Smart contracts

als specifieke toepassing van de blockchain-technologie

Eerste verkenning naar vragen rond wet- en regelgeving en opleidingsbehoeften als gevolg van blockchain en meer specifiek smart contracts

Smart Contract Werkgroep – Dutch Blockchain Coalition

Dutch Blockchain Coalition
connect and create

www.dutchblockchaincoalition.org


Dutch
Blockchain
Coalition
connect and create

Smart contracts als specifieke toepassing van de blockchain-technologie

Eerste verkenning naar vragen rond wet- en regelgeving en opleidingsbehoeften als gevolg van blockchain en meer specifiek smart contracts.

Smart Contract Werkgroep – Dutch Blockchain Coalition
Ir. Olivier Rikken MBA
Mr. Sandra van Heukelom - Verhage
Mr. Sander Mul
Drs. Jacob Boersma
Mr. Inger Bijloo
Dhr. Pascal Van Hecke
Mr. Arne Rutjes
Mr. Femke Stroucken
Mr. Joost Linnemann
Ir. Hidde Terpoorten
Ir. Robert Reinder Nederhoed

Samenvatting

In de loop van 2016 werd duidelijk dat de behoefte aan kennis van blockchain toenam. Met het oog op een inventarisatie van de benodigde kennis is in juni 2016 de blockchain expert groep van de Dutch Digital Delta van start gegaan. Vanuit dit initiatief is een verdiepingsgroep samengesteld met de naam Smart Contract/ Legal Programming werkgroep. Deze werkgroep had tot doel de volgende vragen te beantwoorden:

1. **Stel vast welke vragen (en eventueel hiaten) kunnen bestaan ten aanzien van wet- en regelgeving die het onderwerp van smart contracts raakt.**
2. **Stel vast welke kennis in de toekomst nodig is en identificeer wie of welke instantie op welke termijn een invulling zou kunnen geven aan deze kennisbehoeftes.**

Uit de verschillende werkgroepbijeenkomsten en de onderzochte literatuur kwam naar voren dat, alvorens er een eenduidig antwoord kon worden gegeven op de hoofdvragen, eerst moest worden bepaald wat smart contracts precies zijn. Daarbij staat voorop dat het bij smart contracts - als gevolg van hun natuurlijke verschijningsvormen als computercode - voornamelijk om de operationele semantiek c.q. de operationele afspraken draait, en niet zozeer om de denotatie semantiek (bv onder welk recht, onderhevig aan algemene voorwaarden etc). Vastgesteld is dat smart contracts slechts in specifieke gevallen een *juridische* verschijningsvorm kennen. Welk recht (dan) van toepassing is, hangt af van de aard van die juridische verschijningsvorm.

Uiteindelijk is de werkgroep tot de volgende bevindingen gekomen:

1. Een blockchain smart contract is in de eerste plaats een deterministisch computerprogramma dat op een blockchain wordt gerepliceerd en uitgevoerd.
2. Een smart contact kan juridische betekenis hebben, maar dat hoeft niet.
3. Een smart contract kan in verschillende juridische domeinen worden ingezet (privaatrecht, bestuursrecht, strafrecht) en dus verschillende verschijningsvormen kennen.
4. Niet elke juridische verschijningsvorm (wettelijke bepaling, verbintenis etc.) leent zich voor omzetting naar code.
5. Waar omzetting naar code wel mogelijk is, wordt aanbevolen om dit alleen te doen ter uitvoering van de kenbare verschijningsvorm. In het bestuurs- en het strafrecht lijkt dit - waar rechten en plichten worden vastgesteld - uit het oogpunt van rechtszekerheid hoe dan ook de aangewezen weg, maar ook in het privaatrecht kan dit vereist zijn, bijvoorbeeld ter bescherming van de consument.
6. Wanneer het bij een privaatrechtelijke verschijningsvorm wel de bedoeling van partijen is om met de code een verbintenis te scheppen en wellicht ook de uitkomst daarvan bij voorbaat te aanvaarden, zou deze bedoeling ten minste schriftelijk (lees: niet in code, maar bijvoorbeeld in een overeenkomst) moeten worden vastgelegd. Ook dit zou via de blockchain kunnen.
7. Steeds moet vooraf worden nagedacht over de feitelijke en juridische mogelijkheden om (a) de automatische executie van het contract aan daaraan voorafgaande voorwaarden te verbinden (bijvoorbeeld toestemming van partijen of een derde) en (b) de (gevolgen van de) executie achteraf 'ongedaan te maken'

(herstel in de oude toestand, waardevergoeding, schadevergoeding etc.). Daarbij moet ook aandacht worden besteed aan het toepasselijke recht en de bevoegde instantie (mediator, arbiter, rechter etc.) in geval van een geschil.

8. Het is van belang steeds onderscheid te maken tussen *permissioned* en *permissionless* blockchain, omdat deze een ander governance model kunnen kennen. Een permissioned blockchain kan worden afgeschermd met een zogenaamde *access control layer*. Anders dan bij een permissionless blockchain kan niet iedereen deelnemen. Hiervoor is voorafgaande goedkeuring vereist. Bovendien kunnen lees- en schrijfrechten verschillen per gebruiker, waardoor ook taken en verantwoordelijkheden kunnen worden verdeeld. Achter een permissioned blockchain zit kortom een organisatie, veelal een samenwerkingsverband.
9. In smart contracts kunnen persoonsgegevens worden verwerkt. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een levend natuurlijk persoon. Burgers hebben (op grond van de Wbp en de AVG) recht op bescherming van hun persoonsgegevens. In geval van een permissioned blockchain kan worden geregeld wie verantwoordelijk is voor de naleving van de eisen in de Wbp. Dat ligt ander bij een permissionless blockchain. Daar voert niemand én iedereen de regie en zijn dat soort afspraken, als gevolg van de vrije toetredingsmogelijkheid en de gebrek aan regie op de governance, veel lastiger te maken. De mogelijkheid van het beschermen van de privacy in dergelijke situaties zal nader moeten worden onderzocht.

Ten aanzien van de kennisbehoefte zijn er drie hoofdpijlers met elk twee subpijlers geïdentificeerd. De drie hoofdpijlers waarin kennisopbouw gedaan zal moeten worden zijn:

1. Blockchain kennis, met als subgroepen:
    a. algemene (technische) blockchain kennis
    b. kennis van nieuwe bedrijfs- en industrie modellen als gevolg van blockchain en smart contract implementaties
    c. hoe om te gaan met governance.
2. Software & IT kennis, met als subgroepen:
    a. programmeertalen, zowel van bestaande als nieuwe opkomende talen zoals “Solidity”
    b. front end to back end interactie en integratie, doelend op de verschillende vertaalslagen die gemaakt zullen worden bij implementaties en de integratie in huidige modellen en systemen.
3. Legal & Risk, met als subgroepen:
    a. legal, zowel algemeen blockchain gerelateerde rechtsvraagstukken als bijvoorbeeld jurisdictie en privacy als specialisaties in verschillende rechtsgebieden en risk & governance
    b. hoe een goede governance en risk management structuur in te bouwen in smart contracts en blockchain omgevingen.

Er zal een behoefte zijn in twee richtingen in de geïdentificeerde pijlers en sub pijlers. Aan de ene kant in specialisaties in de verschillende geïdentificeerde subgebieden. Aan de andere kant zal een sterk groeiende behoefte naar cross kennis van deze kennisgebieden resulteren in multidisciplinaire personen waarbij er nog steeds wel sprake kan zijn van een specialisatie in een hoofd- of subpijlers, maar ook een gedegen kennis van (een van) de andere pijlers.

Naar aanleiding van deze eerste verkenning zijn de volgende aanbevelingen voor vervolgstappen gedefinieerd:

1. Een preciezere verkenning naar de juridische vraagstukken die rijzen als gevolg van het gebruik van smart contracts.
2. Ten aanzien van de beschreven kennisbehoefte (sub)pijlers dient er met de geïdentificeerde instanties gekeken te worden in welke behoefte al voorzien kan worden en in welke pijlers er nieuwe modules aangeboden dienen te worden.
3. Daarbij dient er naast eventuele diepte-uitbouw per pijler ook gewerkt worden aan een cross-pijler kennisopbouw aan multidisciplinaire kennis.
4. Het aanwijzen van een duidelijk centraal aanspreekpunt voor zowel de verdere ontwikkeling van wet- en regelgeving als monitoring en ontwikkeling in het voorzien van kennisbehoefte;
5. Onderzoek naar de mogelijkheden voor standaardisatie van smart contracts ten aanzien van drie zaken te weten: pattern design, ontologie en standaardisatie van individuele data elementen.

Leeswijzer

Dit rapport is opgesteld voor zowel de algemeen geïnteresseerde lezer, als voor personen met een technische achtergrond en personen met een juridische achtergrond. Daar blockchain en meer specifiek smart contracts overlap vertonen van twee werelden die voorheen veelal gescheiden waren en uit de werkgroepsessie duidelijk naar voren kwam dat een eenduidige vocabulaire zeer gewenst is, hebben wij deze leeswijzer toegevoegd. Ter verduidelijking, als er gerefereerd wordt naar smart contracts in dit rapport wordt er, tenzij anders aangegeven, bedoeld smart contracts op een blockchain.

Voor eenieder is het raadzaam om het hoofdstuk rond **begripsvorming en duiding** te lezen aangezien in de praktijk bleek dat hier de meeste verwarring ontstond. Met name het stuk rond *smart contracts wordt ten zeerste aangeraden*, ook in het geval uw voorkennis ten aanzien van blockchain al goed is.

Voor de lezers met een juridische achtergrond willen wij verder verwijzen naar het stuk met de juridische verdieping, **juridische vragen en hiaten rond smart contracts**. Hierin worden aan de hand van verschillende juridische verschijningsvormen smart contracts verkend en gekeken of dit al dan niet in een smart contract gevat kan worden. In dit hoofdstuk zijn voor de mensen met een meer technische achtergrond en focus met name de aanwijzingen wanneer smart contracts wellicht meer zijn dan code een must om te lezen.

Het hoofdstuk ten aanzien van **kennisbehoefte** is relevant voor lezers met zowel juridische als technische achtergrond, met name om beter te begrijpen welke additionele kennis een persoon zou moeten opdoen om goed met smart contracts om te kunnen gaan.

Inhoudsopgave

Inleiding - achtergrond - doelstellingen

Op 22 juni 2016 kwam op initiatief van de Dutch Digital Delta een blockchain expert-groep bij elkaar bij het Verbond van Verzekeraars onder leiding van Ad Kroft, programmamanager binnen Dutch Digital Delta. Uit dit initiatief is later onder andere de Dutch Blockchain Coalition[1] ontstaan.

Het doel van deze groep is meerledig. Naast het delen van kennis en ervaring en het koppelen van verschillende experts in het vakgebied van blockchain en daaraan gerelateerde onderwerpen, zijn verschillende aandachtsgebieden onderkend waarbinnen vragen dienen te worden beantwoord voordat blockchain in brede(re) zin kan worden ingezet door overheid en bedrijfsleven. Middels de Dutch Blockchain Coalition wil Nederland voorop lopen op het gebied van blockchain.

Tijdens een van de sessies van de Dutch Digital Delta blockchain expert-groep is naar aanleiding van een presentatie van Olivier Rikken op 28 september 2016 een werkgroep (de "Werkgroep") van start gegaan die een inventarisatie is gaan houden ten aanzien van de behoefte op het gebied van kennisontwikkeling en vragen ten aanzien van wet- en regelgeving specifiek rond smart contracts, als één van de belangrijkste producten/diensten [toepassingen] die voortbouwen op blockchain-technologie. De (internationaal) breed gedragen verwachting is immers dat men in praktijk steeds meer in aanraking zal komen met en gebruik zal gaan maken van de blockchain-technologie, in het bijzonder van smart contracts.

Tijdens de eerste bijeenkomst van de Werkgroep is als aanleiding van het starten van die werkgroep opgetekend:

> *"De opkomst van smart contracts middels verschillende blockchains en de vaak daaraan gekoppelde eigenschappen ('irreversibility' in combinatie met daadwerkelijke directe uitbetaling/waardeoverdracht bij een valide trigger van een smart contract zonder dat er nog een tussenkomst van mensen nodig is) en mogelijke nieuwe business modellen, zorgt ervoor dat het juist (juridisch en risico technisch) programmeren van deze contracten essentieel zal worden.*
>
> *Daarom deze verkenning naar kennisbehoeften nu en in de toekomst, als gevolg van smart contracts. Zowel op het gebied van mogelijke kennisbehoefte in de toekomst als mogelijke juridische vraagstukken rond dit onderwerp."*

Blockchain is een zogenaamde 'fundamentele' technologie en daarmee niet gekoppeld aan één enkele of specifieke toepassingen. Vele toepassingen in vele industrieën zijn mogelijk op basis van blockchain-technologie. Blockchain kan dus de *enabler* zijn van nog veel meer producten en diensten. De Werkgroep heeft zich voor deze eerste verkenning en in het onderhavige rapport echter specifiek gericht op smart contracts.

Dit rapport is het eerste resultaat van de Werkgroep-bijeenkomsten en omvat een eerste inventarisatie van de toekomstige kennisbehoefte en vragen ten aanzien van wet- en regelgeving. Daar het een eerste inventarisatie in een zeer volatiel vakgebied betreft, geeft het rapport dus beperkt antwoorden.

[1] https://www.dutchdigitaldelta.nl/blockchain

Doelstellingen en samenstelling van de Werkgroep

De Werkgroep heeft bij aanvang twee verschillende doelstellingen gedefinieerd waar men mee aan de slag is gegaan. Deze doelstellingen zijn ingegeven door praktische problemen waar verschillende bedrijven, proofs of concept en startups tegenaan liepen. Allen gerelateerd rond smart contracts.

Doelstellingen

De eerste doelstelling van de werkgroep is gerelateerd aan (het gebrek aan) zowel technische als juridische kennis rond smart contracts. In de praktijk blijken slechts weinig mensen in staat smart contracts te maken. Bovendien is het begrip *smart contract* nog niet voldoende bekend bij het bredere publiek; het begrip kent (nog) geen eenduidige definitie anders dan technische en conceptuele beschrijvingen wat smart contracts zijn. Dat maakt het voor personen die minder of niet ingelezen zijn in blockchain moeilijker te begrijpen wat een smart contract nu precies is, hoe het tot stand komt en vervolgens werkt.

De eerste doelstelling richt zich op vragen die kunnen ontstaan aan de hand van de wet- en regelgeving die het onderwerp van smart contracts raakt. Immers, er is nog geen specifieke regelgeving ontwikkeld ten aanzien van de blockchain-technologie, laat staan ten aanzien van smart contracts. De eerste doelstelling van de smart contract werkgroep luidt dan ook:

Stel vast welke vragen (en eventueel hiaten) kunnen bestaan ten aanzien van wet- en regelgeving die het onderwerp van smart contracts raakt.

De tweede doelstelling is in lijn met de eerste doelstelling. Deze is echter voornamelijk gericht op een kennisgebied dat dient te worden ontwikkeld. De huidige afgebakende kennisgebieden zoals die van Informatietechnologie (IT) enerzijds en juridische kennis anderzijds zijn vermoedelijk niet afdoende om deze definitie en derhalve duidelijkheid te geven. Een coöperatie tussen deze twee kennisgebieden lijkt geboden. De tweede doelstelling van de smart contract werkgroep luidt dan ook:

Stel vast welke kennis in de toekomst nodig is en identificeer wie of welke instantie op welke termijn een invulling zou kunnen geven aan deze kennisbehoeftes.

Samenstelling en deelnemers aan de werkgroep

Vanaf de eerste bijeenkomst van de Werkgroep is het de intentie geweest zo breed mogelijk vertegenwoordigd te zijn vanuit de volgende sectoren:

1. Overheid
2. Toezichthouders
3. Onderwijsinstellingen
4. Bedrijfsleven

Ook binnen deze sectoren is altijd gestreefd naar een zo'n breed mogelijke vertegenwoordiging. De Werkgroep bestaat derhalve uit: afgevaardigden van 4 universiteiten en hogescholen, 2 toezichthouders, 4 overheden en diverse technische en juridische bedrijven, van startups tot gevestigde grote corporates. Uiteindelijk hebben de volgende partijen bijgedragen aan en input geleverd in de Werkgroep:

1. Overheden
    a. Ministerie Economische Zaken
    b. Ministerie van Veiligheid en Justitie
    c. Ministerie van Financiën
    d. Academie voor Wetgeving

2. Toezichthouders
    a. De Nederlandsche Bank
    b. Autoriteit Financiële Markten

3. Onderwijsinstellingen
    a. Universiteit Tilburg
    b. Universiteit Leiden
    c. Nyenrode Business Universiteit
    d. Jheronimus Academy of Data Sciences
4. Bedrijfsleven
    a. Deloitte
    b. APG
    c. AXVECO
    d. BLandLord
    e. IBM
    f. Unchain
    g. Kennedy van der Laan Advocaten
    h. Pels Rijcken Advocaten
    i. Van Doorne Advocaten
    j. CMS
    k. Token Engineers

De Werkgroep heeft altijd open gestaan voor nieuwe deelnemers. Het stond deelnemers en personen van buiten de Werkgroep ook altijd vrij om nieuwe partijen aan tafel uit te nodigen.

Werkwijze

De Werkgroep is vanaf december 2016 gemiddeld eenmaal per maand bij elkaar gekomen.

Tijdens de eerste bijeenkomst van de Werkgroep zijn de doelstellingen afgestemd, de deelnemerslijst is uitgebreid en de “overige” afspraken voor de Werkgroep zijn gemaakt. Onder meer is afgesproken dat alle discussies en conclusies altijd openbaar en dus voor eenieder toegankelijk moesten zijn. In de daarop volgende bijeenkomst is dieper ingegaan op de technische achtergrond van smart contracts.

Tijdens deze Werkgroep-bijeenkomst bleek dat, wanneer men puur vanuit de theorie blijft redeneren, deze discussie niet verder zou komen dan slechts theorie en hypotheses. De werkgroep heeft het toepassen van de techniek tot uitgangspunt genomen. Die toepassing is geanalyseerd. De werkgroep heeft geen wetenschappelijke analyse gemaakt van de techniek of de dogma's van smart contracts.

Daarom is vanaf de tweede bijeenkomst van de Werkgroep het overleg steeds gestart met praktijkvoorbeelden, zoals live use cases en proofs of concept van diverse partijen om praktische problemen in kaart te brengen en deze binnen de bekende theoretische kaders vanuit verschillende andere rapporten te plaatsen. Daarnaast zijn ook buitenlandse “lessons learned” gebruikt. De volgende praktijk casussen zijn tijdens de bijeenkomsten behandeld:

1. Vastgoed contract toepassingen
    a. BLandLord – crowdownership smart contracts en blockchain toepassing - koopcontracten[2]
    b. Deloitte – Handelsgebouw Rotterdam smart contract en blockchain based huurcontracten[3]
2. Financial services smart contract toepassingen (non banking)
    a. APG – verschillende pensioen smart contract toepassingen[4]
    b. OurSurance – peer2peer verzekeren en verzekeraarsmodel unbundling middels smart contracts[5]

[2] https://www.blandlord.com/

[3] https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/huurcontracten-voor-het-eerst-vastgelegd-in-blockchain.html

[4] https://www.apg.nl/nl/artikel/innovatiefonds-apg/1947

[5] www.oursurance.nl

3. Overheidstoepassingen
    a. Een samenvatting van de verschillende overheids blockchain en smart contract cases[6]
    b. IBM - registreren, verzekeren en volgen van elektrische fietsen[7]

Diverse auteurs hebben bijgedragen aan de totstandkoming van dit rapport. De inhoud van het rapport reflecteert niet noodzakelijk het standpunt van de organisatie waaraan deze auteurs verbonden zijn.

[6] https://www.blockchainpilots.nl/

[7] https://www.linkedin.com/pulse/how-blockchain-helps-reduce-bike-theft-bram-havers

Begripsvorming en duiding

De term *smart contract* is dubbel verwarrend. In de eerste plaats is bij de toepassing van deze technologie juridisch gezien namelijk niet noodzakelijk sprake van een contract. In de tweede plaats valt een smart contract niet per se slim te noemen. In wezen voert een smart contract uit wat het is opgedragen, enig nadenken of pro-activiteit komt er niet bij kijken, alle regels zijn voorgeprogrammeerd. Een smart contract kan technisch gezien wellicht het beste worden gezien als een deterministisch computerprogramma dat wordt gerepliceerd en uitgevoerd op een blockchain en (daardoor) niet per definitie onder controle is van één partij. Hoe een smart contract juridisch wordt geduid hangt helemaal af van de specifieke toepassing.

Een smart contract maakt het bijvoorbeeld mogelijk om online een automatische (al dan niet economische) transactie uit te voeren, zodra het programma vaststelt dat aan bepaalde, vooraf in de code vastgelegde, voorwaarden is voldaan. Hier zou men inderdaad kunnen denken aan een overeenkomst, waarbij het dan weer de vraag is of de code de overeenkomst vormt, of slechts bedoeld is ter uitvoering daarvan (er is dan bijvoorbeeld een schriftelijke overeenkomst of een ander document waaruit de bedoeling van partijen blijkt). Maar ook andere toepassingen zijn heel goed denkbaar. Denk bijvoorbeeld aan schenking, het oormerken van subsidiegelden, het verlenen van een vergunning en toezicht houden. Daarmee komen niet alleen andere privaatrechtelijke rechtshandelingen in beeld (schenking), maar ook bestuursrechtelijke rechtshandelingen (vergunning verlenen) en vormen van bestuursrechtelijk optreden waarbij besluitvorming, toezicht en handhaving als het ware in elkaar opgaan (oormerken van subsidiegelden).

Om de inzet van smart contracts juridisch te kunnen duiden moet men weten wat de werking is van blockchain technologie, smart contracts en oracles. Deze begrippen worden daarom hieronder nader toegelicht.

Blockchain

Blockchain is een verzamelnaam voor technologieën die tot doel hebben om verspreid (op verschillende computers en of servers) opgeslagen gegevens via een netwerk te synchroniseren, zodat deze gelijk blijven. Hierbij wordt gebruik gemaakt van een consensus protocol om de integriteit van de inhoud van de gegevens te garanderen, cryptografie speelt daarbij een grote rol.
De crux van blockchain is dat synchronisatie peer-to-peer plaatsvindt, hetgeen inhoudt dat geen van de computers het voor het zeggen heeft in het netwerk. Hiermee zouden op termijn bepaalde taken van zogenaamde "trusted third parties", zoals bijvoorbeeld een Kadaster, notarissen of een Centrale Bank, anders kunnen worden vormgegeven of wellicht zelfs overbodig worden. Het gaat dan met name om het onweerlegbaar registreren van bepaalde gegevens en het uitvoeren van standaardcontroles.

Elke deelnemende computer zal een voorgestelde mutatie in de set aan gegevens pas aanvaarden nadat deze zelf heeft vastgesteld dat de mutatie volgens vooraf bepaalde regels gebeurt (in het meest voorkomende geval is zo'n regel: "gebeurt de mutatie door de partij waarvan is vastgelegd dat die het recht heeft om die mutatie uit te voeren"). Omdat het systeem peer-to-peer is, en er dus geen "gezaghebbende" partij in het netwerk is, kan het ook gebeuren dat op verschillende plekken in het netwerk mutaties worden uitgevoerd en doorgegeven die elk op zich aan de regels voldoen, maar met elkaar in tegenstrijd zijn (d.w.z. ze resulteren in van elkaar verschillende gegevenssets).
Het in de blockchain software vastgelegde mechanisme dat ervoor zorgt dat het netwerk aan

computers uiteindelijk toch overeenstemming bereikt over de “echte” gegevensset, wordt het consensus protocol genoemd. De precieze invulling van dit protocol kan per blockchain verschillen.

Bitcoin - de eerste blockchain implementatie

Blockchain vindt zijn oorsprong in bitcoin, een zogenaamde cryptocurrency. De ontwerper van bitcoin wilde een systeem realiseren waarbij partijen elkaar online kunnen betalen, zonder de tussenkomst van banken of andere financiële instituties (!). De vraag was dan wel wie bij gebreke van een zogenaamde trusted third party (zie volgende paragraaf) gaat controleren of de betalende partij wel voldoende saldo heeft en of deze niet stiekem probeert dezelfde waarde twee keer uit te geven (double spending probleem). De oplossing was dat het netwerk dit zelf gaat doen: elke deelnemende computer controleert *of* een transactie kan worden uitgevoerd, en is getuige dat het saldo niet twee keer wordt uitgegeven.
En zo werd de blockchain geboren, in wezen een register (men vergelijkt het vaak met een grootboek) waarin de geschiedenis van alle door het netwerk vertrouwde bitcoin transacties worden bijgehouden. Als er in het netwerk een keer een computer uitvalt, is dat geen probleem, er zijn immers nog vele andere computers met een kopie van het register en elke computer kan zelfstandig voorgestelde transacties controleren. Een bijzondere eigenschap van blockchain is dat alle gegevens bewaard blijven en achteraf niet eenzijdig meer kunnen worden gewijzigd, er komen dus in principe alleen gegevens bij.

Blockchain als vervanging van Trusted Third Parties

We zagen net dat dankzij blockchain technologie met bitcoin veilig kan worden betaald zonder dat de tussenkomst van een bank nodig is. Anderen hadden al snel door dat de blockchain in wezen een generieke technologie is, die kan worden gebruikt in alle situaties waarin de behoefte bestaat aan een gegevensset die gezamenlijk wordt bijgehouden en door geen van de partijen eenzijdig kan worden gemanipuleerd. Met blockchain kan, anders gezegd, een *shared single source of truth* worden gerealiseerd tussen twee partijen, zonder dat deze partijen beroep moeten doen op een neutrale vertrouwde derde - in de literatuur doorgaans met de Engelse term trusted third party aangeduid.

In die gegevens kan men uiteraard vastleggen wat men maar wil; naast de eigendom van bitcoins[8], bijvoorbeeld ook de eigendom van een zaak, een bevoegdheid, een diploma, een vergunning of medische gegevens. Ook kan blockchain technologie worden gebruikt om (al dan niet symbolisch) *waarde over te dragen*. Zou bijvoorbeeld een bepaalde zaak (zeg een huis) uniek kunnen worden geïdentificeerd op een blockchain, dan is ook denkbaar dat dit huis via de blockchain van eigenaar wisselt (zie echter het voorbehoud hierna).

Ondertussen moet wel een belangrijk voorbehoud worden gemaakt: de intentie van één of meer partijen om een rechtshandeling via een blockchain toepassing uit te voeren en mogelijk ook in het leven te roepen, maakt nog niet dat

[8] Hoewel het misschien lijkt alsof er munten van eigenaar wisselen, is onder water alleen sprake van afschrijvingen en bijschrijvingen.

juridisch aan alle eisen daarvoor is voldaan. Zo kan de verkoop van een huis via een smart contract technisch en economisch gezien relatief makkelijk gerealiseerd worden, maar zou wel de vraag worden gesteld of hiermee ook een geldige overeenkomst tot stand is gekomen. Verder is (in Nederland) naar huidig recht voor de overdracht van een huis de tussenkomst van een notaris vereist.

De mogelijkheid om zonder de tussenkomst van vertrouwde derden gegevens bij te houden en eventueel ook waarde over te dragen, betekent dat de snelheid van zaken doen omhoog kan, terwijl de kosten kunnen worden verlaagd. Niet alleen transactiekosten, maar bijvoorbeeld ook de kosten van beveiliging, toezicht en handhaving. Het kan daarbij een zichzelf organiserende groep personen/instanties in staat stellen om een eigen set van regels op te stellen voor het doen van transacties en die uit te voeren zonder inzet van een derde partij. Dit verklaart het disruptieve potentieel van toepassingen van blockchain technologie, zeker in combinatie met de toepassing van smart contracts.

Eerder is al aangegeven dat bepaalde taken van Trusted Third Parties op het gebied van administratie en controles mogelijk verdwijnen, d.w.z. anders vorm kunnen worden gegeven. Tegelijkertijd moet niet worden vergeten dat TTP's vaak wel meer zijn dan een veredelde administrateur. Zo kunnen ze een rol spelen bij de bescherming van de betrokken partijen of de rechten van derden. Hiermee kunnen conflicten worden voorkomen en dat is ook in het belang van de overheid.

Permissioned vs Permissionless blockchains

Een zeer belangrijk aspect rond blockchain is het fenomeen permissioned versus permissionless blockchain. Beiden zijn in basis hetzelfde, namelijk data-opslag vindt op een vergelijkbare manier plaats, door middel van het opbouwen van blocks. Het verschil zit hem in deelname en rechten. Dit leidt op zichzelf weer tot hele andere discussies en feiten rond zaken als privacy en governance.

- Een permissionless blockchain is een blockchain waarbij het iedereen volledig vrij staat om er (anoniem) aan deel te nemen. Dit betekent dat iedereen die wil, direct deel kan nemen aan deze blockchain, als gewone gebruiker of als een zogenaamde "full node". Op permissionless blockchains vindt geen identificatie en authenticatie plaats. Deelnemers zijn in die zin dus nagenoeg anoniem al is pseudoniem meer correct. Om transacties te kunnen uitvoeren wordt gewerkt met zogenaamde cryptografische sleutelparen: een openbare (hash van een) *public key* en een geheime *private key*. Alle transacties en alle informatie in de betreffende blockchain zijn openbaar. Iedereen kan ook voorstellen doen voor software updates - maar een upgrade van het netwerk gebeurt alleen maar als (de meerderheid van) de deelnemers vrijwillig de software op hun eigen machines updaten. In een permissionless blockchain is er dus geen enkele partij "de baas" en de chain kent dus ook geen super users of dergelijke constructies. Wanneer software updates door een deel van het netwerk niet worden aanvaard, kan een *network split (ook wel fork)* ontstaan, met twee verschillende

blockchains, die een gemeenschappelijke voorgeschiedenis hebben tot aan het block waar de split zich voordeed. Een permissionless blockchain wordt ook wel public blockchain genoemd. Bitcoin en Ethereum zijn de bekendste permissionless blockchains.
Aan permissionless blockchains kleven issues van duurzaamheid (energieverbruik), kosten (energie, hardware, rekenkracht), verwerkingssnelheid en schaalbaarheid (een blok per 10 minuten bij Bitcoin), en governance (gedistribueerd).

- Een permissioned blockchain wordt afgeschermd met een zogenaamde *access control layer*. Een permissioned blockchain is een blockchain waaraan niet zonder meer iedereen deel kan nemen, maar waarbij toegangsaanvraag/goedkeuring vereist is en waarbij bijvoorbeeld lees- en schrijfrechten kunnen verschillen per gebruiker. In theorie kan het zelfs zijn dat de data slechts op een computer ("node") wordt bewaard en er dus een soort super user gemaakt kan worden. Permissioned blockchains worden ook wel hybride, consortium of private blockchains genoemd, afhankelijk van de hoeveelheid verschillende nodes en soorten gebruikers. Verschillende softwareprojecten om permissioned blockchains te bouwen, werken onder het Hyperledger project van de Linux Foundation (bijvoorbeeld Hyperledger Fabric, oorspronkelijk bijgedragen door IBM, of Hyperledger Burrow, dat verder bouwt op Ethereum).

Er zit een enorm verschil ten aanzien van governance en compliance tussen permissioned en permissionless blockchains. Zo kan ten aanzien van governance in een permissioned blockchains wel degelijk een (groep van) verantwoordelijke(n) worden aangewezen, terwijl in een permissionless blockchain iedereen en dus niemand verantwoordelijk lijkt.[9] In een permissioned blockchain kan bijvoorbeeld door middel van verschillende lees-, en schrijfrechten privacy makkelijker geborgd worden, dit is door de transparantie van een permissionless blockchain lastiger.

Consensus-mechanismen en immutability

Zoals in alle computernetwerken moet ook bij blockchain toepassingen rekening worden gehouden met aanvallen op het netwerk. Zo is denkbaar dat een aantal computers in het netwerk samenspant om de andere computers een onjuist beeld van de waarheid te voor te schotelen. Dit lijkt met name een gevaar op zogenaamde *permissionless* blockchains, waarbij de toetreding vrij is en iedereen ter wereld die beschikt over een computer die is verbonden met internet, anoniem kan meedoen, zowel aan het gebruik van de toepassing (bijv. iemand betalen), als aan het bijhouden en beveiligen van de blockchain in het kader van dat gebruik. Dit houdt in dat in het ontwerp rekening moet worden gehouden met anonieme kwaadwillenden, die zullen proberen het systeem te compromitteren.

Om aanvallen af te weren is bij Bitcoin en veel andere permissionless blockchain momenteel gekozen voor een zogenaamd *proof-of-work* systeem.

[9] Veel permissionless blockchains kennen wel "core development teams" die de grootste bijdrage leveren aan doorontwikkeling van de open source software en de facto een governance rol hebben binnen de community. Voorbeelden zijn het Bitcoin Core team en de Ethereum Foundation. Echter staat het iedereen vrij om aan de software toe te voegen dan wel aan de community deel te nemen.

Dit systeem wijst gemiddeld om de tien minuten[10] een 'willekeurige'[11] computer aan die de andere computers in het netwerk een blok met transacties mag voorstellen.[12] Voor de andere computers is dankzij wiskundig bewijs (cryptografie) eenvoudig vast te stellen dat:

1. Deze computer inderdaad het recht heeft verdiend om het voorstel te doen.
   Bewijs: proof-of-work.
2. De voorgestelde transacties inderdaad bestaan, afkomstig zijn van een partij die die transacties mag uitvoeren, en dat met de inhoud niet is geknoeid.
   Bewijs: digitale handtekening.
3. De voorgestelde transacties volgens de daarvoor geldende regels inderdaad mogen worden uitgevoerd (bijvoorbeeld er is voldoende saldo). Dit betekent dat ook moet kunnen worden aangetoond dat niet is geknoeid met de transactiegeschiedenis.
   Bewijs: blockchain in de vorm van onverbrekelijk met elkaar verbonden Merkle trees.

Een op proof-of-work gebaseerd consensus proces kost (veel) geld, namelijk energie, afschrijvingen op hardware en rekenkracht die ook anders (tegen een hogere opbrengst) benut had kunnen worden. Dat het proces geld kost is natuurlijk geen toeval: door de kosten worden 'spammers' afgeschrikt. Aan de andere kant gaat voor niets de zon op: om het goedwillenden aantrekkelijk te maken om geld uit te geven aan het proces van beheer en beveiliging van de blockchain wordt de computer die een blok met transacties goedgekeurd weet te krijgen, beloond, in het geval van Bitcoin met nieuwe bitcoins (zo ontstaan bitcoins) en met de zogenaamde *transaction fees*. Bij proof-of-work systemen wordt aangenomen dat de transacties beter beveiligd zijn (en dus niet meer terug te draaien) naarmate ze langer staan geregistreerd. In de praktijk wordt een Bitcointransactie na een uur als onwijzigbaar beschouwd.

Het proof of work mechanisme is al veel ouder dan blockchain technologie. Daarmee is het momenteel het meest bewezen mechanisme om consensus in een gedecentraliseerde omgeving te bewerkstellen. Dit is ook de reden dat de meeste permissionless en ook enkele permissioned blockchains dit mechanisme gebruiken. Echter zoals aangegeven kleven er ook meerdere nadelen aan dit mechanisme. Er zijn daarom ook veel andere consensus mechanismen die worden toegepast. Onder de meest voorkomende alternatieven[13] zijn:

1. Proof-of-Stake
2. Proof-of-Capacity
3. (P)BFT
4. PAXOS
5. RAFT

Bij permissionless blockchains ziet men voornamelijk het proof of work en proof of stake mechanisme. Bij permissioned ziet men een grotere verscheidenheid.

Een van de belangrijkste elementen van een blockchain is de zogenaamde immutability. Als iets op een blockchain is geplaatst zou dat niet meer teruggedraaid kunnen worden. Dit dient echter genuanceerd te worden tot: "kan niet *eenzijdig* teruggedraaid worden". Als er algemeen consensus is tussen alle nodes dat iets teruggedraaid dient te worden dan kan dat wel degelijk gebeuren, getuige ook de zogenaamde hardfork van Ethereum in 2016[14].

[10] Bij andere blockchains kan deze gemiddelde tijdspanne verschillen, bijvoorbeeld Ethereum ~15 seconden.

[11] Willekeurig in die zin dat elke computer evenveel kans maakt, afhankelijk van de rekenkracht, wie over meer rekenkracht beschikt (en dus meer geïnvesteerd heeft), maakt natuurlijk wel meer kans.

[12] Zie voor de wijze waarop blokken met transacties worden 'gepubliceerd' bijvoorbeeld: https://blockchain.info/nl

[13] http://www.coindesk.com/short-guide-blockchain-consensus-protocols/

[14] https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/

De uitdaging hierin is echter dat als men dat in een permissionless blockchain wilt doen, alle nodes in het netwerk mee zullen moeten werken om een split in het netwerk te voorkomen. Probleem daarbij is dat niet alle nodes in het netwerk voor iedereen bekend zijn, dus het overtuigen van iedereen in het netwerk is een lastig proces. In een permissioned blockchain zijn alle full nodes, de boekhouders van het netwerk, wel degelijk bekend. Daardoor is het terugdraaien van transacties in een permissioned blockchain waarbij iedereen moet instemmen eenvoudiger dan in een permissionless omgeving.

Tot slot: immutability wil alleen maar zeggen dat zeker is dat een bepaald gegeven ooit in een blockchain was geregistreerd, niet noodzakelijk dat dat gegeven ook klopt. Bijvoorbeeld, als door een menselijke fout in een eigendomsregister van fietsen een verkeerde eigenaar wordt geregistreerd is dat niet meer uit te wissen, maar dat maakt de persoon in kwestie nog niet de juridische eigenaar.In toepassingen waar men gebruik wil maken van een blockchain om real-world assets (zie ook volgende paragraaf) te representeren, zal het dan ook zaak zijn om de toepassing zo te bouwen dat de representatie op de blockchain “in sync” kan worden gebracht met de juridische werkelijkheid (door bijvoorbeeld uitzonderingsprocedures in te bouwen).

Native currencies versus issued assets

De meest bekende toepassing van (permissionless) blockchains bij het brede publiek zijn de zogenaamde cryptocurrencies zoals bitcoin, ether, dash etc. Momenteel zijn er al meer dan 750 blockchains met een eigen currency waarin publiekelijk kan worden gehandeld.[15]
Elk van die currencies is “inherent” of “native” aan de blockchain waarop ze functioneert: de currency is een manier om een kostprijs te verbinden aan transacties - als transacties namelijk gratis waren zou het netwerk worden platgespamd in een permissionless blockchain, zoals al wel eens gebeurd is op een ethereum test netwerk[16]. Het is ook het middel waarmee partijen vergoed worden die het netwerk beveiligen (met proof of work of proof of stake). De currency kan alleen maar bestaan samen met de bijhorende blockchain en de waarde van deze currencies is dus onlosmakelijk verbonden met het nut dat die blockchain aan de gebruiker geeft.
Al snel vond men toepassingen op blockchain die verder gaan dan het verhandelen van de native currency. Met een paar kunstgrepen (technieken als “colored coins” of Omni en Counterparty) kun je in Bitcoin je eigen “muntjes" aanmaken en via de blockchain verhandelen. Andere blockchains zoals Nxt (“assets”) en Ethereum (“tokens”) maken dat nog makkelijker - het aantal populaire crypto-assets loopt in de honderdtallen[17].
Assets kunnen monetaire waarde representeren, bijvoorbeeld een claim op goederen (assets die goud in een kluis vertegenwoordigen zijn populair!), een aandeel, of een ander soort security. In tegenstelling tot de native currency waarvan de waarde intrinsiek aan het functioneren van de onderliggende blockchain verbonden is, hangt de waarde van een asset volledig af van de issuer ervan. Impliciet of expliciet ga je als houder van de asset een overeenkomst aan met de issuer dat je de achterliggende waarde op kunt opeisen.
Assets kunnen echter ook abstracte dingen representeren als lidmaatschap, of het recht om bepaalde software te gebruiken. De issuer is dan vaak niet eens een rechtspersoon, maar een pseudonieme groep developers. Met name in de wereld van Ethereum tokens en smart contracts wordt er geëxperimenteerd met heel nieuwe business modellen en organisatievormen, met name waarbij tokenhouders een soort van virtueel bedrijf vormen (een “Distributed Autonomous Organization”) doordat elke houder gemotiveerd is om de waarde van het token te verhogen.

[15] https://coinmarketcap.com/currencies/views/all/

[16] https://www.coindesk.com/ethereum-spam-attacks-back-time-test-network/

[17] https://coinmarketcap.com/tokens/views/all/

Smart contracts en oracles

Smart contracts zijn toepassingen die op een blockchain geplaatst kunnen worden. In de basis is een smart contract een deterministisch computerprogramma dat wordt gerepliceerd en uitgevoerd op een blockchain. Een computerprogramma is deterministisch als het, gegeven een bepaalde input en bepaalde beginwaarden, altijd dezelfde output zal genereren. De werking is anders gezegd volledig voorspelbaar. Anders dan de naam doet vermoeden wordt met een smart contract niet noodzakelijk een contract of een andere rechtshandeling gecreëerd of uitgevoerd. Met een verzameling van interacterende smart contracts en oracles kan bijvoorbeeld ook een bedrijfsproces in een keten worden bestuurd.

Om te kunnen vaststellen of aan de voorwaarden voor de uitvoering van een smart contract is voldaan, zal veelal data (input) van buiten de blockchain nodig zijn, bijvoorbeeld de bevestiging dat het pakketje is afgeleverd. Een blockchain is "doof en blind": de blockchain software kan geen informatie van buiten ophalen (anders dan wat opgelegd is door het protocol)[18]. Hier komen zogenaamde oracles in beeld. Oracles kunnen inputs leveren aan een smart contract.

Een oracle is een partij (dan wel een technische bron zoals een database, dan wel een persoon die die rol toebedeeld is) die voor een smart contract de rol speelt van "bron van waarheid". De andere partijen die gebruik maken van het smart contract, vertrouwen erop dat het oracle de juiste informatie zal aanleveren voor de executie (van een functie) van het smart contract maar kunnen niet 'on chain' verifiëren dat dit daadwerkelijk de juiste informatie was. Als partijen niet willen varen op één bron, zouden ze zelfs verschillende bronnen kunnen laten "stemmen".
De rol van een oracle doet weer denken aan een "Trusted Third Party". Een oracle kan enkel een informatiebron zijn, en niet betrokken bij de executie van het contract. Verder hoeft een oracle zelfs geen weet te hebben van het verder gebruik van de aangeleverde informatie. Een oracle hoeft geen technische bron zoals een database te zijn, maar achter een oracle zou ook een notaris kunnen zitten, of een mediator wiens handtekening nodig is voor de executie van een (bepaalde functie in) het contract.
Algemeen vertrouwde instituten als b.v. KNMI, Rijkswaterstaat enz zouden digitaal gesignde datafeeds kunnen aanleveren die door oracles in diverse blockchains gebruikt worden om bv verzekeringen automatisch te laten afhandelen, maar zoals eerder aangegeven zou een aangewezen persoon met de juiste bevoegdheid ook deze rol kunnen vervullen (bijvoorbeeld in de vorm van bindend advies).

Als gezegd kunnen smart contracts ook worden gebruikt om (al dan niet symbolisch) waarde over te dragen.Voor zover betaald wordt met cryptocurrencies of assets/tokens, kunnen deze worden 'opgesloten' in een smart contract, totdat is vastgesteld dat aan de voorwaarden voor betaling is voldaan, dan wel een bepaalde termijn is verstreken, waardoor het ingelegde bedrag weer liquide wordt. Tokens kunnen in bepaalde gevallen zelfs voorwaardelijk zijn voor de feitelijke uitoefening van een recht. Denk bijvoorbeeld aan een huurauto die niet start zonder dat men beschikt over een bepaalde virtuele sleutel.

[18] Bij public blockchains is security een belangrijke reden: de software is "gesandboxed" en bv smart contracts hebben geen toegang tot netwerk of harde schijf. Omdat elke node in een verschillende omgeving zit, en dus verschillende dingen "ziet", zou consensus ook onmogelijk zijn.

Juist voor de overdracht van waarde worden smart contracts steeds vaker ingezet, bijvoorbeeld op het zogenaamde Ethereum blockchain. Als men kijkt waaruit een smart contract op het Ethereum blockchain bestaat, heeft het deze drie belangrijkste hoofdelementen:

1. Een balans (waar een variërend bedrag van de cryptocurrency ether op bewaard kan worden).
2. Een mogelijkheid tot (al dan niet overschrijfbare) dataopslag – Hier kunnen statussen in bewaard worden, bijvoorbeeld een pakket is onderweg of afgeleverd, maar hier kunnen ook virtuele tokens en hun hoeveelheid worden bijgehouden waarbij een token bijvoorbeeld een aandeel kan vertegenwoordigen.
3. De contract code – deze code bepaalt, op basis van het bericht wat een smart contract binnen krijgt, al dan niet in combinatie met waardes in de dataopslag, of de data opslag dient te worden aangepast of dat er cryptocurrencies overgemaakt dienen te worden.

Deze smart contracts hebben een adres (zie het als een “rekeningnummer”) en hier kan een bericht of een geldbedrag in cryptocurrencies naartoe gestuurd worden. Smart contracts zijn reactief. Dat houdt in dat ze niets doen totdat ze een bericht (transactie) binnen krijgen. Na ontvangst van de transactie wordt de code geactiveerd en wordt er bepaald door de code of er iets met het bericht moet worden gedaan.

De code van het contract is, als deze eenmaal is vastgelegd op de blockchain, niet meer te veranderen. Ook is de balans of de opslag niet meer te manipuleren, anders dan via een specifiek bericht dat middels een transactie naar het contract kan worden gestuurd. En ook dit kan alleen als de code functies bevat die een verandering toestaan.

De juridische vragen rond blockchain en smart contracts

De conclusie van het vorige hoofdstuk is dat een smart contract in de eerste plaats een deterministisch computerprogramma is dat op een blockchain wordt gerepliceerd en uitgevoerd. In dit hoofdstuk draait het om de juridische vragen rondom smart contracts.

Sommigen beschouwen smart contracts als de revolutie die juristen overbodig maakt. Smart contracts maken het voor partijen immers mogelijk om hun afspraken in onwijzigbare programmacode te gieten, die bovendien - zodra aan de voorwaarden daarvoor is voldaan - geautomatiseerd worden uitgevoerd. Ongetwijfeld biedt dit in bepaalde toepassingen grote voordelen. Echter, de DAO-affaire heeft laten zien dat het ook mis kan gaan: hier ging iemand er vandoor met miljoenen dollars aan ether (het betaalmiddel op Ethereum), omdat zij/hij de fout in de programmacode doorzag en die voor eigen gewin exploiteerde. Dit riep natuurlijk de vraag op wat nu eigenlijk de doorslag geeft: de bedoeling waarmee een smart contract is opgesteld, of de wijze waarop die bedoeling in code is gegoten. Ook riep het de vraag op naar de aansprakelijkheid van de betrokkenen, denk bijvoorbeeld aan de programmeur, aan degene in wiens opdracht de programmeur handelde, of aan het platform dat de smart contract functionaliteit aanbood. Merk hier ook op dat niet op voorhand duidelijk hoeft te zijn naar welk nationaal recht deze vragen moeten worden beantwoord en door welke rechter. Ten slotte riep de affaire de vraag op of en hoe herstel in de oude toestand nog mogelijk is. Uiteindelijk werd het gevolg van de programmeerfout ongedaan gemaakt door een aanpassing van de blockchain software zelf waarbinnen smart contracts worden uitgevoerd.

De term ‘smart contract’ is niet alleen ongelukkig omdat een smart contract niet steeds juridische betekenis heeft, maar ook omdat de term suggereert dat een contract tot stand komt. Zoals we hieronder nader uiteen zullen zetten, kunnen smart contracts in diverse rechtsgebieden een rol spelen en moet ook goed opgelet worden hoe de inzet ervan bedoeld is: als een bron van rechten en plichten of slechts ter uitvoering daarvan. Een relevante vraag in dit verband is ook in hoeverre (de uitvoering van) rechten en plichten nu eigenlijk te vangen is in programmacode. Op deze vraag wordt nu eerst ingegaan. Vervolgens komen diverse privaatrechtelijke en publiekrechtelijke ‘verschijningsvormen’ aan de orde. Het hoofdstuk wordt afgesloten met een aantal algemene juridische vraagstukken en een voorlopige conclusie.

In hoeverre is het recht te vangen in programmacode?

Voordat wordt ingegaan op de juridische verschijningsvormen van smart contract loont het de moeite om de vraag te stellen in hoeverre recht en programmacode nu eigenlijk vergelijkbaar zijn. Aan de oppervlakte lijkt immers ook het recht een algoritme: als dit gebeurt, dan is dat het gevolg, ofwel if (X) then (Y). De beroemde wiskundige Gottfried Leibniz voorzag in de 17e eeuw al een calculus voor het berekenen van juridische rechten en plichten. Hij had dat goed voorzien: grote delen van de uitvoering van wet- en regelgeving worden tegenwoordig ondersteund met informatiesystemen. Maar betekent dat nu ook dat alle wet- en regelgeving en alle contractuele verplichtingen in code zijn te vertalen? Hoewel vermoedelijk heel wat zaken zich lenen voor geautomatiseerde afdoening, kleven aan de idee

'code is law' ook problemen. Deze zijn door de rechtsfilosoof Hart bondig onder woorden gebracht: door ons gebrekkige inzicht in de feiten, hebben we ook een gebrekkig inzicht in de normen. Hart zegt hier dat de werkelijkheid ons altijd kan verrassen. Het gaat dan niet alleen het *onverwachte* (datgene wat niemand nog kon weten), maar ook het *ongedachte* (datgene wat reeds bestond, maar waaraan niet werd gedacht).
Wanneer de werkelijkheid ons verrast, kan ook de norm problematisch worden, zo kunnen wij met Hart constateren. Mogelijk ontbreekt nog een norm, is niet helemaal duidelijk of de norm van toepassing is of lijkt de norm wel van toepassing, maar zal dit leiden tot ongewenste uitkomsten. Hoewel het recht zeker niet oneindig plooibaar is, zijn in de loop van de tijd wel diverse oplossingen gevonden voor het geval dat de werkelijkheid ons verrast. Voorbeelden hiervan zijn: hardheidsclausules, de redelijkheid en de billijkheid, de beginselen van behoorlijk bestuur, de onrechtmatige daad als een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt en niet-limitatieve opsommingen. Maar zelfs zonder deze constructies die specifiek bedoeld zijn om ruimte te scheppen voor het onverwachte of ongedachte, blijft het recht een sociale praktijk, waarbij de betekenis van regels context gebonden is. Denk bijvoorbeeld aan een termijnoverschrijding die de rechter wegens overmacht door de vingers ziet zonder dat enige regel dit toelaat of aan een norm die buiten toepassing blijft omdat die niet het belang beoogt te beschermen van degene de norm inroept. Of nog eenvoudiger: denk aan de parkopzichter die niet eens op het idee zal komen om een boete uit te delen aan een kind met een radiografisch bestuurbare auto, omdat voertuigen in het park verboden zijn. Kortom, de interpretatie van normen wordt geschraagd door de onderliggende sociale praktijken of liever nog: tussen feiten en normen bestaat een circulaire relatie: de feiten bepalen aan welke normen worden gedacht, de normen worden ingekleurd door de feiten,

Maakt het voorgaande de idee van smart contracts hopeloos? Allerminst, het lijkt er eerder op dat de ene school (recht als algoritme) het accent legt op de regelmatigheden in het recht en de andere school op de onregelmatigheden. Zo bezien gaat het dus vooral om de vraag in welke context een algoritme doorgaans bevredigende resultaten zal opleveren en welke veiligheidsventielen worden ingebouwd om menselijke interventie mogelijk te maken, omdat deze reeds was voorzien (open norm, hardheidsclausule etc.), of omdat het resultaat niet kan worden aanvaard (bijvoorbeeld wegens onvoorziene omstandigheden, de bijzonderheden van het geval etc.).

In dit verband zijn oracles interessant, omdat het hiermee mogelijk is een proces te pauzeren, hetgeen ook ruimte schept voor menselijke tussenkomst. Smart contracts die op een rechtmatige manier (zie volgend hoofdstuk voor meer toelichting) de uitvoering van een overeenkomst of regelgeving automatiseren, zullen dan ook in hun ontwerp een rol voorzien voor een menselijke actor die onder voorwaarden en bij wijze van uitzonderingsprocedure de uitvoering van een smart contract kan beïnvloeden of terugdraaien - denk aan rollen als escrowpartij, mediator of rechter in de huidige manier van werken.

Juridische verschijnings-vormen van smart contracts

De crux van een smart contract is dat de inhoud (de code) niet (achteraf) kan worden gemanipuleerd en dat de uitvoering ervan niet kan worden tegenhouden.[19] Zoals gezegd is de term 'smart contract' niet alleen ongelukkig omdat een smart contract niet steeds juridische betekenis heeft, maar ook omdat de term suggereert dat een contract tot stand komt.

Zoals uit de behandeling van diverse verschijningsvormen zal blijken, kunnen smart contracts in diverse rechtsgebieden een rol spelen. Bij de behandeling van deze vormen gaan we uit van Nederlands recht, hoewel dat dit niet altijd van toepassing hoeft te zijn (zie hierover nader onder Algemene juridische vraagstukken: Toepasselijk recht).

De door de werkgroep bestudeerde use cases tonen aan dat smart contracts verschijningsvormen *kunnen* hebben die een juridische handeling vertegenwoordigen (zie hieronder de verschijningsvormen 1-4), of die betekenis kunnen hebben voor de rechtsorde of de rechtsrelatie waarin het smart contract wordt ingezet (zie hieronder de verschijningsvormen 5-7). Is dat het geval, dan zal men zeker moeten weten dat het smart contract zo is geprogrammeerd, dat wordt voldaan aan de wettelijke eisen die gesteld worden aan de juridische handeling waarin het smart contract voorziet, dan wel aan de eisen die gesteld worden aan de rechtsorde of rechtsrelatie waarin partijen zich bevinden. Er zal, met andere woorden, voor moeten worden gezorgd dat het smart contract een rechtmatige situatie vertegenwoordigt en dat de transactie die met het smart contract wordt gegenereerd, rechtmatig is. De vraag kan dan rijzen wie de rechtmatigheid van de situatie kan en mag beoordelen. Onze opvatting is dat als een IT-oplossing wordt overwogen waarbij het scheppen, uitvoeren of naleven van juridische verbintenissen een rol speelt, het noodzakelijk is om reeds in de ontwerpfase aandacht te besteden aan alle relevante juridische vragen, zoals normstelling in code of zuivere uitvoering, hoe wordt omgegaan met zaken die zich niet in code laten gieten, specifieke casus specifieke wettelijke vereisten en meer algemene juridische vraagstukken (aansprakelijkheid, toepasselijk recht, jurisdictie, algemene beginselen, dispute resolution, privacy en digital identity). Het is dus goed om dan een jurist te laten aanhaken.

Meest voorkomende juridische verschijnings-vormen

Ons rechtsstelsel kent tal van juridische handelingen, van meerzijdige privaatrechtelijke rechtshandelingen, zoals contracten, tot eenzijdige privaatrechtelijke rechtshandelingen (zoals schenkingen) en publiekrechtelijke rechtshandelingen. De vraag is of al die verschillende juridische handelingen in een smart contract kunnen worden 'gevangen', of dat de wet aan die juridische rechtshandelingen zodanige 'analoge' eisen stelt, dat die niet kunnen worden vervangen door de code van het smart contract.

[19] Uiteindelijk is natuurlijk alles te manipuleren, maar dat zou op een blockchain wel een enorme inspanning vergen. Niet toegestaan, maar wel kansrijker wellicht is dat men probeert om het signaal dat naar het contract gaat te manipuleren.

We hebben met de Werkgroep de meest voorkomende juridische verschijningsvormen van smart contract geïdentificeerd.

1. Contract en/of executie van een contract
2. Opschortende of ontbindende voorwaarde in een contract
3. Eenzijdige rechtshandeling
4. Publiekrechtelijk besluit
5. Bewijsmiddel/-functie
6. Automatische uitvoering van een (wettelijk) proces
7. Naleving (fiscale) wettelijke verplichting

We sluiten niet uit dat er (veel) meer juridische verschijningsvormen zijn te identificeren. De lijst is daarom niet uitputtend bedoeld, maar dient louter om duiding te geven aan de meest voorkomende juridische handelingen door in een smart contract worden uitgevoerd. We hebben hieronder per juridische verschijningsvorm de wettelijke vereisten in kaart gebracht en beschreven welke uitdagingen er ontstaan als die juridische handelingen in de vorm van een smart contract worden gegoten.

1. Contract en/of executie van een contract

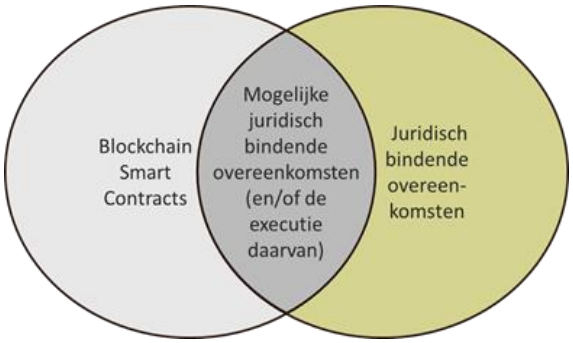
Zaken doen via internet is geen nieuw verschijnsel. Het vernieuwende van smart contracts zit erin dat een computerprogramma bepaalde handelingen automatisch uitvoert, zodra aan de voorwaarden daarvoor is voldaan. In een smart contract kan bijvoorbeeld geprogrammeerd zijn dat een webwinkel automatisch wordt betaald nadat de klant de levering van het bestelde artikel digitaal heeft bevestigd. Om zekerheid te verschaffen over de 'betaling' kan het afgesproken bedrag van tevoren worden 'opgesloten' in het smart contract. Het adres waarop het te betalen bedrag wordt bewaard fungeert dan als een soort derdenrekening, welke wordt beheerd door een computerprogramma. Dit betekent uiteraard wel tijdelijk verlies van liquiditeit.

Een contract is een vorm van een overeenkomst. Volgens het Burgerlijk Wetboek (BW) is sprake van een overeenkomst bij aanbod en aanvaarding. De wijze waarop een overeenkomst tot stand komt is in beginsel vormvrij. Een overeenkomst kan bijvoorbeeld ook mondeling tot stand komen en zelfs impliciet, namelijk door zich op een bepaalde manier te gedragen. Eén van de belangrijkste eisen aan een overeenkomst is uiteraard dat het voor partijen duidelijk is wat er is afgesproken. Het BW eist dan ook dat verbintenissen voldoende bepaalbaar zijn. Smart contracts worden geschreven in een programmeertaal zoals Solidity of Go en bovendien vaak op de blockchain gepubliceerd in een "gecompileerde" vorm welke alleen door computers kan worden gelezen. Dit rechtvaardigt de vraag of een smart contract bepaalbare verbintenissen kan opleveren. Om twijfel hierover uit te sluiten verdient het aanbeveling de verbintenissen te beschrijven op een wijze die voor alle partijen begrijpelijk is. Voordeel hiervan is ook dat dan ook afspraken kunnen worden vastgelegd die zich minder of niet lenen voor automatisering. Een mogelijk nadeel van afspraken in een gewone taal naast code is dat hiertussen licht kan schijnen. Indien en voor zover een smart contract inderdaad bedoeld is als 'zuivere' uitvoering' van elders beschreven verbintenissen, verdient het aanbeveling dit duidelijk vast te leggen.

Voor zover een partij zich beroept op de code, zou het leerstuk van dwaling een rol kunnen spelen, art. 6:228 BW. Uit de redelijkheid en billijkheid vloeit voort dat partijen hun gedrag mede moeten laten bepalen door de gerechtvaardigde belangen van de wederpartij. Wanneer een partij zich beroept op een ingewikkelde code ten opzichte van een ondeskundige partij, en heeft gezwegen over de precieze betekenis van die code, kan er sprake zijn van een schending van de mededelingsplicht. De ondeskundige partij zou de overeenkomst (deels) kunnen vernietigen op basis van dwaling ex. art. 6:228 lid 1 sub b BW, omdat de deskundige partij heeft gezwegen waar zij had behoren te spreken.

Een smart contract is in de eerste plaats een programma op een blockchain. Er zal dus een verzameling zijn van smart contracts waarmee niet

wordt beoogd om een overeenkomst te scheppen. Andersom zal er een verzameling zijn van schriftelijke overeenkomsten die niet met smart contracts te maken hebben. Op de doorsnede van deze twee verzamelingen zit een deelverzameling waarin smart contracts worden ingezet, in ieder geval om een (gedeelte van een) overeenkomst geautomatiseerd uit te voeren. En mogelijk ook om verbintenissen te scheppen.



Denkbaar is dat smart contracts meer en meer worden ingezet in een vorm waarbij de code onlosmakelijk verbonden is aan uitspraken in natuurlijke taal. De natuurlijke taal kan dan dienen om zaken vast te leggen die niet in code zijn uit te drukken (algemene voorwaarden, toepasselijk recht, bewijsovereenkomst, meer open normen etc.) en eventueel ook om de bedoeling van de code toe te lichten. Een hybride contract waarin code (of uitvoerbare datastructuren) en proza samenkomen wordt ook wel een Ricardian contract genoemd. [20]

Eerder is al gezegd dat het wenselijk zou zijn om een standaard (ontologie) te ontwikkelen waarin onafhankelijk van enig platform rechten en plichten worden uitgedrukt. Een voordeel van zo'n standaard zou zijn dat voor iedereen duidelijk is wat met een bepaalde term wordt bedoeld.

Kan een smart contract gelden als een schriftelijke overeenkomst?

De totstandkoming van overeenkomsten is niet altijd vormvrij: soms eist de wet dat een overeen-komst schriftelijk wordt aangegaan. Dat is bijvoorbeeld zo bij een pachtovereenkomst. Ook als de wet een zogenaamde *akte* voorschrijft is een schriftelijke overeenkomst verplicht. In art. 6:227a BW is beschreven onder welke voorwaarden een langs elektronische weg tot stand gekomen overeenkomst kan doorgaan voor een schriftelijke overeenkomst. Het moet dan gaan om een overeenkomst waarvoor de wet niet de tussenkomst voorschrijft van de rechter, een overheidsorgaan of een beroepsbeoefenaar die een publieke taak uitoefent. Een langs elektronische weg tot stand gekomen overeenkomst kan worden gelijkgesteld met een schriftelijke overeenkomst indien:

a. deze raadpleegbaar door partijen is;
b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;
c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld, en;
d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.

[20] http://iang.org/ricardian/

Ad a Raadpleegbaarheid

De eerste voorwaarde is dat de elektronische overeenkomst raadpleegbaar moet zijn door de partijen bij de overeenkomst. Deze dient blijkens de wetsgeschiedenis op zodanige wijze te worden vastgelegd, dat de partijen in staat zijn om de inhoud daarvan t*er latere kennisneming* te ontsluiten en te bewaren. Dit vereiste kan meebrengen dat de partij, die daarbij gebruik wil maken van een bepaalde techniek, gehouden zal zijn om de wederpartij over de juiste technische middelen te doen beschikken om de inhoud van de overeenkomst te kunnen raadplegen, indien deze daarover niet beschikt. Eerder werd al aangegeven dat een contract in gecompileerde vorm alleen leesbaar is voor computers. Is een smart contract raadpleegbaar als de broncode[21] is gepubliceerd? Hier lopen we opnieuw aan tegen het probleem dat vermoedelijk niet alle zaken zich lenen voor omzetting naar code en dat behoefte kan bestaan aan een uitleg van de (beoogde) werking van de broncode. Eerder werd dan ook al aanbevolen om niet alleen met code te werken en de verbintenissen te beschrijven op een wijze die voor alle partijen begrijpelijk is.

Ad b Authenticiteit

Aan de eis van authenticiteit wordt in zoverre gemakkelijk voldaan dat een smart contract niet eenzijdig kan worden gewijzigd. Een wijziging zou bovendien leiden tot een nieuwe hashwaarde (zeg maar een gewijzigde digitale vingerafdruk). Als gezegd is het echter de vraag onder welke omstandigheden een smart contract op zichzelf bepaalbare verbintenissen kan opleveren. Als daarnaast of in aanvulling daarop ook teksten in gewone taal worden gebruikt, mag worden aangenomen dat de eis van authenticiteit zich ook over deze teksten uitstrekt.

Overigens was het niet de bedoeling van de wetgever om op dit punt strengere eisen te stellen dan een papieren overeenkomst. Voor gelijkstelling is niet meer nodig dan dat een gelijke mate van zekerheid bestaat omtrent de authenticiteit. Hetzelfde geldt m.m. voor de het moment van totstandkoming van de overeenkomst en de vaststelling van de identiteit van partijen (beide onderwerpen worden hierna besproken).

Ad c Moment totstandkoming

Aangenomen dat gebruik wordt gemaakt van onbetwistbare automatische datum/tijdstempels, zal het moment van totstandkoming van de overeenkomst, althans het smart contract deel, met voldoende zekerheid kunnen worden vastgesteld.

Ad d Identiteit

Hoewel dat niet steeds praktisch zal zijn, kan een smart contract zo worden gemaakt dat partijen anoniem blijven, in die zin dat partijen alleen bekend zijn onder een nietszeggende public key. Eerder (zie “Permissioned versus permissionless blockchains”) is al uiteengezet waarom dat niet hoeft te betekenen dat de identiteit van een partij niet kan worden achterhaald. Duidelijk is in ieder geval wel dat als een smart contract moet kunnen doorgaan voor een schriftelijke overeenkomst meer informatie nodig is dan een public key: de identiteit van de partijen moet immers met voldoende zekerheid kunnen worden vastgesteld (Zie verder ook hieronder het kopje “Informatieplichten voorafgaand aan de overeenkomst” en de paragraaf “Identiteit en de digitale handtekening”).

Betaling met bitcoin of een andere cryptocurrency: koop of ruil?

Smart contracts gaan vaak uit van betaling in bitcoin of een andere ‘native cryptocurrency’ zoals Ether. Volgens de rechtbank Overijssel is bitcoin geen geld maar een ruilmiddel[22] Deze uitspraak zou

[21] Met “broncode” wordt de code bedoeld in een programmeertaal die door mensen geschreven en gelezen wordt, dit in tegenstelling tot de “gecompileerde” vorm ervan die alleen door computers kan worden gelezen (afhankelijke van de techniek wordt die laatste machinetaal of bytecode genoemd). Alle smart contract code op een blockchain is weliswaar beschikbaar voor alle deelnemers, maar in een gecompileerde vorm. Wel kan worden ontegensprekelijk worden aangetoond dat een bepaald broncode tot een bepaalde gecompileerde vorm leidt, m.a.w. als de broncode beschikbaar is, kan je daaruit de werking van de gecompileerde vorm afleiden.

[22] Rechtbank Overijssel 14 mei 2014, ECLI:NL:RBOVE:2014:2667

kunnen betekenen dat bij betaling in bitcoin geen sprake is van koop, maar van ruil. Art. 7: 49 BW definieert ruil als een overeenkomst waarbij partijen zich verbinden elkaar over en weer een zaak in de plaats van een andere te geven. Bitcoin is geen zaak, want het is geen stoffelijk object. Het lijkt wel een vermogensrecht, want het is op op geld waardeerbaar. In de de literatuur wordt aangenomen dat ook een vermogensrecht geruild kan worden.
Zou inderdaad sprake zijn van ruil, dan vinden volgens art. 7:50 BW (een zogenaamde schakelbepaling) de bepalingen betreffende koop overeenkomstige toepassing, met dien verstande dat elke partij wordt beschouwd als verkoper voor de prestatie die zij verschuldigd is, en als koper voor die welke haar toekomt (schakelbepaling art. 7:50 BW). Ook alle bepalingen omtrent consumentenbescherming die in deze titel staan, zijn dus van toepassing.
Vraag is dan nog wel of bitcoin een vermogensrecht betreft dat juridisch gezien *overdraagbaar* is. Volgens de Nederlandse wetgeving zijn eigendom, beperkte rechten en vorderingsrechten overdraagbaar, tenzij de wet of de aard van het recht zich tegen een overdracht verzet. Andere dan de vernoemde rechten zijn alleen overdraagbaar als de wet dat uitdrukkelijk toelaat. Omdat geen sprake is van eigendom of een beperkt recht, komt het er dus op aan of bitcoin als een vorderingsrecht kan worden beschouwd. Zo niet, dan dan moet mogelijk de wet worden aangepast om bitcoins overdraagbaar te maken. Rank meent dat geen sprake is van een vorderingsrecht, omdat tegenover een vordering een schuld moet staan. En omdat er geen uitgever is van bitcoin is, is er geen debiteur en dus ook geen schuld. Hij komt er dan ook op uit dat de wet zou moeten worden aangepast om bitcoin overdraagbaar te maken.
Een andere benadering kan zijn dat bitcoin wel een vorderingsrecht oplevert, omdat een bitcoin een aantal rechten belichaamt jegens de bitcoin community, welke zich immers aan een aantal (geautomatiseerd afgedwongen) afspraken heeft gecommitteerd.
Zou bitcoin als een vorderingsrecht kunnen worden beschouwd, dan moet levering op de voet van art. 3:94 BW plaatsvinden door middel van een akte. En dat is volgens art. 156 Rv een tot bewijs dienend en *ondertekend geschrift*. Art. 156a Rv opent de mogelijkheid dat een onderhandse akte in elektronische vorm wordt opgemaakt. De blockchain registreert alle goedgekeurde transacties en de bijbehorende digitale handtekeningen. Hierbij moet wel worden aangetekend dat alleen de afzender de cryptocurrency transactie tekent, maar de ontvanger tekende vermoedelijk wel het smart contract waarin de cryptocurrencies werden opgesloten Ook moet worden bedacht dat Bitcoin een permissionless blockchain is die werkt op basis van pseudoniemen. Welbeschouwd bewijst het gedistribueerde grootboek dus niet meer dan dat een zeker aantal bitcoins van de ene naar de andere public key is verhuisd. Zou de wederpartij ontkennen dat de vordering aan hem is overgedragen, dan zal dus extra bewijs nodig zijn om hem/haar aan de public key te linken waarnaar de vordering was overgedragen. Aan de eis van reproduceerbaarheid van de akte lijkt te kunnen worden voldaan: er zijn verschillende programma's in omloop die een *view* op een blockchain kunnen bieden. Bijvoorbeeld *wallet* programma's waarin niet alleen private keys worden opgeslagen, maar waarin ook alle transacties van en naar de door de gebruiker beheerde adressen worden getoond. Van bitcoin gebruikers mag worden aangenomen dat zij hiermee bekend zijn. Al met al zou de toepassing van art. 156a Rv echter wel om enige juridische lenigheid kunnen vragen.

Informatieplichten voorafgaand aan de overeenkomst
Art. 3:15d BW schept verplichtingen voor aanbieders van diensten van de informatiemaatschappij. Onder deze bepaling vallen onder andere het kopen van zaken en het afnemen van diensten op internet, ook al behoeft er voor de diensten niet te worden betaald, mits de diensten worden aangeboden als een economische activiteit.[23] Een dergelijke aanbieder is onder meer verplicht om informatie te verschaffen over zijn identiteit en adres van vestiging.

[23] Kamerstukken II 2001/02, 28197, 3, p. 12/3.

Art. 6:227b BW bouwt hierop verder. Doel van deze bepaling is het vergroten van het vertrouwen in eCommerce, onder meer door te voorkomen dat onbedoeld een overeenkomst tot stand komt, dan wel dat een overeenkomst tot stand komt met een onbedoelde inhoud. Art. 6:227b BW richt zich in het bijzonder op overeenkomsten die via een website tot stand komen, de bepaling geldt niet voor overeenkomsten die via e-mail of een andere geïndividualiseerde vorm van elektronische communicatie tot stand komen. Blijkens het eerste lid van deze bepaling dient een aanbieder van diensten van de informatiemaatschappij de wederpartij - voordat een overeenkomst langs elektronische weg tot stand komt - ten minste op duidelijke, begrijpelijke en ondubbelzinnige wijze informatie te verstrekken over:

a. de wijze waarop de overeenkomst tot stand zal komen en in het bijzonder welke handelingen daarvoor nodig zijn;
b. het al dan niet archiveren van de overeenkomst nadat deze tot stand zal zijn gekomen, alsmede, indien de overeenkomst wordt gearchiveerd, op welke wijze deze voor de wederpartij te raadplegen zal zijn;
c. de wijze waarop de wederpartij van door hem niet gewilde handelingen op de hoogte kan geraken, alsmede de wijze waarop hij deze kan herstellen voordat de overeenkomst tot stand komt;
d. de talen waarin de overeenkomst kan worden gesloten;
e. de gedragscodes waaraan hij zich heeft onderworpen en de wijze waarop deze gedragscodes voor de wederpartij langs elektronische weg te raadplegen zijn.

In het verkeer met een consument (een partijen die niet handelt in de uitoefening van een beroep of bedrijf) gaat het hier om dwingend recht.

Blijkens het tweede lid dient de aanbieder voor of bij het sluiten van de overeenkomst de voorwaarden daarvan, niet zijnde algemene voorwaarden als bedoeld in artikel 231, op zodanige wijze aan de wederpartij ter beschikking te stellen, dat deze door hem kunnen worden opgeslagen zodat deze voor hem toegankelijk zijn ten behoeve van latere kennisneming.

Een overeenkomst die tot stand is gekomen onder invloed van het niet naleven door de dienstverlener van zijn in lid 1, aanhef en onder a, c of d, genoemde verplichtingen, is vernietigbaar. Indien de dienstverlener zijn in lid 1, aanhef en onder a of c genoemde verplichting niet is nagekomen, wordt vermoed dat een overeenkomst onder invloed daarvan tot stand is gekomen.

Gedurende de tijd dat de dienstverlener de informatie, bedoeld in lid 1, onder b en e en lid 2, niet heeft verstrekt, kan de wederpartij de overeenkomst ontbinden.

In het eerste lid van art. 6:230m BW staat opgesomd welke informatieverplichtingen gelden voor een handelaar indien de consument een overeenkomst op afstand of buiten de verkoopruimte aangaat. In deze gevallen is de consument extra kwetsbaar en dient de handelaar de consument op duidelijke en begrijpelijke wijze onder meer de volgende informatie te verstrekken:

1. de voornaamste kenmerken van de zaken of de diensten, in de mate waarin dit gezien de gebruikte drager en de zaken of diensten passend is;
2. de identiteit van de handelaar, zoals zijn handelsnaam;
3. het geografisch adres waar de handelaar gevestigd is en het telefoonnummer, fax en e-mailadres van de handelaar, indien beschikbaar, alsmede, indien van toepassing, het geografische adres en de identiteit van de handelaar voor wiens rekening hij optreedt;
4. de totale prijs van de zaken of diensten, met inbegrip van alle belastingen, of, als door de aard van de zaak of de dienst de prijs redelijkerwijs niet vooraf kan worden berekend, de manier waarop de prijs moet worden berekend, en, in voorkomend

geval, alle extra vracht-, leverings- of portokosten en eventuele andere kosten of, indien deze kosten redelijkerwijs niet vooraf kunnen worden berekend, het feit dat er eventueel dergelijke extra kosten verschuldigd kunnen zijn. In het geval van een overeenkomst voor onbepaalde duur of een overeenkomst die een abonnement inhoudt, omvat de totale prijs de totale kosten per factureringsperiode. Indien voor een dergelijke overeenkomst een vast tarief van toepassing is, omvat de totale prijs ook de totale maandelijkse kosten. Indien de totale kosten niet redelijkerwijze vooraf kunnen worden berekend, wordt de manier waarop de prijs moet worden berekend, medegedeeld;

5. de wijze van betaling, levering, uitvoering, de termijn waarbinnen de handelaar zich verbindt de zaak te leveren of de diensten te verlenen en, voor zover van toepassing, het klachtafhandelingsbeleid van de handelaar;
6. informatie rondom het (bestaan van) een recht tot ontbinding.
7. een herinnering aan het bestaan van de wettelijke waarborg dat de afgeleverde zaak aan de overeenkomst moet beantwoorden;
8. de duur van de overeenkomst, voor zover van toepassing, of, wanneer de overeenkomst voor onbepaalde duur is of stilzwijgend vernieuwd wordt, de voorwaarden voor het opzeggen van de overeenkomst;
9. voor zover van toepassing, het bestaan en de voorwaarden van waarborgsommen of andere financiële garanties die de consument op verzoek van de handelaar moet betalen of bieden;
10. voor zover van toepassing, de functionaliteit van digitale inhoud met inbegrip van toepasselijke technische beveiligingsvoorzieningen;
11. de mogelijkheid van toegang tot buitengerechtelijke klachten- en geschillenbeslechting procedures waarbij de handelaar zich heeft aangesloten, en de wijze waarop daar toegang toe is.

Deze voorschriften illustreren hoe belangrijk het is dat een partij, zeker als dit een consument is, wordt geïnformeerd over wat er precies wordt afgesproken over wat er wordt geleverd en tegen welke prijs, de duur van de overeenkomst, de wijze van opzegging en met wie men zaken doet. Merk ook op dat het bestaan en de voorwaarden van waarborgsommen of andere financiële garanties moet worden gemeld: bij een smart contract wordt vaak een garantie geboden door Bitcoins of een andere cryptocurrency op te sluiten in het contract.

Uitleg van overeenkomsten

Voor zover een overeenkomst tot stand is gekomen, kan de vraag rijzen naar de *uitleg* van die overeenkomst. De crux van een smart contract is dat de inhoud (de code) niet (achteraf) kan worden gemanipuleerd en dat de uitvoe-ring ervan niet kan worden tegenhouden. Wie niet oppast kan dus worden geconfronteerd met voldongen feiten. Dit pleit ervoor reeds in het smart contract voorzieningen op te nemen voor *dispute resolution*. Men zou bijvoorbeeld naast het smart contract ook een smart contract kunnen maken dat de gevolgen van het eerste contract weer ongedaan maakt, bijvoorbeeld na tussenkomst van een vertrouwde derde. De vraag is dan wel wat digitaal is te herstellen en wat een handeling vergt in de fysieke wereld.

Indien na de uitvoering van een smart contract de vraag rijst of de gevolgen wel gewild waren, kan ook het 'klassieke recht' te hulp schieten. In de eerste plaats bevat het BW dwingend recht, dat hoe dan ook geldt. In de tweede plaats bevat het BW regelend recht, dat geldt als partijen daarvan niet afwijken. Ook de redelijkheid en billijkheid spelen een rol bij de uitleg van overeenkomsten, ze kunnen zowel aanvullend werken op wat was afgesproken, als beperkend. Volgens het bekende Haviltex criterium moet bij de uitleg van een contract moet niet alleen naar de letterlijke bewoordingen worden gekeken, maar ook naar de betekenis die partijen in de gegeven

omstandigheden over en weer redelijkerwijs aan deze bepalingen mochten toekennen en op hetgeen zij te dien aanzien redelijkerwijs van elkaar mochten verwachten.

In het voorgaande ging het over de totstandkoming en uitleg van overeenkomsten en over plichten die reeds voor de totstandkoming kunnen bestaan. Overeenkomsten kunnen ook eindigen. In de eerste plaats kan sprake zijn van volledige nakoming, de overeenkomst is dan in beginsel uitgewerkt (er is geleverd en betaald). Denkbaar is ook dat partijen instemmen met ontbinding, dat de overeenkomst eenzijdig wordt opgezegd, dat de overeenkomst wordt ontbonden of dat deze door de rechter wordt vernietigd. Ook kan blijken dat nooit een overeenkomst tot stand is gekomen. Weliswaar kan in het laatste geval niet worden gezegd dat de overeenkomst is geëindigd, maar het kan wel betekenen dat (de gevolgen van) bepaalde acties moeten worden teruggedraaid. Op de voorgaande situaties gaan we nu niet nader in. Maar het mag wel duidelijk zijn dat ook hiermee rekening moet worden gehouden als het smart contract wordt geprogrammeerd.

2. Opschortende of ontbindende voorwaarde

Opschorten betekent kort gezegd uitstellen. Een opschortende voorwaarde is dus een voorwaarde die het intreden van een bepaald rechtsgevolg uitstelt. In geval van een overeenkomst onder opschortende voorwaarde komt de overeenkomst pas tot stand (en krijgt dus rechtskracht en betekenis) wanneer de opschortende voorwaarde wordt vervuld[24]. Wel ontstaat er - voordat de opschortende voorwaarde is ingetreden - tussen de partijen een voorwaardelijke verbintenis. Van belang is dat de opschortende voorwaarde geen zelfstandige betekenis heeft; het wordt in zijn verschijningsvorm pas relevant, als het wordt gekoppeld aan een andere juridische verschijningsvorm, zoals de overeenkomst of eenzijdige rechtshandeling[25].

De opschortende voorwaarde lijkt zich goed te lenen voor het concept smart contract, wat immers in wezen een 'als dit gebeurt – dan gebeurt dat'-toepassing van de blockchain technologie is. Van belang is dat vooraf goed wordt vastgesteld wat de opschortende voorwaarde van de beoogde rechtshandeling precies is, zodat duidelijk is dat en wanneer de verbintenis aanvangt.

Er rijst een aantal vragen bij deze verschijningsvorm. Wat gebeurt er bijvoorbeeld als de opschortende voorwaarde op een andere manier of op een andere grondslag wordt vervuld dan in de code van het smart contract is voorzien? Zo bepaalt de wet bijvoorbeeld dat als een partij die bij de niet-vervulling van de opschortende voorwaarde belang had, de vervulling heeft belet, de voorwaarde toch als vervuld geldt, indien redelijkheid en billijkheid dit verlangen[26]. Of wat gebeurt er wanneer een eenzijdige gerichte rechtshandeling wordt herroepen voordat de opschortende voorwaarde intreedt, aangenomen dat in de "analoge wereld" herroeping mogelijk zou zijn? Van belang is dat dit soort situaties bij aanvang worden geïnventariseerd en dat bij het modelleren van de smart contracts rekening wordt gehouden met die situaties.

Een volgende vraag is, hoe moet worden omgegaan met verjaring. Wanneer de schuldeiser lange tijd geen actie onderneemt om de asset in het smart contract te innen, zal de vordering na een bepaalde termijn verjaren. De verjaring van een vordering houdt feitelijk in dat de vordering na verloop van een bepaalde termijn niet meer in rechte kan worden afgedwongen. Ieder type vordering (voortkomend uit een overeenkomst of anderszins) heeft een eigen verjaringstermijn die op verschillende plaatsen in de wet zijn geregeld. Wanneer men zich rekenschap geeft van die termijn, kan een smart contract een oplossing

[24] Zie bijv. Rb Leeuwarden 28 april 2014, ECLI:NL:RBLEE:2010:BM3063, r.o. 5.2.

[25] Zie bijv. HR 31 mei 2002, ECLI:NL:HR:2002:AE0745, NJ, 2002/470.

[26] Artikel 6:23 BW.

bieden. Men kan de opeisbaarheid van een vordering koppelen, afhankelijk maken van, een opschortende voorwaarde. De vervulling van de opschortende voorwaarde doet dan de verjaringstermijn aanvangen[27].[4]

Ten slotte wordt hier nog genoemd het ontbinden van een overeenkomst onder opschortende voorwaarden voordat de opschortende voorwaarde intreedt. Een overeenkomst onder opschortende voorwaarde kan natuurlijk ook worden ontbonden. De wederpartij van een tekortschietende partij heeft op grond van de wet de bevoegdheid om de overeenkomst te ontbinden, mits de tekortkoming de ontbinding met haar gevolgen rechtvaardigt. Na ontbinding ontstaat voor beide partijen een verbintenis tot ongedaanmaking van de reeds door hen ontvangen prestaties. Als ongedaanmaking onmogelijk is, treedt daarvoor een waardevergoeding in de plaats. We lopen in zo'n situatie tegen de onveranderbaarheid van een smart contract aan. Dit kan mogelijk worden opgelost door de mogelijkheid tot ontbinding (geheel) uit te sluiten of vooraf, bij de codering, rekening te houden met ontbindingsmogelijkheden en de gevolgen daarvan.

De ontbindende voorwaarde is het tegenovergestelde van de opschortende voorwaarde; deze doet de (voorwaardelijke) verbintenis met het plaatsvinden van de gebeurtenis vervallen. Ook de ontbindende voorwaarde doet zich in combinatie met een andere juridische verschijningsvormen voor. De ontbindende voorwaarde lijkt zich minder goed te lenen voor een smart contract dan de opschortende voorwaarde. Immers, bij een smart contract is precies vastgelegd wat er gaat gebeuren indien zich een bepaalde (vooraf vastgelegde) gebeurtenis voordoet, terwijl bij een ontbindende voorwaarde een voorwaardelijke verbintenis ontstaat, waarbij de werking van een zekere rechtshandeling van een toekomstige onzekere gebeurtenis afhankelijk is gesteld[28].[5]

De grootste moeilijkheid van een smart contract in de vorm van een verbintenis onder ontbindende voorwaarden lijkt te zitten in de gevolgen van het intreden van de ontbindende voorwaarde. Immers, het intreden van de ontbindende voorwaarde heeft ontbinding van de verbintenis tot gevolg. Partijen (of betrokkenen) bij de verbintenis dienen te worden teruggebracht in de staat waarin zij verkeerden ten tijde van het aangaan (of ontstaan) van de verbintenis. Eenmaal verrichte prestaties (of andere acties) onder de verbintenis dienen ongedaan te worden gemaakt. Betalingen die bijvoorbeeld hebben plaatsgevonden op basis van een overeenkomst, zullen door ontbinding van de overeenkomst onverschuldigd zijn betaald en moeten worden terugbetaald. Indien mogelijk, dient een en ander zorgvuldig te worden voorzien in de codering van een smart contract.

Net als bij de opschortende voorwaarde, kan ook deze verbintenis worden ontbonden op grond van een andere reden dan de ontbindende voorwaarde. Uitsluiten van de ontbindingsmogelijkheid lijkt dan een oplossing. Hetzelfde geldt voor de situatie waarin de ontbindende voorwaarde – los van daadwerkelijke ontbinding op grond van de wet als hiervoor genoemd – wordt ingevuld op een andere manier dan in het smart contract is voorzien. Ook deze uitdaging is al opgeworpen bij de opschortende voorwaarde.

3. Eenzijdige privaatrechtelijke rechtshandeling

Rechtshandelingen (handelingen gericht op een bepaald rechtsgevolg) kunnen meerzijdig zijn, zoals we hiervoor hebben gezien bij bijvoorbeeld de overeenkomst, maar ze kunnen ook eenzijdig zijn. Het eerste onderscheid dat kan worden gemaakt bij eenzijdige rechtshandelingen is tussen de eenzijdige publiekrechtelijke rechtshandeling en de eenzijdige privaatrechtelijke rechtshandeling.

[27] HR 23 december 2016, ECLI:NL:HR:2016:2988

[28] Art. 6:21 BW.

Hieronder, in onderdeel 4, wordt ingegaan op de publiekrechtelijke rechtshandeling, het publiekrechtelijke besluit.

De eenzijdige privaatrechtelijke rechtshandeling kan vervolgens worden onderscheiden in de gerichte eenzijdige (privaatrechtelijke) rechtshandeling en de ongerichte eenzijdige rechtshandeling. Bij (eenzijdige) gerichte rechtshandelingen moet bijvoorbeeld worden gedacht aan het opzeggen van de huur of het ontslag van een werknemer. Dergelijke rechtshandelingen kenmerken zich hierdoor dat zij tot stand komen door een verklaring die is gericht tot één of meer rechtstreeks of impliciet aangeduide personen, en eerst werking krijgen indien de desbetreffende verklaring die persoon of personen heeft bereikt. Voor de totstandkoming van de (eenzijdige) ongerichte rechtshandeling is geen instemming van een andere persoon, noch de ontvangst door een bepaalde persoon noodzakelijk. Een voorbeeld hier is afstand van een gemeenschap.

Van belang is dat de eenzijdige rechtshandeling meerdere verschijningsvormen kent die op meerdere plaatsen in de wet staan opgenomen. De verschillende verschijningsvormen kunnen een ander (wettelijk) regime kennen. We proberen het ten behoeve van dit onderzoek toch algemeen te houden.

Eenzijdige gerichte privaatrechtelijke rechtshandeling

Aan de gerichte rechtshandeling, zoals opzegging, ontslag of vernietiging (van een rechtshandeling), gaat vrijwel altijd een andere rechtshandeling vooraf.

Gelet hierop ligt het voor de hand om de gerichte rechtshandeling op te nemen in het smart contract van de betreffende andere rechtshandeling. Zo is het denkbaar om in een overeenkomst te beschrijven in welke situatie opzegging of ontslag mogelijk is en aan die situatie (die mogelijk wordt vastgesteld met behulp van oracles) automatisch die gerichte rechtshandeling te verbinden.

Niet onbelangrijk is echter dat er in de rechtspraktijk veelal eerst gezocht wordt naar andere oplossing, hetgeen gelet op de redelijkheid en billijkheid ook soms vereist kan worden. Dat moet mogelijk blijven. De kans is voorts groot dat er bepaalde situaties over het hoofd worden gezien waarin men de gerichte rechtshandeling wel zou willen uitvoeren, terwijl dat niet in het smart contract geregeld is.

Een volgende uitdaging is – los van de ontbindende en opschortende voorwaarde die aan een eenzijdige rechtshandeling kan worden gesteld – de intrekking van zo'n rechtshandeling. Een eenzijdig gerichte rechtshandeling heeft namelijk pas rechtsgevolg wanneer de wilsverklaring degene voor wie het aanbod is bestemd heeft bereikt. Een verklaring die nog niet is ontvangen, kan men nog intrekken[29]. Met deze mogelijkheid zal rekening moeten worden gehouden bij de codering van een eenzijdige rechtshandeling.

Een nóg grotere uitdaging zit in de vernietiging van de eenzijdig gerichte rechtshandeling, aangezien de vernietiging in beginsel terugwerkende kracht heeft tot het moment van het verrichten van de rechtshandeling. Over en weer ontstaan dan verbintenissen tot ongedaanmaking van de reeds verrichte, maar onverschuldigde prestaties. Hiermee zal rekening moeten worden gehouden bij het coderen van een smart contract.

Eenzijdige ongerichte privaatrechtelijke rechtshandeling

In deze categorie kennen we enerzijds het opstellen van een testament. Het gaat het bestek van dit

[29] Intrekking moet worden onderscheiden van herroeping. Intrekking verhindert dat er een aanbod tot stand komt, er is nimmer gebondenheid van de aanbieder geweest. (Alleen relevant voor de situatie dat het aanbod de wederpartij nog niet heeft bereikt.) Herroeping heeft rechtsgevolg wanneer de herroepingsverklaring degene tot wie het aanbod was gericht, heeft bereikt (art 3:37 lid 3). Herroeping is slechts mogelijk zolang het bericht/aanbod niet is aanvaard, maar kan niet meer worden herroepen wanneer de wederpartij de aanvaarding reeds heeft verzonden maar deze verklaring de aanbieder nog niet heeft bereikt (art 6:219 lid 2).

rapport te buiten om alle (zeer complexe) wettelijke bepalingen die op deze verschijningsvorm zien te bespreken. Maar met al deze wettelijke bepalingen zal wel rekening moeten worden gehouden wanneer een testament in een smart contract wordt vastgelegd. Het vermelden waard is in ieder geval dat een erfgenaam een erfenis kan aanvaarden óf verwerpen, welke twee opties op zichzelf ook weer eenzijdige ongerichte rechtshandelingen zijn. Een eenzijdige ongerichte rechtshandeling op een ongerichte eenzijdige rechtshandeling dus. Ook daarmee moet bij de codering rekening worden gehouden.

Anderzijds kennen we de verschijningsvormen van eenzijdige ongerichte rechtshandelingen die voor hun werking niet opgevolgd moeten worden door een andere (rechts)handeling. Naast de voornoemde voorbeelden zijn dat ook: erkenning van een kind, het prijsgeven van bezit en het afgeven van een 403-verklaring in het vennootschapsrecht.
Ook deze vormen kennen verschillende wettelijke regelingen, waar rekening mee moet worden gehouden. Kijken we bijvoorbeeld naar de 403-verklaring[30], dan zien we dat deze verklaring slechts één van de voorwaarden is waaronder een rechtspersoon die behoort tot een groep is vrijgesteld van inrichtingsvereisten van de jaarrekening. Kortom, met alleen die verklaring kom je er niet.

4. Publiekrechtelijk besluit

Publiekrechtelijke besluiten zijn afkomstig van bestuursorganen (zoals colleges van burgemeester en wethouders, ministers en belastinginspecteurs) en worden beheerst door het bestuursrecht. Langzaamaan begint het bestuursrecht steeds meer in te spelen op de mogelijkheden van het digitale tijdperk. Elektronisch verkeer tussen burger en bestuur is in toenemende mate mogelijk en gebruikelijk en zal in de nabije toekomst nog verder worden bevorderd met de Wet modernisering elektronisch bestuurlijk verkeer[31]. Op dit moment kan een bericht van het bestuur dat tot een of meer geadresseerden is gericht elektronisch worden verzonden voor zover de geadresseerde kenbaar heeft gemaakt dat hij langs deze weg voldoende bereikbaar is (art. 2:14, eerste lid, Awb; gedacht kan worden aan het bericht dat een aangevraagde vergunning of subsidie is verleend of geweigerd). Bij aanvragers die een app downloaden en langs deze weg een aanvraag indienen lijkt dit weinig problematisch. Maar bij beschikkingen die niet op aanvraag worden verleend en berichten aan derde-belanghebbenden wel.
Een burger kan op zijn beurt berichten elektronisch naar een bestuursorgaan verzenden voor zover het bestuursorgaan kenbaar heeft gemaakt dat deze weg is geopend. Door een app beschikbaar te stellen zal hier ogenschijnlijk aan voldaan zijn. Een aanvraag kan verder ondertekend worden met een elektronische handtekening als de methode die wordt gebruikt voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt (art. 2:16, eerste lid, Awb). Een tweede grote uitdaging ligt echter in het onderscheid tussen het elektronisch verkeer *mogelijk* maken en het verplichten. In dit geval dus tussen het uitsluitend werken met een app en onderliggend smart contract en tussen óók (als optie voor de burger) werken met een app en onderliggend smart contract. Het bestuur kan namelijk niet *eisen* dat burgers hun berichten

[30] Een schriftelijke verklaring die de consoliderende rechtspersoon deponeert bij het handelsregister van de Kamer van Koophandel, waarin zij verklaart hoofdelijk aansprakelijk te zijn voor de schulden van de vrijgestelde rechtspersonen (dochtervennootschappen).

[31] De Wet modernisering elektronisch bestuurlijk verkeer wijzigt het onderdeel van de Algemene wet bestuursrecht (Awb) dat betrekking heeft op het elektronisch bestuurlijk verkeer. Het wetsvoorstel ligt momenteel voor aan de Afdeling advisering van de Raad van State. Als het voorstel tot wet wordt verheven, dan heeft dit voor bestuursorganen twee concrete gevolgen: 1) een verplichting om digitale kanalen open te stellen voor ieder elektronisch formeel bericht gericht aan het bestuursorgaan; 2) een verplichting om digitale kanalen zodanig aan te passen dat aan de wettelijke eisen wordt voldaan (alleen noodzakelijk gegevens vragen, ontvangstbevestiging sturen, e-formulier beschikbaar stellen, bewijslast bij bestuursorgaan, mededeling bij weigering verkeerd ingezonden bericht).

elektronisch doorgeven of van hen alleen elektronisch kunnen ontvangen[32].

Naast het feit dat bestuursorganen regelmatig met burgers communiceren, nemen ze ook publiekrechtelijke besluiten. Een publiekrechtelijk besluit is een schriftelijke beslissing van een *bestuursorgaan*, inhoudende een publiekrechtelijke rechtshandeling (art. 1:3, eerste lid, Awb). Er zijn twee hoofdcategorieën van besluiten: beschikkingen (besluiten voor een individueel of concreet geval; art. 1:3, tweede lid, Awb) en besluiten van algemene strekking (zoals algemeen verbindende voorschriften, beleidsregels en plannen). Het gaat hier verder over die eerste categorie: beschikkingen.

Een *individuele* beschikking is tot één of meer belanghebbenden gericht (veelal, maar niet altijd tot de aanvrager). Een *concrete* beschikking is niet tot een of meer belanghebbenden gericht (maar een concreet geval of object, zoals een object dat aangewezen wordt als monument). Een beschikking is gericht op het *bindend vaststellen* dan wel op het *scheppen of opheffen* van een rechtsbetrekking (een relatie met een juridische betekenis). Wat betreft dat laatste kan gedacht worden aan: 1) vergunningen, ontheffingen, vrijstellingen en dergelijk, waardoor iets wordt toegestaan wat anders verboden zou zijn; 2) statusverleningen, waardoor op iemand of iets een bepaald rechtsregime van toepassing wordt; 3) subsidietoekenningen en andere prestaties van overheidswege, zoals uitkeringen, leningen, beurzen en garanties; 4) bevelen om iets te doen, te laten of te dulden; 5) goedkeuring, schorsing of vernietiging van een besluit van een decentraal bestuursorgaan door een ander bestuursorgaan.

Een beschikking noemen we *gebonden* voor zover de uitkomst en inhoud wordt bepaald door de wettelijke regeling waarop de beschikking rust; ze is *vrij* voor zover de wettelijke regeling het bestuursorgaan beoordelings- of beleidsvrijheid toekent. De gebonden beschikking leent zich goed voor het concept van smart contracts, omdat er weinig ruimte zit tussen de regel en de toepassing in een concreet geval. Er is helaas zelden sprake van een beschikking met een volledig gebonden karakter; vaak zijn beschikkingen gemengd, dat wil zeggen deels gebonden en deels vrij. Daarin zit mogelijk de grootste uitdaging: naar mate – met name – de beoordelingsvrijheid van het bestuur in individuele gevallen groter is, is de uitkomst van de beoordeling door het bestuursorgaan minder goed te voorspellen. Dat maakt het gebruik van smart contract lastiger.
De vraag rijst hoeveel beoordelingsvrijheid het bestuur – vooraf, los van het individuele geval – mag invullen via een smart contract en hoeveel ruimte er dan is om recht te doen aan de individuele belangen en omstandigheden. In gevallen waarin de uitkomst van de bestuurlijke afweging of beoordeling niet op voorhand te voorspellen is, kan door middel van de inzet van oracles de uitkomst van bestuurlijke oordeelsvorming in het smart contract worden gehaald. Oracles kunnen ook gebruikt worden om (verplichte of wenselijk geachte) oordelen en adviezen van derden binnen te halen. Al dan niet – voor zover verplicht of wenselijk – nadat het bestuur heeft de zorgvuldige totstandkoming heeft gecontroleerd dan wel het advies heeft betrokken in de eigen nadere oordeelsvorming. Verder kunnen via oracles direct gegevens uit eigen en externe datasets, bronnen en registers worden binnengehaald. Voor zover het bestuur wettelijk verplicht is zich hierop te baseren lijkt er geen probleem. Waar zo'n wettelijke plicht ontbreekt en het bovendien een dataset, bron of register betreft dat niet wordt beheerd door het bestuur zelf, stuiten we mogelijk op complicaties. Naast het werken met oracles kan aan eventuele complicaties tegemoet te komen door het besluitvormingsproces op te knippen in delen (bijvoorbeeld vooronderzoek, aanvraagproces, besluitvorming) of door een smart contract enkel te gebruiken voor het stroomlijnen en automatiseren van het interne proces (waarbij bijvoorbeeld

[32] Tenzij dit in een wet is geregeld, zoals met betrekking tot de verplichting voor ondernemingen om digitaal de belastingaangifte in te dienen. Particulieren hebben op grond van de wet de keuze om aangifte te doen op een papieren aangiftebiljet, met behulp van een aangiftediskette, of rechtstreeks via internet.

handmatig input wordt ingevoerd en/of gewerkt wordt met eigen geverifieerde datasets).

Al het handelen van bestuursorganen – waaronder dat in het kader van de besluitvorming – moet uiteraard in overeenstemming zijn met het recht. Daaronder vallen tevens de algemene beginselen van behoorlijk bestuur. Ook in dat kader kan werken met smart contracts zowel uitkomst als uitdaging bieden. Daarop zal hieronder worden stilgestaan bij de meer uitvoeriger behandeling van de algemene beginselen van behoorlijk bestuur.

5. Bewijsmiddel/-functie

Op grond van art. 152 van het Wetboek van Burgerlijke Rechtsvordering (Rv.) kan bewijs geleverd worden door alle middelen tenzij de wet anders bepaalt. Op grond van art. 156 Rv. zijn akten ondertekende geschriften bestemd om tot bewijs te dienen. De wetgever onderscheidt voorts authentieke en onderhandse akten[33].

Met de invoering van de Wet geschrift en elektronisch rechtsverkeer in 2010[34], wordt de elektronische onderhandse akte gelijk gesteld aan een schriftelijke onderhandse akte. Artikel 156a lid 1 Rv bepaalt namelijk dat het mogelijk is om een onderhandse akte op een andere wijze dan bij geschrift op te kunnen maken. Een elektronisch document met een digitale handtekening (eisen die aan een akte worden gesteld) kwalificeert derhalve als een elektronische onderhandse akte. Echter indien er een wettelijke verplichting is tot het verschaffen van een onderhandse akte kan dat alleen op andere wijze dan bij geschrift worden voldaan met uitdrukkelijke instemming van degene aan wie de akte moet worden verschaft (art. 156a lid 2 Rv). Daarnaast zal er op grond van het bepaalde in artikel 6:227a Burgerlijk Wetboek nog voldaan moeten worden aan de in dat artikel opgenomen vereisten:

1. de akte moet raadpleegbaar zijn voor alle partijen;
2. de authenticiteit is voldoende gewaarborgd; hiermee wordt gedoeld op de inhoud van de akte niet is of kan worden gemanipuleerd;
3. het moment van totstandkoming van de akte kan met zekerheid worden vastgesteld;
4. de identiteit van partijen kan met voldoende zekerheid worden vastgesteld.

Wanneer aan bovengenoemde vereisten voldaan is, kan gesteld worden dat in ieder geval voldaan is aan het schriftelijkheidsvereiste en levert de elektronische onderhandse akte, net als de schriftelijke onderhandse akte, dwingende materiële bewijskracht op tussen partijen.[35]

Daarnaast kunnen partijen onderling een bewijsovereenkomst sluiten. Partijen kunnen daarin onder meer af spreken dat er van het wettelijk bewijsrecht wordt afgeweken, wie (in dat geval) wat moet bewijzen en welke bewijskracht aan een elektronisch gegeven toekomt. Afwijking van het wettelijk bewijsrecht kan alleen onder omstandigheden plaatsvinden. Zo wordt een bewijsovereenkomst niet geaccepteerd, wanneer het BW dat bepaalt, alsmede wanneer zij betrekking hebben op het bewijs van feiten waaraan het recht gevolgen verbindt, die niet ter vrije bepaling van partijen staat (art. 153 Rv).

De vraag die nu rijst, is of hetgeen in een blockchain wordt opgenomen of uit een smart contract voortvloeit, aan voornoemde uitgangspunten voldoet en (dus) als dwingend bewijs kan worden aangemerkt, en/of dat partijen kunnen afspreken dat hetgeen in een blockchain is opgenomen en/of uit een smart contract voortvloeit, als dwingend bewijs wordt aanvaard. In zijn algemeenheid kan

[33] Een voorbeeld van een authentieke akte is bijvoorbeeld een notariële akte of een akte van een ambtenaar van de burgerlijke stand. Onderhandse akten zijn akten die niet authentiek zijn.

[34] *Kamerstukken II* 2007-2008, 31 358, nr 3.

[35] Dit geldt enkel ten aanzien van de onderhandse akte, voor het langs elektronische weg verlijden van een notariële akte geldt dat de wet op diverse punten aangepast dient te worden.

worden opgemerkt dat er uit de blockchaintechnologie als zodanig of uit smart contracts belemmeringen voortvloeien die beletten dat aan de wettelijke eisen kan worden voldaan. Vereist is dan dus wel dat de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld, alsmede dat een bewijsovereenkomst de wil van de partijen tot uitdrukking brengt. Ook hier geldt dus dat de grootste uitdagingen bestaan in de wijze waarop de wilsovereenstemming tussen partijen kan worden aangetoond. Bepaald zal moeten worden op welke wijze het voor de andere partij duidelijk is wanneer hij/zij een tot hem of haar gerichte verklaring redelijkerwijs als een op zijn/haar verklaring aansluitende wilsverklaring mocht opvatten.

6. Automatische uitvoering van een (wettelijk) proces

Bij deze verschijningsvorm gaat het om het vervullen c.q. uitvoeren van processen waaraan de wet eisen stelt, met behulp van een smart contract. Vanuit de kant van de overheid kan gedacht worden aan een toezichts- of onderzoekstraject of bijvoorbeeld de procedure voor het opleggen van een bestuurlijke boete (afd. 5.4.2 Awb). Hierbij geldt dat het proces aan bepaalde wettelijke vereisten moet voldoen en er verplicht bepaalde (volgtijdelijke) stappen gezet moeten worden (alvorens tot handhaving mag worden overgegaan, een rapport geopenbaard mag worden, respectievelijk een bestuurlijke boete mag worden opgelegd).
Zoals eerder opgemerkt moet al het handelen van bestuursorganen in overeenstemming zijn met het recht, waaronder de algemene beginselen van behoorlijk bestuur. Dat geldt dus zowel voor feitelijke handelingen als handelen in het kader van besluitvorming. Toezicht en onderzoek zijn domeinen waar met name ook veel feitelijk wordt gehandeld (gegevens worden gevorderd, verzameld en geanalyseerd, locaties worden bezocht, etc.). Afd. 5.2 Awb voegt aan de algemene normen voor bestuurshandelen twee specifieke normen toe voor het optreden door toezichthouders: de legitimatieplicht (art. 5:12 Awb) en de materiële zorgvuldigheidsnorm van art. 5:13 Awb (toezicht mag niet verder gaan dan nodig is).

De grootste uitdagingen zitten hem hier in de wijze waarop de fysieke/analoge werkelijkheid en het smart contract worden samengebracht. Het doorlopen van een wettelijke processtap zal vaak een fysieke procedure blijven. Fysieke processen lijken niet te kunnen worden gecodeerd. Bepaald zal moeten worden op welke wijze en met welke middelen daarvan in een smart contract bewijs wordt geleverd. Het werken met oracles zou hier uitkomst kunnen bieden. Het betrekken van dergelijke feitelijke handelingen in de uitvoering van smart contracts stelt ons wel voor een tweetal uitdagingen:

1) Hoe kan de juistheid van op feitelijk handelen gebaseerde inhoudelijke input in een smart contract worden gewaarborgd? Het smart contract gaat uit van de input, niet van de werkelijke situatie (als die anders blijkt te zijn).
2) Hoe kan worden gewaarborgd dat het feitelijk handelen op juiste wijze is uitgevoerd? Waar dat niet zo is zou dit tot gevolg kunnen hebben dat verzamelde gegevens geheel of gedeeltelijk niet betrokken mogen worden bij het verdere proces.

Vanuit de kant van de burger kan gedacht worden aan meldingen stelsels, die de laatste jaren vergunningstelsels steeds vaker vervangen. Bepaalde handelingen zijn dan niet verboden behoudens vergunning, ze worden in beginsel toegestaan als de gegeven algemene regels in acht worden genomen of als aan de daar gestelde eisen voor toelaatbaarheid wordt voldaan. Tot die regels of vereisten hoort dan de plicht om het voornemen van tevoren te melden. Bij sommige meldingen stelsels kan niet worden volstaan met de melding van het voornemen, maar moeten ook gegevens of documenten worden overgelegd of aangeven worden hoe met bepaalde aandachtspunten rekening gehouden zal worden.

Soms wordt volstaan met de ontvangst van de melding, soms moet op de melding worden gereageerd met ontvangstbevestiging of acceptatie, soms is bepaald dat nadere eisen of maatvoorschriften gesteld kunnen worden of dat de gemelde activiteit om een beperkt aantal redenen verboden kan worden, al of niet binnen een bepaalde termijn. Als een activiteit alsnog verboden wordt of er naar aanleiding van de melding voorschriften of beperkingen aan verbonden worden, dan is er sprake van een publiekrechtelijk besluit. Als de termijn om dit te doen verstrijkt zonder dat het bestuur reageert, dan is er sprake van toestemming-van-rechtswege. In beide situaties is bezwaar en beroep mogelijk en is wat eerder is opgemerkt over publiekrechtelijke besluiten van toepassing.

Onafhankelijk van of de overheid of het bestuur aan zet is, de daadwerkelijke, rechtmatige naleving van de wettelijke vereisten kan worden 'geregistreerd' in een blockchain (waarmee invulling gegeven wordt aan het transparantiebeginsel). Door middel van autorisaties kan daarbij aangetoond worden dat is voldaan aan eisen rondom 'Chinese walls' (met het oog op het verbod van vooringenomenheid) en deskundigheid (met het oog op de toepassing van het formeel zorgvuldigheidsbeginsel)[36]. De volgtijdelijkheid van de wettelijke stappen kan worden geprogrammeerd in een smart contract, bijvoorbeeld door aan te geven dat na een fase van onderzoek een fase van hoor- en wederhoor volgt. Het resultaat of de uitkomst van de verschillende fases kan binnengehaald worden via oracles (die bijvoorbeeld linken aan datasets of waarmee 'handmatig' input verwerkt wordt) en geregistreerd worden in de blockchain waarop het smart contract draait. Als aan het eind van een dergelijk proces een besluit genomen moet worden, dan geldt wat eerder is opgemerkt bij de uiteenzetting over publiekrechtelijke besluiten.

[36] Op de hier genoemde en andere algemene beginselen van behoorlijk bestuur wordt verderop meer uitvoeriger ingegaan.

7. Naleving (fiscale) wettelijke verplichting

De afdracht van belastingen kan naar verwachting bij toepassing van smart contracts grotendeels worden geautomatiseerd.

Zo zou het mogelijk moeten zijn dat automatisch gevolg wordt gegeven aan de fiscale consequenties die partijen (en hun adviseurs) aan een transactie verbinden, dat wil zeggen de afdracht van (bijvoorbeeld) de door hen aldus omschreven verschuldigde btw (en/of overdrachtsbelasting). Bij internationale transacties zou – als voldoende parameters juist zijn ingevuld – waarschijnlijk zelfs kunnen worden vastgesteld in welk land belasting is verschuldigd, over welke grondslag en tegen welk tarief.

Een grote uitdaging vormt de situatie waarin de aard van de transactie bepalend is voor de hoogte van de verschuldigde belasting en die aard niet uit een externe database kan worden afgeleid. In zo'n situatie zullen belastingautoriteiten niet willen vertrouwen op de inschattingen van belastingplichtigen en de bevoegdheid willen houden om naheffingsaanslagen op te leggen. In die situatie kan op basis van de blockchain en het smart contract niet onherroepelijk komen vast te staan welke belasting verschuldigd is.

Laten we Nederlands vastgoed als voorbeeld nemen.

Bij de aan- en verkoop van in Nederland gelegen onroerende zaken kan btw en/of overdrachtsbelasting verschuldigd zijn, afhankelijk van de aard van het vastgoedobject. Op dit moment bestaat er evenwel geen objectieve bron, waaruit blijkt of een dergelijk object bijvoorbeeld kan worden aangemerkt als bouwterrein, "vernieuwbouwd" pand of als woning. Wat betreft dat laatste, geeft de gemeentelijke bestemming (die kan worden geverifieerd via ruimtelijkeplannen.nl) nadrukkelijk slechts een aanwijzing voor de mogelijke kwalificatie als woning. Dergelijke kwalificatiediscussies doen zich

overigens voor bij allerlei typen transacties en bijvoorbeeld combinatielevering van verschillende goederen en/of diensten waarvoor een afwijkend tarief geldt. (Ook) dit kan mogelijk worden opgelost door gebruik te maken van oracles, waarbij de bevoegde instantie (buiten het smart contract om) een oordeel geeft in geval van kwalificatievraagstukken.

Tegelijkertijd is goed denkbaar dat wél te kwalificeren goederen en diensten in een blockchain worden geregistreerd en dat de afdracht van verschuldigde door een smart contract wordt geregeld. Ook dan zal overigens steeds de mogelijkheid van naheffing moeten zijn ingebouwd.

Van belang is dat de er veel verschillende belastingen bestaan, met afzonderlijke wettelijke bepalingen. Gelet op de enorme diversiteit in eisen, zal niet uitputtend worden ingegaan op die eisen. Benadrukt wordt dat de specifieke eisen van de aan de orde zijnde belasting bij de bouw van het smart contract in ogenschouw worden genomen. Daarnaast geldt dat belastingen publiekrechtelijke besluiten zijn, waarvoor de uitgangspunten gelden die hiervoor zijn geschetst. In dergelijke gevallen staat bezwaar open, hetgeen geregeld moet worden.

Algemene juridische vraagstukken

Naast de verschijningsvormen, bestaan er algemene juridische vraagstukken rondom smart contracts. Te denken valt aan aansprakelijkheid, toepasselijk recht, jurisdictie, algemene beginselen, dispute resolution, privacy en identity.

Aansprakelijkheid

De vraag wat aansprakelijkheid precies is, is een vraag die vooral wordt beantwoord vanuit het privaatrecht. Van (wettelijke) aansprakelijkheid spreekt men als sprake is van een onrechtmatige daad of wanprestatie die aan een persoon (of bedrijf) kan worden toegerekend. In dat geval is die persoon aansprakelijk en dient hij/zij de schade die is ontstaan te vergoeden.

Bij wanprestatie ziet de aansprakelijkheid op het vergoeden van schade die ontstaan is als gevolg van niet (of onjuiste) naleving van een contract. Bij onrechtmatige daad is in beginsel geen sprake van een verbintenis, maar wordt “zomaar” schade toegebracht door iemands handelen of een nalaten. Iemand kan aansprakelijk zijn voor een onrechtmatige daad die hij zelf heeft gepleegd (schuldaansprakelijkheid). Gesproken wordt dan over “schuld”. Het kan ook zo zijn dat iemand aansprakelijk is voor de daden van een ander: dan heeft men het over “kwalitatieve” aansprakelijkheid of risicoaansprakelijkheid. Een ouder is bijvoorbeeld aansprakelijk voor schade die zijn kind (jonger dan 14 jaar) heeft veroorzaakt. Een andere (privaatrechtelijke) vorm van aansprakelijkheid is bijvoorbeeld de productaansprakelijkheid of de beroepsaansprakelijkheid.
Hoewel ongetwijfeld meerdere juridische uitdagingen te verzinnen zijn wanneer het aankomt op (privaatrechtelijke) aansprakelijkheid, noemen we er hier een paar die in het oog springen.

De eerste uitdaging zit in het feit dat de blockchain-techniek het mogelijk maakt onder een pseudoniem te handelen. Eerder in dit rapport is al toegelicht dat in de gevallen waarin de wet een schriftelijke overeenkomst eist, een elektronische overeenkomst alleen als schriftelijk kan gelden als de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld. Het is echter nog de vraag of de cryptografische handtekening van een partij die interacteert met een smart contract wel voldoende zekerheid daaromtrent waarborgt. Immers, met die cryptografische handtekening wordt wel gewaarborgd dat deze partij het smart contract kan en mag aanroepen, maar dat wil nog niet zeggen dat ook de identiteit van die partij met zekerheid is vast te stellen (zie daarover ook het onderwerp Digital Identity).

Minstens zo ingewikkeld is de aansprakelijkstelling in geval van een onrechtmatige daad. Bijvoorbeeld wanneer de code van het smart contract wordt gehackt door een onbekende partij. Ook hier geldt: hoe stel je iemand aansprakelijk als je niet weet wie het is?
Hoewel gemakkelijker op te lossen dan het "anonimiteits-probleem" zit de tweede uitdaging van aansprakelijkheid ten aanzien van smart contracts in de vele relaties rond het smart contract en het feit dat nog weinig best practices bestaan. In het hoofdstuk Toepasselijk recht werden genoemd de relatie; (i) van degene die het smart contract laat coderen, (ii) van de programmeur, (iii) in sommige gevallen van degene die input levert op het smart contract, en (iv) in sommige gevallen van de "begunstigde" van de output van het smart contract.

Voorts kunnen wij ons voorstellen dat bij een smart contract ook nog een externe partij betrokken is die fungeert als bijvoorbeeld "bewaarder" van output van een smart contract. Omdat dit echter zó in strijd lijkt met de basisfilosofie van de blockchain-technologie (nl het weghalen van de noodzaak van zogenaamde trusted third parties) laten we dit hier bewust buiten beschouwing.

Wanneer is iemand aansprakelijk ten aanzien van een smart contract? De partijen die een smart contract laten coderen zouden in theorie ten aanzien van elkaar aansprakelijk kunnen zijn in geval van wanprestatie. Maar wanneer is daar sprake van? Immers, vooraf is exact afgesproken wat gebeurt bij een bepaalde input – het is in een code vastgelegd. Zeker wanneer de input (activering) afhankelijk is van een oracle (en niet van een persoon), is het ingewikkeld vast te stellen wanneer sprake is van wanprestatie. Is de input afhankelijk van een natuurlijke (of rechts-)persoon, dan kan men zich nog voorstellen dat de overeengekomen input niet of onjuist wordt geleverd en de uitwerking van het smart contract anders (of niet!) is dan overeengekomen. Dit brengt ons bij het volgende: wanprestatie van een contractspartij geeft de andere partij recht op (i) nakoming met schadevergoeding, (ii) vervangende schadevergoeding, (iii) opschorting van de verplichtingen en (iv) het ontbinden van de overeenkomst. De aan schadevergoeding gerelateerde oplossingen kunnen buiten het smart contract om geregeld worden. Opschorting moet, zo zagen we eerder, mogelijk zijn op basis van de code van het smart contract; is daarmee geen rekening gehouden bij de codering van een smart contract, dan is dat niet mogelijk. Ook bij ontbinding zien we een uitdaging die we al eerder zijn tegen gekomen: partijen (of betrokkenen) bij de verbintenis dienen te worden teruggebracht in de staat waarin zij verkeerden ten tijde van het aangaan (of ontstaan) van de verbintenis. Echter, de uitvoering van een smart contract kan niet worden tegengegaan.

Aansprakelijkheid van een "programmeur" lijkt makkelijker vast te stellen; deze zal handelen op basis van een opdracht. Komt hij de opdracht niet na, of niet volgens hetgeen partijen hebben afgesproken, dan is hij aansprakelijk voor de schade die dientengevolge ontstaat. Ook deze aansprakelijkheid gaat buiten het smart contract om.

Het voorgaande brengt ons ten slotte bij de verzekerbaarheid van aansprakelijkheid in verband met smart contracts. Tegen vele aansprakelijkheidsclaims kun je je doorgaans verzekeren. Maar omdat er nog geen best practices bestaan ten aanzien van smart contracts, is het de vraag of dat hier ook het geval is. Zien verzekeraars heil in het verzekeren van aansprakelijkheidsrisico's in verband met smart contracts en zo ja, onder welke voorwaarden?

Toepasselijk recht

Een belangrijke en veel gestelde vraag is die naar het toepasselijke recht op smart contracts. En met toepasselijk recht wordt hier bedoeld: "het recht van welk land is van toepassing?". Vooropgesteld zij dat vanuit het Nederlandse internationale privaatrecht bezien, deze vraag alleen opkomt indien niet bij voorbaat een rechtskeuze is gemaakt.

Om duidelijkheid te verkrijgen welk recht van toepassing is, dienen altijd een aantal stappen te worden gezet:

1. Van welke juridische verschijningsvorm is sprake?
2. Welke nationaliteiten hebben de betrokken partijen?
3. Door welke (internationale) regelgeving (verdrag, verordening, enz.) wordt de verbintenis tussen de partijen beheerst?
4. Welk nationaal recht wordt door de internationale regels als toepasselijk recht aangewezen in de specifieke casus?

Eerder hebben we al gezien dat een smart contract ten eerste moeilijk te vangen is voor een (juridische) definitie en voorts dat het begrip – zou al sprake zijn van een (overlap met een) juridische verschijningsvorm – niet zonder meer gelijk te stellen is met een overeenkomst (contract!). Dat maakt de vraag welk recht van toepassing is op de rechtsverhouding tussen partijen extra moeilijk, want iedere juridische verschijningsvorm kent zijn eigen regime[37]wanneer het aankomt op die vraag. Vervolgens bestaan met betrekking tot het smart contract meerdere relaties; (i) die van degene die het smart contract laat coderen, (ii) die van de programmeur, (iii) in sommige gevallen die van degene die input levert op het smart contract, en (iv) in sommige gevallen die van de "begunstigde" van de output van het smart contract. In al die verhoudingen kan ander recht van toepassing zijn. Technisch gezien kunnen de verschillende hiervoor benoemde personen ook in één persoon vervat zijn. Als we kijken naar de juridische verschijningsvormen die wij in het onderzoek voor dit rapport hebben geïdentificeerd, dan kunnen we stellen dat bij iedere verschijningsvorm tenminste één persoon met een op een rechtshandeling gerichte wilsuiting is betrokken. Ten slotte is – voor zover we kunnen overzien – een complicerende factor dat alle handelingen ten aanzien van smart contracts in feite worden verricht door of met behulp van nodes. De plaats van de betrokken node(s) en de woonplaats van de met een op een rechtshandeling gerichte wilsuiting betrokken persoon zijn niet vanzelfsprekend hetzelfde.

Jurisdictie – internationaal[38]

Jurisdictie is een ander woord voor rechtsmacht en heeft betrekking op het gebied waarover een overheidsorgaan bevoegd is. Zowel de wetgevende, uitvoerende als rechtsprekende machten hebben hun specifieke jurisdictie. Hier gaan wij alleen in op de rechtsprekende machten; rechters.

Mocht het namelijk tot een geschil komen rondom het smart contract, dan is de vraag die volgt op de vraag naar het toepasselijk recht, die naar de bevoegde rechter. Ook hier geldt[39]: deze vraag komt natuurlijk alleen aan de orde als geen forumkeuze is gemaakt, wat wil zeggen dat vooraf een keuze is gemaakt voor de bevoegde rechter (of ander rechtsprekend orgaan, zoals een arbitrage instituut).

[37] Wet- en regelgeving.

[38] Dit hoofdstuk ziet op de vraag naar de rechter die vanuit internationaal perspectief wordt aangewezen. De vraag welke rechter bevoegd is (absolute bevoegdheid) en hoe moet worden geprocedeerd, wordt hier niet behandeld. Deze vraag kan evenwel ook uitdagingen oproepen.

[39] Uitgaande van het Nederlandse internationale privaatrecht.

Om te komen tot het antwoord op de vraag welke rechter bevoegd is, dienen in principe dezelfde stappen te worden gezet als bij de vraag naar het toepasselijke recht:

1. Van welke juridische verschijningsvorm is sprake?
2. Welke nationaliteiten hebben de betrokken partijen?
3. Door welke (internationale) regelgeving (verdrag, verordening, enz.) wordt de verbintenis tussen de partijen beheerst?
4. Welke rechter wordt door de internationale regels als bevoegde rechter aangewezen om van het geschil kennis te nemen in de specifieke casus?

Een eerste probleem, of uitdaging, bij de vraag naar de bevoegde rechter is – net als bij de vraag naar het toepasselijke recht – dat verschillende juridische verschijningsvormen ten aanzien hiervan een ander regime kunnen kennen. Kijken we bijvoorbeeld naar een verbintenis tussen partijen die ieder woonplaats[40] hebben in een andere lidstaat binnen de EU, dan zal veelal de EEX-verordening[41] van toepassing zijn. Deze verordening is echter alleen van toepassing op burgerlijke - en handelszaken. Bovendien vermeldt artikel 1 van de verordening expliciet dat deze niet van toepassing is op fiscale zaken, douanezaken of administratief-rechtelijke zaken. Helder moet dus zijn (of en) in welke juridische verschijningsvorm het smart contract is gegoten.
Overigens is daarmee de uitdaging nog niet opgelost; in een voorkomend geval kan de uitkomst leiden tot bevoegdheid van meerdere rechters. In dat geval kan worden gekozen bij welke rechtbank men het geschil aanhangig wil maken.

[40] Met woonplaats wordt ten aanzien van een natuurlijk persoon bedoeld: “zijner woonstede” en bij gebreke van woonstede zijn werkelijk verblijf. Ten aanzien van een rechtspersoon wordt bedoeld daar waar hij volgens wettelijk voorschrift of volgens zijn statuten of reglementen zijn zetel heeft.

[41] Verordening (EG) nr. 44/2001 van de Raad van 22 december 2000 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken.

Ook de tweede uitdaging is reeds eerder genoemd: de plaats van de betrokken node(s) en de locatie (of woonplaats) van de bij het smart contract betrokken partijen zijn niet vanzelfsprekend hetzelfde. De vraag is echter in hoeverre dat tot een probleem leidt. Men komt immers pas aan bij de vraag welke rechter bevoegd is van een geschil kennis te nemen als duidelijk is tegen welke (rechts)persoon men een procedure wil starten. Bovendien zal men in dat geval een procedure willen (en tot heden slechts kunnen) starten en maatregelen treffen tegen een (rechts)persoon en niet tegen een node of- breder- een systeem. Soms rijst om die reden de vraag of een systeem *als zodanig* niet aan het rechtsverkeer zou moeten kunnen deelnemen c.q een zelfstandige positie zou moeten hebben. Dat is momenteel wettelijk niet mogelijk c.q. niet het geval.

Algemene beginselen van behoorlijk bestuur

Eerder is al opgemerkt dat al het handelen van bestuursorganen in overeenstemming moet zijn met het recht en dat ‘het recht’ ook de algemene beginselen van behoorlijk bestuur omvat. Als we ons meer specifiek richten op besluitvormingsprocessen, dan onderscheiden we formele en materiële beginselen. De formele beginselen zien op (a) de voorbereiding en (b) de besluitvorming en de inrichting van besluiten. De materiële beginselen betreffen de inhoud van besluiten, die bepalend is voor het rechtsgevolg van het besluit. De algemene beginselen van behoorlijk bestuur zijn deels gecodificeerd in de Awb, deels zijn ze gegrond in ongeschreven recht. In de context van toepassing van de inzet van smart contracts verdienen de onderstaande wat ons betreft in bijzonder aandacht.

Transparantiebeginsel (art. 3:2 Awb (deels)): Transparantie betekent dat belanghebbenden over de informatie kunnen beschikken die zij nodig hebben om te kunnen beoordelen of zij eerlijk worden behandeld en om de juiste keuzes te kunnen maken. Er mag geen bevoordeling of oneerlijke concurrentie optreden. Ook de

besluitvorming moet transparant zijn, zowel wat betreft de procedure als de motivering. Het smart contract, de code, zal dus op enigerlei toegankelijke wijze 'uitgelegd' moeten worden aan de betrokken partijen. Dat geldt in onze optiek overigens voor alle smart contract die een juridische handeling vertegenwoordigen, zie hieronder onder het kopje 'overige aandachtspunten'.

(Formeel) zorgvuldigheidsbeginsel (art. 3:2, afd. 3.3-3.5, 4.1.1 en 4.1.2 Awb): Bij de voorbereiding van een besluit moet een bestuursorgaan de nodige kennis omtrent *de relevante feiten en de af te wegen belangen* vergaren (art. 3:2 Awb). Hoe kan een smart contract dit op individueel niveau bepalen? Moet hier ook weer teruggegrepen worden op het gebruik van oracles? Er rust een onderzoeksplicht op het bestuur, van een belanghebbende burger kan enkel verlangd worden dat deze bepaalde gegevens levert als daar bijzondere reden voor is. Gaat het om een besluit dat wordt genomen op aanvraag, dan zal van die belanghebbende mogen worden verwacht dat hij het bestuur de van belang zijnde gegevens verschaft waarover hij kan beschikken. Als het bestuursorgaan bij de behandeling gegevens mist of twijfelt aan de juistheid, dan moet contact gezocht worden met de aanvrager. Gegevens waaraan het bestuursorgaan gemakkelijker kan komen dan de aanvrager, die zal het zelf moeten vergaren.
Uit de aard van de aanvraag of van het te nemen besluit kan voortvloeien dat het bestuursorgaan advies moet inwinnen of een inspraakprocedure moet organiseren, ook als daartoe geen uitdrukkelijke specifieke wettelijke verplichting bestaat. Indien een besluit berust op een onderzoek naar feiten en gedragingen dat door een adviseur is verricht, dient het bestuursorgaan zich ervan te vergewissen dat dit onderzoek op zorgvuldige wijze heeft plaatsgevonden (art. 3:9 Awb). Mogelijk geldt er analoog een vergelijkbare verplichting voor alle gegevens die uit oracles worden betrokken (dus zowel waar het betreft gebruikte datasets en registers, als waar het betreft 'handmatig' ingevoerde zijnswijzen en bevindingen van derden).

Verdedigingsbeginsel (art. 4:7 en 4:8 Awb (deels)): De hoorplichten in de artikelen 4:7 en 4:8 Awb bieden de belanghebbende de keuze om schriftelijk of mondeling hun zienswijze naar voren brengen. Er zal dus mogelijk een oracle gecreëerd moeten worden om de (gehoorde) zienswijze in het smart contract te verwerken.

Gebod van belangenafweging; specialiteitsbeginsel (art. 3:4, eerste lid, Awb): Alle *relevante rechtstreeks betrokken belangen* moet het bestuursorgaan in de afweging betrekken (voor zover niet uit een wettelijk voorschrift of uit de aard van de uit te oefenen bevoegdheid een beperking voortvloeit). Kan een smart contract zulk onderscheid maken? Is er anders altijd een 'handmatige' controle vanwege het bestuur nodig? Moet ook hier steeds weer teruggegrepen worden op het gebruik van oracles?
M.b.t. de toelaatbaarheid van een gereguleerde handeling, mogen enkel de belangen van de aanvrager én de belangen die de wettelijke regeling wil dienen worden afgewogen. M.b.t. de aan beschikking te verbinden voorschriften moeten ook de belangen van andere belanghebbenden worden afgewogen. De vraag rijst: is dit op voorhand in code te vatten?

Gebod van draagkrachtige en kenbare motivering (art. 3:46-3:48 en 3:50 Awb): Ieder besluit moet berusten op een deugdelijke motivering (art. 3:46 Awb). Als hoofdregel geldt dat deze wordt vermeld bij de bekendmaking van het besluit, met - zo mogelijk - vermelding van de wettelijke basis (art. 3:47, eerste en tweede lid, Awb). De vermelding kan – tenzij er alsnog om wordt verzocht – achterwege blijven als *redelijkerwijs kan worden aangenomen dat daaraan geen behoefte bestaat*[42].[1] Er kan ons inziens niet

[42] In dergelijke gevallen (waarbij iets 'kan, als', gekoppeld aan criterium dat afhankelijk is van een (subjectieve) beoordeling van een individueel geval) lijkt het niet goed mogelijk om dit op voorhand te programmeren in een smart contract. Er zou dan teruggegrepen kunnen worden op het gebruik van oracles. In bepaalde gevallen (waar 'kan, als', maar sowieso altijd *mag*) kan dit

volstaan worden met een motivering dat (bijvoorbeeld) uit het smart contract volgt dat een vergunning wordt verleend of juist geweigerd.

Vertrouwensbeginsel: Vertrouwen dat door bestuursorganen is gewekt en dat heeft geleid tot gerechtvaardigde verwachtingen, mag niet worden beschaamd. Wat betekent dit als er een fout in de code zit? Of een verschil tussen wat uit de code volgt en wat de partijen anderszins is voorgehouden?
Gelijkheidsbeginsel: Gelijke gevallen moeten gelijk worden behandeld; ongelijke gevallen ongelijk naar de mate waarin zij verschillen. Passend en noodzakelijk onderscheid mag worden aangebracht. Kan een smart contract dit onderscheid maken of is wederom de enige uitweg het gebruik van oracles?

Materiële zorgvuldigheid en evenredigheidsbeginsel (art. 3:4, tweede lid, Awb): De uit een besluit voor iemand voortvloeiende lasten mogen niet zwaarder zijn dan strikt noodzakelijk. Ze mogen niet onevenredig zwaar zijn, in verhouding tot de doelen die het besluit wil dienen. Een besluit, genomen ter wille van het algemeen belang, mag niet slechts op één of sommige belanghebbenden zware lasten opleggen. Valt dit allemaal in code te vatten?

Toetsingskader bestuursrechter
De voornoemde beginselen worden, afzonderlijk of in onderlinge samenhang, door de (bestuurs) rechters tot uitgangspunt bij het toetsen van geautomatiseerde besluitvormingsprocessen vervat in smart contracts. In haar uitspraak van 17 mei 2017 heeft de hoogste bestuursrechter - de Afdeling bestuursrechtspraak van de Raad van State[43] - geoordeeld dat in een situatie van een geautomatiseerd besluitvormingsproces een gebrek aan inzicht in de gemaakte keuzes en gebruikte gegevens en aannames ertoe kan leiden dat er een ongelijkwaardige procespositie van partijen kan ontstaan. Dat zal aan de orde zijn, als de burgers niet kunnen controleren op basis waarvan tot een besluit wordt gekomen. De geautomatiseerde besluitvorming op basis van een programma is van hun perspectief dan te beschouwen als een black box. Om dit te voorkomen rust in die gevallen op de overheid de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigener beweging openbaar te maken, zodat deze voor burger toegankelijk zijn. Dit moet bovendien op een passende wijze gebeuren, aldus de Afdeling bestuursrechtspraak van de Raad van State; simpelweg de code van het smart contract publiceren zal dus niet voldaan. Aannemelijk is dat de overheid de code voor de burger in begrijpelijke taal moet kunnen vertalen. Voldoet de overheid hier aan, dan is het voor alle partijen, inclusief de burgers, mogelijk de gemaakte keuze en gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten. Alleen op deze wijze is in de optiek van de bestuursrechter reële rechtsbescherming mogelijk.

Dispute Resolution

Bij onenigheid over het al dan niet juist executeren van een contract of andere juridische overeenkomst heeft men meerdere vormen van dispuut resolutie tot zijn beschikking staan, zoals een uitspraak via een rechter of mediator.

Dit is in het geval van een dispuut tussen partijen die hun juridische overeenkomst in een smart contract hebben staan niet anders, met dien verschil dat smart contracts extra functionaliteit zouden kunnen bieden om de signalering van een dispuut sterk te vereenvoudigen. Bovendien zou, als sprake is van waardeoverdracht via een smart

mogelijk omzeild worden door het simpelweg altijd wel te doen. Zeker als dit via programmering in het smart contract geautomatiseerd kan worden en verder geen uitvoeringslasten met zich meebrengt (mogelijk reduceert het die dan zelfs). Daarnaast kunnen in bepaalde gevallen mogelijkheden worden ingebouwd in de app of de website waarmee aanvragers e.d. (indirect) in aanraking komen met het smart contract (bijvoorbeeld door de mogelijk in te bouwen via het aan- of uitvinken aan te geven of er behoefte is aan een uitgebreide toelichting.

[43] ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o.14.2 ev. Zie al eerder ABRvS 16 september 2015, ECLI:NL:RVS:2015:2938 en ABRvS 7 september 2016, ECLI:NL:RVS:2016:2415

contract, kunnen worden geregeld dat er altijd een garantie tot waardeoverdracht bestaat, dan wel een waarde teruggaaf kan plaatsvinden, omdat een partij niet tussentijds de waarde kan vernietigen. Het smart contract is in die gevallen te vergelijken met een escrow of derdengelden bankrekening, waarbij de waarde kan vrijvallen indien beide partijen via een bericht (een stemmechanisme) doorgeven dat aan de afspraken voor de uiteindelijke waardeoverdracht is voldaan. Als men niet wil voorzien in een dergelijk stemmechanisme - waarbij uitsluitend de opvatting van partijen leiden is, is een alternatief dat de betrokken partijen een oracle aanwijzen aan de hand waarvan wordt bepaald of aan de eisen van de transactie is voldaan. Zo zou men kunnen afspreken dat als de database van een weerdienst aangeeft dat er op een bepaalde plaats op een bepaald tijdstip storm was, men automatisch tot betaling overgaat van bijvoorbeeld een verzekeringsbedrag en niet nog in conclaaf gaat of er wel daadwerkelijk een storm was. Men legt zich dan vooraf, bij het opstellen van het smart contract, neer bij de status van de overeengekomen oracle als weerlegbaar vermoeden, of, als dat is overeengekomen in een bewijsovereenkomst, als bindend bewijs.

Is geen sprake van consensus, dan kan worden voorzien in dispute resolution, bijvoorbeeld door een signaleringsfunctie in te bouwen waarmee partijen hun geschil direct aan een derde kunnen voorleggen. Die derde kan dan bijvoorbeeld mediation, of een bindend oordeel geven. Gedurende de periode waarin het conflict niet is opgelost, kan de waarde dan in het smart contract blijven rusten. Denkbaar is vervolgens dat de geschilbeslechtende instantie, zoals een mediator, maar ook een rechter, de bevoegdheid krijgt om te bepalen naar welke partij de in het smart contract opgenomen waarde (terug)vloeit. Dat heeft wel tot gevolg dat in geval van een langlopend conflict partijen geen toegang hebben tot de waarde op het smart contract.

Van belang is dus dat men het vooraf eens wordt hoe conflicten worden opgelost, wie de rol van mediator of geschiloplosser zal innemen en over diens bevoegdheden. Duidelijke afspraken bij het opstellen van het smart contract zijn dus zeer gewenst.

Privacy

Bij Privacy gaat het om de bescherming van persoonsgegevens. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een levend natuurlijk persoon. Burgers hebben op grond van de Wet bescherming persoonsgegevens (nu) en de Algemene Verordening Gegevensbescherming (per mei 2018) verschillende rechten ten aanzien van hun persoonsgegevens, onder andere het recht op correctie van de persoonsgegevens, op verwijdering en om vergeten te worden (AVG).

In smart contracts kunnen persoonsgegevens worden verwerkt. Er zullen in dat geval als gevolg van de toepasselijke wetgeving allereerst kwalificatievraagstukken rijzen. Zo maakt de wetgeving onderscheid tussen een verantwoordelijke en een verwerker. Er gelden verschillende wettelijke eisen voor de verantwoordelijke en de verwerker. Aannemelijk is bijvoorbeeld dat alle deelnemers aan/gebruikers van een blockchain en smart contract waarbinnen persoonsgegevens worden uitgewisseld *verantwoordelijke* zijn en (zelfstandig) moeten voldoen aan (alle) wettelijke eisen. Minder duidelijk is of de overige partijen die deelnemen aan de blockchain (alle partijen dus die de nodes draaien), ook een bepaalde status op grond van de Wbp vervullen. Wij kunnen ons voorstellen dat die nodes moeten worden aangemerkt als verwerkers van persoonsgegevens. Is dat het geval, dan moeten (ook zij) voldoen aan de uitgangspunten van de Wbp en bijvoorbeeld met de verantwoordelijken verwerkersovereenkomsten sluiten.

Voor het naleven van de eisen op het gebied van privacyrecht is het, net als we hiervoor al een aantal keer hebben gezien, relevant om onderscheid te maken tussen permissionless en permissioned blockchains. In de laatste variant is het goed mogelijk om invloed uit te oefenen op de

governance van de blockchain en (onder meer) te regelen wie verantwoordelijk is voor de naleving van de eisen in de Wbp. Zo kan in die gevallen worden bepaald door wie en op welke wijze rechten van de burger, zoals het correctierecht, worden gewaarborgd. Daarover kunnen bij aanvang van de blockchain afspraken worden gemaakt tussen de deelnemers. Dat ligt ander bij een permissionless blockchain. Daar voert niemand én iedereen de regie en zijn dat soort afspraken, als gevolg van de vrije toetredingsmogelijkheid en de gebrek aan regie op de governance, veel lastiger te maken. De mogelijkheid van het beschermen van de privacy in dergelijke situaties zal nader moeten worden onderzocht.

Digital Identity

Om smart contracts van betekenis te laten zijn in de juridische wereld, is het noodzakelijk dat beschikt kan worden over een betrouwbaar systeem van digitale identificatie (van natuurlijke en rechtspersonen) en autorisatie. Tegelijkertijd kan de blockchain zelf een platform zijn om de identiteit en autorisatie van personen vast te leggen en te borgen.

Teneinde de betrouwbaarheid te garanderen, is het wenselijk en noodzakelijk om (de fysieke verschijningsvorm van) een persoon (onlosmakelijk) te koppelen aan een digitale identiteit, alsmede om die koppeling betrouwbaar vast te leggen en steeds per transactie te (kunnen) vereisten en te (kunnen) controleren. Dat vereist een constante match tussen (de fysieke verschijningsvorm van) een persoon en diens digitale identiteit. Dit zou onder meer bereikt kunnen worden door de digitale identiteit van een persoon te verrijken met zijn biometrische gegevens, dan wel zijn biometrische gegevens te benutten bij het verkrijgen van toegang tot digitale systemen.

Op dit moment beschikken burgers in Nederland nog niet over een dergelijke digitale identiteit. De huidige wijze van identificatie en autorisatie in digitale systemen beperkt zich tot het ingeven en controleren van een digitaal toegangsbewijs *zonder* dat er constante, state of the art koppeling plaatsvindt met (de fysieke verschijningsvorm van) de persoon die houder is van het digitale toegangsbewijs. Daardoor kan niet worden vastgesteld dat de houder van het digitale toegangsbewijs de persoon is aan wie het digitale toegangsbewijs is afgegeven, of dat de houder van het digitale toegangsbewijs daadwerkelijk de persoon is die geautoriseerd is om de gegevens in een smart contract te kunnen bekijken of beïnvloeden.

De Dutch Blokchain Coalition werkt momenteel (in actielijn 1) aan gestandaardiseerde, interoperabele en breed toepasbare blockchain-oplossingen voor de identificatie van personen, juridische entiteiten en objecten. Het is goed om de voortgang van deze actielijn te blijven monitoren.

Voorlopige conclusies

De werkgroep komt op grond van het voorgaande tot de volgende voorlopige conclusies:

1. Een blockchain smart contract is in de eerste plaats een deterministisch computerprogramma dat op een blockchain wordt gerepliceerd en uitgevoerd.
2. Een smart contact kan juridische betekenis hebben, maar dat hoeft niet.
3. Een smart contract kan in verschillende juridische domeinen worden ingezet (privaatrecht, bestuursrecht, strafrecht) en dus verschillende verschijningsvormen kennen.
4. Niet elke juridische verschijningsvorm (wettelijke bepaling, verbintenis etc.) leent zich voor omzetting naar code.

5. Waar omzetting naar code wel mogelijk is, wordt aanbevolen om dit alleen te doen ter uitvoering van de kenbare verschijningsvorm. In het bestuurs- en het strafrecht lijkt dit - waar rechten en plichten worden vastgesteld - uit het oogpunt van rechtszekerheid hoe dan ook de aangewezen weg, maar ook in het privaatrecht kan dit vereist zijn, bijvoorbeeld ter bescherming van de consument.
6. Wanneer het bij een privaatrechtelijke verschijningsvorm wel de bedoeling van partijen is om met de code een verbintenis te scheppen en wellicht ook de uitkomst daarvan bij voorbaat te aanvaarden, zou deze bedoeling ten minste schriftelijk (lees: niet in code, maar bijvoorbeeld in een overeenkomst) moeten worden vastgelegd. Ook dit zou via de blockchain kunnen.
7. Steeds moet vooraf worden nagedacht over de feitelijke en juridische mogelijkheden om (a) de automatische executie van het contract aan daaraan voorafgaande voorwaarden te verbinden (bijvoorbeeld toestemming van partijen of een derde) en (b) de (gevolgen van de) executie achteraf 'ongedaan te maken' (herstel in de oude toestand, waardevergoeding, schadevergoeding etc.). Daarbij moet ook aandacht worden besteed aan het toepasselijke recht en de bevoegde instantie (mediator, arbiter, rechter etc.) in geval van een geschil.
8. Het is van belang steeds onderscheid te maken tussen *permissioned* en *permissionless* blockchain, omdat deze een ander governance model kunnen kennen. Een permissioned blockchain kan worden afgeschermd met een zogenaamde *access control layer*. Anders dan bij een permissionless blockchain kan niet iedereen deelnemen. Hiervoor is voorafgaande goedkeuring vereist. Bovendien kunnen lees- en schrijfrechten verschillen per gebruiker, waardoor ook taken en verantwoordelijkheden kunnen worden verdeeld . Achter een permissioned blockchain zit kortom een organisatie, veelal een samenwerkingsverband.
9. In smart contracts kunnen persoonsgegevens worden verwerkt. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn tot een levend natuurlijk persoon. Burgers hebben (op grond van de Wbp en de AVG) recht op bescherming van hun persoonsgegevens. In geval van een permissioned blochain kan worden geregeld wie verantwoordelijk is voor de naleving van de eisen in de Wbp. Dat ligt ander bij een permissionless blockchain. Daar voert niemand én iedereen de regie en zijn dat soort afspraken, als gevolg van de vrije toetredingsmogelijkheid en de gebrek aan regie op de governance, veel lastiger te maken. De mogelijkheid van het beschermen van de privacy in dergelijke situaties zal nader moeten worden onderzocht.

Toetsing van die verschijningsvormen aan het recht, leidt tot de voorlopige conclusie dat er geen majeure wijziging van wet- en regelgeving noodzakelijk lijkt om smart contracts in de juridische rechtsorde in te zetten. Niettemin is weliswaar een aantal vragen geïdentificeerd. Ook vergt het alertheid op de bijzondere regels die in een bepaalde casus op het smart contract van toepassing zijn en op de algemene juridische vraagstukken.

Blockchain: juridische aspecten op lange termijn

Blockchain technologie en smart contracts zijn relatief jonge verschijnselen. Het is daarom onvermijdelijk en terecht dat dit onderzoek naar de juridische aspecten van de technologie de nadruk legt op de mogelijke juridische belemmeringen voor de ontwikkeling ervan. Maar het is ook goed om - al is het maar kort - stil te staan bij een grotere vraag: stel dat blockchain en smart contracts de belofte volledig inlossen, en de wereld veranderen zoals de believers schetsen, wat zouden dan de gevolgen zijn voor wet- en regelgeving en voor de juridische praktijk?

Juristen die begin jaren '90, kort na het ontstaan van het world wide web, moesten adviseren over de juridische impact daarvan, spraken bijvoorbeeld over domeinnaamgeschillen, auteursrechtinbreuken en de aansprakelijkheid van tussenpersonen. Allemaal belangrijke onderwerpen, maar nu, meer dan twintig jaar later, kunnen we vaststellen dat de (indirecte) invloed op de wet- en regelgeving veel groter is geweest. Regels over onder meer de bescherming van persoonsgegevens, financiële dienstverlening (met name betalingsverkeer) en mededinging zijn sterk veranderd onder invloed van het web. Andere regels zouden zonder het web zelfs niet of in elk geval niet in hun huidige vorm hebben bestaan. Denk aan regels over elektronische handel en over elektronische identiteiten en vertrouwensdiensten.

Bij het nadenken over de langere termijn-impact van blockchain, spelen twee belangrijke kenmerken een rol: het gaat bij blockchain om het vastleggen van gegevens en om het creëren van vertrouwen in die vastlegging. Onze huidige wet- en regelgeving kent een veelheid aan verplichtingen om gegevens vast te leggen. Veel andere wettelijke bepalingen hebben tot doel het vertrouwen in die vastlegging te vergroten. Ook veel bepalingen in overeenkomsten zien hierop.

Een voorbeeld van de verplichting om zelf gegevens vast te leggen is de boekhoudverplichting voor rechtspersonen (artikel 2:10 BW). Er zijn ook verplichtingen om gegevens bij derden vast te leggen. Vaak gaat het daarbij om bij of krachtens wet aangewezen derden. Denk bijvoorbeeld aan de verplichting voor een onderneming tot inschrijving in het handelsregister (bij de Kamer van Koophandel, op grond van de Handelsregisterwet). Het feit dat de gegevens door een door de overheid aangewezen centrale autoriteit worden vastgelegd is op zichzelf al een manier om het vertrouwen in de vastlegging te vergroten. Maar er zijn ook andere manieren. Zo wordt het vertrouwen in de door een rechtspersoon op te stellen jaarrekening (en daarmee in de door de rechtspersoon gevoerde boekhouding) vergroot door de wettelijk verplichte accountantscontrole. Om het vertrouwen nog verder te vergroten mag een dergelijke controle alleen worden uitgevoerd door een accountant die beschikt over een vergunning van de AFM. Aldus wordt stapsgewijs het vertrouwen in de vastlegging vergroot. Ook de strafbaarstelling van valsheid in geschrifte kan worden beschouwd als een wettelijke maatregel ter verhoging van het vertrouwen van de vastlegging van gegevens. Marktpartijen die beogen middels hun diensten vertrouwen te vergroten, staan onder omstandigheden ook onder toezicht (krachtens de Europese eIDAS-verordening voor aanbieders van vertrouwensdiensten).
Ook veel contractuele bepalingen hebben betrekking op de vastlegging van gegevens. Denk aan de verplichting voor een leverancier om de gegevens vast te leggen op grond waarvan hij facturen stuurt of zogenaamde service level-rapportages verstrekt. Dikwijls wordt, om het vertrouwen in die vastlegging te vergroten, een auditrecht bedongen. Omdat de leverancier zijn afnemer doorgaans onvoldoende vertrouwt, wordt meestal bepaald dat de audit alleen door een onafhankelijke derde mag worden uitgevoerd.

Kortom, er zijn veel wettelijke én contractuele regelingen over de vastlegging van gegevens en het verhogen van vertrouwen in die vastlegging. Er is ook een veelheid aan partijen actief op de “vertrouwensmarkt”: accountants, notarissen, organisaties die centrale registers beheren, zoals de Kamer van Koophandel, het Kadaster, de RDW, DUO, maar ook private verleners van vertrouwensdiensten. Blockchaintechnologie kan het vertrouwen in wat in de blockchain is vastgelegd voor een deel zelf genereren. Niet volledig, want er is voor volledig vertrouwen meer nodig dat de zekerheid dat gegevens achteraf niet zijn gewijzigd. Maar toch: als blockchaintechnologie echt doorzet, zal dat ongetwijfeld vergaande consequenties hebben voor wet en regelgeving, voor contracten, en voor spelers op de vertrouwensmarkt. Gelukkig is er nog alle tijd om over dit soort langetermijneffecten van blockchain na te denken.

Inventarisatie kennisbehoefte

Inleiding

Hiervoor zijn de begrippen blockchain en smart contract geduid en zijn de juridische vragen aan de orde gekomen. In dit hoofdstuk gaat het om de kennis die nodig is om blockchains en smart contracts verantwoord toe te kunnen passen. Eén van de reacties naar aanleiding van de DAO affaire was dat behoefte is aan een nieuwe discipline: legal engineering, waarin diverse disciplines verenigd worden of de beoefenaars daarvan in ieder geval vruchtbaar samenwerken: juristen, it'ers, risk managers etc. Daarbij is behoefte aan werkwijzen, tooling, standaarden etc. Nederland lijkt in een goede positie om legal engineering verder te ontwikkelen, want er is, bijvoorbeeld onder de noemer 'regelbeheersing' al veel ervaring mee opgedaan bij de uitvoering van overheidstaken, Ook is er al een grote academische 'body of knowledge'. Eerst staan we echter stil bij de ervaringen en praktische noden van diverse ondernemers, om daarna de brug te slaan naar de ervaringen in de uitvoering en de academische kennis omtrent regelbeheersing.

Eigen waarnemingen en ervaringen

De momenteel grootste en meest gebruikte permissionless blockchain voor de ontwikkeling van smart contracts is Ethereum. De Ethereum Virtual Machine is specifiek ontworpen om met smart contracts om te kunnen gaan. De meest gangbare codetaal om smart contracts op Ethereum op te maken is Solidity. Deze taal wordt niet beheerst door de meeste juristen en risk managers, maar alleen door IT'ers. Echter juist bij de IT'ers ontbreekt het vaak weer aan de benodigde juridische kennis voor het opstellen van contracten of genoeg ervaring in risk management om er zeker van te zijn dat de contracten geen loopholes kennen waardoor kwaadwillenden transacties van het contract zouden kunnen triggeren die niet geoorloofd zijn (zoals uitgebreid beschreven rond de DAO hack), die wellicht in strijd zijn met huidige wet en regelgeving of waardoor er zelfs door ongeoorloofden valuta van het contract kon worden overgemaakt, zoals in de Parity hack.

Momenteel is Solidity kennis zeer schaars. Slechts weinige programmeurs in Nederland zijn deze programmeertaal echt eigen. Daarbij is het programmeren van een contract in solidity niet afdoende om deze ook daadwerkelijk te laten werken. Daartoe dient dit contract gecompileerd te worden in hex code en via een transactie gepubliceerd op een blockchain. Vervolgens om met een contract te kunnen communiceren dient men goed op de hoogte te zijn van de ABI (abstract binary interface). Dit luistert zeer nauw. Als een naam niet goed is ingevuld kan het contract niet meer herkennen welke functie wordt getriggerd. Dit gebeurt meestal via een javascript en HTML interface. Hierin ligt ook gelijk een lastigheid in meerdere opzichten, namelijk om én een contract op te stellen én daar goed mee te kunnen communiceren moet men al vrij snel bekend zijn met meerdere soorten programmeertalen.

Naast kennis van de code is het van belang dat er gewerkt gaat worden naar standaardisatie op verschillende niveaus, zeker aangezien iedere blockchain momenteel nog zijn eigen smart contracts ontwikkelt. We onderscheiden de volgende niveaus hierbij:

1. Ten eerste het gebruik van zogenaamde design patterns: best practices en terugkerende code structuren voor bepaalde juridische elementen. Zo zou men de code structuur voor bijvoorbeeld dispute resolution in een smart contract

op dezelfde manier vorm willen geven op de Ethereum blockchain als op Hyperledger Fabric.

2. Ten tweede is het belangrijk om te gaan kijken naar standaardisatie van ontologie. Wat we in een smart contract een owner noemen zou idealiter dat in het andere smart contract op een andere blockchain ook moeten zijn. Dit zou ook sterk bijdragen aan de leesbaarheid voor niet IT personen.
3. Als derde is het raadzaam om te kijken naar standaardisatie van data elementen. Het feit dat we onder een owner in verschillende contracten hetzelfde verstaan is een eerste stap, de beschrijving van deze owners zou ook hetzelfde moeten zijn (bijvoorbeeld een eigenaar bestaat altijd uit 3 letters 10 cijfers en weer drie letters).

Het is zeer waarschijnlijk dat in de nabije toekomst men vanuit de uitvoering van een audit de smart contract code op een blockchain als verantwoording van een technologische oplossing zou willen analyseren. Om te kijken dat dit representeert wat er ooit op bijvoorbeeld een website of een wetboek beloofd is zou men dit moeten de-compileren. Iets wat momenteel lastig is. Op dit moment is het alleen mogelijk om door het publiceren of het delen van broncode te controleren of een bepaalde input aan broncode daadwerkelijk tot dit contract in bytecode heeft geleid.
Zoals al aan het begin aangegeven dient daar dan ook nog opgeteld worden dat men in de toekomst moet verwachten dat juridisch onderlegde mensen dit gaan doen. Iets wat tot op heden niet in enige opleiding bestaat en daarmee dus echt extreem zeldzaam is.

Daarnaast blijkt in veel gevallen dat bij mensen die zich wellicht de computertaal eigen zouden willen maken, de kennis van blockchain in het algemeen ontbreekt. Dit was bijvoorbeeld initieel het geval bij OurSurance waardoor destijds de werking van smart contracts niet juist begrepen werd - wat in het oorspronkelijke smart contract leidde tot de situatie zoals al beschreven in de documentatie van bijvoorbeeld de Universiteit van Maryland: dat het contract vanuit een programmeer oogpunt correct werkte, maar vanuit een risk en compliance oogpunt niet voldeed aan de eisen. Uit de praktijk blijkt dan ook dat een gedegen procesontwerp rond de bedrijfsmodellen die men bouwt op blockchain en smart contracts nog meer dan voorheen cruciaal is om te voldoen aan alle compliance eisen. Denk hierbij aan juiste financiële afhandeling bij incorrecte transacties in welke vorm dan ook, of hoe om te gaan met data storage in publieke blockchains.

Uit meerdere projecten blijkt dat de kennis verder dient te gaan dan specialisme in een bepaald vakgebied. Juist een gedegen kennis van vakgebied overschrijdende elementen kan zeer goed bijdragen aan gedegen ontwerp en implementatie van blockchain en smart contract oplossingen.

Denk bijvoorbeeld aan de mate van vertrouwelijkheid van de gegevens. Pas door de gewenste functionaliteit grondig te begrijpen kan de blockchain- en smart contract specialist de juiste vragen stellen en voorkomen dat er onjuiste aannames worden gemaakt. Dit wordt alleen maar urgenter als het gaat om een consortium van bedrijven waarbij op nieuwe manieren wordt samengewerkt. Nog los van het beheer van het onderlinge blockchain netwerk moeten alle details op smart contractniveau worden overwogen. Welke informatie wordt gedeeld, wat leggen we vast in het smart contract en wat daarbuiten, hoe worden de gevolgen bekrachtigd, hoe doen we updates of eindigen we de overeenkomst? Wat zijn de eisen voor een derde partij om toe te treden, stellen we eisen aan de beveiliging van de computerprogramma's die transacties doen namens de wederpartij? Het beantwoorden van vragen zoals deze vraagt een grote flexibiliteit van degenen die bij dit soort onderhandelingen betrokken zijn en het vermogen om een groot aantal scenario's in kaart te brengen.

Hoe meer een smart contract eigenschappen van een overeenkomst bezit, des te belangrijker is het dat partijen de inhoud begrijpen en bewust aanvaarden. Een leesbare bijlage, zoals deze steeds vaker ook bij algemene voorwaarden wordt bijgesloten, zou uitkomst kunnen bieden. Daarnaast zullen er waarschijnlijk programmeertalen worden ontwikkeld die de werkelijkheid op een hoger niveau van abstractie omschrijven en daarmee begrijpelijker maken. Natuurlijk zal elke gebruiker van een smart contract over een zekere basiskennis en gezond verstand moeten beschikken. Daarnaast kunnen we ervan uitgaan dat er audits worden gedaan door experts die aan de bel trekken als er iets niet in de haak is, net als nu met open source software en algemene voorwaarden van bekende diensten. Maar dan moeten er wel voldoende van deze experts rondlopen - wat gezien de snelle ontwikkelingen zeker geen gegeven is.

Ook voor compliance is het van groot belang dat we de kloof tussen de juridische en de technische wereld overbruggen; er is grote behoefte aan juristen die de techniek kunnen doorgronden. De praktijk leert dat techneuten vaak te lichtzinnig denken over juridische eisen (‘het gaat niet om gevoelige persoonsgegevens dus dat loopt wel los’) en juristen de techniek niet voldoende begrijpen. Deze uitdagingen zijn niet met een cursusje op te lossen.

Bij openbare blockchains, waarbij dikwijls betaald moet worden voor het doen van een transactie, is voor het maken van een succesvol smart contract kennis vereist die verder gaat dan programmeren of een ondernemersgeest; enig speltheoretisch en economisch inzicht is ook gewenst. De gebruiker zal een duidelijke drijfveer moeten hebben om gebruik te maken van het contract en mogelijk misbruik moet worden uitgebannen. De nadelige gevolgen van een bug hebben we gezien bij de DAO hack, maar een ‘bug’ in een smart contract kan ook bestaan uit het overzien van een prikkel die tot ongewenste resultaten leidt.

Regelbeheersing

De praktijkervaringen van ondernemers met smart contracts illustreren dat behoefte bestaat aan een robuuste methode om juridische normen uit te werken naar specificaties voor de geautomatiseerde uitvoering daarvan en deze werking tot op het niveau van de machinetaal te garanderen. Hiermee is in Nederland, onder bijvoorbeeld de noemen ‘regelbeheersing’ al veel ervaring mee opgedaan. Ook is er al een grote academische ‘body of knowledge’, De idee achter regelbeheersing is dat programmacode voor mensen uit de ‘business’ niet leesbaar is en dat hen dus iets moet worden aangeboden aan de hand waarvan zij kunnen controleren of de regels juist zijn vertaald, dan wel dit zelf kunnen doen. Afhankelijk van de mate van formalisatie van het voor de vertaling gebruikte hulpmiddel leent het zich in meer of mindere mate voor geautomatiseerde omzetting naar uitvoerbare programmacode. De uit de juridische normen voortvloeiende specificaties worden bij voorkeur vastgelegd op een (leveranciersonafhankelijke) laag tussen de normen en de IT-oplossing waarmee deze normen worden uitgevoerd. Aangenomen dat zoveel mogelijk zal worden gestreefd naar een geautomatiseerde vertaalslag van modellen naar code, dataobjecten, configuraties etc. zal in deze tussenlaag een afweging moeten worden gemaakt tussen gebruiksvriendelijkheid en de mate van formalisering ten behoeve van geautomatiseerde omzetting. Voor zover bij deze omzetting nog keuzes moeten worden gemaakt, dienen ook deze met de relevante partijen te worden besproken om vervolgens te worden gedocumenteerd.

Het eerste voordeel van een tussenlaag voor het vastleggen de specificaties is dat de vanuit de business betrokken disciplines zich op een voor hen (wat meer) natuurlijke manier kunnen buigen over de specificaties, bijvoorbeeld door deze te presenteren in een visuele omgeving, in een beslissingstabel of in een op natuurlijke taal lijkende standaard als SBVR. Een tweede voordeel hiervan is dat de kennis van de organisatie niet

verdwijnt in de code, maar wordt vastgelegd in (op standaarden gebaseerde) tussenlaag, ook om afhankelijkheid van een specifieke leverancier te voorkomen. Een derde voordeel is dat de specificaties (mits formeel genoeg) kunnen worden onderzocht op logische consistentie: is aan alle gevallen gedacht, is er geen tegenspraak etc. Zogenaamde reasoners kunnen bovendien door logische gevolgtrekkingen ook kennis 'ontdekken'. Een vierde voordeel is dat de kennis beter herbruikbaar wordt en daarmee een asset op zichzelf. Het opdelen van specificaties in logische componenten tenslotte, opent de weg naar service georiënteerde oplossingen (knowledge-as-a-service) die om baat of om niet kunnen worden gedeeld met derden.

Bij de vertaling van juridische normen naar meer of minder geformaliseerde modellen is het van wezenlijk belang dat de specificaties steeds in verband kunnen worden gebracht met de norm, of dat nu een wet is, een beleidsregel of een contractuele afspraak. Dit maakt de vertaling traceerbaar en maakt het bovendien mogelijk om een impact analyse te doen op de gevolgen van een verandering in de norm (what-if?) Bij deze analyse kan ook naar de data worden gekeken, bijvoorbeeld hoeveel nog lopende contracten worden geraakt door de wijziging in de wet? Idealiter is elke vertaalslag (tot aan de machinetaal) te traceren, zowel heen als terug.

Denkbaar is dat de tussenlaag op termijn steeds minder een omgeving wordt voor vertaling van juridische teksten en steeds meer een omgeving waarin direct wordt ontworpen, met behulp van herbruikbare objecten, (bijv. configurabele) standaardcontracten en design patterns voor veel voorkomende juridische constructies.

Er bestaat al een grote body of knowledge rond regelbeheersing in ICT. Tot op heden zijn er er echter weinig studies gedaan naar de integratie van risk management en juridische vraagstukken rondom smart contracts en blockchains. Het aantal studies is momenteel aan het toenemen, getuige het aantal PhD's die aan dit onderwerp werken en ook hebben inmiddels de nodige master studenten al proof of concept / proof of technology onderzoeken gedaan naar dit onderwerp. Het SARNET project, DL4LD en andere grote NWO projecten adresseren deze zaken en met verschillende andere partners wordt er gewerkt aan oplossingen, waarbij een interdisciplinaire aanpak gehanteerd wordt met inclusie van juristen, accountants en auditors en natuurlijk AI experts en IT-ers, inclusief cryptografie experts.

Bij een onderzoek als onderdeel van een undergraduate security class aan de Universiteit van Maryland[44] zijn studenten gewezen op het feit dat er naast het traditioneel netjes programmeren van dergelijke contracten er ook rekening gehouden dient te worden met algemene risico vraagstukken zoals financial risk en operational risk (kan iemand bijvoorbeeld fraude plegen binnen een smart contract). Het bleek dat in nagenoeg alle gevallen er meerdere iteraties nodig waren om er voor te zorgen dat studenten acceptabele smart contracts wisten te programmeren, niet alleen uit het oogpunt van programmeren, maar ook vanuit risk management. Het eventuele juridische kader was in deze nog niet eens meegenomen. In andere cursussen zoals Policy making and Rule management van de UVA, wordt dit aspect wel belicht.

Een andere studie van de National University of Singapore/Yale-NUS college[45] richtte de aandacht op een andere component, namelijk de technische vertaalslagen die er gemaakt worden. Daar de contractcode zoals deze getypt wordt niet ook als zodanig op een blockchain gezet wordt, maar gecompiled wordt naar bytecode, dient men er zeker van te zijn dat deze gecompileerde code de juiste representatie was van de code daarboven. Hierin zijn enkele verbetergebieden aangekaart welke geadresseerd konden worden. Deze studie richtte zich slechts op de vertaling van een high level computer taal naar een low level computer taal, maar in praktijk zal in de toekomst nog een

[44] https://eprint.iacr.org/2015/460.pdf

[45] https://www.comp.nus.edu.sg/~hobor/Publications/2016/Making%20Smart%20Contracts%20Smarter.pdf

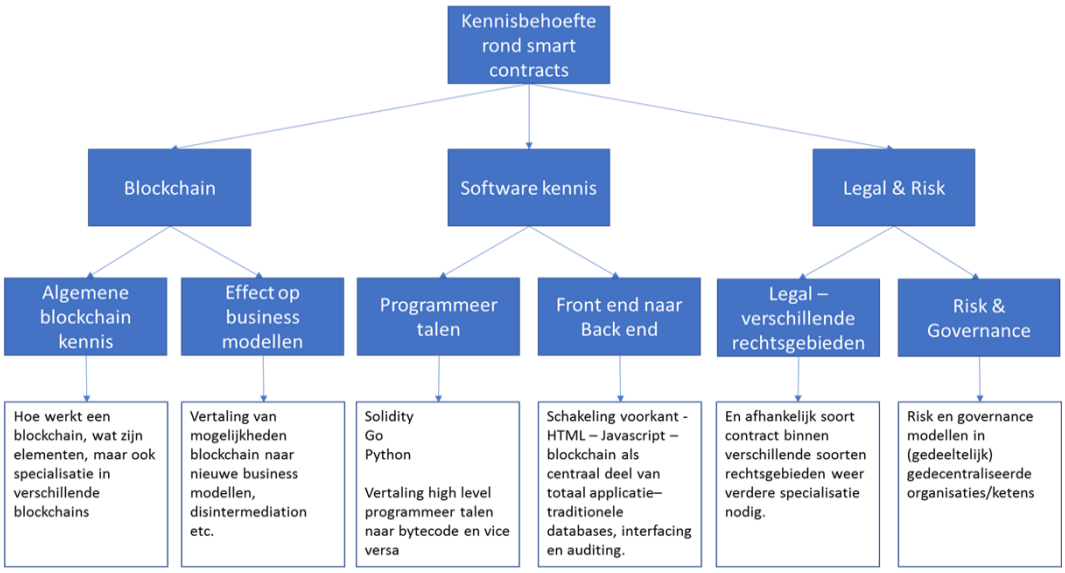
additionele laag hierboven komen, namelijk de vertaling van natuurlijke taal naar computertaal, daar de meeste individuen niet goed in staat zijn om computertalen te lezen. Dus moet er aandacht gericht worden op het feit dat meerdere talen de juiste vertaalslag dienen te maken. Hyperledger Composer is een voorbeeld van een hogere abstractielaag die de kloof tussen realiteit en blockchain probeert te slechten. Hiermee kunnen applicaties worden gemodelleerd die op een Hyperledger Fabric blockchain draaien.

Waar in de aangehaalde studies in mindere mate naar is gekeken, is de vertaling van juridische taal naar code. Hier zou dus goed moeten worden gekeken naar wat 'regelbeheersing' al te bieden heeft. Juist op deze vertaalslag en op de audit trail (zowel m.b.t de vertaling van de normen door de diverse lagen van het systeem heen als de aantoonbaar correcte uitvoering hiervan) zullen juristen, auditors en toezichthouders hoogstwaarschijnlijk gaan focussen. Over dit soort zaken dient dan ook bij het ontwerp worden nagedacht, evenals over zaken als geschilbeslechting, de mogelijkheid van hybride contracten (taal én code) etc.

Een beweging richting 'regelbeheersing' in de context van smart contracts valt zeker toe te juichen. In het kader van ISO/TC 307 worden mogelijke standaarden voor *blockchain en distributed ledger technologies en smart contracts* ontwikkeld. Wellicht kan in dit kader (op termijn) ook een internationale standaard worden ontwikkeld voor het uitdrukken van juridische normen in smart contracts, dit met het oog op interoperabiliteit en ook om vendor lock-in te voorkomen, in lijn met de geïdentificeerde standaardisatiebehoeftes ten aanzien van smart contracts eerder in dit hoofdstuk. Naast standaarden voor contracten acht de Dutch Blockchain Coalition ook standaarden noodzakelijk voor andere zaken, zoals de identificatie van personen, juridische entiteiten en objecten.

Clustering geïdentificeerde deelgebieden kennisbehoefte

Zoals aangegeven zal de kennisbehoefte verder gaan dan alleen technische of legal kennis. Naast de benodigde kennis deze twee gebieden, dient voor goede implementaties van smart contracts en business modellen op basis van blockchain en smart contracts een breder perspectief in ogenschouw te worden genomen. Een eerste visualisatie van de kennisbehoefte naar de toekomst is onderstaand neergezet.



Uit de analyses vanuit de literatuur wat er al bekend is rond kennisbehoefte van blockchain en smart contracts en met name ook vanuit de verschillende individuele use cases zijn er een drietal hoofdgebieden te identificeren waarin kennisontwikkeling nodig is en waarin men kennis dient te hebben om effectief met smart contracts en blockchain business modellen in de toekomst om te gaan.

Deze drietal gebieden zijn:

1. Blockchain kennis
2. Software kennis
3. Legal & Risk kennis

Alle hoofdgebieden waar men op dit moment van aangeeft dat er kennisontwikkeling gewenst is zijn weer op te delen in verschillende subgebieden. Binnen deze subgebieden zijn op hun beurt weer zeer veel specialistische deelgebieden te onderkennen. Verder dan de verdieping van de subgebieden is deze eerste verkenning niet gegaan. Het verder uitdiepen van de specifieke kennisgebieden en specialisaties in de subgebieden zal meegenomen worden in de aanbevelingen voor vervolgstappen.

Blockchain kennis

Het hoofdgebied blockchain kennis is opgedeeld in twee subgebieden, te weten:

1. *Algemene blockchain kennis.*
   Dit subgebied omvat alles rond wat blockchain is en hoe het werkt. Dit omvat, maar is niet beperkt tot, kennis over de werking van blockchain, kennis van cryptografie, kennis van de verschillende elementen en karakteristieken die een blockchain kan hebben, kennis van de verschillende soorten blockchains, kennis van verschillende soorten consensus mechanismen, kennis van producten en diensten op blockchain zoals cryptocurrencies en smart contracts.
2. *Effect op business- en industriemodellen.*
   Dit subgebied omvat alles over wat het effect van blockchain kan zijn op proces-, bedrijfs-, en industriemodellen. In dit deel zal kennis opgebouwd moeten worden op algemeen modelleren, herontwerp, design thinking in de breedste zin van het woord en ook een stuk historische model ontwikkeling, waar komen huidige modellen vandaan. Dit om beter te begrijpen wat het effect van blockchain kan zijn op toekomstige modellen en om op deze manier bijvoorbeeld een effectieve governance structuur rond gedecentraliseerde smart contract based modellen te kunnen ontwerpen.

Van deze twee deelgebieden is het eerst wat technischer van aard daar het ingaat op de daadwerkelijke werking van blockchain en haar elementen. Het tweede deel is minder technisch van aard en zal meer gericht moeten zijn op de bedrijfs-, en maatschappelijke impact als gevolg van blockchain in combinatie met een historisch besef hoe organisaties en maatschappijen zich ontwikkeld hebben.

Software (en IT) kennis

Het tweede hoofdgebied is het meest technisch van aard en omvat de technische software kennis benodigd om met smart contracts om te kunnen gaan. Ook dit hoofdgebied is op te delen in twee subgebieden:

1. *Programmeertalen.*
Dit subgebied is traditioneel de wereld van programmeurs. De kennisopbouw die hier zal moeten plaatsvinden is naast de traditionele programmeertalen zoals Java, JavaScript, Python, C++ en C# en Go vooral ook de opbouw van kennis van nieuwe programmeertalen zoals de, op moment van schrijven, grootste programmeertaal voor smart contracts Solidity, maar ook toekomstige, meer visueel ingestelde concepten zoals Babbage. Zeker op het gebied van deze laatst genoemde programmeerkennis is momenteel een groot tekort. Ook zal constant gekeken moeten worden of er geen nieuwe talen in ontwikkeling zijn.
2. *Front-end to back end interactie en integratie*.
Dit stuk richt zich op het correct vertalen van wat er op een voorkant gebeurt (bijvoorbeeld een website gebouwd met HTML/CSS/JavaScript) naar wat er aan de achterkant wordt geëxecuteerd. Dit kan zijn juiste executie in traditionele databases, maar uiteraard ook in smart contracts op een blockchain. Deze vertaling gaat verder dan alleen een digital voorkant zoals een website, maar geldt ook voor bijvoorbeeld pdf samenvattingen die aan een eindgebruiker wordt meegegeven op een site en gedownload kunnen worden. De vertaling van de geschreven en naar de eindgebruikers gecommuniceerde belofte en verwachtingen dienen uiteraard juist vertaald te worden door de verschillende lagen heen waarbij er vaak een veelvoud van programmeertalen aan elkaar gekoppeld zullen worden.

Ook zal er kennis opgedaan moeten worden rond zijdelingse integratie. Dit houdt bijvoorbeeld in het koppelen van smart contracts aan traditionele databases welke bijvoorbeeld dienen als “Oracle”. Naast de front to back end interactie zal hier ook kennis opgedaan moeten worden ten aanzien van standaardisatie zoals eerder in dit rapport beschreven op het gebied van design patterns, ontologie en standaardisatie van data elementen om niet alleen de interne integratie en interactie op orde te hebben, maar ook de communicatie en interactie met andere smart contracts, op termijn zelfs over blockchains heen, goed te kunnen laten verlopen.
Zoals hierboven al aangegeven is dit het meest technisch van aard, naast het eerst subgebied van blockchain kennis zoals eerder beschreven.

Legal & Risk

De derde hoofdpijler van kennisbehoefte in deze is die rond legal & risk. Ook deze is wederom op te breken in 2 subgebieden:

1. *Verschillende rechtsgebieden.*
   Dit is waarschijnlijk een van de breedste subgebieden die geïdentificeerd is. Ten eerste dient er, wil men effectief met smart contracts om kunnen gaan, een gedegen kennis te zijn van algemeen recht en een gedegen begrip van de specifieke aandachtsgebieden in het recht als gevolg van blockchain zoals eerder in dit rapport geïdentificeerd. Daarnaast zal men wellicht specialisaties hebben in verschillende rechtsgebieden waarin men contractvormen kent welke wellicht ook als een smart contract opgezet kunnen worden.
2. *Risk & Governance*.
   Aangezien veel smart contracts waarde vast kunnen houden en mede als doel hebben ergens in de executie wellicht waarde te transporteren tussen verschillende partijen dient er extra aandacht besteed te worden aan zaken als operationele en financiële risico’s en hoe deze bij ontwerp al te mitigeren en waar nodig ook in het ontwerp van smart contracts ruimte te laten om eventueel in te grijpen waar nodig. Zeker gezien het immutable karakter van de code van een smart contract op een blockchain is de noodzaak dus extra groot om dit bij voorbaat al uitgedacht te hebben. Daarom is een gedegen kennis van risico’s en management van dergelijke risico’s, inclusief heldere verantwoordelijkheden, noodzakelijk bij het neerzetten van een robuust smart contract. Dit gaat dus verder dan of alleen de code waterdicht is gemaakt tegen hackers, maar ook het kunnen omgaan met onbedoelde acties.

Zoals al aangegeven zijn deze subgebieden op zichzelf nog veel verder uit te werken in verschillende specialisatie en superspecialisatie gebieden. Zoals verder in het rapport ook beschreven is er de verwachting dat er aan de ene kant een groeiende behoefte is aan deze individuele specialismen, echter ligt een groot deel van de huidige kennishiaten vooral in de kruisbestuiving van deze individuele kennisgebieden. Er zal een groeiende behoefte ontstaan aan multidisciplinaire vakgebieden in deze.

Overige kennisgebieden

De geïdentificeerde clustering van kennisgebieden in deze verkenning zijn grotendeels gericht op de kennisbehoefte voor het werken aan of werken met smart contracts of smart contract gerelateerde trajecten aangezien dit ook het doel was van deze werkgroep. Daar blockchain uiteraard breder is dan smart contracts zijn er natuurlijk nog veel meer gebieden waar kennis van nodig is in andersoortige blockchain gerelateerde werkgebieden. Een goed voorbeeld is het veld van cryptocurrencies, waar bijvoorbeeld traders is kennis van economie en financiële markten meer van belang, echter zijn deze gebieden niet meegenomen in deze verkenning.

Cross functionele kennis

Misschien nog meer dan bij de implementatie van andere systemen is het van groot belang dat er bij deze projecten experts betrokken zijn die zowel een diepe domeinkennis als kennis van de onderhavige techniek als kennis van de juridische en of risico kant hebben.

Er is een grote verscheidenheid aan blockchain en smart contract implementaties, wat makkelijk tot misverstanden kan leiden over de eigenschappen, de vereisten en (on)mogelijkheden van de te kiezen oplossingen. Juist op dit snijvlak van verschillende expertises is waar er een tekort is van vakmensen. Naast een opbouw in kennis van de individuele specialismen dient er in toenemende mate een opbouw van multidisciplinaire kenniswerkers te komen.

Deze personen dienen genoeg gespecialiseerd te zijn in een van de pijlers om daar als professional in aan het werk te zijn, maar ook genoeg kennis van zaken van de andere pijlers te hebben om met deze beroepsgroepen te kunnen communiceren en zodoende in een coördinerende, leidende rol te kunnen fungeren.

Vervolgstappen en mogelijke partijen voor ontwikkeling kennisbehoefte

Ten aanzien van de opleidingsbehoeften kan op korte termijn het bedrijfsleven een rol spelen door het verzorgen van verschillende masterclasses en cursussen. Dit behoeft geen centrale coördinatie daar marktwerking dit initieel zou kunnen bewerkstelligen. Echter dient er ook een lange termijn oplossing te worden aangekaart.

Op lange termijn zal er een structurele oplossing voor gevonden moeten worden voor de kennisbehoefte die ontstaat als gevolg van blockchain en smart contracts. Dat zou kunnen liggen in samenwerkingen tussen universiteiten en faculteiten die tot op heden nog niet eerder (structureel) hebben samengewerkt zoals juridische faculteiten en technische faculteiten.

Bemoedigend in deze is dat dit soort cross-functionele opleidingen in het verleden behoorlijk succesvol zijn geweest met als voorbeelden LifeScience & Technology opleidingen of Technische Bestuurs/Bedrijfskunde.

Hierin is dus duidelijk een rol weggelegd voor de traditionele onderwijs- en onderzoeksinstanties zoals universiteiten en hogescholen. De meest voor de hand liggende universiteiten voor de verdieping van de individuele elementen zijn die met een technische achtergrond, zoals Delft, Eindhoven en Twente en die met een juridische achtergrond, zoals Amsterdam, Groningen, Leiden, Nijmegen, Maastricht, Rotterdam, Utrecht en Tilburg. Zeker die faculteiten die al veel langere tijd met regelbeheersing, IT en recht bezig zijn.
Voor multidisciplinaire opleidingen kan er gekeken worden naar bestaande “joint-degree” samenwerkingen zoals combinaties Leiden-Delft-Rotterdam of Tilburg-Eindhoven en kijken hoe dit als een aparte opleidingsrichting kan worden opgesteld. Dit zou ook op niet-universitair niveau onderzocht moeten worden.

Aangezien dit onderzoek een eerste verkenning betreft, is het raadzaam om met verschillende van de geïdentificeerde partijen zoals hierboven beschreven een verdiepingsslag te maken ten aanzien van de inhoud en de behoefte aan verschillende profielen tussen de vakgebieden en waar de huidige opleidingen al (gedeeltelijke) oplossingen bieden. Zo kan er in de voorgestelde multidisciplinaire opleidingsrichting behoefte zijn aan een profiel met meer nadruk op het juridische vlak of juist meer nadruk op het technische vlak.

Daar het een samenwerking vereist van veel verschillende partijen willen wij voorstellen de coördinatie hiervan te leggen bij de Nationale Blockchain Coalitie in een vervolg werkgroep voor Human Resources. Deze groep kan uiteraard deels bestaan uit mensen die in deze verkenning hebben meegewerkt om consistentie en snelle voortgang te kunnen garanderen.

Ten aanzien van tijdslijnen is het raadzaam om te proberen hier snel in te schakelen aangezien de ontwikkelingen binnen blockchain en smart contracts zeer snel gaan, evenals de geïnvesteerde bedragen die hiermee gemoeid zijn. Wij stellen dan ook voor om in november 2017 de vervolg werkgroep voor het eerst samen te laten komen om te kijken. Het streven zou moeten zijn om al in jaargang 2018-2019 hier invulling aan te kunnen geven.

Samenvatting aanbevelingen en vervolgstappen

Gerichtere aanpak vanuit de overheid voor wat betreft opleidingsbehoefte en ontwikkeling van wet en regelgeving
De blockchain expert groep is een zeer goede start geweest, temeer omdat de verschillende experts elkaar daardoor beter kennen en veel gemakkelijker kunnen vinden. Hierdoor is men ook veel beter op de hoogte van verschillende initiatieven die er spelen op blockchain gebied in Nederland. Wat daar helaas bij opvalt is dat er nog steeds te veel initiatieven langs elkaar leven. Als we als Nederland nog slagvaardiger willen zijn op het gebied zullen we dit nog beter moeten coördineren om nog beter en sneller te kunnen schakelen.

Verder onderzoeken kennisbehoefte rond blockchain en smart contracts
Door de samenstelling van de werkgroep en de werkwijze is ten aanzien van de toekomstige kennisbehoefte een sterke focus op de directe behoefte vanuit de praktijk (overheden en bedrijfsleven) geweest in deze verkenning en lag er minder focus op de wetenschappelijke kennisbehoefte. Het is aan te raden om in een vervolgtraject een sterkere focus op de wetenschappelijke kant van de kennisbehoefte mee te nemen en daarnaast een dieper onderzoek te doen naar het al bestaande aanbod rond kennisopbouw.

Onderzoeken diepere en multidisciplinaire opleiding IT en recht
Daar er twee gebieden die van oudsher niet veel kruisbestuiving hadden, namelijk techniek, specifiek computer programmeren, en legal samen kunnen komen in smart contracts is het raadzaam om een verkenning te doen tussen de technische en de rechten universiteiten om te kijken of er een opleiding in deze multidisciplinaire richting gevormd moet en kan worden. Hierin dient dan niet IT en recht als holistisch gegeven benaderd te worden, maar dient men echt verstand en ervaring op te doen van computertalen en recht, waarbij, aangezien smart contracts verschillende soorten legal contracts zou kunnen representeren er ook een specifieke richting in het recht nog gekozen zou moeten kunnen worden.

Verder onderzoeken vragen en hiaten wetgeving
Zoals eerder in dit rapport aangegeven zijn er in veel gevallen ook nog zeker wel meerdere vragen aan de juridische kant van smart contracts die beantwoord dienen te worden. Het is daarom raadzaam om met de vervolggroep te starten waarbij meerdere betrokkenen van deze werkgroep zouden kunnen deelnemen. Zeker met het toenemend aantal use cases is het raadzaam om continuïteit in deze te bewerkstelligen.

Vastleggen opgebouwde kennis in vastgestelde definities
Een van de belangrijkste bevindingen van de werkgroep is dat er veel onduidelijkheid bestond vooraf ten aanzien van definities. De semantiek zorgde in veel gevallen voor bijna Babylonische spraakverwarringen. Het is daarom raadzaam om eenduidige definities vast te leggen om toekomstige debatten en verkenningen zo duidelijke en soepel mogelijk te laten verlopen.

Onderzoek naar mogelijke standaardisatie
Aangezien het standaardiseren van smart contracts per blockchain platform niet te reguleren is, zal de standaardisatie zich moeten richten op de vorm en de inhoud van smart contracts en dan met name design patterns, ontologie en standaardisatie van individuele data elementen.

Kaders - Besproken Use Cases

BLandLord - Crowdownership op Bitcoin Blockchain

Blandlord introduceert crowd-ownership in Nederland en zet Blockchain technologie in om dit mogelijk te maken.

Crowd ownership staat voor gezamenlijk bezit. Eigendom is verdeeld over een groep eigenaren; dit past in de trend van de sharing economy. Elke mede-eigenaar heeft inspraak en deelt naar rato in de inkomsten. Dit maakt crowd-ownership egalitair en democratisch; een groep gelijken neemt gezamenlijk verantwoordelijkheid.

Blandlord gebruikt smart contracts het verdelen van eigendom, voor de financiële stromen en voor de inspraak van de eigenaren bij beslissingen. Hiermee wordt gezamenlijk bezit mogelijk waarbij duizenden eigenaren volledig decentraal inspraak hebben en profiteren van hun eigendom.

Deloitte - Handelsgebouw Rotterdam

Blockchain in vastgoed

Begin 2017 is door Deloitte Real Estate, in samenwerking met gemeente Rotterdam en Cambridge Innovation Center (CIC) gewerkt aan de eerste concrete blockchaintoepassing voor huurcontracten.
Door de toepassing van blockchaintechnologie ontstaat er een uniforme bron van vastgoedinformatie waar diverse stakeholders gebruik van kunnen maken, waardoor meervoudige controle van dezelfde data niet langer nodig is. Binnen het project zijn vijf belangrijke stappen gezet.

1. Digitaliseren van gebouwgegevens

Een belangrijke eerste stap ziet op het creëren van een blockchain grootboek met vastgoedinformatie van elk gebouw dat op de blockchain geregistreerd wordt. Met het digitaliseren van het gebouw wordt een digitale eigendomsmunt van het gebouw ‘geslagen’.Deze zogenaamde ‘token’ is een digitale vingerafdruk van het gebouw, en al zijn bijbehorende details. De digitale vingerafdruk verwijst naar een database waarin de gebouwdetails zijn opgeslagen. Voor de basis van deze eerste stap wordt, op dit moment, gebruik gemaakt van bestaande registers, zoals het Kadaster en de BAG. Deze gegevens kunnen aangevuld wordt met andere basisdata, zoals de vierkante meters van een gebouw, het energielabel, gebouwindeling en plattegronden. Dit zijn slechts een aantal datapunten die nu in het gebouwdossier/paspoort opgenomen worden. Door de inzet van de blockchain technologie worden deze gegevens van een tijdsstempel voorzien en wordt onweerlegbaar vastgelegd op welk moment en uit welke database de gegevens zijn gehaald.

2. Digitaliseren van de eigendomssituatie

De volgende stap na het digitaliseren van de gebouwgegevens is het koppelen van een eigenaar aan de digitale munt die het gebouw c.q. het gebouwdeel representeert. Om dit te kunnen doen moet een digitale identiteit van de eigenaar gecreëerd worden. Voor deze stap wordt eveneens geput uit de bestaande registers, zoals het Kadaster en de Kamer van Koophandel. In de Nederlandse praktijk worden deze registers al jaren gebruikt en in het rechtsverkeer wordt vertrouwd op deze registers. In de huidige stand van de techniek is het onomstotelijk vastleggen van de digitale identiteit een groot vraagstuk. Momenteel wordt gebruik gemaakt van de centrale autoriteiten (zoals de eerder genoemde Kamer van Koophandel) bij het doen van transacties. In een toekomstige situatie waarin blockchain gemeengoed is geworden, kan de rol van de centrale partijen (de trusted third parties), aanzienlijk wijzigen.

3. Eigendom overdragen

De onroerend goed markt kent tal van spelers, belanghebbenden en betrokken partijen. De enige constante factor in dit gehele proces is feitelijk de onroerende zaak. Eigendom gaat, na verloop van jaren, over van partij a naar partij b. Dit geldt evenzeer voor de huurder, financiering en andere verplichtingen. In de huidige situatie wordt onroerend goed overgedragen met behulp van de notaris. De financiële, juridische en fiscale verplichtingen van de huidige eigenaar en toekomstige eigenaar worden in beeld gebracht en betrokken in de transactie.

Met behulp van de digitale tokens (digitale eigendomsmunt) die het gebouw representeren en een betrouwbare digitale identiteit wordt het overdragen van het eigendom eenvoudiger. Het eigendomsbewijs van het gebouw kan met behulp van een online transactie eenvoudig worden overgedragen. De houder van de zogenoemde eigendomsmunt is de enige partij die gerechtigd zal zijn om deze munt te ‘bezwaren’ met juridische verplichtingen, zoals een huurcontract. Voor de huidige praktijk zal dit een forse omslag in het denken betekenen en zullen er tal van juridische en fiscale vragen opdoemen die opgelost moeten worden.

4. Huurcontracten sluiten

De volgende stap is het eenvoudig, online, ondertekenen van huurcontracten. Met de opkomende behoefte aan flexibeler gebruik van kantoren van, bijvoorbeeld de start-up community in het Groothandelsgebouw, moet het proces voor het aangaan van huurverplichtingen worden omgegooid. Binnen de zogenoemde customer journey van de huurder/gebruiker zijn dan ook tal van optimalisaties te bereiken. In het kader van het project is gekozen voor een contractentemplate module waarmee in een digitale omgeving meerdere partijen kunnen werken aan de ondertekening van het huurcontract. Aan de hand van de finale onderhandelingsresultaten wordt online het contract op maat gemaakt voor de concrete huurder. Met behulp van een blockchain transactie wordt dit huurcontract digitaal ondertekend door één contractspartij en ter ondertekening aan de wederpartij gestuurd. De wederpartij krijgt een notificatie en ondertekent, na controle van het contract, eveneens digitaal het contract. Hier komt wederom een blockchaintransactie aan te pas. Na afronding van deze stappen is een door beide partijen ondertekende versie van het huurcontract toegevoegd aan de blockchain. Hierdoor is onweerlegbaar vastgelegd welke afspraken huurder en verhuurder met elkaar gemaakt hebben. Belangrijkste voordeel is daarnaast dat het veel tijdwinst oplevert in het proces voor zowel huurder als verhuurder.

5. Contractinformatie ontsluiten voor derde partijen

Gedurende de levenscyclus zal de vastgoedeigenaar op gezette tijden informatie over zijn pand delen met derde partijen. De bank in het kader van een (her)financiering, een auditor in het kader van de jaarrekening controle, een taxateur ten behoeve van een waardering en een (potentiele) koper bij een verkoop van het pand. Bij elk van deze gebeurtenissen worden controles uitgevoerd op actualiteit en volledigheid door de verschillende betrokken partijen. Blockchain heeft de potentie dat de betrokken partijen in het netwerk van dezelfde (decentrale) bron van informatie gebruik maken.

Daarnaast zorgt de blockchain ervoor dat de vastgelegde gegevens op betrouwbare, uniforme, veilige en snelle wijze zijn te delen met derde partijen.

OurSurance - Peer2Peer verzekeringen

OurSurance is een Peer2Peer verzekeringsproject waarbij door middel van Smart Contracts op de Ethereum blockchain mensen met een verzekeringsbehoefte een op een gekoppeld worden aan investeerders die in individuele polissen willen investeren. Hierbij kennen de verzekerde en de investeerder elkaar niet. Iedereen die wil kan investeerder worden op het platform, van individuen tot bedrijven. Na aanvraag wordt via een veilingmechanisme de investeerder aan de verzekerde middels een smart contract gekoppeld, inclusief het mogelijke claimbedrag. Door de smart contracts loopt de verzekerde geen risico dat er in geval van een valide claim niet wordt uitbetaald. Claim afhandeling gebeurd door onderling stemmen, waarbij bij een conflict een onafhankelijke 3e de doorslag moet geven. In de uiteindelijke premiestroom en eventuele uitbetaling heeft OurSurance geen deel. Na afsluiten van de verzekering bestaat de polis als smart contract op de Ethereum blockchain en krijgt de verzekerde een pdf samenvatting. Alle polissen zijn eenmalig. Na afloop worden de verzekeringscontracten gesloten.

APG – Pensioenwaarde-overdracht

APG en PGGM hebben in een gezamenlijk experiment onderzocht hoe waardeoverdrachten tussen pensioenfondsen met behulp van Smart Contracts mogelijk gemaakt kunnen worden. Als iemand een nieuwe stap maakt in haar of zijn carrière kan het zijn dat daarbij, via een andere CAO, ook een stap wordt gemaakt van het ene pensioenfonds naar het andere. Op dit moment wordt dan een administratief proces in gang gezet waarbij via verschillende brieven en formulieren door de werknemer aangegeven moet worden dat de reeds opgebouwde pensioenwaarde kan worden meegenomen van het ene naar het andere pensioenfonds. In het experiment zijn Smart Contracts gebruikt om automatisch op te zoeken of en waar iemand nog opgebouwde pensioenwaarde heeft staan om vervolgens een automatische, of via een enkele muisklik, overdracht van de pensioenwaarde te doen naar het pensioenfonds waarbij de werknemer via zijn nieuwe werkgever is aangesloten. Het Smart Contract bevat in dit experiment dus de functionaliteit om op basis van gegevens van het individu op te zoeken bij welk ander pensioenfonds de individu is aangesloten en de overdacht van de pensioenwaarde af te handelen.

IBM - fietsplan

In dit werkende prototype, dat draait op de permissioned blockchain Hyperledger Fabric, zetten IBM en RDW de fietseigenaar centraal. De eigenaar van een elektrische fiets kan deze registreren, overdragen, zijn eigenaarschap bewijzen en aangifte doen van diefstal. Het zogenaamde 'smart lock' op de fiets registreert de locatie van de fiets wanneer deze op slot wordt gezet. Bij diefstal kan de politie de laatste positie inzien om direct te kunnen reageren. Verzekeringsmaatschappijen kunnen de claim automatisch afhandelen door middel van een smart contract. Verschillende aspecten zoals de originele waarde, datum van afsluiting van de verzekering, of de fiets op slot stond en of er aangifte is gedaan kunnen allemaal worden meegenomen bij de beslissing om uit te betalen. Het is een mooi voorbeeld van hoe het opzetten van een ecosysteem al snel tot grote en soms onvoorziene innovaties kan leiden en hoe sensoren de kracht van een smart contract kunnen versterken. Het project is genomineerd voor de Computable Awards 2017 in de categorie Digital Transformation of the Year.

Dutch
Blockchain
Coalition

connect and create

Dutch Blockchain Coalition

connect and create

Founding partners

ABN·AMRO

alliander

Brightlands

CGI
Experience the commitment®

C/M/S/
Law . Tax

CWI
Centrum Wiskunde & Informatica

ECP
Platform voor de InformatieSamenleving

ENEXIS
NETBEHEER

ING

kamer van koophandel

KNB
Koninklijke Notariële Beroepsorganisatie

Ministerie van Economische Zaken en Klimaat

Ministerie van Infrastructuur en Waterstaat

Ministerie van Justitie en Veiligheid

nationale nederlanden

NWO
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Port of Rotterdam

pwc

Rabobank

Radboud Universiteit

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Tilburg University

TNO innovation for life

TU Delft

de volksbank

www.dutchblockchaincoalition.org