruik van een gehackte sleutel, dwang, wilsonbekwaamheid e.d. Het nut van de controle door de notaris is dat wordt verzekerd dat de overdracht van het schip geldig is en niet om zulke redenen moet worden teruggedraaid.[354] Ook bevat de huidige praktijk waarborgen tegen vergissingen van registerpartijen.[355] Zulke controles zijn niet mogelijk bij een blockchain. Daardoor is de betrouwbaarheid van een registratie op een blockchain lager: het is minder zeker dat de blockchain de daadwerkelijke juridische positie van een schip weergeeft.
4. De ongecontroleerde openbaarheid van een permissionless blockchain levert verder privacy-problemen op. Privacy-oplossingen voor permissionless blockchain gaan meestal uit van zogenaamde off-chain opslag (externe opslag), maar dat is niet mogelijk bij een openbaar register waar de informatie immers juist wel toegankelijk moet zijn. Hoewel privacyproblemen ook bij gewone openbare registers spelen,[356] kunnen zulke registers technische maatregelen treffen om de toegang enigszins te beperken (zoals het beperken van het aantal opvragingen, eisen dat het belang voor opvragen wordt onderbouwd).[357] Bij een permissionless blockchain zijn zulke maatregelen niet mogelijk.
5. Een (klein) risico is de mogelijkheid van een *fork*. In theorie kunnen twee registraties op ongeveer hetzelfde moment worden aangeboden. Het is mogelijk dat een blockchain dan splitst waardoor elke registratie in een ander deel van de blockchain wordt aanvaard als eerste registratie.[358][359] De kans hierop is echter klein. Wel laat het zien dat het nodig is dat er een mogelijkheid moet zijn om in te grijpen in de blockchain om zulke situaties op te lossen.[360] Het gebrek aan governance bij een gewone permissionless blockchain is ook problematisch als het gaat om het regisseren van updates van het register.[361] Er kan voor worden gekozen om het Kadaster een doorslaggevende stem te geven in de governance van het register (door opname van passende regels in het blockchainprotocol).[362]

Een permissionless blockchain voor het scheepsregister heeft als voordelen: kostenbesparing en tijdsbesparing, doordat geen tussenkomst van notaris en de bewaarder van het kadaster nodig is, en controles en verwerking geautomatiseerd plaatsvinden. Daar staan echter diverse nadelen tegenover.
Nadeel 1: de kadastrale registratie komt te vervallen, wat leidt tot aanzienlijke kosten en tijdsverlies bij latere transacties met schepen. Als de kadastrale registratie in stand zou moeten blijven bij een

[353] Vos, *JBN* 2018/11-45. Er zijn publiekrechtelijke mogelijkheden (zoals het DigiD), maar geen privaatrechtelijke. Eén van de initiatieven op dit gebied is de gebruiksproef in Eindhoven en Utrecht waarmee men zich kan identificeren via een telefonische app. Zie voor meer informatie: https://dutchblockchaincoalition.org/nieuws/digitale-identiteit-voor-op-je-telefoon. Oplossingen zonder gebruik van een blockchain zijn uiterard evenzeer mogelijk. Zie bijvoorbeeld IRMA: https://privacybydesign.foundation/irma/ .
[354] Zie Tjong Tjin Tai 2018 ten aanzien van onroerende zaken.
[355] Om de betrouwbaarheid van de informatie te waarborgen, wordt er daarom gebruik gemaakt van het vier-ogen-principe, controle op de volledigheid van de notariële akte door de bewaarder (en andersom), Vos, *JBN* 2018/11-50
[356] Zie A. Berlee 2017 en meer algemeen Louwman, *WPNR* 2018/7209. De minister van Binnenlandse zaken heeft aangegeven de huidige praktijk te handhaven: Brief van de Minister van Binnenlandse Zaken van 29 juni 2018.
[357] Art. 107b Kadasterwet biedt een grondslag voor zulke maatregelen.
[358] Vos, *JBN* 2018/11-50
[359] Zie hiervoor verder w.b.v.t. landregistraties Vos *ELRA* p. 22 e.v..
[360] In bekende blockchains als bitcoin en Ethereum vindt dit nu plaats door informele governance, zie par. 3.2.3.
[361] Daarom worden in andere landen waar blockchains worden gebruikt voor landregistratie ook niet gekozen voor een gewone permissionless blockchain.
[362] Dan zal moeten worden geregeld dat het Kadaster hier alleen in uitzonderingsgevallen gebruik van maakt, waarbij dan ook hoort dat het Kadaster niet verantwoordelijk of aansprakelijk is voor de inhoud van het register. Anders zou het Kadaster zich verplicht voelen om de inhoud van het register nauwgezet te controleren, wat zou leiden tot kosten voor het Kadaster (die uit de algemene middelen moeten worden betaald, omdat het bij een permissionless blockchain niet mogelijk is om een bijdrage van gebruikers te vragen), en tijdsverlies (wat men juist wilde voorkomen met een permissioneless blockchain).

scheepsregister op een permissionless blockchain vervallen de kostenbesparing en tijdsbesparing grotendeels en vermindert de betrouwbaarheid van de kadastrale registratie nog steeds.

Nadeel 2: de identificatie van de werkelijke personen kan niet geautomatiseerd plaatsvinden, en er is een publiek belang bij de identificatie (het bestrijden van witwassen en financiering van terrorisme).

Nadeel 3: de controles door de notaris en bewaarder van het kadaster verkleinen de kans dat een transactie moet worden teruggedraaid wegens fraude, misbruik, dwang of vergissingen. Als die controles vervallen wordt het scheepsregister minder betrouwbaar.

Nadeel 4: privacybescherming is moeilijk of zelfs onmogelijk op een permissionless blockchain met een openbaar register.

Nadeel 5: er is een kleine kans op een splitsing waardoor de toestand van een schip onbepaald is, en dat kan alleen worden opgelost met effectieve governance van de blockchain. Dat is echter moeilijk te verenigen met een permissionless blockchain.

Een alternatief is om de toegang tot blockchain te beperken tot de zogenaamde registerpartijen. Het gaat dan om een *permissionless, private* blockchain of om een *permissioned* blockchain. De bewaarder van het kadaster (en de notaris) functioneren als een *trusted third party*, waardoor de kwaliteit gewaarborgd blijft. Daarnaast wisselen de registerpartijen via de blockchain gegevens met elkaar uit en gaan daarbij uit van één set gegevens. Ook de reder (aanvrager voor de registratie) kan zien in welk deel van het proces zijn aanvraag zit.[363] Voordelen van deze opzet zijn:
- grotere transparantie van het proces voor de reder, die steeds kan zien bij welke stap de teboekstelling is.
- informatie tussen de verschillende registerpartijen worden gedeeld. De governance-structuur van deze scheepsregistratie kan daarbij helder worden neergezet,[364] wat de nu bekritiseerde complexiteit ten goede kan komen. Daarbij wordt communicatie verminderd en gestroomlijnd, doordat er van één set gegevens wordt uitgegaan, waarbij informatie niet meer bij verschillende registerpartijen opgevraagd hoeft te worden. Momenteel zorgt dit aspect voor langere doorlooptijden, met deze blockchaintoepassing zouden deze doorlooptijden en de administratieve lasten bij de reder worden verminderd.

De hierboven besproken nadelen en risico's bij een gewone permissionless public blockchain spelen niet bij de hier besproken varianten. Het bezwaar is echter dat een dergelijk systeem weinig meerwaarde heeft boven een traditioneel ICT-systeem.[365] Het komt in feite neer op automatisering met gebruik van een specifieke technologie. De specifieke voordelen van een blockchain spelen hier niet of nauwelijks een rol. Hierdoor is overigens ook geen wijziging van de wettelijke regels nodig.

Een permissioned blockchain of permissionless, private blockchain voor scheepsregistratie heeft niet de nadelen van een permissionless blockchain, maar daar staat tegenover dat het ook niet de voordelen oplevert die met een blockchain worden geassocieerd.

De slotconclusie is dat het gebruik van een blockchain voor scheepsregistratie voor Nederland weliswaar tot kosten- en tijdsbesparing bij registratie kan leiden, maar ertoe leidt dat het register minder betrouwbaar wordt. Gebruikers van het register moeten daardoor hoge kosten maken en tijd besteden om de actuele toestand van een schip met voldoende zekerheid vast te stellen. Een blockchain zou de goede en betrouwbare kadastrale registratie tenietdoen, tenzij de blockchain wordt gebruikt als interne administratie van het kadaster.

Conclusie: Het gebruik van een permissionless public blockchain voor het scheepsregister leidt slechts tot een verschuiving van kosten en tijd (van initiële registratie naar latere transacties) en

[363] Een derde optie die in de literatuur wordt genoemd is een hybride vorm: een gesloten omgeving waarbij verschillende partijen samenwerken om data of transacties te delen. Hierbij kan iedereen de kadastrale registraties en de openbare registers inzien, maar zijn enkele partijen gerechtigd d.m.v. schrijfrechten om wijzigingen aan te brengen. Een voorbeeld kan men zien in 3R, een consortium van banken die in een vertrouwde omgeving transacties willen uitvoeren. Voor een uitgebreidere beschrijving, zie Vos, *ELRA*, en Vos, *JBN* 2018/11-50.

[364] Vos, *JBN* 2018/11-50.

[365] Dit was de conclusie van pilots van het Kadaster op het gebied van het afgeven van vergunningen, zie de pilot Eenvoudig Beter Bouwen http://www.eenvoudigbeterbouwen.nl/, laatst geraadpleegd op 30-10-2018.

heeft een lagere betrouwbaarheid van de Nederlandse scheepsregistratie tot gevolg. Daarnaast zijn er risico's voor fraude, privacy, en misbruik voor witwassen e.d. Voor Nederland, wegens de hier bestaande kwalitatief hoogwaardige scheepsregistratie, is een permissionless public blockchain daarom geen zinvolle optie. Andere blockchainvarianten zijn mogelijk maar hebben niet de voordelen van een permissionless public blockchain. Afhankelijk van de gekozen opzet zullen ook wettelijke regels in meerdere of mindere mate moeten worden aangepast.

4.3 Use-case 2: geautomatiseerde compliance en administratieve lastendruk – schatkistbankieren en onderwijshuisvesting[366]

De use-case in steekwoorden

Probleem: een gecompliceerd proces van aanvragen en besluiten rond schatkistbankieren
Relevante partijen: onderwijsinstelling, Agentschap van het Ministerie van Financiën, Ministerie van OCW, Auditdienst Rijk, de gemeente
Geclaimde bijdrage van blockchain: het verlichten van de administratieve lastendruk.
Juridische implicaties: blockchain is blind voor wat buiten de blockchain gebeurt, blockchain garandeert niet dat gegevens correct zijn ingevoerd.
Balans: De meerwaarde van een blockchain blijft onduidelijk ook voor verantwoordingsprocessen.

In deze use-case bespreken wij een reeds afgeronde pilot die binnen het Ministerie van Financiën heeft plaatsgevonden in het kader van schatkistbankieren.[367] Er is in de pilot concreet gekeken naar de toepassing van blockchain technologie in het proces voor het verstrekken van een lening voor nieuwbouw aan een onderwijsinstelling. Het betreft hier een fictieve casus met een aantal duidelijke afbakeningen en simplificaties. Zo is er in de pilot geen rekening gehouden met de transactiegeschiedenis tussen de verschillende betrokken partijen, maar wordt er enkel gekeken naar de specifieke transactie van financiering voor nieuwbouw. Daarnaast is het proces van de financiering enigszins vereenvoudigd vormgegeven, aangezien dit traject in de praktijk talloze iteraties tussen de verschillende betrokken partijen met zich meebrengt. Ook is er in de pilot geen rekening gehouden met de relevante huidige wettelijke kaders; het hoofddoel van deze pilot was namelijk om de technische mogelijkheden van schatkistbankieren door middel van blockchain technologie te verkennen (een “proof of technology”). Een en ander heeft als logisch gevolg dat de scope van deze use-case relatief beperkt is. Wel biedt deze use-case een interessante context om in het bijzonder te reflecteren op de mogelijke gevolgen van blockchain technologie met betrekking tot het verminderen van administratieve lastendruk. Voordat de invulling van de use-case wordt beschreven is het van belang om eerst de huidige situatie uitvoerig uiteen te zetten, zodat de voor- en nadelen van toepassing van blockchain technologie in de context van schatkistbankieren beter in perspectief kunnen worden geplaatst.

4.3.1 Korte beschrijving van de use-case

Het bestaande proces begint met een besluit tot nieuwbouw van het bestuur van de onderwijsinstelling. Vervolgens worden de voorwaarden van de nieuwbouw door het Ministerie van Onderwijs, Cultuur en Wetenschappen (OCW) en de gemeente gecontroleerd. Als er aan deze voorwaarden wordt voldaan wordt er gekeken naar de financiële kant van het project. In deze fase dient er in elk geval een raming te komen van de kosten van het project die is goedgekeurd door het bestuur van de onderwijsinstelling (op basis van offertes van architect en aannemer), alsmede een inschatting van de betaalcapaciteit en de reserves van de onderwijsinstelling. Indien ook deze horde genomen is zal er gezocht worden naar financieringsmogelijkheden.

Er zijn in het huidige systeem verschillende manieren waarop een onderwijsinstelling nieuwbouw kan financieren. Ten eerste kunnen gemeenten zelf huisvesting financieren door hun reserves aan te spreken. In dit geval vindt het besluitvormingsproces voor het grootste deel binnen

[366] De beschrijving van deze use-case is grotendeels gebaseerd op de Notities “Nadere uitwerking pilot blockchain” en “Evaluatie pilot blockchain” van het Ministerie van Financiën.
[367] De pilot heeft geresulteerd in een prototype waarvoor gebruik is gemaakt van blockchain technologie (https://www.youtube.com/watch?v=tOFO11Shvw4).

de gemeente plaats en is er slechts beperkte betrokkenheid van bijvoorbeeld OCW. Voor de huidige pilot is deze situatie minder relevant, aangezien blockchain technologie vooral geschikt lijkt om processen te optimaliseren waarbij meerdere publieke en / of private partijen betrokken zijn. Onderwijsinstellingen kunnen ook gebruik maken van een commerciële lening om nieuwe huisvesting te realiseren. Omdat de lening in dit geval wordt aangegaan op basis van marktconforme voorwaarden wordt deze variant in de praktijk weinig gebruikt. In de pilot ligt de nadruk dan ook op een derde variant, namelijk financiering door middel van het zogenaamde schatkistbankieren.

Schatkistbankieren stelt onderwijsinstellingen in staat om op vrijwillige basis een lening af te sluiten via het Ministerie van Financiën ten behoeve van investeringen in huisvesting.[368] In de pilot is vooral gekeken naar de rol van de partijen in dit proces, namelijk de onderwijsinstelling, de gemeente (in dit specifieke geval, de gemeente Amsterdam), OCW, het Agentschap van het Ministerie van Financiën en de Auditdienst Rijk. De partijen zijn op verschillende momenten bij het proces betrokken. Het Agentschap speelt zowel in de aanvraag- als afhandelingsfase van het proces een rol. In de aanvraagfase benadert de onderwijsinstelling haar accountmanager met het verzoek om een lening af te sluiten bij het Ministerie van Financiën ten behoeve van huisvesting. De accountmanager deelt de onderwijsinstelling mede dat goedkeuring van OCW vereist is. Ook moet de onderwijsinstelling een financieel toetsingsdocument invullen waarin inzicht wordt gegeven in de financiële situatie van zowel de afgelopen als de komende vijf jaar. Daarnaast is er een garantstelling voor de lening nodig van OCW (dit is de verantwoordelijkheid van de onderwijsinstelling) en de gemeente (dit is de verantwoordelijkheid van OCW).

De hoogte van de uiteindelijke lening is afhankelijk van de omvang van de garantstelling van de gemeente. De aanvraag voor schatkistbankieren wordt behandeld in het College van B&W en na goedkeuring door de gemeenteraad wordt de garantstelling teruggekoppeld naar OCW. OCW ontvangt op haar beurt van het Agentschap 1) een gespreksverslag tussen de onderwijsinstelling en het Agentschap over de behoefte, 2) de goedgekeurde en ondertekende aanvraag en 3) het financieel toetsingsdocument. Binnen OCW zelf bestaat het proces om een garantstelling te verlenen in het kader van schatkistbankieren uit vijf stappen. De eerste stap is het toetsen van de aanvraag na ontvangst. Vervolgens vindt de verrekening plaats als gevolg van overschrijding van de kredietlimiet door de onderwijsinstelling. Hierna wordt de risicopremie ontvangen, de hypotheekakte gepasseerd en tot slot worden kwartaaloverzichten gecontroleerd. De volledige aanvraag wordt goedgekeurd indien diverse betrokken partijen, waaronder de Inspectie van het Onderwijs, akkoord zijn.

Binnen het Agentschap voert de accountmanager nu de gegevens in voor de offerte. Een andere accountmanager controleert deze gegevens en parafeert het berekende tarief. Voordat de offerte wordt opgestuurd naar de onderwijsinstelling parafeert het hoofd Cash Management en Kapitaalmarktoperaties. Nu wordt ook de “Overeenkomst van geldlening” opgesteld, die wordt ondertekend door het hoofd van Staatsschuld- en Schatkistbeheer. De overeenkomst wordt in tweevoud per post naar de onderwijsinstelling verzonden voor ondertekening. Als de door beide partijen ondertekende overeenkomst is ontvangen wordt de geldlening uiterlijk op de ingangsdatum door een accountmanager ingevoerd. Een andere accountmanager controleert en accordeert de gegevens. De hoofdsom van de geldlening wordt automatisch op de rekening-courant van de onderwijsinstelling gestort en een bevestiging hiervan wordt opgestuurd naar de onderwijsinstelling. Tot slot wordt het originele document gescand en gearchiveerd in het elektronisch dossier van de onderwijsinstelling.

De stroom van informatie behorende bij het proces zoals hierboven uiteengezet is op verschillende manieren vormgegeven. De gemeente Amsterdam gebruikt een drietal informatiesystemen, te weten het “Amsterdamse Financiële Systeem”, het subsidiebeheersysteem en het digitale schooldossier. OCW maakt gebruik van Office-pakketten; zo worden bijvoorbeeld Microsoft Word, Excel en Outlook gebruikt bij het ontvangen en controleren van een aanvraag. Het Agentschap gebruikt tijdens de aanvraag enkel IRC/LEDA (een Oracle-gebaseerd

[368] Het is voor onderwijsinstellingen ook mogelijk om door middel van schatkistbankieren onder voorwaarden een rekeningcourantkrediet af te sluiten. Gezien de invalshoek van deze use-case gaan wij hier nu niet verder op in.

administratiesysteem voor rekening-courant, lening– en depositoadministratie). Tijdens de afhandeling worden naast IRC/LEDA nog Digidoc (een documentbeheer- en archiefsysteem) en Office-pakketten (Word, Excel en Outlook) gebruikt.

Het bovenstaande overzicht toont aan dat het proces voor nieuwbouw van een onderwijsinstelling door middel van schatkistbankieren uit een groot aantal stappen bestaat, waarbij meerdere partijen betrokken zijn. Het proces als geheel brengt ook de nodige administratieve lasten met zich mee. We komen hier later uitgebreid op terug.

4.3.2 Kansen en risico's

Het hierboven beschreven proces is in de pilot in een blockchain geïmplementeerd. Zoals gezegd was het doel van de pilot om het proces te stroomlijnen vanuit het perspectief van de onderwijsinstelling en de bijbehorende administratieve lastendruk voor de betrokken partijen zoveel mogelijk te beperken. Concreet betekent dit dat de bestaande procedure zoveel mogelijk "as is" is vormgegeven in een blockchain. In de pilot is de procedure geprogrammeerd in de vorm van smart contracts. Een smart contract houdt ruwweg in dat de procedure voor het verstrekken van een lening voor huisvestingsdoeleinden geautomatiseerd wordt. Het verstrekken van een lening kan in een smart contract gecombineerd worden met (strikte) voorwaarden over bestedingsdoeleinden door gebruik te maken van cryptocurrency (digitale valuta). In de huidige context ligt de controle op de voorwaarde om de lening voor nieuwbouw in te zetten bij de gemeente. Omdat het op dit moment nog niet mogelijk is om de euro rechtstreeks in de blockchain te integreren is ervoor gekozen om twee afzonderlijke geldstromen bij te houden: een cryptobudget (waarmee uitvoering is gegeven aan het smart contract) en een "fysiek" budget waarop de euro's werden overgeboekt.

Door gebruik van blockchain technologie gaat (na de nodige checks and balances, zie de bovenstaande beschrijving) het bedrag van de financiering eerst van de schatkist naar het Agentschap. Vervolgens doet het Agentschap een financieringsvoorstel aan de onderwijsinstelling ten behoeve van de nieuwbouwplannen. Indien de onderwijsinstelling akkoord is met het voorstel maakt het Agentschap het geld (in cryptovaluta) over naar de onderwijsinstelling. De onderwijsinstelling ontvangt via een smart contract ook een offerte van de aannemer. Indien de onderwijsinstelling akkoord is wordt het geld (in cryptovaluta) overgeboekt naar de aannemer. Uiteindelijk stuurt de aannemer een factuur voor het geleverde werk. De onderwijsinstelling voldoet deze factuur in euro's en de cryptovaluta vloeit terug naar de schatkist. Hiermee is het proces van schatkistbankieren voor nieuwbouw voltooid.

Wat zijn nu concreet de (mogelijke) voordelen van het toepassen van blockchain technologie in het kader van schatkistbankieren voor nieuwbouw? In de eerste plaats zijn er de algemene voordelen van blockchain op het onderdeel transparantie. Aangezien blockchain een gedeeld platform is hebben betrokken geautoriseerde partijen toegang tot dezelfde beveiligde informatie. Ook valt uit de blockchain duidelijk af te lezen waar het proces van schatkistbankieren zich op elk moment bevindt en welke documentatie eventueel nog ontbreekt. Hierdoor wordt het minder waarschijnlijk dat dossiers onnodige vertraging oplopen doordat ze "op iemands bureau blijven liggen", of informatie op een verkeerde of omslachtige wijze wordt aangeleverd. Hierbij dient opgemerkt te worden dat in beginsel andere IT-toepassingen ook eenzelfde mate van transparantie zouden kunnen bieden. Uit de pilot is gebleken dat de betrokken partijen verschillende applicaties gebruiken om informatiestromen te laten plaatsvinden en dat deze niet of nauwelijks met elkaar gekoppeld zijn. Het koppelen van deze bestaande applicaties zou, ook zonder toepassing van blockchain, de transparantie van het proces al vergroten.

Het koppelen van deze bestaande applicaties zou, ook zonder toepassing van blockchain, de transparantie van het proces al vergroten.

De belangrijkste meerwaarde die toepassing van blockchain in de context van schatkistbankieren voor nieuwbouw te bieden heeft lijkt het verminderen van administratieve lastendruk te zijn die komt kijken bij het verzamelen, aanleveren en delen van gegevens. Zo kunnen door middel van smart contracts offertes door verschillende aannemers worden ingediend, die

vervolgens op eenvoudige wijze - en zonder extra papierwerk - door de onderwijsinstelling kunnen worden goedgekeurd of afgewezen. Deze interacties zijn vervolgens ook direct inzichtelijk voor andere partijen, zoals OCW. Dit betekent dat een onderwijsinstelling minder tijd en geld kwijt is aan het aanleveren van informatie aan afzonderlijke partijen. Ook wordt het door toepassing van blockchain technologie mogelijk om bepaalde controle- en beveiligingsmechanismen te beperken. Partijen gebruiken op dit moment nog hun eigen mechanismen voor controle- en beveiligingsdoeleinden (zoals firewalls om datasets af te schermen), die kunnen overlappen of zelfs conflicteren. Blockchain technologie biedt de mogelijkheid om de beveiliging en controle van een proces te stroomlijnen en onnodige overlap te beperken. Dit resultaat kan echter ook behaald worden door in algemenere zin informatiestromen beter te synchroniseren en koppelen. Uiteraard moet ook worden opgemerkt dat er beperkingen vanuit wet- en regelgeving bestaan die het delen van informatie aan banden legt.

Niet alleen in de aanvraagfase, maar ook bij de verantwoordingsfase biedt blockchain technologie mogelijkheden om de administratieve lasten terug te dringen, of mogelijk zelfs volledig te schrappen. In het bovenstaande proces is de financiering van de nieuwbouw op een dergelijke wijze geautomatiseerd dat de fondsen enkel voor dit specifieke doeleinde kunnen worden ingezet. Een uitgebreide controle om te bepalen of het geoormerkte bedrag daadwerkelijk op de juiste plek terecht is gekomen is dan ook niet meer nodig. Op deze manier kunnen in elk geval twee soorten kosten bespaard worden. Ten eerste betekent het oormerken van fondsen dat er minder middelen hoeven worden ingezet om bestedingen te controleren. Ten tweede worden de kosten die gemaakt moeten worden om eventuele foutieve bestedingen in het bestaande systeem te corrigeren vermeden indien fondsen per definitie op de juiste plek terecht komen. De gedeelde informatie die op de blockchain staat houdt ook in dat controlerende instanties (een groot deel van) de benodigde gegevens rechtstreeks uit de blockchain kunnen aflezen. Hierdoor kunnen de administratieve lasten bij controlerende instanties, zoals de Algemene Rekenkamer en Auditdienst Rijk, worden teruggedrongen. Ook biedt blockchain technologie de mogelijkheid om bestaande backend-systemen binnen organisaties te vervangen, waarbij de huidige grotendeels ongestructureerde systemen (met relatief veel administratieve lastendruk) worden vervangen door een zeer gestructureerd systeem (met relatief weinig administratieve lastendruk). Andermaal moet worden opgemerkt dat de wijziging van ongestructureerde naar gestructureerde systemen ook zonder blockchain technologie tot stand kan komen.

Hoewel de toepassing van blockchain de administratieve lastendruk voor betrokken partijen kan verlichten is het van belang om op te merken dat dit niet noodzakelijkerwijs het geval zal zijn. In de bestaande academische literatuur wordt namelijk onderscheid gemaakt tussen objectieve en gepercipieerde lastendruk.[369] De objectieve lastendruk, die vooral betrekking heeft op de hoeveelheid papierwerk, de regelgevingsdichtheid op een bepaald terrein en het aantal procedurele stappen dat gevolgd dient te worden zou door een (correcte) implementatie van blockchain verminderd moeten worden. Echter, administratieve lastendruk wordt door individuen veelal *gepercipieerd* als een overkoepelend probleem dat veel meer omvat dan deze objectieve componenten. In een onderzoek naar administratieve lasten bij de Nederlandse politie concludeerden Kort en Terpstra onder andere dat het niet alleen gaat om “een veelheid van tijdrovende administratieve procedures, maar in de meeste gevallen ook om gebrekkige of gebruikersonvriendelijke politie-ICT, of om een complexe en weinig eenduidige wijze waarop het werk is georganiseerd.”[370] Bij de toekomstige implementatie van blockchain (of vergelijkbare technologieën) is een gebruiksvriendelijke interface dan ook van groot belang. Bestaand onderzoek heeft ook aangetoond dat percepties van administratieve lastendruk onder meer samenvallen met de organisatiestructuur (in termen van hiërarchie en centralisatie), het type functie dat bekleed wordt en de gewenstheid van procedurele uitkomsten. Dit zijn allemaal dimensies van administratieve

[369] Zie bijvoorbeeld B Bozeman en M K Feeney, Rules and Red Tape: A Prism for Public Administration Theory and Research (M.E. Sharpe 2011).
[370] J. Kort en J. B. Terpstra, ‘ ‘Onnodige’ Bureaucratie binnen het Basispolitiewerk: Onderzoek naar de Achtergronden van een Hardnekkig Verschijnsel’ (2015) Politie en Wetenschap 1.

lastendruk waar de implementatie van blockchain technologie normaliter geen (directe) invloed op zal uitoefenen.

De pilot die in deze use-case beschreven is heeft een exploratief en beperkt karakter. De proof of technology heeft zich dan ook gericht op een klein deel van het volledige proces en met betrokkenheid van een beperkt aantal partijen. Het is dan ook duidelijk dat het opschalen van een blockchain naar een volledig ketenproces de nodige moeilijkheden met zich meebrengt, waarbij nog geen eenduidig antwoord kan worden gegeven of de mogelijke baten de lasten overstijgen. Er bestaan in elk geval een vijftal risico's en knelpunten die van invloed zullen zijn op de haalbaarheid van blockchain technologie in de context van schatkistbankieren; ontbrekende infrastructuur en knowhow, beperkte toepasbaarheid, onduidelijkheid over transformatie van ketenprocessen, mogelijke veiligheidsproblemen van het systeem en het ontbreken van de koppeling tussen blockchain en de euro.

In de eerste plaats moet worden geconstateerd dat de infrastructuur en knowhow voor toepassing van blockchain nog niet afdoende aanwezig is. Uit de pilot is concreet naar voren gekomen dat betrokken partijen gebruik maken van verschillende back-end systemen ter ondersteuning van hun deel van het ketenproces. Daarnaast zijn blockchain initiatieven op dit moment voorbehouden aan een kleine groep early adopters. Op dit moment worden er afzonderlijke pilots uitgevoerd op verschillende deelterreinen, maar het is gegeven de aard van blockchain technologie goed mogelijk dat in de toekomst verschillende ketenprocessen aan elkaar gekoppeld gaan worden. Het is een noodzakelijke voorwaarde voor het succes van blockchain technologie dat alle partijen met hetzelfde systeem werken, maar voor het zover is zullen flinke investeringen gedaan moeten worden in hardware en software.

Er zal ook aandacht geschonken moeten worden aan de verschillen in draagkracht van de betrokken partijen; zo hebben OCW en het Ministerie van Financiën aanzienlijk meer middelen tot hun beschikking voor blockchain implementatie dan bijvoorbeeld een kleine onderwijsinstelling. Desondanks zullen alle betrokken partijen uiteindelijk in staat moeten zijn om van dezelfde smart contracts gebruik te maken, wil de toepassing van blockchain succesvol zijn. De benodigde investeringen zullen in deze specifieke context waarschijnlijk niet snel renderen, aangezien schatkistbankieren voor onderwijshuisvesting meer van incidentele dan van structurele aard is. Daarnaast dient, in algemenere zin, nagedacht te worden over de wijze waarop een mogelijke transitie naar blockchain plaats zal vinden. Worden bestaande systemen in relatief korte tijd volledig vervangen door een nieuw systeem, of wordt gekozen voor een transitiefase waarbij bestaande systemen enige tijd zij-aan-zij bestaan met blockchain technologie? De toepassing van blockchains brengt de reguliere problematiek met zich mee die zich voordoet wanneer verschillende partijen nauw moeten samenwerken, maar voegt daar ook onzekerheid over en onbekendheid met een nog nieuwe technologie aan toe.

Blockchain technologie heeft, evenals andere ICT-toepassingen, potentie om de transparantie van ketenprocessen te vergroten en administratieve lasten te verminderen. Echter, het is in deze eerste implementatie fase minstens zo belangrijk voor beleidsmakers en leidinggevenden om na te denken over welke zaken beter *niet* in een blockchain gevat kunnen worden. Zo zal bijvoorbeeld de "voorfase" van het proces van nieuwbouw, waarbij de onderwijsinstelling diverse mogelijkheden voor nieuwbouw onderzoekt, vaak weinig gestructureerd en meer verkennend zijn. Het is dan ook niet zinvol om deze fase te proberen in een zeer gestructureerd smart contract te vangen. Zo worden aan de kant van de gemeente voorafgaand aan de financieringsfase regionale plannen opgesteld, waarbij bijvoorbeeld afspraken met onderwijsinstellingen worden gemaakt over welke instellingen vervangende ruimte nodig hebben. Bij dit soort strategische processen is het van belang om vooruit te denken, belangen tegen elkaar af te zetten en een menselijke norm te gebruiken; de toepassing van blockchains is in deze situatie dan ook niet voor de hand liggend.

Deze bevindingen impliceren dat, zelfs wanneer een bepaald proces als geheel in aanmerking komt voor toepassing van blockchain technologie, er bij de ontwikkeling van toekomstige wet- en regelgeving expliciete keuzes moeten worden gemaakt over welke elementen van een bestaand proces in een blockchain vervat gaan worden en welke niet. Indien gekozen wordt voor een brede toepassing van blockchains ontstaat er een risico dat noodzakelijke creativiteit en

flexibiliteit in het proces verloren gaat, terwijl een gelimiteerde toepassing van blockchain technologie in een ketenproces slechts tot beperkte voordelen zal leiden. Toekomstige discussies dienen dus niet alleen gericht te zijn op de geschiktheid van processen en procedures als geheel voor toepassing van blockchains, maar juist ook op de specifieke onderdelen van deze processen en procedures.

In toekomstige wet- en regelgeving moeten expliciete keuzes worden gemaakt over welke elementen van een bestaand proces in een blockchain vervat gaan worden en welke niet. Indien gekozen wordt voor een brede toepassing van blockchains ontstaat er een risico dat noodzakelijke creativiteit en flexibiliteit in het proces verloren gaat, terwijl een gelimiteerde toepassing van blockchain technologie in een ketenproces slechts tot beperkte voordelen zal leiden.

De situatie wordt nog complexer indien bepaalde ketenprocessen en activiteiten *zelf* getransformeerd worden door de toepassing van blockchain technologie. Zo zal bijvoorbeeld de rol van auditors door de toepassing van blockchains wezenlijk kunnen veranderen. Het gebruik van smart contracts zorgt ervoor dat de rechtmatigheid, doelmatigheid en doeltreffendheid van processen en procedures automatisch gewaarborgd kunnen worden, mits de kwaliteit van de data hiervoor afdoende is. Auditing op deze vlakken is dus niet langer, of in mindere mate, nodig. In plaats daarvan zullen auditors zich meer moeten richten op een controle “ex ante” van de implementatie van blockchain, gekoppeld met een controle naderhand om te bepalen of het toegepaste systeem later niet onrechtmatig gewijzigd is. Een dergelijke verandering in de functie en taakopvatting van organisaties, of zelfs volledige sectoren, is een zeer ingrijpend proces dat jaren, zo niet decennia, zal duren. Gegeven de uiterst dynamische aard van blockchain en vergelijkbare technologieën zal de precieze vorm van de transformatie van ketenprocessen en activiteiten pas gaandeweg zichtbaar worden.

Een ander belangrijk aandachtspunt is het waarborgen van de veiligheid van de gebruikte systemen. Op dit moment is de identificatie en authenticatie van gebruikers nog niet volledig gewaarborgd in de pilot. De betrouwbaarheid van het systeem, alsmede de bereidheid van ketenpartners om van het systeem gebruik te maken en de uiteindelijke maatschappelijke acceptatie, zal gebaat zijn bij een situatie waarin zekerheid bestaat over “wie er precies achter de knoppen zit”. Op dit moment houdt een werkgroep vanuit de Dutch Blockchain Coalition zich al met deze problematiek bezig.

Tot slot is er nog het concrete knelpunt dat in de huidige situatie de euro niet direct in de blockchain gebruikt kan worden. Om die reden is er een afzonderlijke boekhouding noodzakelijk waarmee euro’s daadwerkelijk kunnen worden overgeboekt. Het moge duidelijk zijn dat het bijhouden van zo’n alternatieve, traditionele boekhouding een deel van de voordelen van blockchain technologie tenietdoet. Dit probleem doet zich niet alleen voor bij de huidige use-case, maar treft blockchain initiatieven in het algemeen. Op dit moment vindt overleg plaats tussen onder andere het Ministerie van Financiën en De Nederlandsche Bank om te bepalen hoe een “Central Bank Digital Currency” mogelijk vorm kan krijgen.

4.3.3 Juridische knelpunten

In deze use-case is met name het gebruik van blockchain als middel om verantwoording af te leggen juridisch interessant.[371] In dit kader wordt nader ingegaan op de rol van de Auditdienst Rijk. De Auditdienst Rijk heeft onder andere als taak het financiële beheer van het Rijk te controleren.[372] Daarbij wordt gekeken of het beheer voldoet aan normen van doelmatigheid,

[371] De Wet op het Primair Onderwijs is voornamelijk relevant voor situaties waarin de gemeente nieuwbouw bekostigt. Dat valt buiten deze use-case. Art. 91 e.v. Wet op het primair onderwijs stellen regels ten aanzien van de bekostiging door de gemeente van huisvestingsvoorzieningen. Als de bouwplannen van een niet door de gemeente in stand gehouden school niet met gemeentelijke voorzieningen gerealiseerd worden (terwijl dat wel had gekund), behoeven de bouwplannen en begrotingen toch instemming van B&W (art. 104 WPO).
[372] Art. 4(3) Besluit Auditdienst Rijk.

rechtmatigheid, ordelijkheid en controleerbaarheid.[373] Doelmatigheid ziet hier op zowel op efficiency, i.e. het hebben van het optimale effect tegen zo min mogelijk kosten en zuinigheid, i.e. doelmatigheid van de verwerving en het gebruik van de apparaatsmiddelen.[374]

Een blockchain die schatkistbankieren ten behoeve van de nieuwbouw van een schoolgebouw structureert zal controles door de Auditdienst Rijk allicht vereenvoudigen. Uit de informatie opgenomen in de blockchain kan allicht afgeleid worden dat de juiste procedure is doorlopen en dat de benodigde goedkeuringen verkregen zijn. Dat is van belang voor de rechtmatigheid. De blockchain zal ook bijdragen aan de ordelijkheid van het financieel beheer, indien hij een duidelijke workflow ondersteunt. Het feit dat alle stappen in het proces worden vastgelegd maakt het geheel ook controleerbaarder. Er zijn echter twee kanttekeningen te plaatsen. In de eerste plaats zijn de genoemde voordelen ook zonder een blockchain te realiseren. Met andere woorden, de automatisering die nodig is bouwt niet op kenmerken die specifiek zijn voor blockchains. In de tweede plaats dekt een blockchain implementatie niet alle dimensies die de Auditdienst zou willen controleren af. Voor het beoordelen van efficiency (van belang voor het oordeel over doelmatigheid) zal een blockchain bijvoorbeeld niet alle benodigde informatie bevatten. Ter illustratie: uit de blockchain zal niet blijken of het schoolgebouw ook voor een lager bedrag gerealiseerd had kunnen worden. Ook kan een smart contract helpen ervoor te zorgen dat de financiering uitsluitend besteed wordt om een aannemer te betalen, maar niet of de aannemer goed werk levert (dit is weer van belang voor de doelmatigheid). Een blockchain is immers blind en kan alleen zien wat in de blockchain staat of via een oracle binnenkomt. De blockchain maakt de Auditdienst Rijk dus niet overbodig.

De betrokken ministers zijn gehouden aan de Auditdienst Rijk alle goederen, administraties, documenten en andere informatiedragers waarvan de raadpleging van belang kan zijn voor haar onderzoek voor dat doel beschikbaar te stellen.[375] Het is aan te nemen dat de ministers aan deze plicht kunnen voldoen door de Auditdienst Rijk toegang te geven tot de blockchain, althans die delen die betrekking hebben op het schatkistbankieren ten behoeve van de nieuwbouw van scholen. Administraties en informatiedragers kunnen ter beschikking worden gesteld door toegang daartoe te geven. Overigens is het bij blockchains die gebaseerd zijn op crypto-economische prikkels niet eenvoudig gedifferentieerd toegang te geven. Eenieder moet immers toegang kunnen hebben tot de volledige blockchain om te controleren welke versie de langste is die uitsluitend bestaat uit geldige blokken. Dan zit men al snel vast aan off-chain opslag met on-chain een versleutelde hash van de off-chain opgeslagen gegevens. Gedifferentieerde toegang is dan mogelijk via het sleutelbeheer.

[373] art. 3.3 Comptabiliteitswet 2016.
[374] Kamerstukken TK, 2015-2016, 34.426, MvT, p. 72.
[375] Art. 5(1) Besluit Auditdienst Rijk.

4.4 Use-case 3: Het vervoer van afvalstoffen op grond van de EVOA

4.4.1 Korte beschrijving van de use-case, inclusief kansen en risico's

De use-case in steekwoorden

Probleem: een gecompliceerd proces van meldingen en controles van afvaltransporten
Relevante partijen: afval vervoerders, ILT, buitenlandse autoriteiten
Geclaimde bijdrage van blockchain: een vlottere workflow
Juridische implicaties: het corrigeren van gegevens wordt lastiger/onmogelijk, blockchain garandeert niet dat gegevens (correct) zijn ingevoerd en verschillende nationale interpretaties van de EVOA zijn lastig te accommoderen binnen een blockchainoplossing.
Balans: blockchain lost een aantal relevante problemen niet op.

De Europese Verordening Overbrenging Afvalstoffen (EVOA Verordening)[376] stelt regels voor het vervoer van afvalstoffen binnen de Europese Unie. Iedere lidstaat houdt toezicht op het vervoer binnen zijn eigen grondgebied en in Nederland is het Ministerie van Infrastructuur en Waterstaat, Inspectie Leefomgeving en Transport daarmee belast.[377]

Het in de EVOA voorgeschreven proces komt in hoofdlijnen op het volgende neer. Bedrijven die afval transporteren binnen de EU zijn vergunningplicht. Aan de verleende vergunningen zijn voorwaarden verbonden, zoals bijvoorbeeld de maximale hoeveelheid afval die in een jaar vervoerd mag worden. Voor aanvang van ieder transport moet het bedrijf de Inspectie Leefomgeving en Transport van het voorgenomen transport in kennis stellen. De Inspectie controleert dan of het transport binnen de vergunningsvoorwaarden valt. Indien dat het geval is, wordt toestemming verleend. Tevens wordt een melding doorgezet naar de autoriteiten van de transitlanden en het bestemmingsland. Het stelsel vergt derhalve het een en ander aan meldingen en controles. De Inspectie wil verkennen of de voorgeschreven meldingen en daarmee samenhangende controles via smart contracts in een blockchain afgewikkeld kunnen worden.

Daartoe wordt bij wijze van proof-of-concept een blockchaintoepassing gebouwd. Deze toepassing draait op een permissioned blockchain van een BaaS-aanbieder. Dat wil zeggen dat er sprake is van een infrastructuur van nodes die door een aanbieder wordt aangeboden en waarop meerdere cliënten applicaties kunnen bouwen. De in opdracht van de Inspectie gebouwde blockchaintoepassing is schaalbaar zodat zij bij wijze van test in de praktijk gebruikt kan worden. Een beperkt aantal vervoerders en de bevoegde autoriteit in België verkrijgen toegang tot de blockchain. Afhankelijk van hun rol kunnen zij gegevens op de blockchain schrijven of deze lezen. Sommige gegevens, zoals bijvoorbeeld bedrijfsgevoelige informatie is alleen toegankelijk voor het betreffende bedrijf en toezichthouders. Dit wordt gerealiseerd door deze gegevens te versleutelen. Alleen de partijen die bevoegd zijn de informatie te raadplegen krijgen de desbetreffende sleutel in handen. De Inspectie neemt de taak van sleutelbeheer op zich.

De huidige praktijk rond de EVOA is dat documenten via e-mail of fax worden uitgewisseld. De Inspectie hoopt de volgende voordelen te kunnen realiseren bij gebruik van een blockchaintoepassing:

a. Het uitvoeren van toezicht op een meer efficiënte manier.
b. De vervoerders kunnen meldingen efficiënter verrichten en blockchain leidt tot meer transparantie voor de betrokkenen
c. Efficiency en transparantiewinst in de meldingen tussen autoriteiten in verschillende landen.
d. Fysieke controles kunnen efficiënter plaatsvinden omdat de controle van de 'papieren' al ter hand genomen wordt door de smart contracts, zodat alleen de tijd besteed hoeft te worden

[376] Verordening (EG) Nr. 1013/2006 van 14 juni 2006 betreffende de overbrenging van afvalstoffen.
[377] Art. 33 van de EVOA.

aan de daadwerkelijke fysieke controle (stemt het transport overeen met de papieren werkelijkheid?). Fysieke controles blijven wel nodig.

Transporten die nooit ingevoerd zijn in de blockchain kent de blockchain niet. Als ingevoerde gegevens niet overeenstemmen met de werkelijkheid, kan de blockchain zelf dit niet constateren. Dit is een probleem dat de blockchain niet oplost. Uiteindelijk blijven fysieke controles nodig.

Het oplossen van een fraudeprobleem of een gebrek aan vertrouwen tussen nationale toezichthouders heeft niet vooropgestaan. In wezen, heeft de uitvoering van de EVOA altijd al gebouwd op een zeker vertrouwen tussen de toezichthouders. Daarin ligt dus niet de grote meerwaarde van het gebruik van blockchaintechniek. Het gaat meer om efficiency en transparantie. Dat doet overigens de vraag rijzen waarom voor blockchaintechniek is gekozen. Blockchaintechniek heeft namelijk ook nadelen. De onveranderlijkheid van een blockchain kan ook lastig zijn. Dat maakt het bijvoorbeeld lastiger fouten te corrigeren.

Als mogelijke problemen bij de uitrol van de blockchain naar meer landen voorziet de Inspectie de verschillen in interpretatie van en omgang met de EVOA in de verschillende landen. Vooralsnog probeert ze dit probleem voor te zijn door uit gaan van de meest restrictieve interpretatie van de EVOA. De Inspectie voorziet bovendien dat in de toekomst ook persoonsgegevens in de blockchain zullen worden opgenomen, en vraagt zich af of en zo ja, hoe dit te verenigen is met de AVG.

4.4.2 De use-case onder het huidige wettelijk kader

De use-case betreft een door de wet voorgeschreven proces dat gedeeltelijk met behulp van een blockchaintoepassing wordt uitgevoerd. Dit betreft de vraag of een door de wet voorgeschreven proces zich leent voor digitalisering door middel van een blockchain.

Het proces van melding van een voorgenomen transport aan de bevoegde autoriteit bestaat uit vier deelprocessen die centreren rond de volgende elementen: 1. De kennisgeving, 2. Het vervoersdocument, 3. Het vervoerscontract en 4. De waarborgsom.

De kennisgeving
Ten behoeve van de kennisgeving dient het kennisgevingsdocument opgesteld te worden. Een formulier voor dit document is als bijlage IA aan de EVOA toegevoegd. Dit formulier verlangt dat gegevens verstrekt worden over de identiteit van de kennisgever (exporteur), de ontvanger, de vervoerder, de producent van het afval en eventueel de verwijderingsinrichting. Voorts dient informatie verschaft te worden over de te vervoeren afvalstoffen en over de doorvoer- en bestemmingslanden van het vervoer. Deze gegevens kunnen rechtstreek op de blockchain geplaatst worden of een hash van de gegevens kan daar geplaatst worden. Het kennisgevingsdocument kan persoonsgegevens bevatten. Een belangrijke vraag is of die gegevens in klare taal opgenomen mogen worden of dat er enige vorm van technische bescherming toegepast moet worden (zoals bijvoorbeeld versleuteling of off-chain opslag met on chain alleen een hash).

De kennisgever ondertekent het document en de bevoegde autoriteiten voorzien het document van een stempel en handtekening ingeval van goedkeuring. Art. 26 lid 4 EVOA laat toe dat het kennisgevingsdocument wordt ingediend en uitgewisseld door middel van elektronische gegevensuitwisseling met elektronische handtekening (mits de bevoegde autoriteiten deze vorm van gegevensuitwisseling toelaten). De EVOA lijkt er daarmee niet aan in de weg te staan om het deelproces rond het kennisgevingsdocument in een blockchainapplicatie te vatten.

Het vervoerdocument
Bij de kennisgeving dient ook een vervoersdocument aan de bevoegde autoriteiten aangeleverd te worden. Dit document bevat grotendeels dezelfde informatie als het kennisgevingsdocument. Het

vervoersdocument moet ook ondertekend worden door de kennisgever. Op grond van art. 26 lid 3 EVOA, mag het vervoersdocument in elektronische vorm, met digitale handtekeningen, worden aangeboden indien het op ieder moment tijdens de overbrenging leesbaar is en indien dit voor de betrokken bevoegde autoriteiten aanvaardbaar is. Aan deze laatste eis kan voldaan worden door middel van een mobiel apparaat. Ook het proces rond het vervoersdocument kan daarmee in een blockchain applicatie worden vormgegeven.

Het vervoerscontract

Op grond van art. 4 lid 4 EVOA, moeten de kennisgever en de ontvanger een contract sluiten over de nuttige toepassing of verwijdering van de afvalstoffen waarop de kennisgeving betrekking heeft. Bij de kennisgeving aan de betrokken bevoegde autoriteiten verklaart de kennisgever dat dit contract bestaat. Omdat het slechts om een (ondertekende) verklaring van het bestaan van het contract gaat lijkt er geen reden aan te nemen dat dit niet ook via een blockchainapplicatie kan geschieden. In de toekomst kan allicht het contract als een smart contract worden afgesloten en beschikbaar zijn op de blockchain. Er zijn geen vormvereisten voor dit contract, maar het moet wel een bindend contract zijn.

De borgsom
Voor elke overbrenging van afvalstoffen waarvoor een kennisgeving is vereist, wordt een borgsom of gelijkwaardige verzekering verlangd ter dekking van: a) de vervoerskosten; b) de kosten van nuttige toepassing of verwijdering, inclusief nodig geachte voorlopige handelingen; en c) de opslagkosten voor 90 dagen (art. 6 EVOA). De kennisgever verklaart in het kennisgevingsdocument dat er een borgsom is gedeponeerd of verzekering is gesloten. Evenals bij de verklaring over het contract is geen reden aan te nemen dat de verklaring niet via een blockchain applicatie afgelegd kan worden.

De bevoegde autoriteit stuurt een ontvangen kennisgeving door aan de andere relevante autoriteiten binnen drie dagen na ontvangst. De EVOA staat er niet aan in de weg dat ook deze doorzending via de blockchainapplicatie geschiedt.

Op grond van art. 20 EVOA, bewaren de autoriteiten alle ontvangen documenten gedurende een periode van tenminste drie jaar. Indien de documenten persoonsgegevens bevatten moeten in verband met het beginsel van data minimalisatie de persoonsgegevens na verloop van tijd verwijderd worden. Dat kan problematisch zijn in de blockchain.

Het niet kunnen verwijderen van persoonsgegevens uit de blockchain is een onopgelost probleem.

Op grond van art. 21 EVOA kunnen de bevoegde autoriteiten de informatie betreffende kennisgevingen van overbrengingen waarmee zij hebben ingestemd, via passende instrumenten, zoals het internet, openbaar maken, indien deze informatie niet vertrouwelijk is krachtens nationale of Gemeenschapswetgeving. Dit opent de mogelijkheid om de betreffende informatie onversleuteld in de blockchain op te nemen.

4.4.3 Aandachtspunten

De EVOA staat niet in de weg aan het uitvoeren van de relevante processen via de blockchain. Het is aan de Inspectie om af te wegen of de inzet van blockchaintechniek opportuun is.

De onmogelijkheid van het verwijderen van op de blockchain geplaatste persoonsgegevens is een punt van aandacht.

Uiteindelijk blijven fysieke controles nodig. Transporten die nooit ingevoerd zijn in de blockchain kent de blockchain niet. Als ingevoerde gegevens niet overeenstemmen met de werkelijkheid, kan de blockchain zelf dit niet constateren.

4.5 Use-case 4: Het delen van privacygevoelige gegevens door de overheid -- het CAK

De use-case in steekwoorden

Probleem: een gecompliceerd facturatieproces met eigen bijdragen
Relevante partijen: zorgafnemers, zorgaanbieders, gemeente, CAK
Geclaimde bijdrage van blockchain: een vlottere workflow
Juridische implicaties: het is bewerkelijker om de vertrouwelijkheid van gegevens te realiseren, het corrigeren van gegevens wordt lastiger/onmogelijk en blockchain garandeert niet dat gegevens correct zijn ingevoerd.
Balans: een vlottere workflow is eenvoudiger te realiseren zonder blockchain.

4.5.1 Korte beschrijving van de use-case

Huidige functie van het CAK in het kader van de Wmo
Als een klant een aanvraag in het kader van de Wet maatschappelijke ondersteuning (Wmo) doet, beoordeelt de gemeente of deze wordt toegekend. De klant ontvangt van de gemeente een Wmo-beschikking. De gemeente levert hetzij direct hetzij via een zorgaanbieder hulpmiddelen en/of voorzieningen aan klanten die een positieve Wmo beschikking hebben en betaalt hier in eerste instantie ook voor. De zorgaanbieder declareert de zorgkosten bij de gemeente. De gegevens over de geleverde zorg worden doorgegeven aan het CAK. Aan de hand van een aantal basisregistraties stelt het CAK de Maximale Periodebijdrage (MPB) van de klant vast. Als de klant zorg afneemt, factureert het CAK de kosten als eigen bijdrage aan de klant tot het bedrag van de MPB. Dit gebeurt eens in de 4 weken. De klant ontvangt een MPB-beschikking en een factuur eigen bijdrage. Het CAK incasseert de desbetreffende eigen bijdragen en sluist deze geaggregeerd door aan de gemeente.

De blockchain pilot
Het CAK heeft een eerste blockchain pilot uitgevoerd. Een tweede pilot is niet tot uitvoering gebracht in verband met de herinrichting van de WMO die het kabinet in haar regeerakkoord heeft aangekondigd.[378] Het doel van de pilot was om te verkennen of een deel van bovenstaande gang van zaken met blockchain technologie ondersteund en geherdefinieerd kan worden. Wij richten ons hier op het aspect dat in de eerste pilot ter hand is genomen, namelijk de vertaling van het facturatieproces van de eigen bijdrage naar de blockchain. Het CAK-systeem met blockchain technologie wordt Smart CAK genoemd. Documentatie over het smart CAK schetst hoe het facturatieproces er uit zou komen te zien bij inzet van blockchaintechniek.[379]

Bij het afnemen van zorg wordt via een mobiele app een transactie aangemaakt. In de app wordt vastgelegd hoeveel uur zorg verleend is en tegen welk tarief. De klant en de zorgverlener controleren dit. Levering van de zorg wordt gevalideerd door middel van een handtekening of vingerafdruk. In de pilot is niet erin voorzien dat een smart contract controleert of de afgenomen zorg

[378] VVD, CDA, D66 en ChristenUnie, Vertrouwen in de toekomst, Regeerakkoord 2017 – 2021, p. 13, beschikbaar op: https://www.rijksoverheid.nl/documenten/publicaties/2017/10/10/regeerakkoord-2017-vertrouwen-in-de-toekomst
[379] http://cdn.instantmagazine.com/upload/6826/blockchain-cak.609ab3b34a98.pdf

binnen de termen van het zorgcontract met de gemeente valt. Als alles in orde is, kan de zorgverlener betaald worden.

Klanten krijgen inzicht in de hoogte van hun eigen bijdrage via een wallet waaruit coins worden weggenomen wanneer zorg wordt afgenomen. Zo, is voor de klant op ieder moment inzichtelijk welke eigen bijdrage in rekening zal worden gebracht. De klant ontvangt periodiek een factuur ter inning van de eigen bijdrage. De maximale periodebijdrage wordt jaarlijks automatisch berekend aan de hand van gegevens afkomstig van de belastingdienst.

Deze aan de documentatie ontleende beschrijving laat vooral zien hoe het systeem zich presenteert aan de actoren die er gebruik van maken.[380] De beschrijving geeft weinig inzicht in hoe het systeem achter de schermen werkt, en meer in het bijzonder hoe blockchaintechniek ingezet wordt. Een functionerende blockchain is niet gerealiseerd. Er zijn wel eerste ideeën gevormd over hoe een permissioned blockchain in grote trekken opgezet zou kunnen worden. Iedere betrokken partij zou off-chain, uitsluitend de (persoons)gegevens opslaan die voor hem of haar van belang zijn. On-chain zouden alleen nog nader te bepalen verwijzingen/hashes naar de off chain opgeslagen gegevens worden opgenomen.
Er is tijdens de uitvoering van de pilot wel discussie geweest over de vraag of het een private of publiek blockchain zou moeten worden. Transparantie is het argument voor een publieke blockchain. Vertrouwelijkheid van de betrokken gegevens is het argument voor een private blockchain. Wie de node-beheerders van de blockchain zouden worden is niet beslist. Een tweede pilot had hierover duidelijkheid moeten brengen.
In de pilot worden coins en een wallet gebruikt om de hoogte van de eigen bijdrage inzichtelijk te maken voor klanten. Het is vooral een middel om de geregistreerde eigen bijdrage en de MPB te visualiseren. Het zijn geen tokens die overdraagbaar zijn. Het was ook geen doel van de pilot om zulke tokens te scheppen.

Overigens laat deze pilot mooi zien dat de inzet van blockchain techniek niet een kwestie is van een enkele globale beslissing om blockchaintechniek in te zetten, maar eerder een opeenvolging is van vele kleinere beslissingen om functionaliteiten in de blockchain te brengen. Zo kan men bijvoorbeeld de ontwerpkeuze maken om zorgverleners in cryptocurrencies te betalen, maar men kan er ook voor kiezen betalingen via een traditionele overschrijving te laten verlopen. Het kunnen verrichten van betalingen binnen de blockchain was geen primaire doelstelling van de pilot. De wijze waarop betalingen verricht worden kan ingericht worden onafhankelijk van hoe de rest van het smart CAK vormgegeven wordt. Men zal zich bij het inrichten van een systeem steeds (bij iedere functionaliteit) opnieuw af moeten vragen of een blockchain oplossing geschikt is en zo ja, waarvoor precies (bijv. alleen voor het vastleggen transacties of ook voor verificaties?) en hoe dit technisch gerealiseerd zal worden (bijv. volledig on-chain of alleen een hash on-chain?). Er bestaat in die zin grote flexibiliteit in de wijze waarop een blockchaintoepassing technisch en organisatorisch wordt ingericht.

Men zal zich bij het inrichten van een systeem steeds (bij iedere functionaliteit) opnieuw af moeten vragen of een blockchain oplossing geschikt is en zo ja, waarvoor precies (bijv. alleen voor het vastleggen transacties of ook voor verificaties?) en hoe dit technisch gerealiseerd zal worden (bijv. volledig on-chain of alleen een hash on-chain?).

4.5.2 Kansen en risico's onder het huidige wettelijk kader

Ten opzichte van de huidige gang van zaken kan een aantal voordelen gerealiseerd worden door de inzet van een blockchain. Zo onderhouden partijen binnen de Wmo-keten nu elk een eigen lokale

[380] http://cdn.instantmagazine.com/upload/6826/blockchain-cak.609ab3b34a98.pdf

administratie. Zij wisselen als gevolg onderling op veel verschillende manieren informatie uit. Vaak loopt de uitwisseling vertraging op. Dit is inefficiënt, tijdrovend en foutgevoelig.
Klanten worden door de lange doorlooptijden in de Wmo-keten soms geconfronteerd met eigen bijdrage-facturen van maanden geleden. Het komt ook voor dat facturen gestapeld binnenkomen. Dit leidt tot veel onduidelijkheid en onzekerheid, en kan ook leiden tot betalingsproblemen voor de klant. Het is bovendien voor klanten onduidelijk waar ze de eigen gegevens kunnen inzien en corrigeren.

Een ander aspect waarin een blockchain betekenis kan hebben is transparantie voor toezichthouders. Het Ministerie en toezichthouders hebben te maken met verschillende partijen, elk met hun eigen verantwoordingen en rapportages. Daardoor kan verwarring over de juiste cijfers ontstaan en is het zeer gecompliceerd om analyses over de keten heen uit te voeren.

Volgens het CAK, kan blockchaintechniek een belangrijke bijdrage leveren aan de oplossing van deze problemen die zich in de huidige situatie voordoen. Indien het project van overgang naar de blockchain doorgezet wordt, wordt het CAK eerder betrokken in het Wmo-proces, waardoor het CAK in staat wordt gesteld tijdig alle benodigde informatie te verzamelen voor het efficiënt uitvoeren van haar dienstverlening. De klant tekent de geleverde ondersteuning of voorziening af, waardoor de transparantie van de dienstverlening wordt vergroot en (latere) geschillen zoveel mogelijk worden voorkomen. Doordat de gegevens over geboden ondersteuning direct gekoppeld en geverifieerd worden kan de zorgaanbieder de geleverde ondersteuning direct declareren bij de gemeente. Mogelijke problemen worden proactief en tijdig gesignaleerd. Zo kan bijvoorbeeld een klant tijdig gewaarschuwd worden als een vooraf afgesproken limiet dreigt te worden overschreden, of kan een gemeente op de hoogte worden gebracht als zorgafspraken niet worden nagekomen.

Volgens het CAK heeft de pilot opgeleverd dat bovenstaande problemen naar verwachting met de inzet van blockchaintechniek opgelost of verminderd kunnen worden. Het CAK kan inderdaad nagegeven worden dat met de inzet van ICT de problemen waarschijnlijk wel aangepakt kunnen worden. Men moet echter wel in aanmerking nemen dat de onderliggende blockchain niet daadwerkelijk gebouwd is, en dat vele ontwerpkeuzes over de blockchain opengelaten zijn. Dat is een belangrijke kwalificatie bij het resultaat van de pilot.
Het is ook lastig in te zien wat de meerwaarde van blockchaintechniek is ten opzichte van andere ICT-technieken. De pilot heeft die vraag niet onderzocht. De pilot was puur een verkenning of blockchaintechniek toepasbaar is voor het facturatieproces van het CAK.
Een vaak gehoorde meerwaarde van blockchain is dat zij samenwerking tussen partijen die elkaar niet volledig vertrouwen mogelijk maakt. Deze potentiele meerwaarde van blockchaintechniek heeft in deze use-case geen noemenswaardige rol gespeeld.[381]

De inzet van blockchain introduceert nieuwe risico’s. Blockchain technologie is nog volop in ontwikkeling, er bestaan nog geen geaccepteerde (open) standaarden voor blockchain implementaties. Er bestaan verschillende blockchain leveranciers en platforms, waarbij momenteel geen garanties kunnen worden gegeven welke leveranciers of platformen op de lange termijn succesvol gaan zijn. Er bestaan vooralsnog risico’s voor de continuïteit.
Het is ook onduidelijk hoe schaalbaar blockchains zullen blijken te zijn. Het CAK heeft te maken met het Ministerie van Volksgezondheid, Welzijn en Sport als opdrachtgever, met meer dan 300 gemeenten en duizenden zorgverleners, waaronder vele ZZP’ers. De pilot heeft niet laten zien dat een inzet van blockchaintechniek op deze schaal mogelijk is.
In de pilot zijn mogelijke juridische problemen niet geïnventariseerd of geanalyseerd.

[381] interview CAK.

4.5.3 Aandachtspunten

Hieronder worden mogelijke juridische knelpunten die uit deze use-case naar voren komen weergegeven.

Onveranderlijkheid van de blockchain
We weten niet voor wat voor blockchain uiteindelijk gekozen zou zijn. Maar als gekozen zou worden voor een blockchain die gebruik maakt van een systeem met crypto-economische prikkels, dan is het lastig oude gegevens te verwijderen, ook als die niet meer nodig zijn bijvoorbeeld omdat iemand niet langer van de Wmo gebruik maakt en misschien zelfs gebruik maakt van zijn recht op vergetelheid. Daarnaast is een blockchain (en dat geldt voor alle typen) ook onveranderlijk in een meer overdrachtelijke zin. Een Wmo klant die aangeeft dat gegevens niet kloppen kan vrij alleen komen te staan indien de incorrectheid van de gegevens wordt betwist. In een niet-blockchain situatie, houdt iedere deelnemer, zoals de gemeente, de zorgverlener, en het CAK, zijn eigen administratie bij. Als zij gegevens verschillend geregistreerd hebben, dan kan dat zeker een steun in de rug zijn voor de klant die de incorrectheid (van een van die registraties) betwist. In de blockchain situatie is er weliswaar sprake van feitelijke redundantie, maar logisch is er maar een databank: gemeente, zorgverlener en CAK zien dezelfde gegevens. Dat kan leiden tot een meer absoluut geloof dat gegevens kloppen ten koste van de klant die de correctheid betwist.

Zonder blockchain, kunnen administraties van deelnemers (gemeente, zorgverlener, CAK) gegevens onderling verschillend registreren. Dit werkt een kritische houding ten aanzien van de correctheid van in een administratie opgenomen gegevens in de hand. Bij een blockchain zijn er geen onderlinge verschillen meer. Dat kan resulteren in een kritiekloos geloof in de correctheid van de op de blockchain aanwezige gegevens. Het betwisten van de correctheid van geregistreerde gegevens wordt daarmee veel lastiger.

Blindheid
Een blockchain kan niet garanderen dat gegevens tijdig worden ingevoerd of de authenticiteit van ingevoerde gegevens controleren. Indien gegevens niet of incorrect ingevoerd worden (bijvoorbeeld meer uren zorg dan daadwerkelijk verleend zijn), dan helpt de blockchain daartegen niet. Natuurlijk is het wel zo dat gegevens door gebruik te maken van mobiele apps misschien direct ingevoerd worden nadat de feiten die ze registreren hebben plaatsgevonden. Dat kan de tijdigheid van registratie en correctheid van de gegevens ten goede komen, maar dit is niet een voordeel dat direct volgt uit het gebruik van een blockchain. Met een ander geautomatiseerd systeem kan dit voordeel eveneens bereikt worden.

Een groot probleem in de bestaande praktijk is dat gegevens niet tijdig geregistreerd worden. De blockchain biedt echter geen oplossing voor dat probleem. Dit onderstreept het belang van een goede probleemanalyse en een goed besef van het potentieel van blockchaintechniek: welke problemen kan een blockchain wel oplossen en welke niet.

Transparantie
Hoe is de vertrouwelijkheid van persoonsgegevens te garanderen? Het is duidelijk dat eenieder slechts kennis mag nemen van feiten die hem of haar aangaan. In een niet-blockchain systeem wordt dit opgelost met leesrechten. Als je in een blockchain situatie met leesrechten zou werken dan kan bijna iedere deelnemer dus maar een klein stukje van de blockchain zien, namelijk alleen de gegevens waarbij hij belang heeft. In een blockchain die met proof-of work werkt kan dus ook bijna niemand meer de integriteit van de blockchain controleren. Hoe zou je hashes kunnen controleren als je de gegevens waarover die hash is genomen niet mag zien? Dan ontstaat de facto toch al gauw weer een situatie waarin deelnemers vertrouwen moeten hebben in een kleine groep beheerders. Dat is misschien niet een probleem (vele niet-blockchain systemen werken zo en

zonder problemen), maar doet wel de vraag rijzen waarom voor een blockchain is gekozen. Een blockchain is namelijk complexer om te realiseren dan andere automatiseringsoplossingen. Een andere optie voor een blockchain-oplossing is dat alle gegevens op de blockchain worden versleuteld. Nog weer een andere optie is dat gegevens off-chain worden opgeslagen en on-chain slechts een versleutelde hash die het mogelijk maakt de integriteit van off-chain opgeslagen gegevens te verifiëren. De sleutels worden dan uiteraard alleen gedeeld met degenen die de gegevens aangaan. Dan kan iedereen de hele blockchain zien (met alle versleutelde gegevens), maar alleen de gegevens ontsleutelen die hem aangaan. Dit geeft dan wel aanleiding tot een gecompliceerd sleutelbeheer. Bovendien is de vraag hoe off-chain gegevens opgeslagen worden. Gaat iedere deelnemer dan toch weer zijn eigen gegevens lokaal opslaan met het risico dat gegevens uiteen gaan lopen?[382] Of worden gegevens ondergebracht in een grote centrale databank? In het laatste geval zou je juist weer een single-point-of-failure scheppen waartegen blockchain met zijn redundantie juist zou moeten waken. De vraag is of de geclaimde voordelen van een blockchain niet verdampen als je nader bekijkt hoe een blockchain uitgewerkt zou moeten worden.

Om de vertrouwelijkheid van persoonsgegevens te waarborgen worden gegevens off chain opgeslagen. De vraag is of daarmee niet mogelijke voordelen van het gebruik van een blockchain weer weggenomen worden.

[382] Bijvoorbeeld, als de discipline ontbreekt om bij wijzigingen een rectificatie aan de blockchain toe te voegen en andere lokale registraties niet op de hoogte worden gebracht.

5. Synthese

5.1 Introductie

In hoofdstuk 2 is in hoofdlijnen aangegeven wat een blockchain is en hoe hij functioneert. Het bleek dat blockchains typisch een aantal eigenschappen bezitten: onveranderlijkheid, blindheid, redundantie en decentralisatie en transparantie. Voorts bleek het relevant te zijn onderscheid te maken tussen permissioned en permissionless blockchains. In hoofdstuk 3 is een aantal juridische aspecten belicht. Daaruit kwam reeds een aantal knelpunten naar voren waartoe de inzet van blockchaintechniek aanleiding kan geven. In hoofdstuk 4 is een viertal use-cases behandeld om zicht te krijgen op de knelpunten die bij inzet van blockchaintechniek in de praktijk naar voren komen. Dit alles levert een breed palet van knelpunten op waartoe de inzet van blockchains aanleiding geeft. In dit hoofdstuk wordt een poging ondernomen de grotere lijnen te distilleren uit het gedetailleerde beeld dat uit de voorgaande hoofdstukken naar voren komt.
Daartoe wordt onderscheid gemaakt in regulerings- en pure handhavingskwesties. In paragraaf 5.2.1 wordt een kader gegeven voor het in beeld brengen van reguleringsvragen. De kansen en risico's van blockchaintoepassingen worden in paragraaf 5.2.2 gestructureerd in beeld gebracht aan de hand van dit kader. Paragraaf 5.3 zal ingaan op pure handhavingskwesties.

5.2 Reguleringsvragen

5.2.1 Een kader

Blockchaintechniek is een techniek die zich met enige dwingendheid oplegt aan eenieder die met een blockchain in zee gaat. Het is feitelijk niet gemakkelijk zich aan de gevolgen van gebruik van een blocktechniek te onttrekken nadat men eenmaal ingestapt is. Het is dan ook niet verwonderlijk dat in de literatuur blockchain vaak in verband wordt gebracht met code-as-law of technoregulering.[383] Dat gebeurt op verschillende manieren, of in verschillende gradaties.

Soms – maar niet in dit rapport – wordt betoogd dat blockchain een volledig alternatief vormt voor het recht. In crypto-libertaire groepen, wordt code als de enige legitieme vorm van regulering gezien, zou code het recht overbodig maken, en zou het recht niet in staat zijn code te reguleren. Die claims gaan te ver. Het recht heeft algemene gelding.[384] Niemand staat boven de wet.

Blockchaintechniek zet het recht niet opzij, maar er is wel wederzijdse beïnvloeding van techniek en recht. In dit verband is het volgende citaat van Yeung illustratief. Yeung onderscheidt drie typen doelstellingen die aan blockchaintoepassingen ten grondslag liggen en brengt deze in verband met het recht:[385]

> I suggest that three different classes of blockchain applications can be identified, based primarily on the purposes and intentions of particular blockchain participants in relation to the conventional legal system and the potential harms which these applications might generate, which I refer to as (a) hostile evasion, referring to the use of blockchain systems with the express intention of evading the substantive constraints of conventional law (b) efficient alignment, in which blockchain systems are employed for the purposes of complementing and/or supplementing conventional law in order to streamline or enhance compliance with legal standards, and (c) alleviating transactional friction, referring to blockchain applications aimed at co-ordinating actions across and between multiple participants, motivated by a

[383] Yeung 2018.
[384] Yeung 2018, par. 1.
[385] Yeung 2018, par. 2.3.

> desire to avoid the procedural inefficiencies and complexities associated with the legal process, including the transaction costs, monitoring costs and agency costs associated with conventional law.

Het is duidelijk dat ook bij aanvaarding van de suprematie van het recht er wederzijdse beïnvloeding is en afwegingen gemaakt moeten worden: het recht beoogt bescherming te bieden, maar wil ook ruimte laten voor innovatie.

Onder welke omstandigheden is aanvaardbaar dat techniek meestuurt, mede invulling geeft aan de onderlinge verhoudingen tussen deelnemers aan een blockchain. Koops heeft een stevige aanzet gegeven voor een kader voor het beoordelen van de aanvaardbaarheid van normatieve technologie.[386] Koops stelt de vraag welke criteria aangelegd zouden moeten worden om de aanvaardbaarheid van normatieve technologie te beoordelen, in het licht van democratische en constitutionele waarden. Zijn analyse leidt hem naar een onderscheid tussen materiële, procedurele en resultaatscriteria (in volgorde van afnemend belang). In dit rapport wordt voortgebouwd op het door Koops ontwikkelde kader. Het kader wordt hier gebruikt om de kansen en risico's van blockchain techniek in beeld te brengen en de bespreking ervan te structureren.

De analyse die hieronder volgt zal zowel overheids- en niet-overheidsblockchains betreffen. Alleen waar dat nuttig is, zal expliciet onderscheid gemaakt worden. Het door Koops ontwikkelde kader is bruikbaar zowel voor private als voor publieke regulering. Regulering is steeds polycentrischer geworden. Regulering is horizontaal en verticaal een complex en interactief proces. Private regulering gaat als het ware steeds meer op in een amalgaam van publieke en private regulering. Vanuit die visie verdient private regulering het bestreken te worden door generieke criteria voor regulering.

Als substantiële criteria worden mensenrechten en andere morele waarden onderscheiden. De belangrijkste procedurele criteria zijn legitimiteit[387] en democratie. Overige procedurele criteria betreffen de transparantie van het stellen van regels, efficiëntie en proportionaliteit, en verantwoording. Als resultaatscriteria zijn te noemen: keuze versus effectiviteit,[388] flexibiliteit en transparantie van regels.

Blockchains zijn verschillend en toepassing van het kader op de ene blockchain geeft aanleiding tot andere bevindingen dan toepassing op een andere blockchain. De analyse hieronder gaat noodzakelijkerwijze uit van een gegeneraliseerd beeld van blockchains. Voor het doel van de analyse is dit echter voldoende: het nader aanscherpen van het beeld van de risico's en kansen van blockchain in juridisch perspectief met het oog op een eventuele daaruit voortvloeiende reguleringsbehoefte.

5.2.2 Aanvaardbaarheid van blockchain techniek

Materiële criteria: bescherming van mensenrechten en andere morele waarden

Het recht heeft de functie mensenrechten en ander morele waarden te beschermen. De introductie van blockchains in de samenleving leidt tot een nieuw speelveld waarin de verhoudingen tussen betrokken actoren opnieuw ingedeeld worden. Daarbij kunnen mensenrechten en andere morele

[386] Koops 2007.
[387] Koops noemt dit criterium Rule of Law, hetgeen volgens hem mede omvat due process, legality en legal certainty.
[388] De effectiviteit van de handhaving van een in techniek ingebakken norm zal doorgaans groter zijn als de techniek niet de mogelijkheid openlaat om van de norm af te wijken. De mogelijkheid van afwijking kan echter van belang zijn voor bijzondere situaties waarin de norm niet zonder meer opgaat. Het inbouwen van de mogelijkheid om af te wijken houdt weer het risico van misbruik in (afwijking in situaties waarin de norm eigenlijk gehandhaafd zou moeten worden). De aanvaardbaarheid vergt hier een afweging van het belang van handhaving tegen autonomie.

waarden onder druk komen te staan. Welke mensenrechten en andere morele waarden in een blockchain onder druk komen te staan hangt ten dele af van het toepassingsdomein van de blockchain of blockchain toepassing. Niettemin kunnen wel enkele bredere reflecties gegeven worden over de mogelijke implicaties van blockchains op genoemde rechten en waarden. We onderscheiden hier twee categorieën van implicaties: 1. Directe problemen met betrekking tot mensenrechten en ander morele waarden en 2. Sluipende implicaties van de inzet van blockchain techniek.

Directe problemen

Er doen zich problemen voor in relatie tot velerlei mensenrechten en morele waarden. Zo zijn er duidelijke knelpunten rond privacy en gegevensbescherming. De onveranderlijkheid van vooral permissionless blockchains leidt ertoe dat oude gegevens niet uit de blockchain verwijderd worden. De naleving van het beginsel van data minimalisatie en de handhaving van het recht op vergetelheid komen daardoor onder druk te staan. Er zijn wel technieken die compliance met de eisen van de AVG rond wissing dichterbij brengen, maar het is onduidelijk of zij daadwerkelijk aan de AVG voldoen (par 3.3.4). Smadelijke of lasterlijke informatie kan evenmin verwijderd worden.
Een belangrijk element in de rechtmatige omgang met persoonsgegevens is dat verantwoordelijkheden voor de verwerking ervan duidelijk belegd zijn. In permissionless blockchains bestaat er evenwel nog grote onduidelijkheid over wie als verantwoordelijke en wie als bewerker heeft te gelden. Dit is een probleem dat voortvloeit uit de decentralisatie van blockchains. Tevens is onduidelijk wie de doorzettingsmacht heeft om de omgang met persoonsgegevens daadwerkelijk aan te passen waar dat nodig is (par 3.3.1). Het recht op correctie van persoonsgegevens kan onder druk komen zoals hieronder zal blijken.

In de kern hebben veel problemen te maken met autonomie. Wie zich eenmaal met een smart contract inlaat kan zich vanwege de onveranderlijkheid ervan nauwelijks nog aan de voorgeprogrammeerde gevolgen onttrekken. Transparantie van de blockchain is niet steeds zodanig dat een betrokkene alle gevolgen voorziet. Dit wordt in de hand gewerkt doordat smart contracts (die overigens meestal niet ‘smart’ zijn) meestal een strikt logische afwikkeling volgen, zonder ruimte voor flexibiliteit. Menselijk betrokkenen, gewend als zij zijn aan intermenselijke relatie waarin ruimte is voor flexibiliteit, kunnen zich moeilijker een voorstelling maken van een strikt logische afdoening.

Hoewel een blockchain slechts informatie bevat (en uiteraard geen fysieke objecten) kan toch het recht op eigendom onder druk komen. In de scheepsregister use-case zagen we bijvoorbeeld dat er een kleine kans is op een splitsing in de blockchain waardoor de rechtstoestand van een schip onbepaald kan raken.

Effectenwetgeving dient ter bescherming van het beleggend publiek. De wetgeving voorziet in uitgebreide informatieplichten, omdat ondernemingen die kapitaal aantrekken juist niet altijd op hun blauwe ogen vertrouwd kunnen worden. Het is onduidelijk of de uitgifte van tokens onder deze wetgeving valt. De AFM waarschuwt op haar website voor ICOs (Initial Coin Offerings) omdat ongereguleerde ICOs grote risico’s inhouden voor beleggers.[389] Blockchains kunnen niet voorkomen dat het beleggend publiek schade ondervindt van ongereguleerde ICOs.

[389] https://www.afm.nl/en/professionals/onderwerpen/ico

Sluipende implicaties

Gelijkheid en non-discriminatie

Er is sprake van een steeds verdergaand vertrouwen en bouwen op data in de samenleving. Data vormen steeds meer de werkelijkheid die bepalend is. Blockchains passen naadloos in deze ontwikkeling. Blockchains zijn niet alleen verzamelplaatsen van data, maar dragen er ook aan bij dat rechtssubjecten beoordeeld worden volgens hun digitale evenbeeld (par. 3.4.1).[390][391] Algoritmische besluitvorming kan theoretisch gelijke behandeling en non-discriminatie in de hand werken. De techniek werkt zonder aanziens des persoons. Er is echter groeiend bewijs dat dataverzamelingen en besluitvormingsalgoritmen bestaande vooroordelen weerspiegelen en deze zelfs uitvergroten.[392] Algoritmische besluitvorming kan ook expliciet ingezet worden om onderscheid te maken op basis van (echte of vermeende) kenmerken van personen: personalisering.[393] Toepassing van blockchains houdt daarmee het risico in dat gelijkheid en non-discriminatie onder druk komen te staan.[394]

Correctierecht onder druk

Zonder blockchain, kunnen administraties van deelnemers (gemeente, zorgverlener, CAK) gegevens onderling verschillend registreren. Dit kan een zekere gezonde twijfel opwekken over de correctheid van in een administratie opgenomen gegevens. Bij een blockchain zijn er geen onderlinge verschillen meer. Dat kan resulteren in een kritiekloos geloof in de correctheid van de op de blockchain aanwezige gegevens. Het betwisten van de correctheid van geregistreerde gegevens wordt daarmee veel lastiger (par 4.5).

Normondermijning

Hoe verhoudt blockchain zich tot de menselijke waardigheid? Blockchain werkt mogelijk een opvatting in de hand waarin een mens niet meer gezien wordt als een vertrouwenswaardig rechtssubject, maar als een entiteit die gedisciplineerd moet worden. Juist de mogelijkheid om zich niet aan de regels te houden is een belangrijk aspect van het mens zijn. Is de mogelijkheid van burgerlijke ongehoorzaamheid niet juist datgene wat de mens een moreel waardig wezen maakt?[395]

> Een mogelijke implicatie hiervan kan zijn dat techno-disciplinering het gezag van rechtsnormen ondermijnt. De norm raakt immers ondergesneeuwd. De technische disciplinering treedt op de voorgrond. Het wordt een spel om de technische disciplinering te omzeilen.[396] Het wordt allicht niet eens meer onderkend dat er een norm aan technoregulering ten grondslag ligt.

The DAO hack laat zien dat dit een reëel risico is. De toe-eigening van cryptocurrencies uit een ICO gaf aanleiding tot een fork in de blockchain.[397] Een fractie van de gemeenschap vond dat de regels zoals die uit het smart contract volgden de geldige norm representeerden. Een andere fractie achtte de maatschappelijk (of juridische?) norm dat middelen opgehaald in een ICO gebruikt moeten worden voor het doel waarvoor ze zijn opgehaald bepalend.

---

[390] De bitcoin blockchain aanvaardt bijvoorbeeld een transactie van een ieder die kan aantonen over de betreffende private sleutel te beschikken. Of deze persoon ook bevoegd is, is in wezen niet van belang voor de blockchain.
[391] Dat geautomatiseerde besluitvorming plaatsvindt in een blockchain neemt niet het risico weg dat het beeld dat uit de data spreekt niet klopt. (par 3.4.1)
[392] Barocas & Selbst 2016.
[393] Finck 2018, p.88-90, De Filippi & Wright 2018, p. 202.
[394] Bodo et al 2019, par. V (B).
[395] Brownsword 2005, par. 3..
[396] De Filippi & Wright 2018, p. 200.
[397] Finck 2018, p. 187-189.

Kern procedurele criteria

Legitimiteit

Als er inbreuk wordt gemaakt op mensenrechten of andere morele waarden gebeurt dat dan op een juridische grondslag en met waarborgen die de inbreuk kunnen dragen?

Een overheidsorgaan dat een besluit neemt via een blockchain moet zorgen dat zij handelt op wettelijke basis, volgens wettelijke procedures en met een voorspelbare uitkomst. Aangenomen dat een bestuursorgaan gebruik maakt van een smart contract op een blockchain ter oefening van een haar toegekende bevoegdheid, welke waarborgen moet zij daarbij in acht nemen? De voorbereiding van de besluitvorming (het verzamelen van informatie) moet voldoen aan gebruikelijke voorwaarden rond zorgvuldigheid (art. 3.2 AWB), authenticiteit en integriteit. De laatste voorwaarden zijn bij een blockchain niet vanzelfsprekend vervuld: een blockchain is in beginsel blind. Er moeten afdoende maatregelen genomen worden om de authenticiteit en integriteit van aan de besluitvorming ten grondslag liggende informatie te waarborgen. De eigenlijke besluitvorming moet voldoen aan eisen van formele en materiele zorgvuldigheid: alle betrokken factoren moeten meegenomen worden en proportionaliteit moet in acht genomen worden. Dit laatste sluit het uitsluitend gebruik van blockchain voor besluiten op basis van open normen zo goed als uit.[398] Een open norm laat zich niet precies in code vertalen. Bij het ‘omzetten’ van rechtsregels in code raken deze vaak vervormd. Code kent niet de flexibiliteit van natuurlijke taal en kan moeilijker omgaan met vaagheid, de 'open texture' van begrippen en onverwachte gebeurtenissen.[399] Kunstmatige intelligentie kan hier in de toekomst misschien verandering in brengen. Een blockchain zal gewoon aan alle voornoemde voorwaarden moeten voldoen en het is niet vanzelfsprekend dat een blockchain daaraan voldoet.

Een private partij heeft vrijheid van handelen, tenzij deze wordt weggenomen door dwingendrechtelijke bepalingen of positieve rechten van anderen. Het contractenrecht laat bijvoorbeeld toe dat er contracten met behulp van een blockchain worden gesloten en/of uitgevoerd. Smart contracts wijken echter wezenlijk af van de gewone manier waarop mensen een contract opvatten: als een onderdeel van een intermenselijke relatie, die niet tot in detail vooraf regelt hoe er met verschillende omstandigheden moet worden omgegaan (par. 3.2.8). Wie eenmaal met een smart contract in zee is gegaan kan zich niet meer zo gemakkelijk aan de gevolgen onttrekken. Gebondenheid zal onder geschikte omstandigheden wel worden aangenomen, maar helemaal zo vanzelfsprekend is het niet. Is een gebruiker van een smart contract voldoende duidelijk waar hij zich aan bindt bij gebruik van het smart contract? Kan toestemming de basis zijn? Dit vergt per geval een waardering van omstandigheden waaronder een en ander plaatsvindt.

Bovendien is veel afhankelijk van de intenties waarmee een blockchain ingezet wordt.
Yeung illustreert mooi wat het risico is. Een belangrijke motivatie om deel te nemen in een blockchain is: [400]

> ‘to engage in novel forms of cooperation in ways that avoid the procedural burdens and associated costs and formalities associated with conventional legally-supported forms of coordination’.

De frictie, de vertraging die het gevolg is van de rule of law is juist reden om in blockchain een alternatief te zien. Als voorbeelden noemt zij de initial coin offerings en blockchains voor het coöperatief genereren, delen en verdelen van energie. Het streven naar het vergroten van efficiëntie houdt het risico in dat procedurele waarborgen afkalven. Yeung zegt hierover:[401]

[398] Groothuis 2005, p. 60-61.
[399] Prakken 1993.
[400] Yeung 2018, par. 2.2.3.
[401] Yeung 2018, par 2.2.3 (b).

> In part, controversy surrounding ICOs is rooted in recognition that the procedural burdens of securities legislation are ultimately intended to provide substantive protection to the investing public and which should not therefore be so readily side-stepped simply by entrepreneurs using of blockchain technology to finance their risky ventures.

Het streven naar innovatie en efficiëntie is de prikkel en de geclaimde legitimatie om juridische waarborgen ter zijde te schuiven.[402] Als de blockchain de functie van die waarborgen niet overneemt (quod non), laat zich de vraag stellen of dit nog wel als een gewenste ontwikkeling gezien moet worden.[403]

Democratie en transparantie van het stellen van regels

Normatieve technologie raakt al degenen die met de technologie in aanraking komen. Als het gebruik van de technologie niet berust op vrije keuze, bijvoorbeeld omdat er geen redelijke alternatieven zijn, dan vergt aanvaardbaarheid dat de betrokkenen in enige vorm worden meegenomen in de ontwikkeling, adoptie of het gebruik van de technologie. Daarvoor is in de eerste plaats nodig dat de normativiteit transparant is voor de betrokkenen.

De meeste blockchains kennen een of andere vorm van governance. Dat geldt ook voor permissionless blockchains.[404] Het bestaan van een governance structuur in een blockchain is in zekere zin uit noodzaak geboren. Het protocol en de core code moeten regelmatig aangepast worden in verband met onvoorziene omstandigheden, veranderde behoeften of het opheffen van programmeerfouten.[405] De governance structuur maakt dit mogelijk. Zij biedt theoretisch (en vaak ook praktisch) de mogelijkheid om participatie van betrokkenen vorm te geven. Er bestaat veel variatie in de governance structuur tussen verschillende blockchains.

Bij de beschrijving van governance in permissionless blockchains in paragraaf 2.3, is onderscheid gemaakt tussen twee hoofdtypen van governance:[406] on chain en off chain governance. Als voordelen van on-chain governance worden snelheid en efficiëntie worden genoemd, maar er zijn vragen in termen van representativiteit van belanghebbende actoren (bijvoorbeeld indien het aantal participerende currency-houders klein is) en vragen rond de bescherming van minderheidsbelangen (bijvoorbeeld omdat de telling van stemmen een te grote invloed heeft).

Bitcoin en Ethereum werken met off-chain governance. Daarin kan eenieder een voorstel in discussie brengen, maar uiteindelijk beslissen de ontwikkelaars welke voorstellen geaccepteerd worden. Dan is het nog aan miners die gezamenlijk tenminste de helft van de rekenkracht bezitten om de aanpassing door te voeren.

Onder aantekening dat iedere blockchain uiteraard vrij is zijn eigen governance structuur te kiezen, is het beeld dat uit het bovenstaande naar voren komt dat een ieder wel de mogelijkheid heeft om te

[402] Wetgevers weten niet goed hoe ze met deze ontwikkelingen om moeten gaan. Omdat het allemaal in kwantitatieve zin nog allemaal erg beperkt is, stellen ze zich afwachtend op. Ze willen deze nieuwe ontwikkelingen niet breken in de knop. Het is niet duidelijk wat het moment is om in te grijpen. Hier doet zich het bekende Collingridge dilemma voor.
[403] Bodo et al 2019, par. V(B) Code as Law.
[404] Een permissionless blockchain leidt op zichzelf niet tot rechten en verplichtingen tussen node-beheerders onderling en node-beheerders en gebruikers, tenzij zij zelf verdere afspraken maken. (par 3.2.2). Een permissionless blockchain heeft geen juridische governance-structuur, maar kan wel een feitelijke vorm van governance hebben. (3.2.3) Een permissioned blockchain heeft een juridische governance-structuur vanwege het permissioned karakter van de blockchain. (par. 3.2.3).
[405] Finck 2018, p.186-187.
[406] Finck 2018, p.192-194.

participeren, maar dat onduidelijk blijft of ‘gewone’ gebruikers wel voldoende participeren en hun belangen in voldoende mate worden meegenomen in de verder ontwikkeling van blockchains.

In een permissioned blockchain is governance allicht eenvoudiger te realiseren. Er is een consortium of partij die de node-beheerders toelaat. Governance kan gecentraliseerd zijn bij deze partij of berusten bij meerdere partijen (bijvoorbeeld de beheerders van nodes).[407] Smart contracts kunnen geprogrammeerd worden door gebruikers zonder daarin andere actoren te betrekken.

In deze gevallen staat de code-ontwikkeling en adoptie veeleer onder controle van een beperkt aantal partijen. Daarmee lijkt dit meer op gebruik van technoregulering buiten een blockchain context. Ook daar speelt uiteraard het belang van democratische betrokkenheid een rol en is het zaak dat relevante stakeholders in een vroegtijdig stadium worden betrokken om te voorkomen dat zij voor voldongen feiten worden geplaatst of dat democratische controle pas kan plaatsvinden nadat implementatie een stevige aanvang heeft genomen. Dit is niet specifiek voor blockchains, maar blijft niettemin een aandachtspunt.

Een ander aspect betreft de informatie-asymmetrie rond code-aanpassingen. Zelfs indien voorgestelde code-aanpassingen gedeeld worden via een openbaar toegankelijke repository, dan nog vergt het doorgronden van een voorstel enige voorkennis op het gebied van informatica en van de wijze waarop de blockchain of het smart contract waarin een wijziging wordt aangebracht geprogrammeerd is. Dit is kennis die niet bij iedereen aanwezig is. Bovendien is voor een grote groep betrokkenen niet zo relevant hoe een adaptatie precies wordt vormgegeven, maar is voor hen meer van belang wat de normatieve implicaties daarvan zijn. Het gaat hen daarbij niet alleen om de directe of beoogde normatieve implicaties, maar ook om de bijeffecten.

Bovendien is code een lastige ingang om normatieve keuzes te bespreken. Er is geen een-op-een vertaling van regels naar code. Hoe de code functioneert en in de praktijk uitwerkt zal vaak pas bij gebruik duidelijk worden (zoals bijvoorbeeld bleek bij de The DAO-zaak).

De toegankelijkheid van informatie over een voorgestelde aanpassing en de implicaties ervan voor mensenrechten, andere morele waarden en procedurele waarborgen, is een aandachtspunt.

Efficiëntie en proportionaliteit

Blockchains worden voor velerlei doeleinden in gezet. Als overkoepelende doelcategorieën worden de volgende in de literatuur genoemd: het oplossen van een vertrouwensprobleem,[408] het ondersteunen van het recht,[409] zoals transparantie en tenslotte efficiëntiewinst.[410] [411]
Hiervoor is aangegeven dat de toepassing van blockchains om materieel aanvaardbaar te zijn tenminste mensenrechten, andere morele waarden en procedurele waarborgen moeten respecteren. Dit vormt het kader waarbinnen de proportionaliteit van blockchains getoetst wordt. De doeleinden waarvoor blockchains worden ingezet zijn geconceptualiseerd als verbeteringen ten opzichte van een situatie waarin geen blockchain wordt ingezet. Deze laatste is in brede streken neer te zetten als gebruik van traditionele databanken onder centraal beheer, inzet van traditionele intermediairs en adoptie en uitvoering van code door vertrouwde partijen. De proportionaliteitvraag vertaalt zich daarmee in de vraag of een blockchain een redelijk middel is om tot verbetering van de huidige situatie te komen.

[407] Finck 2018, p.195-197.
[408] Nakamoto 2008, Introduction.
[409] Yeung 2018, Finck 2018, p. 43-44.
[410] Yeung 2018, par. 2.2.3.
[411] Een laatste doel waarvoor een blockchain ingezet zou kunnen worden is het ondermijnen van het recht (zie Yeung 2018). Bij dit doel is de proportionaliteitsvraag niet op zijn plaats. Voor een blockchain die er op uitgelegd is het recht te ondermijnen is vooral de handhavingsvraag van belang die in paragraaf 5.4 wordt behandeld.

Hierbij moet echter de volgende kanttekening geplaatst worden. Het uitvoeren van een proportionaliteitstoets in abstracto is vrijwel onmogelijk. Daarvoor zijn er teveel verschillende blockchains, teveel verschillende toepassingscategorieën en is de non-blockchain situatie te veelvormig. Daarom is in het navolgende volstaan met een aantal globale observaties.

Vertrouwensprobleem

Het maatschappelijk leven vergt dat men vertrouwen moet stellen in personen, bedrijven en instellingen. Volgens Nakamoto (maar niet de use-cases), is dit ongewenst. De blockchain zou zorgen voor controleerbaarheid waardoor vertrouwen niet meer nodig zou zijn.

Bij het vertrouwensprobleem, stelt zich de vraag of traditionele intermediairs inderdaad zo onbetrouwbaar zijn dat inzet van een blockchain geïndiceerd is. De overstap op een blockchainoplossing vergt immers een grote investering. Belangrijker is misschien nog wel dat onzeker is of een blockchain wel leidt tot een situatie waarin niet meer ‘vertrouwd’ hoeft te worden en alles ‘’gecontroleerd’ is.

De blindheid van de blockchain maakt nu juist dat de traditionele intermediairs nog steeds nodig zijn omdat integriteit van de data zich beperkt tot integriteit van die data op de blockchain. Voor verificatie/authenticatie van data voor entree tot de blockchain zijn derden (bijvoorbeeld een oracle of een mens) noodzakelijk zodat vertrouwen via de achterdeur weer binnen komt.

Tevens zal men zich kritisch de vraag moeten stellen of een blockchain geen vertrouwen vergt in de nieuwe intermediairs van blockchain. In dit verband kan gewezen worden op het betoog van Finck, dat blockchains lang niet zo gedecentraliseerd zijn als het lijkt, dat er geen techniek is zonder politiek, het totstandbrengen van een sterke governance structuur van wezensbelang is voor blockchains en dat het realiseren van effectieve governance op een polycentrische manier een enorme uitdaging is.[412] Met andere woorden, blockchains kunnen niet buiten een effectieve, betrekkelijk centrale, bemenste governance structuur heen. Het netto-effect is dat vertrouwen in nieuwe intermediairs in de plaats komt van vertrouwen in oude intermediairs en van een ‘oplossing van het vertrouwensprobleem’ (zo dat al oplossing behoeft) geen sprake is.

Efficiëntiewinst

Efficiëntiewinst is in zichzelf een nastrevenswaardig doel. Het veronderstelt dat de inzet van een blockchain efficiënter is dan traditionele intermediairs en/of dat de dienstverlening beter wordt. Zo wordt bijvoorbeeld verondersteld dat een permissionless blockchain voor het scheepsregister leidt tot kostenbesparing en tijdsbesparing, doordat geen tussenkomst van notaris en de bewaarder van het kadaster nodig is, en controles en verwerking geautomatiseerd plaatsvinden. Een ander voorbeeld van de toegevoegde waarde van blockchaintechnologie is de mogelijkheid van registratie van het tijdstip van transacties (par 3.2.5).

De vraag is echter of een blockchain daadwerkelijk leidt tot efficiëntiewinst. We hebben hierboven al gezien dat een blockchain een beperkte functionaliteit heeft, namelijk het garanderen van de integriteit van data en code. In de praktijk is echter behoefte aan andere functionaliteiten (garantie van authenticiteit, koppeling met de wereld buiten blockchain). Daarvoor is dan vaak weer de inzet van traditionele intermediairs vereist. In de scheepsregister use-case, bleek bijvoorbeeld dat de identificatie van de werkelijke personen niet geautomatiseerd kan plaatsvinden, terwijl er een publiek belang is bij de identificatie, namelijk het bestrijden van witwassen en financiering van terrorisme (par. 4.2). In de CAK use-case, is een groot probleem in de bestaande praktijk dat gegevens niet tijdig geregistreerd worden. De blockchain biedt echter geen oplossing voor dat probleem. In de ILT

[412] Finck 2018, p. 205-209.

use-case bleek dat uiteindelijk fysieke controles nodig blijven. Bij de bespreking van smart contracts (ar 3.), bleek dat bij het gebruik van menselijke 'oracles' voor de beoordeling van omstandigheden het smart contract weer afhankelijk wordt van menselijke tussenkomst en dan niet automatisch verloopt. Juist waar de blockchain communiceert met de 'buitenwereld' gaat de efficiëntie verloren en dat kan de blockchain niet oplossen. Alleen kijken naar de werkzaamheden van de node-beheerders is een te eng perspectief en geeft geen volledig beeld van de (in)efficiëntie.

Hieraan zou men kunnen tegenwerpen dat uit de use-cases naar voren komt dat het bereiken van efficiëntiewinst als een van de belangrijkste argumenten wordt gezien om de mogelijkheden van blockchaintechniek te verkennen. Hoewel de use-cases nog niet in een stadium verkeren waarin een efficiëntiewinst ten opzichte van de bestaande situatie gemeten zou kunnen worden, is inderdaad aan te nemen dat de verwachting dat een efficiëntiewinst te bereiken is, niet volledig uit de lucht is gegrepen. Men moet echter bedenken dat in de use-cases vooral een papieren situatie wordt geautomatiseerd. Onbekend is wat voor efficiëntiewinst kan worden behaald door procesontwerp en traditionele automatisering en of die winst hoger of lager is dan de vermeende winst van een blockchain oplossing.

De claim dat blockchain problemen rond gefragmenteerde werkprocessen, zoals bij het scheepsregister, oplost is discutabel. Alle benodigde data kan weliswaar voor iedere relevante partij op de blockchain beschikbaar zijn, maar daarmee is nog geen workflow gerealiseerd. Inpassing en beoordeling van de data in een werkproces vergt een aparte laag in software die bovenop de blockchain gelegd zal moeten worden. Aangezien die (nog) niet bestaat reist wederom de vraag of een klassieke ICT-implementatie van het werkproces niet efficiënter is of kan zijn.

Als daarenboven een eventuele efficiëntiewinst door de inzet van blockchain techniek ten koste gaat van de effectiviteit, dat is het nog maar de vraag of de efficiëntiewinst überhaupt gewenst is. Zo liet de scheepsregister use-case zien dat controles door de notaris en bewaarder van het kadaster de kans verkleinen dat een transactie moet worden teruggedraaid wegens fraude, misbruik, dwang of vergissingen. Als die controles vervallen wordt het scheepsregister minder betrouwbaar (par. 4.2).

Daarnaast vereist blockchain die met proof-of-work werkt dat veel geïnvesteerd wordt in elektriciteit en computerapparatuur, hetgeen de claim dat automatisering tot kostenbesparing leidt mitigeert.

Ondersteuning van het recht

De inzet van blockchain techniek om het recht te ondersteunen is volgens Yeung redelijk onproblematisch.[413] Yeung noemt het voorbeeld van het Corda platform voor financiële diensten. De betrokken financiële dienstverleners hebben expliciet vastgelegd dat hun onderlinge verhouding geregeerd wordt door de contracten die ze met elkaar hebben gesloten en niet door de verwerkingen die op het Corda platform plaatsvinden. Ook het gebruik van een blockchain ter bevordering van transparantie is nastrevenswaardig.

Niettemin kunnen zich ook hier fricties voordoen tussen het recht en de resultaten waartoe toepassing van de blockchain aanleiding geeft. Yeung noemt als voorbeeld twee banken die hun onderling verkeer via smart contracts afwikkelen. Als het onderling verkeer transacties van cliënten van de banken betreft en een smart contract geeft ongewild negatieve effecten voor de cliënt, dan kan de laatste moeilijkheden ondervinden bij het vinden van genoegdoening, in het bijzonder wanneer dat aanpassing van een smart contract vergt. Zullen de banken bereid zijn die taak op zich te nemen?

[413] Yeung 2018, par. 2.2.2.

Bredere proprotionaliteitskwesties

Blockchains, althans sommige types van blockchains hebben nadelen die hen minder geschikt maken voor alle hierboven genoemde doeleinden, dan wel nadelige neveneffecten vormen. De volgende kunnen worden genoemd: beperkte schaalbaarheid, twijfelachtige duurzaamheid, betrouwbaarheid, en verzet tegen verandering van oude gegevens.

Er is twijfel over de schaalbaarheid van met name permissionless blockchains (scheepsregistratie en CAK use-case). Proof-of-Work vergt te veel tijd om grote transactievolumes aan te kunnen. In de bitcoin blockchain staat de schaalbaarheid voorts nog onder druk door de beperkte blockgrootte. Schaalbaarheidsproblemen kunnen de beschikbaarheid van een blockchain aantasten. Bij een blockchain die het consensusmechanisme Proof-of-Work hanteert en die een groot aantal miners kent, neemt het elektriciteitsverbruik een onacceptabele omvang aan. Er zijn schattingen dat het minen in de bitcoin blockchain evenveel elektriciteit kost als een klein land als Ierland verbruikt.[414] De betrouwbaarheid van permissionless blockchains is niet absoluut. Onder crypto-economische consensusmechanismen is nooit volledig zeker dat de gegevens in de blockchain niet meer veranderd worden. De gegevens kunnen bijvoorbeeld veranderen wanneer een consortium van miners een langere keten van geldige gegevens weet te genereren dan de keten die tot dan toe voor de langste werd gehouden (probleem genoemd in de scheepsregistratie use-case). Dit kan volstrekt onverwacht komen. Permissionless blockchains verzetten zich tegen wijziging van oude gegevens. In sommige contexten (recht op vergetelheid, kinderpornografie, intellectuele eigendom, smaad en laster etc.) kan dit aanleiding geven tot bijzonder lastige, juridische disputen.

Verantwoording

Het onderwerp blockchain en verantwoording betreft vaak de vraag hoe blockchain gebruikt kan worden om verantwoording af te leggen over bedrijfs- of organisatieprocessen. De blockchain is dan middel voor het afleggen verantwoording. In het kader dat hier gehanteerd wordt gaat het echter over het afleggen van verantwoording over normatieve keuzes die in de blockchain dan wel smart contracts zijn neergelegd.

Voor geautomatiseerd genomen overheidsbesluiten rust op de overheid ‘de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn.’[415](par. 3.4.1) In zijn brief aan de Tweede Kamer van 9 oktober 2018 maakt de minister voor rechtsbescherming een onderscheid tussen ‘technische transparantie’ en ‘uitlegbaarheid’.[416] Technische transparantie betreft in de praktijk de broncode en gebruikte databestanden, of in geval van zelflerende algoritmen, het gebruikte model en trainingsdata. Bij uitlegbaarheid van algoritmes gaat het om ‘het beschrijven van het doel dat met het algoritme wordt nagestreefd, welke variabelen doorslaggevend zijn geweest voor de uitkomst, het type gegevens dat wordt gebruikt, en de eventuele beslisregels.’ [417]

In sommige blockchains wordt voorzien in een mate van technische transparantie, bijvoorbeeld waar core code open source is of smart contracts op een openbare blockchain staan. Uitlegbaarheid van besluiten in de blockchain is nog minder ontwikkeld. Sommige informatie kan allicht ontleend worden aan gedocumenteerde discussie in het kader van de totstandkoming van de betreffende code. Het blijft echter de vraag of hieraan voldoende informatie over normatieve keuzes en hun omzetting

[414] The Economist explains, Why bitcoin uses so much energy, 9 juli 2018, beschikbaar op: https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy geraadpleegd op 25 april 2019.
[415] Raad van State 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o. 14.4.
[416] Kamerstukken II 2018/19, 26643, 570.
[417] Kamerstukken II 2018/19, 26643, 570.

ontleend kan worden, en of de informatie voldoende toegankelijk is voor betrokkenen. De toegankelijkheid kan zowel fysieke toegankelijkheid betreffen (vindbaarheid) als de intellectuele toegankelijkheid (begrijpelijkheid). Dit is een aandachtspunt.

Het afleggen van verantwoording kan onder druk komen door dat niet duidelijk is wie daarvoor verantwoordelijk is. Zo bleek in par. 3.3.1, dat het in een permissionless blockchain niet altijd duidelijk is wie als verwerkingsverantwoordelijke heeft te gelden. In permissionless blockchains is bovendien het adequaat aansturen van en contracteren met 'verwerkende' node-beheerders lastig. Een falen bergt het risico in zich dat de verwerking van persoonsgegevens niet transparant wordt bevonden (par 3.3.1).

Resultaatscriteria

Keuze versus effectiviteit

Dit criterium zegt dat het bieden van keuze de effectiviteit van technoregulering kan ondermijnen.[418] Zo zou het bieden van de mogelijkheid om een privé kopie te maken de effectiviteit wegnemen van een technische kopieerbeveiliging. In een blockchain context, zou dan bijvoorbeeld veranderlijkheid van in de blockchain opgeslagen gegevens de effectiviteit van de blockchain kunnen ondermijnen,[419] bijvoorbeeld als middel om traditionele tussenpersonen overbodig te maken. Hierboven is onder het kopje 'Efficiëntie en proportionaliteit' al aangegeven dat blockchains allicht voor minder problemen een effectieve oplossing bieden dan vaak gedacht. Sommigen voorspellen dat permissionless blockchains zich uiteindelijk alleen zullen blijken te eigenen voor niche toepassingen.[420] Dit kan een argument zijn tegen aanvaardbaarheid van inbreuken bijvoorbeeld op het recht op vergetelheid in permissionless blockchains en daarmee misschien een argument dat een oplossing veeleer in de techniek dan in het recht gezocht moet worden. Voor toepassingen waarvoor een permissionless blockchain een effectieve oplossing biedt kan dit uiteraard anders liggen. In de praktijk blijkt dat bedrijven en organisaties meestal kiezen voor de flexibelere permissioned blockchain.[421]

Flexibiliteit

Het criterium vraagt of een normatieve techniek zich voldoende kan aanpassen aan een veranderde gebruikscontext. In de blockchain context kan dit de core code (infrastructuur niveau) of smart contracts betreffen (toepassingsniveau). Voor zover het gaat om de core code hangt dit met name af van de governance structuur die veranderingen aan de code mogelijk moet maken. We zagen hiervoor onder het kopje 'Democratie en transparantie van het stellen van regels' dat niet bij alle permissionless blockchains de governance even goed is geregeld, waardoor niet geborgd is dat de belangen van alle betrokkenen even goed meegenomen worden. Dat kan zijn weerslag hebben op de flexibiliteit van de core code.

Een smart contract in een blockchain kan in zichzelf niet aangepast worden. Er kan echter wel voor gezorgd worden dat een niet langer gewenst smart contract niet langer gebruikt wordt en mogelijke gebruikers doorverwezen worden naar een vervangend smart contract.[422]

Een permissioned blockchain behoort vaak toe aan een of meerdere organisaties. Dat geeft in beginsel een goed uitgangspunt om afspraken te maken over het aanpassen van code in een blockchain.

---

[418] Het verlies aan effectiviteit kan dan een argument zijn voor aanvaardbaarheid van keuzeloze techno-regulering.
[419] Nakamoto 2008, Antonopoulos 2017.
[420] Matt Higginson, Nadeau, and Rajgopal 2019.
[421] Moerel 2019.
[422] In Ethereum, via 'delegatecall'. Bron: Ethereum, Introduction to Smart Contracts, Beschikbaar op: https://solidity.readthedocs.io/en/v0.4.21/introduction-to-smart-contracts.html (geraadpleegd 25 april 2019).

Transparantie van regels

Het theoretische idee achter een openbare blockchain is dat eenieder de code kan lezen. De core code is doorgaans open source software. Een smart contract op een publieke blockchain kan door eenieder geïnspecteerd worden. Het is echter de vraag of transparantie van code ook transparantie van de regels impliceert, zoals hierboven reeds in de paragraaf over verantwoording bleek. Zo zijn smart contracts niet te begrijpen of controleren zonder specialistische kennis, en het inhuren van zulke kennis is kostbaar, terwijl het riskant is om erop te vertrouwen dat het contract doet wat de ontwikkelaar zegt (par. 3.2.8).

5.3 Handhaafbaarheid

Hierboven zijn blockchains benaderd vanuit het perspectief van de aanvaardbaarheid als normatieve technologie. Daarmee is als het ware omlijnd wat de gewenste situatie is. Als zich die gewenste situatie niet voordoet en het recht gehandhaafd moet worden tegen deelnemers aan een blockchain, liggen er risico's in de sfeer van de realiseerbaarheid van handhaving. Dat is het onderwerp van deze paragraaf. Welke risico's in het kader van handhaafbaarheid kunnen onderscheiden worden?

5.3.1 Handhaving tegen wie?

Er zijn vele partijen die potentieel aangesproken kunnen worden. Hier zijn te noemen: internet serviceproviders, miners, beheerders van full nodes, core software developers, gebruikers, tussenpersonen zoals beurzen voor cryptocurrencies of banken, en overheden voorzover zij in de governance van blockchains betrokken zijn. Misschien ook aanbieders van oracles.

5.3.2 Moeilijkheden in het adresseren van degene tegen wie gehandhaafd wordt

5.3.2.1 Territorialiteit

Een blockchain is een netwerk dat zich vaak uitstrekt over grondgebied van meerdere jurisdicties. Blockchains zoals bitcoin strekken zich uit over de hele wereld, en daarmee ook buiten de EU.

Actoren die men zou willen aanspreken kunnen zich in jurisdicties buiten Nederland of de EU bevinden. Het recht in die jurisdicties kan minder bescherming bieden dan wij hier in Nederland of de EU gewend zijn. Formeel betekent dat niet altijd dat zij aan ons recht onttrokken zijn. Het materiele toepassingsgebied van de AVG strekt zich onder omstandigheden ook uit tot buiten de EU gevestigde actoren, mits zij gegevens van EU-burgers verwerken. Ook kan het zijn dat regels over toepasselijk recht toch de Nederlands recht als toepasselijk recht aanwijzen.
Niettemin, zijn er praktische zin wel problemen. Internationaal privaatrecht geeft weliswaar in concrete gevallen aan welk recht van toepassing is en welke rechter bevoegd is, maar de uitkomst kan sterk wisselen afhankelijk van relatief toevallige kenmerken van de zaak. De regels over jurisdictie en toepasselijk recht kunnen tot ongewenste resultaten leiden, zoals moeten procederen in meerdere staten (par.3.2.8)
Het kan wenselijk zijn dat er bij blockchain eenduidiger regels worden opgesteld. Daarbij zouden wel extra beschermingsregels nodig zijn om te vermijden dat blockchains worden opgericht in landen met weinig bescherming. Er is geen eenvoudige oplossing voor internationale geschillen over blockchain. Het verdient aanbeveling om internationale samenwerking te zoeken op dit gebied, door bijvoorbeeld in Europees verband regels te formuleren, waarna de Europese Unie in overleg kan treden met belangrijke landen op het gebied van blockchain (U.S.A., China, Rusland).

Een meer praktische mogelijkheid die verkend zou kunnen worden is te bezien of internet accessproviders gevraagd kan worden buitenlandse nodes te blokkeren. Buiten de blockchain context bestaat hier al enige ervaring mee in de handhaving van het auteursrecht, bijvoorbeeld in The Pirate Bay zaken.

5.3.2.2 Identiteit

Als de identiteit en woon- of verblijfplaats van de wederpartij onbekend zijn, is het niet mogelijk om deze te dagvaarden voor een gerechtelijke procedure. In hoeverre is dit een probleem in zaken over blockchain? Indien een blockchain toebehoort aan een (rechts)persoon kan deze aangesproken worden. Vaak worden ook cryptocurrency-beurzen of andere intermediairs zoals banken aangesproken. In de bitcoin blockchain zijn enorme servers met een groot elektriciteitsverbruik nodig om te minen. De benodigde apparatuur en het elektriciteitsverbruik maken het ook moeilijk om onder de radar te blijven. Niettemin is denkbaar dat er in voorkomende gevallen moeilijkheden zijn in het identificeren van mogelijke gedaagden. In een permissionless blockchain hoeft bijvoorbeeld de identiteit van beheerders van nodes niet bekend te zijn.

5.3.2.3 Verantwoordelijkheid en aansprakelijkheid

Er kan onduidelijkheid bestaan over wie formeel waarvoor verantwoordelijk is, met name in permissionless blockchains. Angela Walch constateert dat er niemand verantwoordelijk is voor het operationeel houden van de Bitcoin software.[423] Overeenkomsten zouden verantwoordelijkheden aan actoren kunnen toedelen. Doorgaans zijn er echter geen overeenkomsten tussen buitenstaanders en beheerders van nodes of tussen beheerders onderling (par. 3.2.3). Het kan in permissionless blockchains onduidelijk zijn wie verwerkingsverantwoordelijke of verwerker in de zin van de AVG is (par. 3.3.1).
Met name in permissionless blockchains kan onduidelijk zijn of er überhaupt verantwoordelijkheid of aansprakelijkheid bestaat, dan wel hoever die reikt. Zijn beheerders van nodes bijvoorbeeld verplicht zich volgens het protocol te gedragen? Zo ja, jegens wie? (par. 3.2.1) Zijn beheerders van nodes tot meer/anders dan het protocol verplicht? Zo ja, jegens wie? (Par. 3.2.1, 3.2.4, 3.2.9).

Toch is hiermee niet gezegd dat niemand verantwoordelijk gehouden kan worden. In de eerste plaats kan het probleem soms omzeild worden door poortwachters aan te spreken. Poortwachters zijn partijen die in de positie zijn om (als groep) de toegang tot een bepaald systeem te bepalen. Bijvoorbeeld zijn er bij bitcoin onofficiële poortwachters, te weten de bitcoinbeurzen. Nieuwe specifieke wettelijke regels kunnen gecreëerd worden die zich op bepaalde poortwachters richten, zoals bijvoorbeeld wettelijke regels inzake aansprakelijkheid van bepaalde partijen betrokken bij blockchain, meldplichten e.d. (par. 3.2.10). Zulke maatregelen zijn echter alleen effectief indien zij internationaal zijn afgesproken. Het verdient dan ook aanbeveling om internationale samenwerking te zoeken op dit gebied, door bijvoorbeeld in Europees verband regels te formuleren, waarna de Europese Unie in overleg kan treden met belangrijke landen op het gebied van blockchain (U.S.A., China, Rusland).

Voorts spreekt bijvoorbeeld Finck de verwachting uit dat blockchains zonder governance structuur het niet zullen redden. Ze zullen naar verwachting interne afspraken moeten maken en dan wordt ook duidelijker hoe de verantwoordelijkheden liggen. Tenslotte is natuurlijk mogelijk dat het recht verantwoordelijkheid toedeelt als partijen dat zelf niet doen. Onder de AVG kan een partij die onvoldoende duidelijk kan maken dat zij slechts verwerker is als verwerkingsverantwoordelijke worden aangemerkt door de toezichthouder.

5.3.3 Het doorzetten van handhavingsmaatregelen

Als het gaat om het wijzigen of verwijderen van gegevens op een blockchain, heeft het aanspreken van een beheerder van een enkele node weinig direct effect. De gegevens zullen immers via andere full nodes nog steeds beschikbaar zijn. Een blockchain kent een hoge mate van redundantie (par. 2.4.1). Het aanspreken van alle beheerders van nodes in een permissionless blockchain is

[423] Walch 2015, p.870.

omslachtig, casu quo praktisch onmogelijk. In met name permissionless blockchain ontbreekt het aan een partij die de doorzettingsmacht heeft om dingen te veranderen (bijv. verwijdering van oude gegevens bij alle full nodes). Er is gebrek aan een (sterke) interne governance structuur (par. 3.2.2). Dit heeft consequenties. Smart contracts hoeven niet overeen te stemmen met de juridische overeenkomst, maar het is bij divergentie lastig om af te dwingen dat het smart contract wordt uitgevoerd op de manier als volgens de juridische overeenkomst nodig is (par.3.2.9). Het is lastig om gegevens uit de blockchain te wissen, ook indien dit juridisch noodzakelijk is.

Uiteindelijk is dit een proportionaliteitsvraag: weegt het belang bij wissing van oude gegevens zwaarder dan de ondernemingsvrijheid van de blockchain ondernemers en het nut dat de blockchain levert? Deze vraag zal aan de hand van de omstandigheden van het geval beantwoord moeten worden: wat is het belang bij wissing? Is er een ingreep in het businessmodel van de beheerders nodig, en zo ja, welke? Welk effect heeft handhaving van het recht op het nut van de blockchain?

6. Conclusie

In de publiciteit worden aan blockchains en smart contracts vele innovatieve eigenschappen toegeschreven. Het zou traditionele intermediairs overbodig maken. Het maakt nieuwe vormen van samenwerking mogelijk (tussen partijen die elkaar niet noodzakelijkerwijze vertrouwen). Het leidt tot verbetering van dienstverlening en kostenbesparing. Blockchain is het internet van waarde.

Tegelijkertijd moet geconstateerd worden dat blockchain een ingewikkelde techniek is. Er bestaan veel misverstanden en onduidelijkheden over wat de techniek precies is en wat ze wel en niet kan.

Het beeld wordt nog verder vertroebeld doordat er verschillende blockchains bestaan met ieder net weer wat andere eigenschappen dan andere blockchains.

In de kern zijn blockchains databanken die op meerdere plaatsen door evenzovele beheerders worden bijgehouden.

Belangrijk is onderscheid te maken tussen permissionless en permissioned blockchains. In eerstgenoemde blockchain kennen de beheerders van de nodes elkaar niet. Een uitgebreid systeem van crypto-economische prikkels waarbij ook een cryptocurrency een belangrijke rol speelt zorgt voor de coördinatie die de blockchain doet functioneren. In permissioned blockchains beslist een centrale instantie of een collectief (bijv. alle beheerders) wie als nieuwe beheerders toegelaten worden. Permissioned blockchains hoeven niet te werken met crypto-economische prikkels en cryptocurrencys. In feite, door dat juist niet te doen, vormen zij een waardevol alternatief voor permissionless blockchains.

De belangrijkste bijzondere eigenschappen van blockchains zijn in onze ogen:

Onveranderlijkheid. Gegevens die eenmaal in een blockchain zijn opgeslagen kunnen niet aangepast worden of uit de blockchain verwijderd worden. Dat is echter vooral een eigenschap van blockchains waarin coördinatie gebaseerd is op een systeem van crypto-economische prikkels. In die blockchains kunnen gegevens niet gewijzigd worden. Maar zelfs daar is niet van absolute onveranderlijkheid van gegevens sprake. Zeer uitzonderlijke situaties, zoals een fork, een 51% aanval of een gezamenlijke beslissing van alle node-beheerders, kunnen aanleiding geven tot een systeembreuk en dan staat de onveranderlijkheid van gegevens op losse schroeven. Een permissioned blockchain (mits niet gebaseerd op crypto-economische prikkels) kan wel vrij gemakkelijk in een governance structuur voorzien die wijziging van opgeslagen informatie mogelijk maakt.

Vaak wordt aan blockchains toegeschreven dat zij alles kunnen controleren. De werkelijkheid is dat een blockchain alleen kan controleren door vergelijking met gegevens die al in de blockchain staan of die van buiten worden aangeleverd via een zogenaamd oracle. Met andere woorden, er is meer dat een blockchain niet weet dan wat hij wel weet. Een blockchain is meer blind dan alwetend.

Blockchains zijn redundant. De gegevens worden op meerdere servers onder beheer van meerdere beheerders opgeslagen. Dat kan bescherming geven tegen natuurrampen of cyber-aanvallen. Het maakt echter ook coördinatie binnen het netwerk moeilijk. Coördinatie in al die gevallen die niet door het protocol zijn voorzien, is lastig.

Blockchains zijn in technische zin transparant. Dit is ook vooral een eigenschap van permissionless blockchains. De technische transparantie is echter een 2-snijdend zwaard. Aan de ene kant is het voor veel toepassingen niet zo handig dat iedereen alles kan zien. Dan moeten weer maatregelen getroffen worden om data aan het zicht van de buitenwereld te onttrekken. Aan de andere kant, kan

de beschikbaarheid van zeer veel gedetailleerde data ook weer de begrijpelijkheid van data ondermijnen.

Op een aantal blockchains is het mogelijk zogenaamde smart contracts te plaatsen. Een smart contract is in wezen uitvoerbare code. Die code hoeft overigens niet smart te zijn (in de zin van werkend met kunstmatige intelligentie) en het hoeft ook geen overeenkomst in juridische zin te zijn. De naamgeving is misleidend. Eenmaal op een blockchain geplaatst kan een smart contract niet gewijzigd of verwijderd worden. De code wordt in beginsel uitgevoerd zonder dat degene die het smart contract op de blockchain heeft geplaatst daarop nog invloed heeft.

Ten behoeve van het onderzoek is een viertal use-cases onderzocht: over het plaatsen van het scheepsregister op een blockchain, een systeem voor schatkistbankieren ten behoeve van de nieuwbouw van scholen, een blockchain voor documentatie rond Europese afvaltransporten en een blockchain verkenning rond vergoedingen in het kader van de Wet maatschappelijke ondersteuning. In al deze casussen, staat een proces centraal waarin vele partijen stukken met elkaar uitwisselen en waarin het proces gefragmenteerd en traag is. De mogelijkheden van blockchain worden voor al verkend met het oog het realiseren van een efficiëntiewinst.

Juridisch kader

Het in beeld brengen van de verschillende juridische aspecten van blockchains vergt een structuur die als ordenend principe kan functioneren. Daartoe is hier gekozen voor criteria van aanvaardbaarheid van normatieve technologie. Blockchain is normatieve technologie. Door haar opzet beoogt zij de verhoudingen tussen betrokken partijen opnieuw te definiëren. Bovendien is het gekozen schema van criteria voldoende algemeen om een breed beeld te gegeven van juridische aspecten. In deze conclusie komen de vier belangrijkste criteria aan bod.

Mensenrechten en morele waarden/beschermingsfunctie van het recht

Welke mensenrechten en morele waarden komen door het gebruik van blockchain onder druk? Sommige komen vrij expliciet onder druk in andere gevallen is het meer een impliciet proces. Gegeven het brede toepassingsgebied van blockchains kunnen mensenrechten en morele waarden onder druk komen. De belangrijkste die in dit onderzoek naar voren zijn gekomen zijn de hierna genoemde.

Tot de expliciet onder druk komende mensenrechten vallen onder andere privacy en gegevensbescherming. Zij komen onder druk door eigenschappen als onveranderlijkheid en redundantie. Met name in permissionless blockchain is het wissen van persoonsgegevens die niet langer nodig zijn of ten aanzien waarvan de betrokkene een beroep doet het recht van vergetelheid een probleem (onveranderlijkheid). Ook onduidelijkheid rond het beleggen van verantwoordelijkheden in permissionless blockchains belet een adequate bescherming van persoonsgegevens (gevolg van de manier waarop redundantie vorm is gegeven).

Autonomie staat onder druk. Informatieplichten ten aanzien van gebruikers zijn onduidelijk en blockchaintoepassingen laten weinig ruimte voor het accommoderen van de autonomie van de gebruiker en eventuele andere betrokkenen (het vatten van processen in code en casu quo onveranderlijkheid).

De geautomatiseerde afloop van processen gebaseerd op een beperkte set data (blindheid van de blockchain) houdt een risico in van ongelijke behandeling en discriminatie.

Ook kan blockchain impliciet tot ondermijning van rechtsnormen leiden. De blockchain/smart contracts kanaliseren gedrag en de toepasselijke rechtsnorm verdwijnt uit zicht. De code gaat in de

gedachten van de betrokkenen de rol overnemen van het recht. Het wordt een spel om de code te ontwijken zonder besef van de onderliggende rechtsnorm. The DAO hack laat dit duidelijk zien. Een deel van de gemeenschap zag de in code ingebakken kanalisering als de enig bindende norm.

Hier is wel reden om de vinger aan de pols te houden.

Legitimiteit

Er wordt vaak geclaimd dat een blockchain vertrouwen overbodig zou maken. Daarbij wordt over het hoofd gezien dat in de code voor de blockchain of voor het smart contract vele keuzes besloten liggen. Wie zich eenmaal met een blockchain ingelaten heeft, kan zich niet meer eenvoudig aan de voorgeprogrammeerde gevolgen onttrekken. In plaats van te geloven dat vertrouwen overbodig is geworden, doet men er beter aan zich af te vragen wat de legitimiteit is van de machtsuitoefening door middel van code. De legitimiteit heeft een formeel aspect (bestuurshandelen vergt een wettelijke basis, private partijen zijn in beginsel vrij te handelen), maar ook een waarborg aspect: er moeten voldoende waarborgen ingebouwd zijn om de eenvoudige gebruiker niet te overleveren aan de willekeur van de bouwer van de techniek. Hier speelt vooral ook de integriteit van de degenen die de relevante code bepalen een rol. Het is mogelijk om blockchaintoepassingen te legitimeren, maar het is evenzeer mogelijk om in naam van innovatie- of efficiëntiebevordering om aan waarborgen en legitimiteit af te doen.

Democratie en transparantie van het stellen van regels

Blockchains hebben implicaties voor veel mensen die niet betrokken zijn geweest bij de ontwikkeling van de code die die implicaties bewerkstelligen. Dat doet de vraag rijzen naar de democratische legitimatie van blockchain: in hoeverre worden degenen die geraakt worden door blockchain betrokken in het vormgeven van een blockchain of blockchaintoepassing? Dit hangt uiteraard af van de wijze waarop governance in een blockchain is vormgegeven. Daarin bestaat geen uniformiteit. De belangrijkste permissionless blockchains hebben een governance structuur waarin weliswaar eenieder kan participeren, maar de beslissingsmacht toch ligt bij miners en core code ontwikkelaars. Zeker als de maatschappelijke impact van blockchains toeneemt, is een effectieve governance een belangrijk aandachtspunt. Voorts is van belang dat democratische betrokkenheid in een vroegtijdig stadium plaats vindt, om te voorkomen dat democratische besluitvorming voor voldongen feiten wordt geplaatst.

Proportionaliteit

Blockchain wordt ingezet voor uiteenlopende doeleinden. Het bereiken van efficiëntiewinst (betere dienstverlening, lagere kosten) is blijkens de use-cases een dominante beweegreden. Tegelijkertijd kunnen mensenrechten en morele waarden door de inzet van blockchains onder druk komen. Is een blockchain in dit speelveld een redelijk middel om het doel (efficiëntiewinst) te bereiken?

In de eerste plaats moet de claim dat een blockchain tot efficiëntiewinst leidt gemitigeerd worden. Een blockchain lost het probleem van de authenticiteit van gegevens die de blockchain ingaan niet op. Het waarborgen van authenticiteit vergt communicatie met de ‘buitenwereld’ (bijvoorbeeld traditionele intermediairs) en daar gaat efficiëntie verloren. Alleen kijken naar de werkzaamheden van de node-beheerders is een te eng perspectief en geeft geen volledig beeld van de (in)efficiëntie. De claim dat blockchain problemen rond gefragmenteerde werkprocessen oplost, zoals bij het scheepsregister, is discutabel. Alle benodigde data kan weliswaar voor iedere relevante partij op de blockchain beschikbaar zijn, maar daarmee is nog geen workflow gerealiseerd. Inpassing en beoordeling van de data in een werkproces vergt een aparte laag in software die bovenop de

blockchain gelegd zal moeten worden. Aangezien die (nog) niet bestaat rijst wederom de vraag of een klassieke ICT-implementatie van het werkproces niet efficiënter is of kan zijn.

Er is reden kritisch te zijn over de efficiëntiewinst die met blockchain projecten te behalen is, terwijl met name blockchains die op basis van crypto-economische prikkels functioneren daar belangrijke nadelen tegenover stellen: problemen rond de onveranderlijkheid van data, twijfels over de schaalbaarheid en bij blockchains die met proof-of-work werken, duurzaamheidsbezwaren.

Concluderend kan gezegd worden dat dit rapport kritisch is over blockchains. Dat neemt niet weg dat waar blockchain kansen biedt die aangegrepen moeten worden. Blockchain blijkt evenwel niet het geneesmiddel tegen alle kwalen te zijn en met name permissionless blockchains hebben bijwerkingen. Het is belangrijk bij het overwegen van nieuwe blockchain projecten om eerst een goede probleemanalyse te maken en nauwkeurig te bezien of een blockchain voor de geïdentificeerde problemen een oplossing biedt. Als dit het geval is dan biedt het in hoofdstuk 5 uitgewerkte kader een eerste handvat om juridische randvoorwaarden in kaart te brengen en er zo een maatschappelijk verantwoorde innovatie van te maken.

Bibliografie

Alharby & Van Moorsel 2017
M. Alharby & A. van Moorsel, 'Blockchain-based Smart Contracts: A Systematic Mapping Study', *Computer Science & Information Technology* 2017, p. 125-140.

Allen 2017
H.J. Allen, '$=Euro=Bitcoin', *Maryland Law Review* 2017, afl. 4, vol. 76, p. 877-939.

Allen 2018
J.G. Allen, 'Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language', *European Review of Contract Law* 2018 (14/4), p. 307–343.

Antonopoulos 2017
A.M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, Inc. 2017.

Asser Procesrecht/Asser 3 2017
W.D.H. Asser, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. Procesrecht. 3. Bewijs*, Deventer: Wolters Kluwer 2017.

Asser/Bartels & Van Mierlo *3-IV* 2013
S.E. Bartels & Van Mierlo, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 3. Vermogensrecht algemeen. Deel IV. Algemeen goederenrecht*, Deventer: Kluwer 2013.

Asser/Hartkamp & Sieburgh *6-IV* 2015
S. Hartkamp & C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Kluwer 2015.

Asser/Japikse *8-II 2012**
R.E. Japikse, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 8. Verkeersmiddelen en vervoer. Deel II. Rechten en voorrechten op zeeschepen: Kapitein, bevoegdheden en verplichtingen*, Deventer: Kluwer 2012.

Asser/Maeijer & Van Olffen *7-VII* 2017
J.M.M. Maeijer & M. van Olffen, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 7. Bijzondere overeenkomsten. Deel VII. Maatschap, vennootschap onder firma en commanditaire vennootschap*, Deventer: Wolters Kluwer 2017.

Asser/Sieburgh *6-I* 2016
C.H. Sieburgh, *Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel I. De verbintenis in het algemeen, eerste gedeelte*, Deventer: Wolters Kluwer 2016.

Atzori 2015
M. Atzori, 'Blockchain technology and decentralized governance: Is the state still necessary?', 2015, p. 1-37, beschikbaar via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713.

Bacon e.a. 2017
J. Bacon e.a., 'Blockchain Demystified', *Queen Mary School of Law Legal Studies* 2017, Research Paper nr. 268/2017, beschikbaar via: https://ssrn.com/abstract=3091218.

Bal 2015
A. Bal, 'How to Tax Bitcoin?', in: D.L.K. Chuen (red.), *Handbook of Digital Currency*, Amsterdam: Academic Press 2015, p. 267-282.

Barocas & Selbst 2016
S. Barocas & A.D. Selbst, 'Big Data's Disparate Impact', 104 *California Law Review* 671 2016.

Barkhuysen & Jak 2017
T. Barkhuysen & N. Jak, 'Afdeling Bestuursrechtspraak formuleert toetsingskader voor geautomatiseerde besluitvormingsprocessen', *Stibbe*, 2017.

Baron e.a. 2015
J. Baron e.a., 'The Current State of Virtual Currencies', in: J. Baron e.a., *National Security Implications of Virtual Currency. Examining the Potential for Non-state Actor Deployment*, Santa Monica: RAND Corporation 2015, p. 5-22, beschikbaar via: http://www.jstor.org/stable/10.7249/j.ctt19rmd78.8.

Bartoletti 2017
C. Bartoletti e.a., 'Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact', *Universita di Cagliari* 2017, beschikbaar via: https://arxiv.org/pdf/1703.03779.pdf.

Baukema 2013
J. Baukema, 'Bitcoin: een (ongereguleerd) betaalmiddel van de toekomst?', *Tijdschrift voor Financieel Recht* 2013/12, p. 411-418.

Bayern 2014
S. Bayern, 'Dynamic Common Law and Technological Change: The Classification of Bitcoin', *Washington & Lee Law Review Online* 2014, afl. 2, vol. 71, p. 22-34.

Beerepoot 2018
Y.S. Beerepoot, 'Blockchain unchained: gevolgen van blockchain voor de faillissementspraktijk', Tijdschrift voor Insolventierecht 2018/34.

Bentke 2017
J. Bentke, 'On-Chain vs Off-Chain', 2017, beschikbaar via: https://energyweb.atlassian.net/wiki/spaces/EWF/pages/17760291/On-Chain+vs+Off-Chain.

Berberich & Steiner 2016
M. Berberich & M. Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers', *European Data Protection Law Review* (2) 2016, p. 422-426.

Berlee 2017
A. Berlee, 'Volledige openbaarheid het doel voorbij', *WPNR* 2017/7169, p. 844-852.

Berlee 2018
A. Berlee, *Access to Personal Data in Public Land Registers* (diss. Maastricht), Den Haag: Eleven 2018.

Berlee 2018a
A. Berlee, 'Pandakteregistratie van Belastingdienst naar blockchain: een verkenning', *Maandblad voor Vermogensrecht* 2018/3, p. 87-93.

Bernardt & Van Vlastuin 2015

M. Bernardt & J.D. van Vlastuin, 'De executie van bitcoins', *Gerechtsdeurwaarder* 2015/1, p. 24-26.

Biemans 2018
J.W.A. Biemans, 'Beslag op en executie van domeinnaamrechten en bitcoins', in: S.J.W. van der Putten & M.R. van Zanten (red.), *Compendium beslag- en executierecht*, Den Haag: Sdu 2018, p. 561-579.

BitFury Group 2015
BitFury Group in collaboration with Jeff Garzik, Public versus Private Blockchains. Part 1: Permissioned Blockchains, White Paper, 2015 (Version 1.0).

Blemus 2017
S. Blemus, 'Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide', *Revue Trimestrielle de Droit Financier* 2017, afl. 4, p. 1-15.

Bochove, Van 2013
L.M. van Bochove, *Betrokkenheid van derden bij contractbreuk* (diss. Rotterdam), Oisterwijk: Wolf Legal Publishers 2013.

Bodo et al. 2019
B. Bodó, V. Ferrari, A. Giannopoulou, J. Quintais, 'Blockchain and the Law: A Critical Evaluation', *Stanford Journal of Blockchain Law & Policy* (2), 1, 2019.

Bogost 2017
I. Bogost, 'Cryptocurrency Might Be a Path to Authoritarianism', 2017, beschikbaar via: www.theatlantic.com.

Böhme & Pesch 2016
R. Böhme & P. Pesch, 'Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie', Datenschutz und Datensicherheit (DuD) 2016, pp 473–481.

Brownsword 2005
R. Brownsword, 'Code, Control, and Choice: Why East is East and West is West', 21 *Legal Studies* 2005, pp. 1-21.

Buterin 2014
V. Buterin, 'DAOs, DACs, Das and More: An Incomplete Terminology Guide', *Ethereum Blog* 2014.

Cafaggi & Clavel 2011
F. Cafaggi & S. Clavel, 'Interfirm networks across Europe: a private international law perspective', in: F. Cafaggi (red.), *Contractual Networks, Inter-Firm Cooperation and Economic Growth*, Cheltenham: Elgar Publishing 2011, p. 201-245.

Casey & Niblett 2017
A.J. Casey & A. Niblett, 'Self-Driving Contracts', *Journal of Corporation Law* (43) 2017, p. 1-33.

Cermeño 2016
J.S. Cermeño, 'Blockchain in financial services: Regulatory landscape and future challenges for its commercial application', *Working Papers* 2016, Nr. 16/20, beschikbaar via: https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf.

Christopher 2016

C.M. Christopher, 'The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain', *Nevada Law Journal* (17) 2016, p. 1-42.

Claringbould 1992
M.H. Claringbould, *Parl. Gesch. Boek 8: Parlementaire geschiedenis van het nieuwe Burgerlijk Wetboek, Boek 8, Verkeersmiddelen en vervoer*, Deventer: Kluwer 1992.

CNIL 2018
CNIL, Blockchain. Premiers éléments d'analyse de la CNIL, 2018.

Connor-Green 2017
D.S. Connor-Green, 'Blockchain in Healthcare Data', *Intellectual Property & Technology Law Journal* (21) 2017, p. 93-107.

Daniell 2017
J. Daniell, 'The Casper Proof-Of-Stake Algorithm: Prepare To Commit', 2017, beschikbaar via: www.ethnews.com.

De Filippi & Loveluck 2016
P. De Filippi & B. Loveluck, 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure', *Internet Policy Review* 2016, afl. 3.

De Filippi & Wright 2018
P. De Filippi & A. Wright, *Blockchain and the Law: The Rule of Code*, Cambridge: Harvard University Press 2018.

De Jonghe & Laan 2017
D. de Jonghe & V.I. Laan, 'Blockchain in de realiteit', *Computerrecht* 2017, afl. 6, nr. 251, p. 349.

Drijber 2001
B.J. Drijber, 'De richtlijn elektronische handel op de snijtafel', *SEW* 2001, p. 122-138.

Drion 2000
C.E. Drion, 'Consumentenbescherming bij e-commerce: een (dreigende) wassen neus?', *Contracteren* 2000, p. 34-35.

Eenmaa-Dimitrievi & Schmidt-Kessen 2017
H. Eenmaa-Dimitrieva & M.J. Schmidt-Kessen, 'Regulation Through Code as a Safeguard for Implementing Smart Contracts in No-Trust Environments', *EUI Department of Law Research Paper* 2017, nr. 13, beschikbaar via: https://ssrn.com/abstract=3100181 of http://dx.doi.org/10.2139/ssrn.3100181.

Eck, Van 2017
M. van Eck, 'Extra waarborgen voor burgers bij het vervangen van ambtenaren door computers', *Bestuursrecht & AI* 2018.

Eersel, Van 2018
M. van Eersel, 'Blockchain-investing of beleggen in de cryptosfeer', VBA-journaal 2018, nr. 134, p. 38-42.

Eersel, Van & Van den Bergh 2017
M. van Eersel & Th. van den Bergh, 'Blockchain en smart contracts: toegang tot een reeks van slimme dingen', Tijdschrift Financieel Recht in de praktijk 2017/4, p. 40-48

Esch, Van 2001
R. van Esch, *Pecunia electronica non olet*, oratie Leiden 2001, Deventer: Kluwer.

European Union blockchain observatory and forum 2018
European Union blockchain observatory and forum, Blockchain and the GDPR, 2018.

Evadgian 2018
M. Evadgian, *De intelligentie van smart contracts bij contractuele dwaling*, (Masterthesis Tilburg), Tilburg: Tilburg University 2018.

Filippi, De, & Loveluck 2016
P. de Filippi & B. Loveluck, 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure', *Internet Policy Review* (5) 2016, p. 1-28, beschikbaar via: policyreview.info/node/427/pdf, doi.org/10.14763/2016.3.427.

Finck 2017
M. Finck, 'Blockchains and Data Protection in the European Union', *Max Planck Institute for Innovation & Competition Research* 2017, Paper No. 18-01, beschikbaar via: SSRN https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322

Finck 2019
M. Finck, *Blockchain Regulation and Governance in Europe*, Cambridge: Cambridge University Press 2019.

Fries & Paal 2019
M. Fries & B.P. Paal (red.), *Smart Contracts*, Tübingen: Mohr Siebeck 2019.

Garau Sobrino 2017
F.F. Garau Sobrino, 'Forthcoming Private International Law: The Future Is Already Here', *Anuario Espanol Derecho Internacional Privado* (17) 2017, p. 303-332.

Geiregat 2018
S. Geiregat, 'Cryptocurrencies Are (smart) Contracts', *Computer Law & Security Review* 2018, p. 1144-1149.

Geiregat 2018a
S. Geiregat, 'Eigendom op bitcoins', *Rechtskundig Weekblad* 81 (27) 2018, p. 1043-1049.

Goossens & Verslype 2019
J. Goossens & K. Verslype, *Blockchain en smart contracts. Het einde van de vertrouwde tussenpersoon?*, Brussel: Larcier 2019.

De Graaf 2018a
T.J. de Graaf, 'Van oud naar nieuw: van internet naar smart contracts en van mensen naar code', *WPNR* 2018 nrs. 7199 en 7200, p. 494-501 en 525-530.

De Graaf 2018b
T.J. de Graaf, 'De lappendeken van de gelijkstelling van elektronisch met schriftelijk in het licht van vormvereisten en bewijskracht', *Maandblad voor Vermogensrecht* 2018, p. 243-248.

De Graaf 2019
T.J. de Graaf, 'De kwalificatie van bitcoins', NJB 2019/2, p. 6-18.

Graaf & Krans 2018
T.J. de Graaf & H.B. Krans, 'Verhaal op bitcoins door gedwongen medewerking van de schuldenaar', *WPNR* 2018.

Grincalaitis 2018
M. Grincalaitis, 'Can a Smart Contract be upgraded/modified? Is CPU mining even worth the Ether? The Top questions answered here…', 2018, beschikbaar via: www.medium.com.

Groothuis 2004
M.M. Groothuis, *Beschikken en digitaliseren: over normering van de elektronische overheid* (dissertatie Leiden), Leiden: Universiteit Leiden 2004.

Helder, in: *GS Vermogensrecht*
E.R. Helder, commentaar op artikel 3:16 BW, in: J. Hijma, *Groene Serie Vermogensrecht*, Deventer: Wolters Kluwer (losbladig en online).

Hertig 2018
A. Hertig, 'Blockchain's Once Feared 51% Attack Is Now becoming Regular', 2018, beschikbaar via: www.coindesk.com.

Higginson et al. 2019
M. Higginson, M-C Nadeau, K. Rajgopal, 'Blockchain's Occam problem', 2019, beschikbaar via: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem.

Hofert 2018
E. Hofert, *Regulierung der Blockchains*, Tübingen: Mohr Siebeck 2018.

Hsiao 2017
J.I.H. Hsiao, 'Smart Contract on the Blockchain-Paradigm Shift for Contract Law', *US-China Law Review* (14) 2017, p. 685-694.

Huijgen 2017
W.G. Huijgen, 'Commentaar op art. 3:21 BW', in: C.J.J.M. Stolker, W.L. Valk & H.B. Krans (red.), *Tekst & Commentaar BW*, Deventer: Kluwer 2017 (boek en online).

Huydekoper & Van Esch 1997
S. Huydecoper & R. van Esch, *Geschriften en handtekeningen: een achterhaald concept?,* Alphen aan den Rijn: ITeR 1997.

Ibáñez et al. 2018
L.D. Ibáñez, K. O'Hara, and E. Simperl, 'On Blockchains and the General Data Protection Regulation', 2018, University of Southampton.

Van Ingen & Smits 2018
M. van Ingen & W.J. Smits, 'Beslag op bitcoin: (praktisch) onmogelijk?', *Beslag, Executie en Rechtsvordering in de praktijk* 2018/2, p. 17-22.

Van Ingen & Smits 2018a
M.J.W. van Ingen & W.J. Smits, 'Het faillissementsbeslag en de nieuwe wereldorde', Tijdschrift voor Curatoren 2018/1, p. 14-17.

Jak & Bastiaans 2018

N. Jak & S. Bastiaans, 'De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid', *NJB* 2018 40, p. 3018-3025.

Janssen 2017
E. Janssen, 'Smart contracts en onvoorziene omstandigheden', in: H.N. Schelhaas, A.I. Schreuder & K.K.E.C.T. Swinnen (eds.), *Nieuwe technologieën, nieuw privaatrecht?* Den Haag: Boom juridisch 2017.

Johnstone 2018
S. Johnstone, Syren, How Can Blockchain and Other Consensus Driven Cryptographic Technology be Regulated? (November 1, 2018), beschikbaar via: SSRN https://ssrn.com/abstract=3278403 or http://dx.doi.org/10.2139/ssrn.3278403

Jones, Eber & Seward 2000
S.P. Jones, J. Eber & J. Seward, 'Composing Contracts: An Adventure in Financial Engineering', in: M. Odersky & P. Walder, *Proceedings of the fifth ACM SIGPLAN international conference on Functional programming*, New York: ACM 2000, p. 280-292.

De Jong 2017
G.T. de Jong, *Niet-nakoming van verbintenissen. Mon. BW B33*, Deventer: Wolters Kluwer 2017.

Knuist 2014
J. Knuist, 'De (virtuele) werkelijkheid van virtuele valuta's', *Vakstudie-Nieuws* 2014, p. 6.

Koops 2007
B.-J. Koops, 'Criteria for Normative Technology: An Essay on the Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values', *Regulating Technologies, Brownsword & Yeung, eds.*, Oxford: Hart Publishing 2017, p. 157-174; TILT Law & Technology Working Paper Series No. 005/2007, beschikbaar via: SSRN https://ssrn.com/abstract=1071745 or http://dx.doi.org/10.2139/ssrn.1071745.

Koops & Leenes 2005.
B.-J. Koops & R.E. Leenes, Code and the slow erosion of privacy, *MTTLR* 12 2005, 1, 117-188.

Koulu 2016
R. Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement', *SCRIPTed* (13) 2016, p. 40-69.

Kunde etal. 2018
E. Kunde, M. Kaulartz, R.B. Naceur, S. Liban, M. Kunz, V. Skwarek, K. Adam, R. Weiß, and M. Liesenjohann, 'Faktenpapier Blockchain und Datenschutz', 2018.

Laan 2018
V. Laan, 'Privacy en blockchain: wanneer is er voor wie privacywerk aan de winkel?', *Tijdschrift voor Internetrecht, IR* 2018, afl. 1, p. 4-11.

Laan & Rutjes 2017
V.I. Laan & A. Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017, afl. 6, nr. 253, p. 364-371.

Lamport et al. 1982
L. Lamport, L., R. Shostak & M. Pease, 'The Byzantine Generals Problem', *ACM Transactions on Programming Languages and Systems,* 4 (3) 1982, p. 387 e.v. doi:10.1145/357172.357176.

Lauslahti, Mattila, Seppälä 2017
K. Lauslahti, J. Mattila & T. Seppälä, 'Smart Contracts – How will Blockchain Technology Affect Contractual Practices?', *ETLA Reports* 2017, nr. 68, p. 1-27, beschikbaar via: https://pub.etla.fi/ETLA-Raportit-Reports-68.pdf.

Lent, Van 2018
D. van Lent, 'Kraamhulp bestellen met blockchain', *NRC* 2018.

Levy 2017
K.E.C. Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law', *Engaging Science, Technology, and Society* (3) 2017, p. 1-15.

Linnemann 2016
J.J. Linnemann, 'Juridische aspecten van (toepassingen van) blockchain', *Computerrecht* 2016/218.

Lodder & Kaspersen 2002
A.R. Lodder & H. Kaspersen, *E-Directives: Guide to European Union Law on E-commerce*, Den Haag: Kluwer Law International 2002.

Louwman, *WPNR* 2018/7209
W. Louwman, 'De Basis Registratie Kadaster: een knecht van twee meesters?', *WPNR* 2018/7209, p. 728-735.

Low & Teo 2018
K.F.K. Low & E.G.S. Teo, 'Legal Risks of Owning Cryptocurrencies', *In: Handbook of Blockchain, Digital Finance, and Inclusion*, Volume 1, 1st Edition, Reed Elsevier 2018, p. 225-247. http://dx.doi.org/10.2139/ssrn.2856137

Marian 2019
O.Y. Marian, 'Blockchain Havens and the Need for Their Internationally-Coordinated Regulation', *North Carolina Journal of Law and Technology,* Vol. 20, 2019, Forthcoming; UC Irvine School of Law Research Paper No. 2019-14, beschikbaar via: SSRN https://ssrn.com/abstract=3357168

Marino & Juels 2016
B. Marino & A. Juels, 'Setting Standards for Altering and Undoing Smart Contracts', in: J.J. Alferes et al. (eds.), *Rule Technologies. Research, Tools, and Applications, Proceedings 10th International Symposium, RuleML 2016*, New York: Springer 2016.

Martini & Weinzierl 2017
M. Martini & Q. Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden', *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 2017, pp 1251–1259.

McJohn & McJohn 2016
S.M. McJohn & Ian McJohn, 'The Commercial Law of Bitcoin and Blockchain Transactions', *Suffolk University Law School* 2016, Research Paper Nr. 16-13, beschikbaar via: https://ssrn.com/abstract=2874463.

Melis & Waaijer 2012
J.C.H. Melis & B.C.M. Waaijer, *De notariswet*, Deventer: Kluwer 2012.

Mendez Gonzalez

Fernando P. Mendez Gonzalez, Cadastres and Land Registries in Europe, Merged Organizations or Separate Institutions? The State of Play.

Meyer 2018
D. Meyer, 'Blockchain Technology is on a Collision Course with EU Privacy Law', 2018, beschikbaar via: https://iapp.org/.

Mijnssen 2017
F.H.J. Mijnssen, *Verbintenissen tot betaling van een geldsom*. *Mon. BW B39*, Deventer: Wolters Kluwer 2017.

Mik 2017
E. Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity', *Law Innovation and Technology* (9) 2017, p. 269-300, beschikbaar via: https://ssrn.com/abstract=3038406 or http://dx.doi.org/10.2139/ssrn.3038406.

Moerel 2019
E.M.L. Moerel, 'Blockchain & Data Protection … and Why They Are Not on a Collision Course', *European Review of Private Law* 6-2019 [825–852].

Nakamoto 2008
S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 2008, beschikbaar via: https://bitcoin.org/bitcoin.pdf.

Nannings 2018
M.A.R. Nannings, *Regulering van Initial Coin Offerings*, Tilburg: Celsus 2018.

Naves 2018
J. Naves, 'Smart contracts. Voer voor juristen?', Onderneming en Financiering 2018 (26) 4, p. 57-67.

Neppelenbroek 2019
E.D.C. Neppelenbroek, Elektronisch contractenrecht, Den Haag: Boom Juridisch 2019.

Norton Rose Fulbright 2016
Norton Rose Fulbright, *Smart Contracts: coding the fine print*, 2016, beschikbaar via: www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print.

O'Shields 2017
R. O'Shields, 'Smart Contracts: Legal Agreements for the Blockchain', *N.C. Banking Inst.* (21) 2017, p. 177-194.

Overwater & Custers 2018
L.J. Overwater & B.H.M. Custers, 'De regulering van Initial Coin Offerings en cryptocurrencies', *Computerrecht* 2018/208, p. 260-270.

Paech 2017
P. Paech, 'The Governance of Blockchain Financial Networks', *Modern Law Review* (80) 2017, p. 1072-1100.

Perugini & Dal Checco 2015
M.L. Perugini & P. Dal Checco, *Smart Contracts: A Preliminary Evaluation*, Italy: University of Bologna 2015, beschikbaar via: ssrn.com/abstract=2729548.

Pilkington 2016
M. Pilkington, 'Blockchain Technology: Principles and Applications', in: F. Xavier Olleros en M. Zhegu (red.), *Research Handbook on Digital Transformations*, Cheltenham: Edward Elgar Publications 2016.

Pitlo/Reehuis, Heisterkamp, Van Maanen & De Jong 2012
W.H.M. Reehuis, A.H.T. Heisterkamp, G.E. van Maanen, G.T. de Jong, *Goederenrecht (Het Nederlands burgerlijk recht: Pitlo deel 3),* Deventer: Kluwer 2012.

Polak 1993
M.V. Polak, *Vermogensrechtelijke meerpartijenverhoudingen*, Deventer: Kluwer 1993.

Policy Research Corporation 2016
Policy Research Corporation, *Rapportage verbetering Nederlands scheepsregister*, Rotterdam: Policy Research Corporation 2016.

Policy Research Corporation 2017
Policy Research Corporation, *Rapportage alternatieve organisatievorm Nederlands scheepsregister - Eindrapport*, Rotterdam: Policy Research Corporation 2017.

Poon & Buterin 2017
J. Poon en V. Buterin, 'Plasma: Scalable Autonomous Smart Contracts', 2017 (Working draft), beschikbaar via: http://plasma.io/plasma.pdf.

Prakken 1993
H. Prakken, 'A Logical Framework for Modelling Legal Argument', in Proceedings of the 4th International Conference on Artificial Intelligence and Law, ed. Anya Oskamp and Kevin Ashley, New York: ACM 1993, p. 1–9.

Putman 2017
F.C.P. Putman, 'Bitcoins en minen in de inkomstenbelasting', *Vakblad Financiële Planning* 2017/114, p. 110-116.

Rank 2015
P. Rank, 'Betaling in bitcoins: geld of ruilmiddel, betaling of inbetalinggeving?', *Ars Aequi 2015*, p. 177-185.

Raskin 2015
M.I. Raskin, 'Realm of the Coin: Bitcoin and Civil Procedure', *Fordham Journal of Corporate and Financial Law* (20) 2015, p. 969-1011.

Raskin 2017
M. Raskin, 'The Law and Legality of Smart Contracts', *Georgetown Technology Review* (1) 2017, p. 305-341, beschikbaar via: ssrn.com/abstract=2959166.

Ray 2018
S. Ray, 'The Difference Between Blockchains & Distributed Ledger Technology', *Towards Data Science Blog* 2018.

Reus, De & Van Nijnatten 2018
M. de Reus & E. van Nijnatten, 'Belastingheffing over cryptobezittingen in box 3', *NJB* 2018/1813, p. 1811-1865.

Reyes 2017
C.L. Reyes, 'Conceptualizing Cryptolaw', *Nebraska Law Review* 2017, afl. 2, vol. 96, p. 384-445.

Rodenburg & Pappas 2017
B. Rodenburg & S.P. Pappas, Quantum Computing and Blockchain, Mitre Technical Report, MTR170487, 2017.

Roest, Van der 2017
J.H.C. van der Roest, *Smart Contracts en niet-nakoming: Een beslismodel voor de praktijk*, (Masterthesis Tilburg), Tilburg: Tilburg University 2017.

Ross 2017
E.S. Ross, 'Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues', *Catholic University Journal of Law & Technology* (25) 2017, p. 353-386.

Sander 2001
C. Sander, *Consumentenbescherming bij transacties op afstand*, Den Haag: Sdu Uitgevers 2001.

Savelyev 2016
A. Savelyev, 'Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law', *Higher School of Economics* 2016, Research Paper Nr. WP BRP 71/LAW/2016, beschikbaar via: ssrn.com/abstract=2885241.

Schroeder 2016
J.L. Schroeder, 'Bitcoin and the Uniform Commercial Code', *University of Miami Business Law Review* 2016, afl. 3, vol. 24, p. 1-79.

Schuringa 2017
H. Schuringa, 'Enkele civielrechtelijke aspecten van blockchain', *Computerrecht* 2017, afl. 6, nr. 254, p. 373.

Shackelford & Myers 2017
S.J. Shackelford & S. Myers, 'Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace', *Yale Journal of Law & Technology* (19) 2017, p. 334-388.

Sklaroff 2017
J.M. Sklaroff, 'Smart Contracts and the Cost of Inflexibility', *University of Pennsylvania Law Review* (166) 2017, p. 263-303.

Snijders 2005
W. Snijders, 'Ongeregeldheden in het vermogensrecht', *WPNR* 2005, nrs. 66607 & 6608, p. 94-101.

Snijders & Tonino 2018
J.L. Snijders & Y.C. Tonino, 'Goederenrechtelijke status van bitcoin (kapitaalkracht)', *Tijdschrift voor Financiering, Zekerheden en Insolventierechtpraktijk* 2018/6, p. 46-55.

Stam 2018
J.K. Stam, 'Smart contracts?', *Contracteren* 2018/2, p. 54-60

Surden 2012
H. Surden, 'Computable Contracts', *UC Davis Law Review* 2012, p. 629-700.

Szabo 1996
N. Szabo, 'Smart Contracts: Building Blocks for Digital Markets', 1996, beschikbaar via: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Szabo 1997a
N. Szabo, 'Formalizing and Securing Relationships on Public Networks', *First Monday* (2) 1997, beschikbaar via: firstmonday.org/ojs/index.php/fm/article/view/548/469/.

Szabo 1997b
N. Szabo, 'The Idea of Smart Contracts', 1997.

Tapscott & Tapscot 2016
D. Tapscott & A. Tapscott, *Blockchain Revolution,* London: Penguin UK, 2016.

Thake 2018
M. Thake, 'What's the difference between blockchain and DLT?', *Medium* 2018.

Timmer, *WPNR* 2011/6875
R.J.L. Timmer, 'Naar een meer positief stelsel van openbare registers en Basisregistratie Kadaster?', WPNR 2011/6875.

Tjong Tjin Tai 2007
T.F.E. Tjong Tjin Tai, *Zorgplichten en zorgethiek* (diss. Amsterdam UvA), Deventer: Kluwer 2007.

Tjong Tjin Tai e.a. 2009
T.F.E. Tjong Tjin Tai e.a., 'Een juridisch beoordelingskader voor samenwerking', *NTBR* 2009/7, p. 238-248.

Tjong Tjin Tai 2012
T.F.E. Tjong Tjin Tai, 'Meewerken aan wanprestatie of onrechtmatige daad, mede toegepast op de rol van de notaris', *WPNR* 2012/6954, p. 902-909.

Tjong Tjin Tai 2017a
T.F.E. Tjong Tjin Tai, 'Smart contracts en het recht', *NJB* 2017/146, p. 176-182.

Tjong Tjin Tai 2017b
T.F.E. Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts' *Tilburg Private Law Working Paper Series* 2017, No. 6, beschikbaar via: SSRN https://ssrn.com/abstract=3038800 or http://dx.doi.org/10.2139/ssrn.3038800.

Tjong Tjin Tai 2017c
T.F.E. Tjong Tjin Tai, 'Juridische aspecten van blockchain en smart contracts', *TPR* (54) 2017, p. 563-608.

Tjong Tjin Tai 2018a
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 2018*, Den Haag: Sdu 2018, p. 99-135.

Tjong Tjin Tai 2018b

T.F.E. Tjong Tjin Tai, 'Force Majeure and Excuses in Smart Contracts', *European Review of Private Law*, 2018-6, p. 787-804, *Tilburg Private Law Working Paper Series* 2018, No. 10, beschikbaar via: SSRN https://ssrn.com/abstract=3183637.

Tweehuysen 2018
V. Tweehuysen, 'Goederenrechtelijk puzzelen met bitcoins', *Ars Aequi 2018*, p. 602-610.

Vakstudie Invorderingswet
J. de Blieck e.a. (red.), *Invorderingswet* (Fiscale Encyclopedie De Vakstudie, deel 10), Deventer: Wolters Kluwer (online).

Valgaeren & Linnemann 2017
E. Valgaeren & J.J. Linnemann, 'Inleiding: Blockchain ontketend', *Computerrecht* 2017/250.

Vandezande 2018
N. Vandezande, *Virtual Currencies A Legal Framework*, Intersentia 2018.

De Vauplane 2018
H. de Vauplane, 'Blockchain and intermediated securities', *NIPR* 2018, afl. 1, p. 94-103.

VBW-studie 2017
VBW, *Blockchain und Smart Contracts Recht und Technik im Überblick*, 2017, beschikbaar via: https://www.vbw-bayern.de/vbw/Aktionsfelder/Standort/Wertsch%C3%B6pfung/Blockchain-und-Smart-Contracts-Recht-und-Technik-im-%C3%9Cberblick.jsp.

Veldhuizen, Van de Berg & Van Goor 2015
M.L. Veldhuijzen, R. van de Berg & E.A. van Goor, 'Bitcoin, income tax and vat - current legislation & policy and an outlook on the future', in: R.A. Wolf (red.), *Bitcoins. Civiele en fiscale aspecten in beeld*, Deventer: Kluwer 2015, p. 57-69.

Verstraete 2018
M. Verstraete, 'The Stakes of Smart Contracts', *Loyola University Chicago Law Journal* 2018 (forthcoming), beschikbaar via: https://ssrn.com/abstract=3178393.

Vos 2017
J. Vos, 'Blockchain-based Land Registry: Panacea, Illusion or something in between? Legal interference of Registrars in the econveyancing process', *ELRA* 2017, p. 1-26.

Vos en Roes, *WPNR* 2018/7180
J. Vos, en B.H.J. Roes, 'Onduidelijkheden rondom inschrijving en registratie', *WPNR* 2018/7180, p. 115.

Vos, *JBN* 2018/11-45
J. Vos, 'Blockchain en de landregistratie – wie bewaakt de bewaarder? (deel 1), *JBN* 2018/11-45.

Vos, *JBN* 2018/11-50
J. Vos, 'Blockchain en de landregistratie – wie bewaakt de bewaarder? (deel 2), *JBN* 2018/11-50.

De Vries 2018
A. de Vries: 'Bitcoin's Growing Energy Problem', *Joule* 2018, afl. 5, p. 801-805.

De Vries 2019

E. de Vries, 'Smart contracts: een keten van vertrouwen reikend tot in de fysieke wereld', Nederlands Tijdschrift voor Burgerlijk Recht 2019/12.

Walch 2017
A. Walch, 'The Path of the Blockchain Lexicon (and the Law)', *Boston University Review of Banking & Financial Law* (36) 2017, p. 713-765.

Walch 2015
A. Walch, The bitcoin blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, 18 *NYU Journal of Legislation and Public Policy* 2015, 837.

Wall 2016
L.D. Wall, '"Smart Contracts" in a Complex World', *Federal Reserve Bank of Atlanta* 2016, beschikbaar via: https://www.frbatlanta.org/cenfis/publications/notesfromthevault/1607.aspx.

Walport 2016
M. Walport, Distributed Ledger Technologies: beyond blockchain, Government Office for Science, 2016.

Weij & Landerbarthold 2018
W. Weij en mr. M.C. Landerbarthold, 'Ruis in de ether en de juridische kwalificatie(s) van cryptovaluta', *Tijdschrift voor Internetrecht* 2018/2, p. 66-68.

Wellink e.a. 2004
A.H.E.M. Wellink e.a. (red.), *De rol van geld in het privaatrecht : symposium over geld en recht*, Amsterdam: Ars Notariatus 2004.

Werbach & Cornell 2017
K. Werbach & N. Cornell, 'Contracts Ex Machina', *Duke Law Journal* (67) 2017, p. 313-382.

Werbach 2018
K. Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law', *Berkeley Technology Law Journal* 2018, afl. 2, p. 18-21.

Werbach 2018a
K. Werbach, *The Blockchain and the New Architecture of Trust*, Cambridge (Mass.): MIT Press 2018.

Wirth & Kolain 2018
C. Wirth & M. Kolain, 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data', *Reports of the European Society for Socially Embedded Technologies* 2018, dx.doi.org/10.18420/blockchain2018_03.

Wolf 2015
R.A. Wolf, 'Bitcoins and EU VAT', in: R.A. Wolf (red.), *Bitcoins. Civiele en fiscale aspecten in beeld*, Deventer: Kluwer 2015, p. 70-79.

Zegveld 2018
C.B.C.M. Zegveld, *Netwerkaansprakelijkheid voor gebrekkige samenhangende zorg* (dissertatie Tilburg), Tilburg: Tilburg University 2018.

Zwitser 1995
R. Zwitser, 'Derdenbeding en de overdracht van spaarzegels', NJB 1995, p. 581-587.

Kamerstukken

***Kamerstukken II* 2011/2012 – 2017-2018, 33 134**
Wetsvoorstel Regels omtrent de verkrijging en het verlies van de nationaliteit van zeeschepen (Rijkswet nationaliteit zeeschepen), *Kamerstukken II* 2011/2012-2017/2018, 33 134 (R1972) 1-13.

Brief van de Minister van Infrastructuur en Milieu van 1 december 2016
Brief van de Minister van Infrastructuur en Milieu van 1 december 2016, IENM/BSK-2016/270243.

Brief van de Minister van Binnenlandse Zaken van 29 juni 2018
Brief van de Minister van Binnenlandse Zaken van 29 juni 2018, Kabinetsreactie op het advies van de Autoriteit Persoonsgegevens over het gemak waarmee persoonsgegevens te raadplegen zijn via het Kadaster.

Rapporten

***Rapportage Alternatieve Organisatievorm Nederlands Scheepsregister - Eindrapport* 2017.**
Policy Research Corporation, *Rapportage alternatieve organisatievorm Nederlands scheepsregister - Eindrapport*, september 2017.

***Rapportage verbetering Nederlands Scheepsregister* 2016.**
Policy Research Corporation, *Rapportage verbetering Nederlands* scheepsregister, 8 november 2016.

Lijst met geraadpleegde organisaties

Experts van de volgende organisaties zijn geïnterviewd ten behoeve van dit onderzoek:

- Het Kadaster
- Gemeente Amsterdam
- Ministerie van Financiën
- Houthoff
- AXVECO
- LegalThings
- KNB
- Ministerie van Infrastructuur en Waterstaat, Inspectie Leefomgeving en Transport
- TNO/Brightland campus
- CAK

Begeleidingscommissie

De leden van de begeleidingscommissie voor dit onderzoek:

- Mireille Hildebrandt (voorzitster)
- Sander Mul
- Michael Veale
- Joost Linnemann
- Oskar Deventer
- Frank Willemsen

Over de auteurs

Betrokken onderzoekers vanuit het departement TILT

Maurice Schellekens
Dr. Maurice Schellekens is a senior researcher at the Tilburg Institute for Law, Technology, and Society (TILT). Maurice has ample experience with research about law and technology, in particular with questions relating to liability, intellectual property, robotics and innovation. Maurice publishes regularly about liability of internet providers and he wrote his PhD thesis about the topic. He is chief editor of DomJur the largest Dutch database about domain name caselaw and caselaw in the field of online intermediary liability in the Netherlands. Maurice lectures in the field internet and liability and intellectual property. Maurice has many publications in the field of law and technology.

Betrokken onderzoekers vanuit het departement Private Law

Eric Tjong Tjin Tai
Prof. Eric Tjong Tjin Tai is hoogleraar privaatrecht aan Tilburg Law School. Daarvoor was hij advocaat, gespecialiseerd in cassatie en ICT-recht. Zijn publicaties bestrijken het aansprakelijkheidsrecht, overeenkomstenrecht en burgerlijk procesrecht, naast ICT en privaatrecht. De laatste jaren heeft hij met name veel gepubliceerd over diverse ontwikkelingen op het gebied van digitalisering en privaatrecht, in het bijzonder over blockchain en smart contracts. Hij verzorgt een cursus over blockchain en smart contracts bij de Academie voor Wetgeving. Eric heeft deelgenomen (deels als projectleider) aan diverse onderzoeken, zoals Duties of care and diligence against cybercrime, in opdracht NCTV (2015), Rapport over gebruik van onderzoeksinformatie van de Onderzoeksraad in juridische procedures, in opdracht van Onderzoeksraad voor Veiligheid (2014).

Femke Schemkes
Mr Femke Schemkes is docente privaatrecht aan Tilburg Law School. Zij heeft de masterstudies Law and Technology en Rechtsgeleerdheid beide met het judicium ‘met genoegen’ aan Tilburg University behaald. Haar masterscriptie voor de master Law and Technology zag toe op een onderzoek naar de mogelijkheid tot een geharmoniseerde regeling voor indirecte auteursrechtinbreuken in de Europese Unie (gewaardeerd met een 8). Voor haar masterscriptie voor de master Rechtsgeleerdheid onderzocht zij de privaatrechtelijke remedies bij het oneigenlijk gebruik van persoonsgegevens, met het oog op de Algemene Verordening Gegevensbescherming (gewaardeerd met een 7,5). Daarnaast heeft zij tijdens haar studie stage gelopen bij gespecialiseerde IE/ICT-recht kantoren, BRight Advocaten te Breda en AKD Advocaten en Notarissen, sectie IP/IT. Hierbij deed zij o.a. literatuur- en jurisprudentie onderzoek naar het intellectueel eigendoms- en gegevensbeschermingsrecht, vaak met betrekking tot het privaatrecht.

Betrokken onderzoeker vanuit Tilburg School of Governance

Wesley Kaufmann
Dr. Wesley Kaufmann is universitair hoofddocent aan de Tilburg School of Governance. Kaufmann doet onderzoek naar zowel de objectieve als perceptuele kant van de effectiviteit van regelgeving. In zijn onderzoek gebruikt hij verscheidene onderzoeksmethoden, te weten experimenten, vragenlijsten, regeltellingen en interviews. Kaufmann heeft in het verleden veelvuldig onderzoek gedaan in opdracht van de Ministeries van Financiën en Economische Zaken in het kader van de naleving van de Nederlandse Corporate Governance Code. Recentelijk heeft hij meegewerkt aan een onderzoek in opdracht van het Ministerie van Binnenlandse Zaken over de economische en sociale betekenis van bestuurlijke instituties. Kaufmann heeft gepubliceerd in toonaangevende internationale bestuurskunde tijdschriften zoals Public Administration, Public Management Review

en International Public Management Journal. Hij is als research fellow verbonden aan de Arizona State University.