

Vergaderjaar 2019–2020

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 653

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 december 2019

Hierbij stuur ik uw Kamer, mede namens de Minister van Financiën en de Staatssecretaris van Economische Zaken en Klimaat, de kabinetsreactie op het verkennende onderzoek «Blockchain en het recht». Het onderzoek is verricht door het Tilburg Instituut for Law, Technology and Society (TILT), in opdracht van het WODC (Ministerie van Justitie en Veiligheid). Het onderzoeksrapport is aangeboden aan uw Kamer op 28 augustus jl. Bij die gelegenheid gaf ik aan te streven naar een reactie voor het einde van dit jaar.¹

Inleiding

Zoals ook aangegeven in de Nederlandse Digitaliseringstrategie² wil Nederland de kansen benutten die digitalisering biedt. Het kabinet streeft naar ruimte voor de economische en maatschappelijke waarde die met technologie kan worden gecreëerd én wil dat publieke belangen en rechtsstatelijke waarden geborgd zijn en blijven; hieraan kan technologie uiteraard ook bijdragen. Het is in dit licht dat wordt bezien of beleid en wetgeving aanpassing behoeven.

Blockchain is een relatief jonge technologie die nog volop in beweging is. Het is van belang om goed zicht te krijgen op de kansen en de risico's. Leren gaat sneller door proberen. Daarom onderzoekt en beproeft de overheid blockchaintechnologie ook zelf.

Naarmate meer wordt geleerd over blockchain, ontstaat ook meer inzicht in de normatieve aspecten ervan. Het verkennende onderzoek «Blockchain en het recht» levert op dit punt een waardevolle bijdrage. Het onderzoek richt zich primair op het privaatrecht, het gegevensbeschermingsrecht en het bestuursrecht. Ook het financieel toezicht op tokens komt aan de orde. Tenslotte nemen de onderzoekers een viertal (door overheidsorganisaties)

¹ Zie Kamerstuk 26 643, nr. 627.

² Kamerstuk 26 643, nr. 541.

geïnitieerde «use-cases» onder de loep.³ Het rapport is kritisch over blockchain technologie, maar noemt ook kansen. Het kabinet ziet in het rapport een oproep aan de samenleving en de overheid tot zorgvuldigheid, opdat het economische en maatschappelijke potentieel van blockchaintechnologie op een verantwoorde wijze kan worden verzilverd. Want kansen zijn er ook. Zo participeren Nederlandse multinationals en financiële dienstverleners de ontwikkeling van het platform KomGo waarmee processen rondom de financiering van grondstoffenhandel via een blockchain platform gaan lopen en doen Nederlandse verzekeraars mee aan het project B3i dat zich richt op het herverzekeren van risico's. Overheidsorganisaties beproeven samen met de wetenschap en bedrijven in nationaal en internationaal verband veilige en verantwoorde blockchain toepassingen met maatschappelijke meerwaarde. Zo is het streven dat burgers in Europa aan kunnen tonen dat diploma's en onderwijscertificaten behaald zijn.

Opbouw van de brief

Deze brief bestaat uit twee delen. Het eerste deel («Verantwoord blockchain gebruik en het recht») bevestigt de boodschap van het onderzoeksrapport dat een verantwoord gebruik van blockchain niet zonder het recht kan. In dat licht onderstreept het kabinet de noodzaak van een ethisch en juridisch verantwoord ontwerp van informatiesystemen. Op de volgende in het rapport aangesneden onderwerpen wordt nader ingegaan: gegevensbescherming, de uitgifte van tokens en financieel toezicht, de goederenrechtelijke status van tokens, buiten-contractuele aansprakelijkheid en tot slot het internationaal privaatrecht (toepasselijk recht en jurisdictie).

Het onderzoeksrapport gaat, mede in relatie tot de onderzochte use-cases, ook in op de meerwaarde van blockchain als «vertrouwenstechnologie». Het kabinet onderschrijft dat een genuanceerd beeld nodig is van de mogelijkheden en de onmogelijkheden. Hierop wordt nader ingegaan in het tweede deel van de reactie («Blockchain en vertrouwen»). In dit deel wordt ook stilgestaan bij het proefproject «Notary Privacy Ecosystem» van de Koninklijke Notariële Beroepsorganisatie (KNB) en bij enkele samenwerkingsverbanden, waarin door overheidsorganisaties wordt geparticipeerd in het streven naar het ontwikkelen van maatschappelijk nuttige, veilige en verantwoorde toepassingen. In de bijlage⁴ bij deze brief wordt een uitleg op hoofdlijnen van blockchain gegeven.

Verantwoord blockchain gebruik en het recht

Blockchain kan niet zonder het recht

Het onderzoeksrapport laat zien dat een verantwoord gebruik van blockchain niet zonder het recht kan. De onderzoekers noemen blockchain een normatieve technologie. Hier speelt in het bijzonder dat blockchains zo worden ontworpen dat de opslag van gegevens of de uitvoering van een programma niet (eenzijdig) ongedaan kan worden gemaakt. Dit noopt tot de nodige voorzichtigheid, bijvoorbeeld omdat de wet kan vereisen dat gegevens worden gecorrigeerd of verwijderd. De geautomatiseerde uitvoering van regels en afspraken biedt kansen, maar bedacht moet worden dat de wet menselijke tussenkomst kan verlangen en/of correctie van de resultaten. Om onrechtmatige, mogelijk zelfs onherstelbare, gevolgen te voorkomen, is het van groot belang dat reeds bij het ontwerp van blockchain toepassingen rekening wordt gehouden met ethische

³ Deze use-cases zijn: Scheepsregistratie, Schatkistbankieren, Vervoer van afvalstoffen en Delen van privacygevoelige gegevens door de overheid/CAK.

⁴ Raadpleegbaar via www.tweedekamer.nl

beginselen en met juridische normen, zowel sectorspecifieke normen als breder geldende normen zoals vastgelegd in onder meer de Algemene Verordening Gegevensbescherming (AVG), het Burgerlijk Wetboek (BW) en de Algemene wet bestuursrecht (Awb).

Het in goede banen leiden van het gebruik van blockchain technologie is niet alleen een kwestie van normering, maar ook van handhaving. Zoals we vaker zien met digitale technologieën, houden ook blockchain toepassingen zich niet noodzakelijk aan landsgrenzen en kan dit de nodige problemen oproepen bij het handhaven van de wet. Dit zou met name kunnen gaan spelen bij permissionless blockchains, waar geen centrale beheerder bestaat die de gegevens van alle op de toepassing aangesloten computers kan verwijderen. Handhaving zou dan moeten plaatsvinden jegens (mogelijk vele) actoren waarvan de identiteit vaak onbekend is en die zich in het buitenland kunnen bevinden. Vanuit de AP zijn geen feiten of omstandigheden aangedragen die nopen tot prioritaire aandacht voor dit onderwerp. Het kabinet blijft alert en neemt de suggestie over om indien nodig Europese c.q. internationale samenwerking te zoeken. Nederland heeft zich in het kader van de evaluatie van de AVG al ingezet om ook te evalueren of het beschermingsniveau dat de AVG bij vaststelling beoogde te bieden bij toepassing van blockchain technologieën in voldoende mate geborgd is, of dat er wellicht aanvullende waarborgen geboden moeten worden.⁵

Technologie en de wet

Het kabinet begrijpt dat nieuwe technologieën juridische vragen kunnen opwerpen. Deze worden door marktpartijen, burgers of maatschappelijke organisaties gearticuleerd, of openbaren zich in samenwerkingsverbanden zoals met de Dutch Blockchain Coalitie of het Odyssey project.⁶ Ook hebben marktpartijen in de financiële sector de mogelijkheid om met vragen te komen. De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) hebben twee gezamenlijke programma's ingericht om innovatie in de financiële sector te faciliteren: de InnovationHub die een vraagbaak functie heeft en Maatwerk voor Innovatie, dat de functie van «regulatory sandbox» heeft.

Dat er een juridische vraag ligt, betekent uiteraard nog niet dat aanpassing van wetgeving aan de orde is. Eerst is onderzoek nodig en dan blijkt ook vaak dat er al veel kan en geregeld is. Ook het rapport getuigt daarvan, het laat bijvoorbeeld zien dat het verbintenissenrecht en het bewijsrecht in het algemeen flexibel genoeg zijn om blockchain in te passen. Met betrekking tot de financiële sector is het wetsvoorstel ter implementatie van de gewijzigde vierde anti-witwasrichtlijn (AMLD5) aan de Tweede Kamer aangeboden en wordt onderzocht of op bepaalde punten nieuwe regels nodig zijn.⁷

Blockchain en gegevensbescherming

In het onderzoek wordt gewezen op de spanningen tussen het gebruik van blockchaintechnologie en gegevensbescherming. Deze spanningen zijn terug te voeren op de decentralisatie die met blockchains wordt nagestreefd. Dit streven leidt er onder meer toe dat een administratie op meerdere computers wordt gerepliceerd. Eenmaal toegevoegde gegevens worden in beginsel niet meer uit deze administratie verwijderd, omdat ze een rol spelen in de beveiliging daarvan.

⁵ Zie verder onder het kopje: «Blockchain en gegevensbescherming».

⁶ Zie nader over deze samenwerkingsverbanden: «Samenwerken aan maatschappelijk nuttige, veilige en verantwoorde toepassingen».

⁷ Zie nader onder: «Uitgifte van tokens en financieel toezicht».

De vraag is hoe dit soort zaken zich verhouden tot privacywetgeving, waaronder de AVG. Zogenaamde permissionless blockchains baren in dit opzicht de meeste zorgen, omdat het hier onduidelijk is wie kan worden aangemerkt als (mede)verwerkingsverantwoordelijke (en op wie dus de plichten van de AVG rusten, in het kader van een rechtmatige en transparante verwerking van persoonsgegevens).

Een belangrijk recht van betrokkenen is het recht op vergetelheid. Persoonsgegevens dienen verder in beginsel vernietigd te worden wanneer deze niet meer nodig zijn voor het doel waarvoor ze verzameld zijn (data minimalisatie). Het wissen van gegevens lijkt op permissioned blockchains al geen sinecure. Op permissionless blockchains lijkt het nagenoeg onmogelijk, omdat een effectieve uitoefening van het recht op vergetelheid hier afhankelijk is van een gecoördineerde actie van over mogelijk vele landen verspreide partijen, die elkaar veelal niet kennen en waartussen geen formele gezagsverhoudingen bestaan.⁸

Of een specifieke gegevensverwerking op een blockchain voldoet aan de eisen van de AVG, zal uiteindelijk van geval tot geval moeten worden beoordeeld. Er bestaan relevante verschillen tussen blockchaintoepassingen voor wat betreft de aard van de verwerkte gegevens, de plaats waar gegevens worden verwerkt (*on chain* dan wel *off chain*), de wijze waarop gegevens worden beveiligd, de wijze waarop de governance is ingericht, de grondslag voor gegevensverwerking etc. In dit verband wijst het kabinet ook op het op het beginsel van *privacy by design* en op de plicht om in voorkomende gevallen een gegevenbeschermingseffectbeoordeling (GEB) uit te voeren.

Met de AVG is beoogd technologie neutrale normen te creëren voor de verwerking van persoonsgegevens. Het onderzoek laat echter zien dat het onduidelijk is hoe een aantal van deze normen moeten worden geïnterpreteerd in het licht van blockchain toepassingen. De European Data Protection Board (EDPD, de koepel van Europese toezichthouders) is de eerst aangewezen om verduidelijking te bieden. In dit verband is verheugend dat blockchain één van de onderwerpen is van het werkprogramma 2019–2020 van de EDPD.

De techniek staat niet stil. Door middel van nieuwe cryptografische technieken, zoals Zero Knowledge proofs, kan een feit worden bewezen, zonder de achterliggende gegevens te onthullen. Zero Knowledge proofs worden beproefd in een pilot van het CJIB, die tot doel heeft burgers en overheden samen te laten werken bij het signaleren van betalingsonmacht. Door aan de burger verklaringen ter beschikking te stellen die – als de burger dat wil – gedeeld kunnen worden met anderen overheidsorganisaties zonder dat vertrouwelijke data op de blockchain wordt vastgelegd. Zoals hiervoor reeds aangegeven heeft Nederland zich ingezet om in het kader van de evaluatie van de AVG ook het onderwerp blockchain te adresseren.⁹

Uitgifte van tokens en financieel toezicht

Tokens kennen verschillende toepassingen (zoals virtuele valuta, effecten, recht om een online dienst te gebruiken etc.). Het rapport beveelt aan om de regelgeving en de uitoefening van het financieel toezicht op tokens (verder) te verduidelijken. Zoals de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) hebben aangegeven kan de uitgifte van crypto's en tokens in bepaalde gevallen onder de regels van financieel

⁸ Zoals de onderzoekers aangeven bestaat de mogelijkheid om persoonsgegevens «off chain» op te slaan. Ze staan dan dus niet op de blockchain zelf, waardoor ze kunnen worden gewist. Wel kan er «on chain» naar worden verwezen. Een en ander dient dan uiteraard nog steeds in overeenstemming met de AVG te gebeuren.

⁹ Zie onder: «Blockchain kan niet zonder het recht».

toezicht vallen.¹⁰ Dit is met name het geval als deze tokens kunnen worden aangeduid als effecten in de zin van de Wet op het financieel toezicht (Wft). In de Kamerbrief over de regulering van crypto's¹¹ heeft de Minister van Financiën aangekondigd om te onderzoeken of het effectenbegrip in de Wft aanpassing behoeft om ervoor te zorgen dat de uitgifte van tokens die neerkomen op effecten, hier zo veel mogelijk onder valt. Ook zal de Minister kijken naar mogelijke aanpassingen van de regels voor de kleinschalige verhandeling, en clearing en settlement van effecten om het gebruik van blockchaintechnologie voor deze doeleinden mogelijk te maken. Daarnaast vindt er op EU-niveau onderzoek plaats of de bestaande EU-regelgeving voor de financiële markten aangepast zouden moeten worden om crypto's en tokens beter te kunnen reguleren.¹² De AFM heeft op haar website verduidelijking gegeven over wanneer de uitgifte van tokens (Initial Coin Offering, Security Token Offering, of andere benamingen hiervoor) onder de Wft valt.¹³ Daarnaast is het wetsvoorstel ter implementatie van de gewijzigde vierde anti-witwasrichtlijn (AMLD5) aan de Tweede Kamer aangeboden.¹⁴ Met dit wetsvoorstel wordt geregeld dat aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta en aanbieders van bewaarportemonnees onder de reikwijdte van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) komen te vallen. Dit betekent onder meer dat deze partijen cliëntenonderzoek moeten verrichten, transacties moeten monitoren en ongebruikelijke transacties moeten melden bij de Financial Intelligence Unit (FIU-Nederland). Partijen die vragen hebben over (de reikwijdte) van toezicht bij het aanbieden van (mogelijke) financiële diensten kunnen zich melden bij de InnovationHub, het gezamenlijke initiatief van de AFM en DNB.¹⁵ Bij de InnovationHub komen met enige regelmaat vragen binnen over de bestaande regels ten aanzien van crypto's en tokens.¹⁶

Goederenrechtelijke status van tokens

De onderzoekers achten het niet nodig de goederenrechtelijke status van tokens te regelen (uit het onderzoek blijkt dat bepaalde tokens zoals bitcoins vatbaar zijn voor beslag en executie), maar geven in overweging dit wel te doen in Europees/internationaal verband. Het kabinet blijft de ontwikkelingen volgen, ook wat betreft beslag en executie, en zal waar nodig en mogelijk in actie komen.¹⁷

Buitencontractuele aansprakelijkheid

De onderzoekers geven aan dat bij blockchains de normale regels van buitencontractuele aansprakelijkheid gelden. De onderzoekers wijzen verder op de bijzondere regeling die, afhankelijk van de precieze omstandigheden, kan gelden voor «diensten van de informatiemaatschappij». De onderzoekers bevelen aan om te verduidelijken wanneer daar sprake van is. Het kabinet merkt hierover op dat dit een begrip is uit het Unierecht (de

¹⁰ Zie het advies van AFM en DNB aan de Minister van Financiën over de regulering van crypto's; Bijlage bij Kamerstuk 32 013, nr. 201

¹¹ Kamerstuk 32 013, nr. 201.

¹² Zie bijvoorbeeld het advies van ESMA aan de Europese Commissie: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

¹³ <https://www.afm.nl/nl-nl/professionals/onderwerpen/ico>.

¹⁴ Kamerstuk 35 245, nr. 2.

¹⁵ <https://www.dnb.nl/toezichtprofessioneel/innovationhub/index.jsp> en <https://www.afm.nl/nl-nl/professionals/onderwerpen/innovation-hub>.

¹⁶ Zie het rapport Continu in dialoog, raadpleegbaar via: https://www.dnb.nl/binaries/Continu%20in%20Dialoog_tcm46-385301.pdf.

¹⁷ Zoals hiervoor aangegeven (onder: «Uitgifte van tokens en financieel toezicht») vindt op EU-niveau al onderzoek plaats naar de bestaande EU-regelgeving voor financiële markten in verband met crypto's en tokens.

zogenaamde e-commerce richtlijn (2000/31/EG) dat autonoom wordt uitgelegd door het Hof van Justitie van de EU. Genoemde richtlijn is in Nederland geïmplementeerd in het BW en in het Wetboek van Strafrecht. Voor zover sprake is van een dienst van de informatiemaatschappij gelden op basis van art. 3:15d BW verschillende informatieverplichtingen voor de dienstverlener, zoals bijvoorbeeld het informeren van gebruikers over zijn identiteit en adres van vestiging. Het begrip speelt ook een rol in de artikelen 6:196b en 6:196c BW (beperking van aansprakelijkheid bij «mere conduit», caching en hosting). Op dit moment is niet zeker of bijvoorbeeld een node in een blockchain een geslaagd beroep op deze bepaling kan doen. Wanneer de rechter zou oordelen dat dat niet het geval is, zou hij overigens nog steeds kunnen bezien hoe ver zijn aansprakelijkheid reikt, gelet op zijn rol in het geheel. De onderzoekers geven aan dat meer duidelijkheid over aansprakelijkheid gewenst kan zijn en dat nadere regels vooral effectief zijn als in internationaal verband wordt opgetrokken.¹⁸ Belangrijk is dat meer kennis wordt vergaard. Met dat doel is Nederland vertegenwoordigd in het International Association of Trusted Blockchain Applications (INATBA). INATBA biedt blockchain-ontwikkelaars en -gebruikers een wereldwijd forum voor interactie met regelgevers en beleidsmakers, waar ook gesproken kan worden over zaken als aansprakelijkheid.¹⁹

Internationaal privaatrecht

Bij een geschil rondom een blockchain kan de vraag rijzen welk nationaal recht van toepassing is en welke nationale rechter bevoegd is. Een permissionless blockchain is slechts een middel dat niet in rechte kan worden betrokken. Een procedure kan zich bijvoorbeeld wel richten op de partij die bij de uitvoering van een overeenkomst blockchain toepast (bijv. «betaling» met crypto's of levering van een token waarmee een dienst kan worden gebruikt). Denkbaar is ook dat een natuurlijke persoon of een rechtspersoon een onrechtmatige daad pleegt op een blockchain, bijvoorbeeld door daarop illegale informatie te plaatsen. De vraag welk recht van toepassing is en welke rechter bevoegd is in internationale geschillen wordt in beginsel beantwoord door verdragen en EU-regelgeving. Bij gebreke daarvan geldt het nationale internationaal privaatrecht zoals neergelegd in het Wetboek van Burgerlijke Rechtsvordering en Boek 10 van het Burgerlijk Wetboek. De onderzoekers geven aan dat deze «standaard regels» altijd leiden tot een bevoegde rechter en een toepasselijk recht, maar dat in bepaalde gevallen relatief ondergeschikte fysieke aanknopingspunten de doorslag kunnen geven, omdat de blockchain virtueel is. Onder omstandigheden kunnen partijen zelf afspreken welk recht van toepassing (rechtskeuze) is c.q. welke rechter bevoegd is (forumkeuze). Partijen die vooraf zekerheid willen kunnen dus – binnen bepaalde kaders – een rechtskeuze en/of een forumkeuze overeenkomen. Het kabinet blijft ook hier de ontwikkelingen volgen. Mocht op enig moment aanpassing van de regels noodzakelijk blijken, dan zal dit in Europees/internationaal verband moeten worden opgepakt.²⁰

¹⁸ Zie m.b.t. de aansprakelijkheid van aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta en aanbieders van bewaarportemonnees: «Uitgifte van tokens en financieel toezicht».

¹⁹ Het onderwerp aansprakelijkheid is recent ook aangesneden in het rapport «Legal and Regulatory Framework of Blockchains and Smart Contracts» van de EU Blockchain Observatory. Zie https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf.

²⁰ Ook het internationaal privaatrecht is een onderwerp in het in de vorige noot genoemde rapport van de EU Blockchain Observatory.

Blockchain en vertrouwen

Naar een genuanceerd beeld van de meerwaarde van blockchain

Een gebruikelijk patroon bij de opkomst van nieuwe technologieën is dat de verwachtingen hooggespannen raken en dan allengs realistischer worden. Voor blockchain geldt dat ook. Ook overheidsorganisaties dragen bij aan betere kennis over de mogelijkheden en onmogelijkheden, door middel van onderzoeken, pilots en dergelijke; en door kennisuitwisseling hierover. Het lijkt erop dat met blockchain technologie in bepaalde gevallen een stukje van de «vertrouwenspuzzel» kan worden ingevuld. Dat wordt nader onderzocht, onder meer in het verband van de Dutch Blockchain Coalition.²¹

Naar het oordeel van het kabinet gaat het nooit om technologie alleen. Of op een technologie kan worden vertrouwd, hangt ook samen met een goede governance. De onderzoekers maken terecht het punt dat zelfs als de code publiek gemaakt is, deze alleen door experts kan worden beoordeeld.²² En zoals de onderzoekers ook aangeven, zullen blockchain toepassingen voor gegevens «van buiten»²³ moeten leunen op zogenaamde oracles, waarop dan wel moet kunnen worden vertrouwd. De onderzoekers wijzen in dit verband terecht op de voordelen van een door de wet voorgeschreven openbaar register (zoals in het onderzoek het Scheepsregister). Juist om te voorkomen dat bedrijven en burgers steeds zelf moeten uitzoeken of een bepaald gegeven klopt, kent Nederland diverse registers, waarop wordt vertrouwd in het rechtsverkeer. Deze registraties geven zekerheid en verlagen de transactiekosten.

Zoals de onderzoekers aangeven is er een belangrijke rol weggelegd voor de notaris bij het letten op zaken als de wilsvorming van partijen, de identiteit van partijen, de juistheid van de akte in het licht van de bedoeling van partijen, het voorkomen van onrechtmatige benadeling van partijen en de controle op de herkomst van gelden.

Volgens de onderzoekers moeten in toekomstige wet- en regelgeving expliciete keuzes worden gemaakt over welke elementen van een bestaand (overheids)proces in een blockchain vervat gaan worden en welke niet. Het kabinet streeft echter – waar mogelijk en verantwoord – juist naar techniekneutrale normen.²⁴

Kansen voor de notaris

Blockchain biedt volgens de KNB aan de beroepsgroep een kans om de praktijk op een innovatieve, toekomstbestendige manier te verrichten en de klantenkring beter van dienst te kunnen zijn. De KNB is daarom reeds vanaf de start in 2016 lid van de Dutch Blockchain Coalition.

De KNB heeft de afgelopen tijd geïnvesteerd in de ontwikkeling van zgn. innovatielabs. In één van de proefprojecten (het «Notary Privacy Ecosystem») is geanalyseerd in hoeverre in de toekomst een aantal klassieke handelingen van de notaris via onder andere blockchaintechnologie zouden kunnen worden toegepast. Het notariaat experimenteert ook op individuele kantoorbasis met blockchain technologieën.

²¹ Zie verder onder: «Samenwerken aan maatschappelijk nuttige, veilige en verantwoorde toepassingen»

²² Zie ook de Kamerbrief «Transparantie van algoritmes in gebruik bij de overheid», waarin onderscheid wordt gemaakt tussen technische transparantie en uitlegbaarheid. (Kamerstukken 26 643 en 32 761, nr. 570), p. 3–4.

²³ Zogenaamde *off chain* gegevens, zoals bijvoorbeeld de aflevering van een bestelde zaak.

²⁴ Zie nader: «Kabinetsreactie inzake advies Raad van State over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen» Kamerstuk 34 972, nr. 2, p. 7.

Het «Notary Privacy Ecosystem»

In het Notary Privacy Ecosystem kunnen partijen efficiënt, controleerbaar en veilig transacties met elkaar afwikkelen. De combinatie met digitale identificatiemiddelen zoals NotarisID maakt dat voor het onweerlegbaar vastleggen van gevalideerde informatie een bijzonder hoge betrouwbaarheidsgraad wordt bereikt. Wanneer bijvoorbeeld een samenlevingscontract is opgemaakt, kan het definitieve document worden omgezet naar een unieke digitale code (een zogenaamde hash) en in combinatie met een tijdstempel worden geregistreerd in de blockchain, zodat zekerheid bestaat dat dit het originele document is. Als een cliënt bijvoorbeeld gegevens verstrekt voor een hypotheek dan hoeft de geldverstrekker (bank) die gegevens niet meer te controleren, omdat via de beveiligde blockchain door de bank na te gaan is of ze zijn verstrekt door de notaris. Deelnemers kunnen informatie ontvangen via hun postbus en documenten veilig opslaan in hun digitale kluis. Onderlinge communicatie wordt mogelijk gemaakt door een chatfunctionaliteit, eventueel aangevuld met video. Adviseurs zoals de notaris of een bemiddelaar kunnen aan een gesprek deelnemen indien gewenst. Het complete gesprek komt in digitale vorm beschikbaar. Deelnemers kunnen het nadien in hun kluis opslaan en vervolgens wordt het via een hash in de blockchain vastgelegd. Het Notary Privacy Ecosystem staat onder notarieel toezicht. De notaris zelf staat uiteraard onder toezicht van de tuchtrechter en het Bureau Financieel Toezicht. Continuïteit, betrouwbaarheid en de toegankelijkheid van vastgelegde gegevens zijn daarmee gegarandeerd.

Rechtszekerheid is een van de kernwaarden van het notariaat, en de blockchain kan daarbij behulpzaam zijn, in de zin van het verkorten en vereenvoudigen van traditionele processen, en het beter ondersteunen van het notariële werk. Juist de combinatie van blockchaintechnologie met een controle door een onafhankelijke functionaris geeft het nodige vertrouwen in het handelsverkeer.

Samenwerken aan maatschappelijk nuttige, veilige en verantwoorde toepassingen

Het kabinet wil door middel van samenwerking de nog jonge blockchain technologie op een maatschappelijk nuttige, veilige en verantwoorde manier verder brengen. De «Dutch Blockchain Coalition» (DBC) is geïnitieerd door het Ministerie van Economische Zaken en Klimaat (EZK) en is een publiek-privaat samenwerkingsverband van partners uit de financiële dienstverlening (banken, verzekeringen), de sectoren logistiek, energie, veiligheid en ICT, ministeries, de kenniswereld, toezichtspartijen als de Autoriteit Financiële Markten (AFM)) en de Koninklijke Notariële Beroepsorganisatie (KNB) en organisaties als de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), Nederlandse Organisatie voor Wetenschappelijk Onderzoek Nederlandse Organisatie voor Wetenschappelijk Onderzoek Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en het Electronic Commerce Platform/Platform voor de Informatiesamenleving. Met het doel de blockchain technologie zichzelf te laten bewijzen in concrete toepassingen, zijn pilots gestart op de gebieden subsidieverlening, logistiek, pensioenen, diploma's en certificaten en Self Sovereign Identity.²⁵ Daarnaast is een Cyber security framework ontwikkeld welke helpt met het veilig toepassen van blockchaintechnologie. Verder nemen verschillende overheidsorganisaties al enkele jaren deel aan het Odyssey programma (voorheen Dutchchain). Het Odyssey Open

²⁵ Meer informatie hierover is te vinden op: <https://dutchblockchaincoalition.org/>.

Innovation Program verbindt overheids-, bedrijfs- en non-profitpartners om gezamenlijk, op basis van blockchain en AI, complexe uitdagingen op te lossen. Daarnaast heeft het Ministerie van EZK in samenwerking met de provincie Groningen en de gemeente Rotterdam via de SBIR («Small Business Innovation Research») getrapte competities voor bedrijven georganiseerd, waarbij prototypes zijn ontwikkeld die een oplossing bieden voor maatschappelijke vragen.

Op Europees vlak heeft de Staatssecretaris van EZK in 2018 tezamen met 27 andere (lid)staten een convenant getekend om samen te werken bij de totstandbrenging van een Europese infrastructuur voor blockchain diensten (EBSI) die de levering van grensoverschrijdende digitale openbare diensten zal ondersteunen, met de hoogste normen op het gebied van veiligheid en privacy. Deze samenwerking, het European Blockchain Partnerschip, is een gezamenlijk streven van de publieke sector met als doel de vruchten te plukken van blockchain.

Tot slot

Zoals het onderzoeksrapport laat zien, kan een nieuwe technologie als blockchain tot juridische vragen en onzekerheden leiden en tot nieuwe kansen en risico's. Het onderwerp is nog volop in beweging. Reden voor het kabinet om de ontwikkelingen nauwgezet te volgen en waar nodig en mogelijk actie te ondernemen. Samen met bedrijven, kennisinstellingen en andere partners wordt nationaal en internationaal ingezet op economisch en maatschappelijk nuttige, veilige en verantwoorde toepassingen.

De Minister voor Rechtsbescherming,
S. Dekker