

Tilburg University

Besturen met blockchain in de digitale netwerksamenleving

van Oirsouw, Charlotte; Goossens, Jurgen

Published in:
Nederlands Tijdschrift voor Bestuursrecht

Publication date:
2022

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

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
van Oirsouw, C., & Goossens, J. (2022). Besturen met blockchain in de digitale netwerksamenleving: Het borgen en operationaliseren van transparantie en accountability. *Nederlands Tijdschrift voor Bestuursrecht*, 2022(2), 78-90. Article NTB 2022/39.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Besturen met blockchain in de digitale netwerksamenleving: het borgen en operationaliseren van transparantie en accountability

NTB 2022/39

1. Inleiding

Het uitvoeren van publieke taken en het uitoefenen van publiek gezag digitaliseren in toenemende mate en in hoog tempo. Algoritmische, geautomatiseerde besluitvorming krijgt dan ook de voorbije jaren steeds meer aandacht in bestuursrechtelijk Nederland. Daarnaast experimenteert en innoveert de overheid ook met nieuwe, opkomende technologieën, zogenaamde *emerging technologies*. Denk bijvoorbeeld aan het gebruik van kunstmatige intelligentie, Internet of Things en blockchain. Met betrekking tot blockchaintechnologie werden in 2018 minstens 36 blockchain use cases ontwikkeld binnen de Nederlandse overheid en waarschijnlijk zijn op basis van een schatting ondertussen al meer dan 200 blockchain use cases opgezet door de Nederlandse overheid in de voorbije vijf jaar.² Desondanks groeien deze use cases van de overheid vooralsnog zelden uit tot voldragen, operationele blockchainteepassingen. De interesse blijft echter groot en het experimenteren met blockchain als voorbeeld van de digitalisering van het besturen in netwerken verdient dan ook onze aandacht als beoefenaars van het publiekrecht.

Deze bijdrage gaat in op de inzet van blockchain (gedistribueerde technologie) en smart contracts ('als a, dan b'-algoritmen) en de impact daarvan op het borgen en operationaliseren van de kernwaarden transparantie en 'accountability'³ bij het uitoefenen van overheidsgezag. Deze bijdrage beoogt voornamelijk aan te tonen dat (kwalitatief) onderzoek noodzakelijk is naar het borgen en operationaliseren van transparantie en accountability in een concrete

context waar de overheid blockchain beoogt in te zetten. Onderzoek naar de concrete context van een blockchainteopassing is namelijk van belang om wetenschappelijk onderbouwde uitspraken te kunnen doen of het recht niet alleen in theorie maar ook in praktijk voldoende waarborgen biedt om transparantie en accountability te borgen.

Aanleiding voor deze bijdrage is het exploratief onderzoek in het kader van een NWO-MVI project⁴ dat we momenteel aan het uitvoeren zijn naar een concrete casestudie, namelijk de blockchainpilot 'de Rode Knop'. We hebben de Rode Knop geïdentificeerd als een *exemplary case*⁵ die de bestudering van elementen mogelijk maakt die ook in andere blockchainpilots van de overheid kunnen voorkomen. Daarnaast is de Rode Knop volgens ons ook exemplarisch voor een context van besturen in de digitale netwerksamenleving. Het CJIB beoogt met de blockchain use case de Rode Knop blockchain in te zetten – onder meer in samenwerking met de gemeenten Den Haag en Eindhoven – om tijdelijk schuldenrust te creëren bij betalingsonmacht door problematische schulden wanneer de burger een gemeentelijk schuldhulpverleningstraject aangaat. Tot nu toe hebben we al een eerste ronde van verkennende interviews met zeven spilfiguren achter de rug. Er volgt nog een tweede ronde van ca. dertig interviews. Daarnaast hebben we allerhande relevante documenten verzameld, zowel publiek toegankelijke documenten als grijze documenten, zoals verschillende versies van het Rode Knop draaiboek dat constant in evolutie is. Ten slotte hebben we op basis van veldonderzoek in het voorbije jaar meer dan vijftig observaties uitgevoerd tijdens interne (digitale) projectmeetings over de Rode Knop.⁶ We volgden in dit kader ook een recente praktijktoets op over de Rode Knop die in het najaar van 2021 plaatsvond met burgers in de gemeenten Den Haag en Eindhoven. Op een later tijdstip publiceren we zeker nog een diepgaande analyse van deze casestudie.

Op basis van een eerste analyse van dit lopend onderzoek blijkt alvast dat op bepaalde vlakken geen algemene conclusies kunnen worden getrokken op basis van een louter abstracte analyse, aangezien de beantwoording van sommige vragen over transparantie en accountability afhankelijk blijkt te zijn van de concrete context. In dit geval gaat het bijvoorbeeld om een schuldhulpverleningstraject met

1 Charlotte van Oirsouw is promovenda en Jurgen Goossens is universitair hoofddocent staats- en bestuursrecht; beide zijn verbonden aan het *Department of Public Law & Governance* van Tilburg University. Auteurs maken deel uit van het interdisciplinaire CHAIN-onderzoeksteam dat onderzoek voert binnen het NWO-MVI project 'De rol en verantwoordelijkheden van publieke actoren in gedistribueerde netwerken. Transparantie, vertrouwen en legitimiteit by design' (juni 2020-november 2024). Het onderzoek voor deze bijdrage is dan ook gefinancierd door NWO als onderdeel van het programma 'Verantwoord Innoveren. Ontwerpen voor publieke waarden in een digitale wereld.' De auteurs wensen ook uitdrukkelijk CHAIN-collega's Esther Keymolen en Gert Meyers te bedanken voor hun rol in het kwalitatief onderzoek.

2 M. Pomp & R. Verhaert, *Blockchain in de praktijk. Meer dan 50 use cases van de overheid in Nederland en België*, Den Haag: Sdu 2018; Zie ook: S. Berns, 'Blockchain – Een praktische handleiding voor overheden', VNG Realisatie rapport, 2^e editie April 2019 https://www.vngrealisatie.nl/sites/default/files/2019-04/863%20VNG%20Blockchain_compleet_editie2.pdf, p. 7; D. Allesie, M. Sobolewski & L. Vaccari, *Blockchain for digital government*, Luxembourg: Publications Office of the European Union 2019.

3 Er is geopteerd om de Engelstalige term 'accountability' aan te houden, omdat er geen een-op-een Nederlandse vertaling is hiervan. Nederlandse woorden die nauw aansluiten, zijn 'rekenschap' of 'verantwoording'.

4 Zie de projectwebsite: <https://chainresearch.eu/>.

5 B. Flyvbjerg, 'Case Study', in: N.K. Denzin & L.Y.S. (red.), *The SAGE Handbook of Qualitative Research*, London: Sage 2011, p. 301-317; P. Swanborn, *Case Study Research. What, why and how?*, London: Sage Publications 2010.

6 Gert Meyers en Charlotte van Oirsouw observeerden het voorbije jaar de projectmeetings van de casestudie en voerden de eerste ronde van interviews uit.

een keukentafelgesprek of de concrete designkeuzes inzake de blockchain-technologie. Bovendien heeft de bestudering van de Rode Knop vragen opgeroepen die bij een eerste abstracte analyse nog niet waren gerez. Daarnaast kunnen we door naar de context te kijken ook inzicht krijgen in het perspectief van betrokken actoren, niet in het minst de burger met een schuldenproblematiek: hoeveel belang hechten betrokken actoren bijvoorbeeld aan transparantie en accountability en is dit afhankelijk van de concrete situatie, in dit geval een situatie waarbij burgers in een zeer precaire situatie betrokken zijn? Onderzoek naar de concrete praktijk kan dan ook onder meer inzicht verschaffen in hoeveel en op welke wijze de burger uitleg krijgt of wenst te krijgen over de inzet van de blockchain-technologie. Onderzoek naar de concrete praktijk kan ten slotte ook inzicht verschaffen in mogelijke discrepanties tussen de mate van transparantie en accountability die wet- en regelgeving opleggen en de concrete realisatie ervan in de praktijk.

De bijdrage is als volgt opgebouwd. Vooreerst kadert deze bijdrage blockchain binnen een bredere context (paragraaf 2). Sinds een aantal decennia vult de opkomst van *network governance*, namelijk besturen op basis van meer horizontale vormen van samenwerking en sturing bij bevoegdheidsuitoefening in netwerken van private en publieke partijen, de traditioneel verticale, eenzijdige uitoefening van overheidsgezag immers aan als wijze van besturen.⁷ Daarnaast zet de overheid in toenemende mate algoritmen in ter ondersteuning of volledige automatisering van het besluitvormingsproces. Deze bijdrage kadert verkenningen inzake de inzet van blockchain-gebaseerde smart contracts dan ook binnen een bredere evolutie, namelijk *'digital network governance'*.

In een context van – in dit geval blockchain-gebaseerde – *digital network governance* bestaan uitdagingen op het vlak van transparantie en accountability, twee publieke waarden die cruciaal zijn voor een goed functionerende democratische rechtsstaat (paragraaf 3).⁸ Het huidige wettelijke kader bevat concrete regelgeving en mechanismen om deze waarden te borgen. Het gaat dan onder meer om de algemene beginselen van behoorlijk bestuur en concrete rechtsregels uit de Awb, de AVG, en het wettelijke kader inzake de toegang tot en de openbaarheid van overheidsinformatie, zoals voornamelijk geregeld in de Wet openbaarheid van bestuur (Wob) die op 1 mei 2022 zal worden vervangen door de Wet open overheid (Woo), de Archiefwet en de Wet hergebruik overheidsinformatie (Who). De operationalisering ervan in de praktijk blijft evenwel een uitdaging en roept talrijke vragen op, zeker in een digitaliserende context waar

al snel sprake is van een zogenaamde 'black box'.⁹ Er kan in dat geval sprake zijn van een discrepantie tussen *the law in the books* en *the law in practice*.

Aangezien de context in dit geval een situatie is waarbij de overheid blockchain en smart contracts beoogt in te zetten, gaan we in deze bijdrage vervolgens kort in op wat blockchain en smart contract technologie inhouden (paragraaf 4). Vervolgens voegen we zelf de daad bij het woord en kijken we naar de concrete blockchainapplicatie 'De Rode Knop', die het CJIB in samenwerking met enkele andere actoren in het netwerk beoogt in te zetten in het geval van betalingsonmacht en een gemeentelijk schuldhulpverlenings-traject (paragraaf 5) en identificeren we enkele vragen op het vlak van transparantie en accountability die in deze fase van ons onderzoek al zijn gerez. Vervolgens gaan we dieper in op drie redenen waarom onderzoek naar het borgen van transparantie en accountability het bestuderen van praktische toepassingen en concrete context behoeft wanneer overheden innoveren met blockchain (paragraaf 6). De bijdrage sluit af met het onderstrepen van het belang van een *'transparency and accountability by design'*-benadering (paragraaf 7).

2. Bredere evolutie: de opkomst van digital network governance

De uitoefening van overheidsgezag gebeurt traditioneel voornamelijk aan de hand van verticale, eenzijdige gezagsuitoefening. De voorbije decennia is deze dominante vorm van publieke gezagsuitoefening aangevuld met vormen van *network governance*, namelijk meer horizontale vormen van samenwerking en sturing in netwerken van private en publieke partijen.¹⁰ Daarenboven worden algoritmen in toenemende mate ingezet ter ondersteuning of volledige automatisering van het besluitvormingsproces. De combinatie van deze twee evoluties leidt tot het ontstaan van *'digital network governance'*, wat in de praktijk tot uitdagingen leidt op het vlak van transparantie en accountability in deze digitale netwerken.

Laten we eerst even stilstaan bij besturen in netwerken. Een *governance network* kan worden gekarakteriseerd als een netwerk van onderling afhankelijke, maar operationeel autonome publieke en/of private actoren die met elkaar samenwerken om publieke taken uit te voeren.¹¹ Binnen deze netwerken is er in beginsel geen sprake van een duidelijke hiërarchie met betrekking tot de bevoegdheidsuitoefening en zijn de relaties eerder horizontaal.¹² Bovendien hebben

7 L. van den Berge, 'Rethinking the Public-Private Law Divide in the Age of Governmentality and Network Governance – A Comparative Analysis of French, English and Dutch Case Law', *European Journal of Comparative Law and Governance* 2018, p. 120-143, p. 121 en p. 143; M. van der Steen, J. Scherpenisse & M. van Twist, 'Sedimentatie in sturing', Nederlandse School voor Openbaar Bestuur, rapport 2015, p. 20.

8 C. Harlow, 'Accountability and Constitutional Law', in: M. Bovens, T. Schillemans & R.E. Goodin (red.), *The Oxford Handbook of Public Accountability*, Oxford: Oxford University Press 2014, p. 196-210, p. 199.

9 Zie F. Pasquale, *The Black Box Society*, Cambridge: Harvard University Press 2015.

10 L. van den Berge, 'Van government naar governance: besturen onder de radar van het bestuursrecht', *NTB* 2018/40.

11 Cfr. J. Torfing, 'Governance Networks', in: D. Levi-Faur (red.), *The Oxford Handbook of Governance*, Oxford: Oxford University Press 2014, p. 99-112, p. 101-102.

12 R. Keast, 'Network governance', in: C. Ansell & J. Torfing (red.), *Handbook on Theories of Governance*, Cheltenham: Edward Elgar Publishing 2016, p. 442-453, p. 443.

de individuele actoren in het netwerk beslissingsruimte met betrekking tot de keuzes die ze maken bij het uitoefenen van bevoegdheden.¹³ De uiteindelijke uitkomst van besturen in een *governance network* is bijgevolg eerder de som van verschillende interacties dan de consequentie van een welbepaalde actie van één actor. Daardoor is niet altijd makkelijk te achterhalen hoe precies tot een specifieke uitkomst van het netwerk wordt gekomen.¹⁴ *Governance networks* hebben vaak eerder een informele en ondoorzichtige aard,¹⁵ waarbij het lastig kan zijn om duidelijke verantwoordelijkheden voor actoren aan te wijzen.¹⁶ Bovendien leidt de hoge connectiviteit van private en publieke actoren tot een vervaging van de grens tussen publiek en privaat.¹⁷ Network governance leidt dus tot uitdagingen op het vlak van *transparantie van informatie* en *accountability van betrokken actoren* in het netwerk.

De tweede evolutie is de toegenomen inzet van algoritmen in besluitvormingsprocedures, wat leidt tot volledig of gedeeltelijk geautomatiseerde besluitvorming. Bij de inzet van algoritmen kunnen echter problemen optreden op het vlak van (een gebrek aan) transparantie en uitlegbaarheid, omdat rechtzoekenden het algoritme – in het geval van simpele, regel-gebaseerde algoritmen en *a fortiori* bij complexe, zelflerende algoritmen – als een *black box* kunnen ervaren.¹⁸ Op basis van de SyRI-zaak bij de rechtbank Den Haag¹⁹ en de AERIUS-zaken bij de Afdeling bestuursrechtspraak van de Raad van State (ABRvS)²⁰ is duidelijk geworden dat transparantie en uitlegbaarheid als middel om controleerbaarheid en accountability te verzekeren bij de inzet van algoritmen door de overheid niet altijd voldoende geborgd blijken. In de SyRI-zaak heeft de rechtbank de wetgeving die de inzet regelt van het Systeem Risico Indicatie (SyRI) voor de bestrijding van fraude bij o.m. uitkeringen, toeslagen en belastingen onrechtmatig bevonden en onverbindend verklaard

wegens strijdigheid met artikel 8 EVRM. Volgens de rechtbank was de wetgeving aangaande de inzet van SyRI immers onvoldoende inzichtelijk en controleerbaar.²¹

In AERIUS-I oordeelde de ABRvS dat de onderbouwing voor de gemaakte keuzes, aannames en beslissingen onvoldoende inzichtelijk is gemaakt betreffende de inzet van het softwaresysteem AERIUS dat besluitvorming ondersteunde in het kader van activiteiten die gepaard gaan met uitstoot van stikstof.²² De ABRvS merkte een recht op informatie en uitleg²³ aan als noodzakelijk om een gelijkwaardige procespositie (*equality of arms*) te waarborgen en oordeelde bijgevolg dat het bestreden besluit gebrekkig was. Volgens de ABRvS moeten burgers immers de juistheid van de gebruikte gegevens, gemaakte berekeningen en daarop gebaseerde aannames, keuzes en beslissingen kunnen begrijpen, controleren, zo nodig inhoudelijk kunnen betwisten en een weloverwogen keuze kunnen maken of zij de overheid ter verantwoording roepen en een beroep doen op rechtsbescherming. In AERIUS-II nuanceerde de ABRvS dat de minister uit eigen beweging op papier of anderszins waarneembaar inzichtelijk moet maken op welke maatwerkinvoergegevens een besluit is gebaseerd.²⁴ Deze plicht heeft echter geen betrekking op alle gegevens. Het is voldoende dat in of met het besluit duidelijk is gemaakt welke keuzen bij de invoer zijn gemaakt ten aanzien van de maatwerkinvoergegevens. Ten aanzien van de standaardinvoergegevens is er geen verplichting tot openbaarmaking uit eigen beweging. Wel geldt t.a.v. de niet verplicht openbaar te maken maatwerkinvoergegevens en de standaardinvoergegevens dat deze op verzoek beschikbaar moeten worden gesteld of moeten zijn in te zien.

Bovendien wordt het gebruik van algoritmen vaak gecombineerd met informatienetwerken waarin veel gegevens afkomstig van verschillende entiteiten gebruikt worden, waardoor het lastig kan zijn om verantwoordelijkheden toe te bedelen aan een concrete actor voor individuele aspecten van een algoritmisch proces of de uitkomsten ervan.²⁵ De inzet van digitalisering versterkt en verhoogt dus de al bestaande complexiteit en connectiviteit van actoren in een context van *network governance*, wat leidt tot een nog hogere mate van ondoorzichtigheid en accountabilityproblemen.

13 E.H. Klijn & J. Koppenjan, 'Complexity in governance network theory', *Complexity, Governance & Networks* 2014, afl. 1 (1), p. 61-70, p. 63.

14 E.H. Klijn & J. Koppenjan, 'Governance network theory: past, present and future', *Policy & Politics* 2012, afl. 40 (4), p. 587-606, p. 591.

15 Zie E. Sorensen, 'Democratic Network governance', in: C. Ansell & J. Torfing (red.), *Handbook on Theories of Governance*, Cheltenham: Edward Elgar Publishing 2016, p. 420.

16 Zie L. van den Berge, 'Bestuursrecht in de netwerksamenleving. Waarom de rechtsmacht van de bestuursrechter een materiële grondslag behoeft', *RM Themis* 2018, afl. 179 (4), p. 124-136; L. van den Berge, 'Macht en tegenmacht in de netwerksamenleving', in: T. Barkhuysen, A.T. Marseille, W. den Ouden, J.A.F. Peters & R.J.N. Schlössels (red.), *25 jaar Awb In eenheid en verscheidenheid*, Deventer: Wolters Kluwer 2019, p. 3-12; W. den Ouden, 'Toetsingsmaatstaven voor geschillen bij integrale besluitvorming: het perspectief van de private zorgaanbieder', *NTB* 2018/10, afl. 1.

17 L. van den Berge, 'Responsief Bestuursrecht', in: L. van den Berge, M.F. Vermaat, M. Lurks, N.A. van Renssen & S. van Heukelom-Verhage (red.), *Maatwerk in het Bestuursrecht Preadviezen* (VAR-reeks, nr. 164), Den Haag: Boom Juridisch 2020, p. 7-61, p. 41.

18 J. Goossens, K. Verslype & E. Tjong Tjin Tai, *Blockchain en smart contracts. Herijking van de rol van de vertrouwde tussenpersoon in de algoritmische samenleving*, Den Haag: Sdu 2020, p. 43.

19 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:1878. Zie ook: S. van Schendel, 'The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI', in: L. Reins (red.) *Regulating New Technologies in Uncertain Times Information Technology and Law Series*, Den Haag: T.M.C. Asser Press 2019.

20 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 en ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454.

21 Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:1878.

22 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, r.o. 14.4, *Computerrecht* 2017/256, m.nt. B.M.A. van Eck.

23 J. de Poorter & J. Goossens, 'Effectieve rechtsbescherming bij algoritmische besluitvorming in het bestuursrecht', *NJB* 2019/2777, p. 3307; ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259.

24 ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454, r.o. 23.3 en T. Barkhuysen & N. Jak, 'Afdeling bestuursrechtspraak verrijnt toetsingskader voor geautomatiseerde besluitvormingsprocessen (AERIUS)', *stibbeblog.nl*, 25 juli 2018, <http://www.stibbeblog.nl/all-blog-posts/environment-and-planning/afdeling-bestuursrechtspraak-verrijnt-toetsingskader-voor-geautomatiseerde-besluitvormingsprocessen-aerius/>.

25 S. Grimmelikhuijsen, 'Verantwoorde algoritmisering: zorgen waardengevoeligheid en transparantie voor meer vertrouwen in algoritmische besluitvorming?', *Bestuurskunde* 2020, afl. 29 (4), p. 18. Zie ook J. Cobbe, 'Confronting the Algorithmic State', *adminlawblog.org*, 24 september 2020, <https://adminlawblog.org/2020/09/24/jennifer-cobbe-confronting-the-algorithmic-state/>.

In het licht van innoveren met blockchain en smart contracts rijst vervolgens de vraag welke uitdagingen zich voordoen op het gebied van transparantie en accountability wanneer deze technologieën als instrumenten van digital network governance worden ingezet in het proces van uitoefening van publiek gezag.

3. Transparantie en accountability

Transparantie en accountability zijn essentieel voor de goede werking van een democratische rechtsstaat, waarbij beide belangrijk zijn voor de legitimiteit van overheidsop treden.²⁶ Het uiteindelijke effect van transparantie en accountability op legitimiteit is evenwel contextafhankelijk. Meer transparantie leidt bijvoorbeeld niet sowieso tot meer legitimiteit.²⁷ Hoewel het in de praktijk vooral de vraag is welke algemene beginselen van behoorlijk bestuur, specifieke regelgeving, relevante jurisprudentie en verantwoordingsmechanismen van toepassing zijn op het vlak van het borgen van transparantie en accountability, is het nuttig om eerst na te gaan wat er juist bedoeld wordt met deze twee begrippen. Het gaat immers om begrippen die vaak gebruikt worden, zeker ook in een context van digitalisering, maar die ook geregeld een uiteenlopende invulling krijgen.

Er zijn veel definities van 'transparantie' terug te vinden in de literatuur. De definitie van Grimmelikhuijsen in zijn dissertatie omvat volgens ons enkele fundamentele elementen die vaak terugkomen in invullingen en definities van het begrip transparantie. Transparantie kan volgens Grimmelikhuijsen als volgt omschreven worden: "*The availability of information about an organization or actor allowing external actors to monitor the internal workings or performance of that organization*".²⁸ Er zijn verschillende variabelen (bv. *wie*, *wat*, *waarom* en *wanneer*) die invloed hebben op wat een betekenisvolle invulling van transparantie is. Transparantie kan gaan over feiten en motiveringen achter besluiten ('*transparency in rationale*') of het proces van besluitvorming zelf ('*transparency in process*').²⁹ Bij algoritmische besluitvorming kan transparantie bijvoorbeeld gaan over de gebruikte gegevens, gemaakte berekeningen en daarop gebaseerde aannames, keuzes en beslissingen (*wat*).³⁰ Transparantie kan vervolgens bekeken worden vanuit verschillende perspectieven, bijvoorbeeld het perspectief van de burger, de overheid, de rechter, of een journalist (*wie*).³¹ Deze verschillende partijen kunnen behoefte hebben aan verschillende vormen van informatie in het licht van het doel dat ze met

de informatie willen bereiken (*waarom*). Denk bijvoorbeeld aan een belanghebbende die inzicht nodig heeft in de totstandkoming van algoritmische besluitvorming om een weloverwogen keuze te kunnen maken een beroep te doen op rechtsbescherming³² of een journalist die geïnteresseerd is in de werking van een algoritmisch systeem om hier een kritisch stuk over te kunnen schrijven ten behoeve van de publieke opinie. Daarnaast kan transparantie worden geboden op reactieve wijze, namelijk op aanvraag, zoals bij de passieve openbaarheid in art. 3 (1) Wob, of op proactieve wijze, zoals bij de actieve openbaarheid in art. 8 Wob (*wanneer*).³³ Bovendien kunnen ongewenste consequenties optreden, zoals een informatie-overload of een zogenaamde transparantieparadox "*high levels of visibility decrease transparency and produce opacity*".³⁴

Ook van accountability bestaan veel verschillende definities. De vaak geciteerde definitie van Bovens omvat enkele kernelementen die vaak terugkomen in verschillende invullingen en definities van het begrip accountability. Bovens omschrijft accountability als volgt: "*a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences*".³⁵ Essentiële vragen die met betrekking tot accountability gesteld kunnen worden zijn: *wie* is verantwoordelijk voor *wat*, *hoe* (op basis van welke standaarden) en *waarom*?³⁶ Ook bij accountability spelen dus verschillende variabelen een rol. Verder laat deze definitie duidelijk zien dat transparantie en accountability met elkaar zijn verbonden. De actor moet namelijk transparant zijn over zijn handelen, door zijn handelen uit te leggen en te rechtvaardigen, om 'accountable' of verantwoordelijk gehouden te kunnen worden door een andere entiteit. Aangezien die andere entiteit de informatie die de actor geeft, moet begrijpen, is dus ook het type en de vorm van informatie belangrijk om accountability betekenisvol te maken.³⁷

In een overheidscontext bestaan er verschillende soorten *public accountability*, zoals *political accountability*, *legal*

26 M. Considine & K. Ali Afzal, 'Legitimacy', in: M. Bevir (red.), *The Sage Handbook of Governance*, Londen: SAGE Publications Ltd 2011, p. 6 en 10; J. de Fine Licht & D. Naurin, 'Transparency', in: C. Ansell & J. Torfing (red.), *Handbook on Theories of Governance*, Cheltenham: Edward Elgar Publishing 2016, p. 217-224, p. 218.

27 J. de Fine Licht & D. Naurin 2016, p. 219.

28 S. Grimmelikhuijsen, *Transparency and Trust: An experimental study of online disclosure and trust in government* (diss. Utrecht University), Utrecht: Utrecht University 2012, p. 55.

29 J. de Fine Licht & D. Naurin 2016, p. 219.

30 Zoals zich bijvoorbeeld voordoet in ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259.

31 J. de Fine Licht & D. Naurin 2016, p. 217-224.

32 Zie ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 en ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454.

33 J. Fox, 'The uncertain relationship between transparency and accountability', *Development in Practice* 2007, afl. 17:4-5, p. 665.

34 C. Stohl, M. Stohl & P.M. Leonardi, 'Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age', *International Journal of Communication* 2016, afl. 10, p. 132.

35 M. Bovens, 'Analysing and assessing accountability', *European Law Journal* 2007, afl. 13 (4), p. 447-468. Deze definitie heeft haar weg gevonden in het debat over algorithmic accountability, zie: M. Wieringa, 'What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability', *Conference on Fairness, Accountability, and Transparency (FAT* '20)*, January 27-30, 2020, p. 2.

36 M. Bovens, T. Schillemans & R.E. Goodin, 'Public accountability', in: M. Bovens, T. Schillemans & R.E. Goodin (red.), *The Oxford Handbook of Public Accountability*, Oxford: Oxford University Press 2014, p. 10; M. Bovens, 'Two concepts of accountability: Accountability as a virtue and as a mechanism', *West European Politics* 2010, afl. 33 (5), p. 954.

37 J. Cobbe, M. Singh Ah Lee & J. Singh, 'Reviewable Automated Decision-Making: A framework for accountable systems', *ArXiv* 2021, 2102.04201v2 [cs.CY].

accountability of administrative accountability.³⁸ De mogelijke gevolgen gekoppeld aan *accountability* kunnen verschillend zijn, gaande van een geldelijke sanctie, een vernietiging van een besluit door de rechter tot reputatieschade door negatieve aandacht in de media.³⁹ Bovens' definitie van *accountability* laat ook zien dat het toewijzen van *accountability* en de effectieve werking van verantwoordingsmechanismen in een *governance network* lastig kunnen zijn, aangezien de relaties tussen actoren en de daarbij horende verantwoordelijkheden vaak onduidelijk zijn.⁴⁰ *Accountability* is dus, net als transparantie, sterk afhankelijk van de context. Hoewel vele wetenschappers schrijven over *accountability*, is er nog steeds relatief weinig systematisch, vergelijkend empirisch onderzoek dat verder gaat dan conceptuele en theoretische analyses.⁴¹

Op het vlak van de juridische borging en regulering van transparantie en *accountability* zijn verschillende beginselen en wet- en regelgeving van belang. Met betrekking tot wettelijke vereisten van *transparantie en uitlegbaarheid* moet onder meer rekening worden gehouden met de algemene beginselen van behoorlijk bestuur en de concrete rechtsregels uit de Awb die daaruit voortvloeien, zoals inzake:

- *de voorbereiding van besluiten*: zorgvuldigheidsbeginsel en vereiste van zorgvuldig feitenonderzoek (art. 3:2 Awb), hoorplicht (art. 4:7 en 4:8 e.v. Awb), vergewisplicht (art. 3:9 Awb);
- *de inhoud van besluiten*: verplichting tot belangenafweging (art. 3:4 lid 1 Awb);
- *de inrichting van besluiten*: formeel rechtszekerheidsbeginsel en vermelding van rechtsmiddelen (art. 3:45 Awb), het motiveringsbeginsel, kenbare motivering (art. 3:47 Awb) en deugdelijke motivering (art. 3:46 Awb);
- *de kennisgeving van besluiten*: bekendmaking en mededeling (art. 3:41 e.v. Awb).

Daarnaast moet ook gedacht worden aan het wettelijk kader inzake de toegang tot en de openbaarheid van overheidsinformatie, zoals voornamelijk geregeld in de Wob die op 1 mei 2022 zal worden vervangen door de Woo, de Archiefwet en de Who. Daarnaast dient bijvoorbeeld ook rekening te worden gehouden met onder meer de AVG als onderdeel van het gegevensbeschermingsrecht. Op basis van de jurisprudentie moet een bestuursorgaan in het geval van algoritmische besluitvorming bovendien de gemaakte keuzes, gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar maken op een passende wijze,

zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn.⁴²

Op het vlak van *accountability en verantwoordingsmechanismen* kan vooral worden gedacht aan het invoeren van rechtsbescherming door de burger tegen overheidsbesluiten op basis van de hoofdstukken 6 en 7 van de Awb over bezwaar, administratief beroep en beroep bij de bestuursrechter. Ook toezichthouders spelen een belangrijke rol inzake het afleggen van verantwoording, zoals de Autoriteit Persoonsgegevens. Op het vlak van politieke verantwoording (art. 42 Gw) speelt de ministeriële verantwoordelijkheid een cruciale rol, waarbij de ministers gezamenlijk en afzonderlijk verantwoording aan het parlement verschuldigd zijn voor hun doen en laten bij de vervulling van hun taken. Ingevolge de vertrouwensregel moet daarbij het kabinet of de minister aftreden wanneer dat/die niet langer het vertrouwen heeft van een meerderheid in de Staten-Generaal. Het parlement moet ten slotte finaal verantwoording afleggen aan de kiezer.

Indien een overheid overweegt om blockchain in te zetten, wordt dit systeem gebruikt om bepaalde activiteiten uit te voeren in een gedistribueerd netwerk dat bestaat uit verschillende individuen en entiteiten. Het recht richt zich in beginsel echter vooral op het optreden van natuurlijke personen of rechtspersonen, en niet per se op bijvoorbeeld het systeem zelf dat ten grondslag ligt aan een besluit.⁴³ Ongeacht bijvoorbeeld of al dan niet blockchaintechnologie is ingezet bij het voorbereiden of nemen van een besluit, zal het bestuursorgaan dus in beginsel verantwoordelijk zijn voor de uitoefening van publiek gezag, zal het moeten voldoen aan bovenstaande substantiële en procedurele regelgevende bepalingen inzake transparantie en uitlegbaarheid, en daar finaal verantwoordelijk voor kunnen worden gehouden. Alvorens in te gaan op een concrete blockchainpilot, lichten we in de volgende paragraaf eerst de basics toe van de onderliggende technologie, namelijk de inzet van blockchain als zogenaamde *Distributed Ledger Technologie* (DLT) in combinatie met smart contracts als simpele, regelgebaseerde algoritmen.⁴⁴

4. Blockchain en smart contracts in een notendop

4.1 Blockchaintechnologie

Blockchain is in essentie een gedistribueerde database, een digitaal gedistribueerd grootboek. Het is een *peer-to-peer* (P2P) netwerk waarbij de participanten of datapunten in het netwerk (de 'nodes') allemaal een eigen (gehele

38 M. Bovens 2007.

39 M. Bovens 2007, p. 452.

40 Y.I. Jarlsson-Vinkhuyen, 'Legitimacy', in: C. Ansell & J. Torfing (red.), *Handbook on Theories of Governance*, Cheltenham: Edward Elgar Publishing 2016, p. 200.

41 Zie in dezelfde zin: M. Bovens, 'Two concepts of accountability: Accountability as a virtue and as a mechanism', *West European Politics* 2010, afl. 33 (5), p. 947.

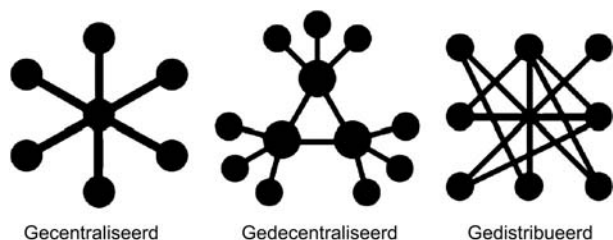
42 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (ov. 4.4).

43 J. Cobbe, 'Administrative law and the machines of government: Judicial review of automated public-sector decision-making', *Legal Studies* 2019, afl. 39 (4), p. 636-655; P. de Filippi, M. Mannan & W. Reijers, 'Blockchain as a confidence machine: the problem of trust & challenges of governance', *Technology in Society* 2020, afl. 62, 101284, p. 12.

44 Zie voor een uitgebreidere, toegankelijke uitleg: J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020.

of gedeeltelijke) identieke kopie van de database bezitten die continu wordt geüpdatet. Hierdoor is in beginsel de controle in het netwerk niet gecentraliseerd bij één centrale server of instantie, maar gedecentraliseerd of zelfs gedistribueerd onder de participanten in het netwerk (zie afbeelding 1). Er is dus in beginsel geen nood aan een intermediaire tussenpersoon of *trusted third party*, zoals een bank of notaris.⁴⁵

Afbeelding 1. Gecentraliseerd, gedecentraliseerd en gedistribueerde netwerk



Binnen dit netwerk worden 'transacties' uitgevoerd. In de blockchainwereld wordt een brede invulling gegeven aan de term transactie. Het gaat niet enkel om de overdracht van waarde (of beter gezegd: een representatie van waarde via een 'token'), maar ook om het registreren van gegevens of het uitvoeren van regels.⁴⁶ Deze transacties vinden plaats onder een pseudoniem (een 'adres'), waarbij elke deelnemer in het netwerk een transactie digitaal kan ondertekenen met een geheime cryptografische 'private sleutel', een soort lang wachtwoord als het ware, om zo te bewijzen dat je de eigenaar bent van het pseudoniem en de bijhorende 'publieke sleutel'.⁴⁷ De nieuwe transacties worden toegevoegd en gebundeld in blokken. Deze blokken worden aan elkaar gekoppeld door middel van unieke cryptografische links, 'hashes'. Deze hashes worden gegenereerd op basis van de inhoud van een blok, waarbij elk nieuw blok telkens verwijst naar het vorige blok. Zo ontstaat een *chain of blocks*, een ketting van blokken. Ieder individueel blok bevat naast de inhoudelijke data, namelijk de transacties van het blok, tevens een 'header' en 'tijdstempels'.⁴⁸ Deze tijdstempels worden door het netwerk collectief gevalideerd, zodat onomstotelijk vaststaat wanneer een transactie in de blockchain is opgenomen.⁴⁹

Blockchain betreft aldus een *append-only* database, waarbij alleen maar blokken met transacties kunnen worden

toegevoegd.⁵⁰ Zodra een transactie wordt toegevoegd, worden alle kopieën van de database in het netwerk geüpdatet. De uitvoering van de transacties vindt plaats door middel van een 'consensusmechanisme', namelijk een set regels waarmee overeenstemming tussen de nodes in het netwerk wordt bereikt over de geldigheid van een transactie.⁵¹ Deze manier van registratie van gegevens op de blockchain beoogt onveranderlijkheid (*immutability*) van data. Als gegevens eenmaal geregistreerd zijn op een blockchain, kunnen deze in beginsel niet meer aangepast of verwijderd worden. Dit zou immers een verandering in de hash teweegbrengen die echter gelinkt is aan de andere blokken. Hierdoor worden antedatering en de wijziging van de inhoud van de blokken uitgesloten, wat zorgt voor het behoud van data-integriteit. Aan de andere kant leidt het ook tot een voortdurende accumulatie van gegevens, wat belangrijke praktische en juridische uitdagingen kan opleveren voor een overheid, onder meer inzake de verplichtingen die uit de AVG voortvloeien bij de verwerking van persoonsgegevens of de zorgplicht van de overheid tot het vernietigen van de daarvoor in aanmerking komende archiefbescheiden ingevolge artikel 3 Archiefwet.⁵²

4.2 Aard van het netwerk en de gegevensopslag

Inzake de *toegang* tot het netwerk kan een blockchain publiek (openbaar of open), privaat (afgeschermd of gesloten) of hybride zijn.⁵³ Bij een publieke blockchain kan iedereen toegang krijgen tot het netwerk en kan iedereen de blockchain dus bekijken. Voorbeelden hiervan zijn Bitcoin en Ethereum. Bij een private blockchain, zoals Hyperledger, daarentegen is de toegang tot het netwerk beperkt tot een bepaalde groep actoren die is uitgenodigd of aan wie toegang is verschaft, al dan niet na het voldoen aan bepaalde voorwaarden. Meestal bepaalt een centrale actor die daartoe is geautoriseerd wie toegelaten wordt. Een hybride blockchain is dan weer een combinatie van beiden, waarbij sommige delen van het netwerk openbaar en andere afgeschermd zijn.

Met betrekking tot *participatierechten* kan een blockchain *permissionless* of *permissioned* zijn. Bij een *permissionless* blockchain kan iedereen die toegang heeft tot de blockchain er ook vrij in participeren. Iedereen is in beginsel gelijkwaardig en heeft gelijke rechten. Iedereen met toegang tot de blockchain kan volwaardig participeren in het netwerk, onder meer door het opzetten van smart contracts, het uitvoeren van transacties en het bijdragen aan het collectief veilig houden van de blockchain. Bij een *permissioned* blockchain kan echter enkel een selecte groep activiteiten uitvoeren. Rond het netwerk bevindt zich dan een

45 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020; F. Schemkes, E. Tjong Tjin Tai, M. Schellekens, W. Kaufmann, & R. Leenes, 'Blockchain en het recht: Een verkenning van de reguleringsbehoefte', Rapport in opdracht van het WDOC, Tilburg University 2019; B.J. Koops, 'Criteria for Normative Technology', *TILT Law & Technology Working Paper 2007*, No. 005/2007 version 0.4 & *Tilburg University Legal Studies Working Paper*, 2007 No. 007/2007; P. de Filippi & A. Wright, *Blockchain and the Law*, Cambridge: Harvard University Press 2018; NEN standaard ISO 22739.

46 Zie NEN standaard ISO 22739.

47 Deze digitale handtekeningen maken toepassing van asymmetrische cryptografie, ook wel publieke sleutelcryptografie genoemd.

48 Voor een voorbeeld van een blok, zie: <https://www.blockchain.com/btc/block/0000000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb>.

49 Zie bv. A. Schram, 'De bewijskracht van de 'blockchain timestamp' in auteursrechtelijke geschillen', *NJB* 2019/2779.

50 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 20.

51 NEN standaard ISO 22739, artikel 3.12 en 3.11.

52 Zie J. Goossens & C. van Oirsouw, 'Transparantie in de blockchain: een juridische verkenning van de toegang tot overheidsinformatie onder de Wob, de Woo en de Archiefwet bij de inzet van gedistribueerde technologie', rapport voor 'Strategische Verkenning Blockchain' van Rijkswaterstaat (ministerie van IenW), november 2021.

53 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 23-24.

controlelaag die autoriseert wie welke acties mag uitvoeren in het netwerk. Een dergelijke blockchain leent zich er in een overheidscontext doorgaans beter toe om dingen goed te regelen, bijvoorbeeld op het vlak van privacy en overeenstemming met overige wet- en regelgeving. In de praktijk zijn publieke blockchains meestal *permissionless* en zijn private blockchains doorgaans *permissioned*.

Ook betreffende de aard van de gegevensopslag moet een belangrijk onderscheid gemaakt worden. Wanneer gegevens op de blockchain zelf geregistreerd worden, noemt men dat *on-chain* registratie van gegevens. Wanneer gegevens in een database buiten de blockchain geregistreerd worden, is er sprake van *off-chain* registratie van gegevens en wordt enkel een cryptografische hash van de gegevens op de blockchain bewaard. Het is aan te raden om persoonsgegevens en vertrouwelijke concurrentiegevoelige bedrijfs- of fabricagegegevens *off-chain* op te slaan, gelet op de onveranderlijkheid en transparantie van gegevens opgeslagen op de blockchain.⁵⁴

4.3 Smart contracts

Blockchain wordt doorgaans ingezet in combinatie met *smart contracts*. Smart contract is een misleidende term. Het *smart contract* is niet 'smart', maar een deterministisch algoritme. Daarnaast kan het smart contract een juridisch bindend contract inhouden, maar kan het ook verscheidene andere rechtsgevolgen inhouden. Een smart contract is een algoritme, namelijk een set regels die automatisch uitgevoerd wordt op het moment dat aan de vooraf vastgestelde condities is voldaan. Bijvoorbeeld, *als* je je huis isoleert, *dan* ontvang je een isolatiesubsidie. Het gebruik van smart contracts vergroot de toepassingsmogelijkheden van blockchain substantieel. In combinatie met smart contracts kan blockchain ingezet worden voor de automatisering van 1° de registratie van informatie, 2° waardeoverdracht en 3° het uitvoeren van regels. Op het vlak van rechtsgevolgen kan een smart contract het sluiten van een overeenkomst of het uitvoeren van verbintenissen uit een overeenkomst inhouden. Een smart contract kan echter ook andere rechtsgevolgen genereren, bijvoorbeeld in de vorm van een opschortende of ontbindende voorwaarde van een overeenkomst, een eenzijdige rechtshandeling, een overheidsbesluit (in dit geval in beginsel een beschikking die voortvloeit uit een gebonden bevoegdheid), een bewijsmiddel, de automatische uitvoering van (al dan niet wettelijke) processen of de naleving van wettelijke verplichtingen (bv. het betalen van belastingen).⁵⁵

Smart contracts op zichzelf zijn 'doof en blind', waarbij ze steeds input nodig hebben om output te genereren.⁵⁶ *Oracles* zijn hardware of software die ervoor zorgen dat informatie die zich bevindt buiten het blockchaineecosysteem

binnen het blockchainnetwerk wordt gebracht. Denk bijvoorbeeld aan een geluidsmeter of bewegingssensor. Een orakel vormt daarmee als het ware een brug tussen de wereld buiten de blockchain en het blockchainnetwerk.

5. Concrete blockchainpilot: De Rode Knop

5.1 De Rode Knop

Een interessant voorbeeld inzake het exploreren van de inzet van blockchain door de overheid is de lopende pilot 'de Rode Knop'⁵⁷ die ontwikkeld wordt op initiatief van het CJIB (ministerie van Justitie en Veiligheid), samen met de VNG, gemeente Den Haag en gemeente Eindhoven.⁵⁸ De ratio achter de Rode Knop komt voort uit de intentie van het CJIB om mensen die hen een bedrag verschuldigd zijn, bijvoorbeeld naar aanleiding van een verkeersboete, maar die niet kunnen betalen, tijdelijk "schuldenrust" aan te reiken eerder dan de schuldenproblematiek ongewild te laten verslechteren. Het CJIB is immers regelmatig een van de schuldeisers waar burgers met "problematische schulden"⁵⁹ mee te maken krijgen. Als bijvoorbeeld een verkeersboete of een boete opgelegd door de rechter niet bijtijds betaald wordt, stuurt het CJIB maximaal twee aanmaningen, waarbij de boete telkens verhoogd wordt. Hoewel sommige burgers de boete bewust *niet willen* betalen (of de boete vergeten te betalen), zijn er ook burgers in een problematische schuldsituatie die de boete, en de verhogingen daarvan, *niet kunnen* betalen.

Het CJIB maakt – na een landelijke invoering van het nieuwe beleid sinds 1 april 2020 – een onderscheid tussen 'kunnen maar niet willen betalen' en 'willen maar niet kunnen betalen' met betrekking tot verkeersboetes en strafrechtelijke geldelijke sancties, zoals door de rechter of het OM opgelegde boetes.⁶⁰ Het CJIB kan de ophogingen en inningen opschorten door middel van een noodstopprocedure voor burgers die niet kunnen betalen en waarbij geen uitzicht bestaat op betaling.⁶¹ Voordat burgers met problematische schulden de verkeersboete of strafrechtelijke geldelijke

54 Zie uitgebreid J. Goossens & C. van Oirsouw 2021.

55 Zie Smart Contract Working Group – Dutch Blockchain Coalition, 'Smart contracts als specifieke toepassing van de blockchain-technologie' 2017, p. 23-37, <https://dutchdigitaldelta.nl/uploads/pdf/Smart-contract-rapport-DBC.pdf>.

56 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 47-78.

57 Voorheen ook wel de 'Digitale Datakluis' en de 'Financial Emergency Break' genoemd. Zie: CJIB, 'CJIB presenteert prototype digitale datakluis', <https://www.cjib.nl/nieuws/cjib-presenteert-prototype-digitale-datakluis>; C. Dieleman, 'CJIB wil schuldenaars helpen via blockchain', *Computable.nl*, 30 oktober 2019 <https://www.computable.nl/artikel/nieuws/overheid/6826515/250449/cjib-wil-schuldenaars-helpen-via-blockchain.html>; E. van Winkoop, 'CJIB Publication the Financial Emergency Brake', *Northsearagon.eu*, 21 mei 2019.

58 Q. Hendrison, 'Rode knop geeft rust en ruimte voor inwoners met schulden', *VNG Realisatie e-Magazine* december 2020.

59 Zie *Kamerstukken II* 2017/18, 36 316, nr. 3: "Schulden zijn problematisch als de som van de geëiste maandelijkse aflossingen op schulden en betalingsachterstanden hoger is dan de aflossingscapaciteit."; zie ook Code of Conduct NVVK, Art. 8.: "Van een problematische schuldsituatie is naar het oordeel van de regering sprake indien van een natuurlijke persoon redelijkerwijs is te voorzien dat hij niet zal kunnen voortgaan met het betalen van zijn schulden, of waarin hij heeft opgehouden te betalen."; zie: *Kamerstukken II*, 2009-2010, 32 291, nr. 3.

60 CJIB, 'Innen & Incasseren', <https://www.cjib.nl/innen-incasseren>.

61 CJIB, 'Kabinet voorkomt stapelen boetes bij mensen met schulden', 4 februari 2020, <https://www.cjib.nl/nieuws/kabinet-voorkomt-stapelen-boetes-bij-mensen-met-schulden>.

sanctie⁶² moeten beginnen te betalen, krijgen zij een adem-pauze in de vorm van uitstel van betaling voor maximaal vier maanden. In die periode moeten zij vervolgens een schuldhulpverleningstraject aangaan, zodat de schulden op orde kunnen worden gebracht. Na de aanvang van het schuldhulpverleningstraject en het stabiliseren van de schulden, kan de noodstop met nog maximaal acht maanden worden verlengd. Uiteindelijk wordt de geldelijke sanctie van het CJIB na de noodstop – eventueel in termijnen – afbetaald, in overeenstemming met de getroffen schuldenregeling. De noodstop kan worden beëindigd als de burger gemaakte afspraken niet nakomt.⁶³

Burgers met problematische schulden blijken in de praktijk echter vaak een drempel te ervaren om in hun situatie hulp te vragen aan het CJIB,⁶⁴ wat in bepaalde gevallen mede kan worden verklaard door '(schuld)schaamte'.⁶⁵ De boetes van personen met problematische schulden worden daardoor vaak alsnog verhoogd, waardoor de schuldsituatie verder verslechtert. De informatie dat een burger andere schulden heeft, is echter vaak al 'ergens' binnen de overheid bekend, bijvoorbeeld bij de gemeente waar de burger inwoner is. Vanwege het gegevensbeschermingsrecht, en dan vooral de AVG, kan deze informatie bijvoorbeeld door de gemeente niet zomaar gedeeld worden met het CJIB. Daarnaast nemen schuldhulpverleningstrajecten vaak veel tijd in beslag, waardoor het signaal vaak te laat, dus na de verhogingen, aan het CJIB wordt afgegeven.⁶⁶

De Rode Knop bevindt zich momenteel in een pilotfase in de gemeenten Eindhoven en Den Haag en de beoogde werking kan als volgt worden omschreven.⁶⁷ Een inwoner benadert zijn gemeente om schuldhulpverlening aan te vragen. Een van de openstaande schulden is bijvoorbeeld een boete van het CJIB voor het overschrijden van een snelheidslimiet. Bij het intakegesprek met de schuldhulpverlener bij de gemeente wordt de Rode Knop ingedrukt middels een applicatie die de inwoner daarvoor op zijn telefoon downloadt. Door het indrukken van de Rode Knop gaat onmiddellijk een geauthentiseerd signaal naar het CJIB dat de inwoner hulp van de gemeente ontvangt betreffende zijn problematische schulden waardoor de inwoner niet in staat is momenteel om de boete van het CJIB te betalen. Op basis van deze informatie kan het CJIB het automatisch verhogen van de boetes stopzetten en de inning opschorten. Dit bericht wordt

ook weergegeven in de MijnApp.⁶⁸ Inzake het delen van het signaal dat er een gemeentelijk schuldhulpverleningstraject loopt, kan de inwoner kiezen of en hoe lang hij deze gegevens wil delen met andere overheidsinstanties. Hij krijgt een bevestiging na het delen en kan op elk moment besluiten om het delen van de gegevens in te trekken.

De Rode Knop implementeert hiermee de principes van *Self Sovereign Identity*, ofwel *SSI*. Een systeem dat met de principes van *SSI* werkt, geeft het individu controle over zijn digitale identiteit zonder afhankelijkheid ten aanzien van een derde partij. Het individu heeft zogenaamd 'regie op gegevens' en maakt daarbij zelf keuzes aangaande het creëren van zijn digitale gegevens, het toestaan van het gebruik ervan alsmede de beëindiging van het gebruik binnen verschillende contexten.⁶⁹ Hoewel er op dit moment binnen de pilot geen gebruik van gemaakt lijkt te worden, werd bij de start van het Rode Knop-traject medegedeeld dat er inzake het delen van gegevens zou worden gewerkt met zogenaamde *Zero Knowledge Proofs* (ZKP's).⁷⁰ Deze methode wordt geregeld gebruikt bij blockchainapplicaties. Het gaat om een cryptografische methode waarbij je kan bewijzen dat je een bepaalde waarde ('een geheim') kent, zonder verdere informatie over die waarde prijs te geven. Deze technologie laat dus toe een statement over gegevens te bewijzen zonder dat de gegevens zelf gedeeld worden. Een voorbeeld is een digitale handtekening, waarbij men bewijst dat men eigenaar is van de private sleutel, zonder die sleutel zelf prijs te geven. Daarenboven is het ook mogelijk om eigenschappen te bewijzen over die gegevens, bijvoorbeeld dat deze zich binnen bepaalde waarden bevinden of deel uitmaken van een gekende set van waarden.⁷¹ Zo kan iemand bijvoorbeeld bewijzen meerderjarig te zijn zonder de exacte leeftijd te openbaren, of bewijzen schulden te hebben zonder nadere informatie over die schulden prijs te geven.

5.2 Digital network governance

Binnen de blockchainpilot de Rode Knop is duidelijk sprake van *digital network governance*, waarbij de blockchainapplicatie bij het indrukken van de knop automatisch en onmiddellijk een digitaal signaal stuurt aan het CJIB. Voor de ontwikkeling en het gebruik van de applicatie wordt samengewerkt door een netwerk van verschillende publieke en private actoren. Het gaat om een samenwerking tussen het CJIB, het

62 Artikel 561 lid 3 Sv bepaalt dat het Openbaar Ministerie uitstel van betaling kan verlenen of betaling in termijnen kan toestaan.

63 Tweede Kamerbrief 'Noodstopprocedure geldelijke sancties', 4 februari 2020.

64 CJIB, 'Financial emergency break', <https://northsearegion.eu/media/9067/cjib-the-financial-emergency-brake.pdf>, p. 10.

65 A. Plantinga, *Poor psychology: Poverty, shame and decision making* (diss. Tilburg University), Tilburg: Tilburg University 2019.

66 Een lange doorlooptijd is een vaak voorkomend probleem binnen de schuldhulpverlening, zie: Q. Hendrison, 'Rode knop geeft rust en ruimte voor inwoners met schulden', *VNG Realisatie e-Magazine* december 2020.

67 Zie voor een videoclip van de VNG hierover: VNG, 'Fieldlab 2020 – Rode Knop in MijnApp', 2 november 2020, https://www.youtube.com/watch?v=8RsoU2MST_I.

68 VNG Realisatie, 'MijnApp: samen werken aan een nieuw informatielandschap', 5 november 2018, <https://www.vngrealisatie.nl/nieuws/mijnapp-samen-werken-aan-een-nieuw-informatielandschap>.

69 Zie voor enkele definities van *SSI*: J. Andrieu, 'A technology free definition of self-sovereign identity', *Rebooting Web Trust Design Workshop*, oktober 2016; C. Allen, 'The Path to Self-Sovereign Identity', *lifewithalacrity.com*, 26 april 2016; A. Tobin & D. Reed, 'The inevitable rise of self-sovereign identity, a white paper from the Sovrin Foundation', *sovrin.org*, 27 maart 2017; S. Ferdous, F. Chowdhury & M.O. Alassafi, 'In search of Self-Sovereign Identity Leveraging Blockchain Technology', *IEEE Access* 2019, afl. 7, p. 103059-103079; S. van Heukelom & S. Ranchordás, 'Digitaal Burger-schap: digitale identiteit', *Bestuursrecht in het echt* 2021/28.3.2; T. Speelman, 'Visiedocument – Dutch Self-Sovereign Identity Framework (DSSIF)', Dutch Blockchain Coalition 2021, p. 4-5.

70 U. Feige, A. Fiat & A. Shamir, 'Zero-knowledge proofs of identity', *Journal of cryptography* 1988, vol. 1, nr. 2, p. 77-94.

71 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 130.

ministerie van J&V en de gemeenten Eindhoven en Den Haag, waarbij ook private actoren zoals blockchainbedrijf Ledger Leopard, adviesbureau Sinzer en advocatenkantoor CMS al betrokken zijn geweest.⁷² Op het moment dat de Rode Knop wordt geïmplementeerd door het CJIB in het geval van een traject van gemeentelijke schuldhulpverlening, wordt deze technologie ingezet binnen een bestaand netwerk, bestaande uit de schuldenaar, de gemeente, eventuele private partijen aan wie schuldhulpverlening door de gemeente wordt uitbesteed, het CJIB en andere publieke en/of private schuldeisers, evenals eventuele vrijwilligersorganisaties die actief zijn op het vlak van schuldhulpverlening. Ieder van deze actoren binnen dit netwerk heeft in beginsel beslissingsruimte met betrekking tot zijn eigen handelen. De inwoner kan bijvoorbeeld besluiten geen gebruik te maken van de Rode Knop, het college van B&W kan besluiten de aanvraag voor schuldhulpverlening af te wijzen of gaandeweg het traject te wijzigen of in te trekken, het CJIB kan besluiten om af te zien van de noodstopprocedure en ook andere schuldeisers kunnen besluiten niet mee te werken aan het schuldhulpverleningstraject.

Op technisch vlak wordt in de huidige fase van de pilot gebruikgemaakt van de Hyperledger Indy blockchain. Dit is een publieke, permissioned blockchain opgezet door de Linux Foundation.⁷³ Naast blockchainbedrijf Ledger Leopard die betrokken is bij de ontwikkeling en codering van de applicatie de Rode Knop, zijn bijgevolg ook indirect nog andere softwareontwikkelaars betrokken. Hyperledger is immers een open source platform, waar meerdere partijen samenwerken aan het ontwikkelen van de code.⁷⁴ De Rode Knop is verder ook geïntegreerd in de MijnApp,⁷⁵ die bestaat uit een eigen technische architectuur en wordt ontwikkeld door verschillende partijen. Verder blijkt uit een eerste analyse van ons veldonderzoek en de eerste ronde van verkennende interviews dat er in deze fase van het ontwikkelproces van de Rode Knop nog onduidelijkheid is over welke gegevens geregistreerd zullen worden, welke smart contracts ingezet zullen worden en is er nog geen eensgezindheid over de meerwaarde van de inzet van blockchain ten opzichte van andere technologieën, zoals een gecentraliseerde database. Bij verdere doorontwikkeling van de Rode Knop zal het dus de vraag zijn of, en zo ja, in welke mate blockchain en smart contracts deel zullen uitmaken van de uiteindelijke technische infrastructuur.

In het licht van transparantie en accountability in een *digital network governance* context roept de toepassing van een blockchainapplicatie zoals de Rode Knop alvast allerhande

interessante vragen op, zowel algemene, abstracte vragen als contextafhankelijke, concrete vragen die nog niet waren geïdentificeerd na een eerste abstracte analyse:

- Welke informatie moet het bestuursorgaan aan een burger verstrekken over de werking van de Rode Knop? Uit een eerste analyse van onze data blijkt in dit opzicht bijvoorbeeld de concrete vraag te zijn gerezen of bij een intakegesprek voor schuldhulpverlening aan de burger moet worden uitgelegd hoe de onderliggende blockchaintechnologie werkt bij het indrukken van de Rode Knop.
- Hoe ziet een zorgvuldig voorbereide en deugdelijk gemotiveerde beslissing eruit wanneer het CJIB beslist om de verschuldigde betaling op te schorten na het indrukken van de Rode Knop? Artikel 4:94 Awb bepaalt namelijk in dit opzicht dat uitstel van betaling wordt verleend bij beschikking. Het gaat dus om een Awb-besluit, waartegen ook in bezwaar en beroep kan worden gegaan.
- Is er een manier voor de burger om op te komen tegen de afwijzing door het CJIB van een aanvraag voor uitstel van betaling (via het indrukken van de Rode Knop) op basis van een technische fout in het systeem? In dit geval is er immers geen sprake van een besluit in de zin van de Awb.
- Tijdens een observatie van een digitale groepsbijeenkomst (7 oktober 2021) in het kader van een recente praktijktoets stelde een burger de concrete vraag hoe het systeem weet waar je schulden hebt en hoe die informatie bij de overheid komt. Vervolgens zal bijgevolg de vraag moeten worden beantwoord of, en zo ja, hoe bij de te organiseren trainingen voor betrokken schuldhulpverleners aandacht moet worden besteed aan hoe dit op een toegankelijke en correcte manier kan worden uitgelegd aan de burger.

Naar aanleiding van de Strategische Verkenning Blockchain van Rijkswaterstaat (RWS)⁷⁶ en ons recent afgerond onderzoek 'Transparantie in de blockchain: een juridische verkenning van de toegang tot overheidsinformatie onder de Wob, de Woo en de Archiefwet bij de inzet van gedistribueerde technologie' in het kader daarvan naar twee blockchain use cases (resp. grondstromen en zoutlogistiek) rezen onder meer ook al de volgende bijkomende vragen op het vlak van transparantie:⁷⁷

- In welke mate is informatie opgenomen in de blockchain Wob-baar en kunnen informatiezoekers zelf informatie in de blockchain opzoeken aangaande de samenstelling van grond en de kwaliteit van strooizout?
- Hoe kan RWS bij de inzet van blockchain zijn rol vervullen als verantwoordelijk archiefvormend orgaan, welke concrete algoritmen moeten worden

72 CJIB, 'Financial emergency brake', ministerie van Justitie en Veiligheid 2019, <https://northsearegion.eu/media/9067/cjib-the-financial-emergency-brake.pdf>; Q. Hendrison, 'Rode knop geeft rust en ruimte voor inwoners met schulden', *VNG Realisatie e-Magazine* december 2020.

73 P.J. Windley, 'Hyperledger Welcomes Project Indy', *Hyperledger.org*, 2 mei 2017, <https://www.hyperledger.org/blog/2017/05/02/hyperledger-welcomes-project-indy>.

74 Hyperledger, 'About Hyperledger', *Hyperledger.org*, <https://www.hyperledger.org/about>.

75 VNG Realisatie, 'MijnApp: samen werken aan een nieuw informatielandschap', *vngrealisatie.nl*, 5 november 2018, <https://www.vngrealisatie.nl/nieuws/mijnapp-samen-werken-aan-een-nieuw-informatielandschap>.

76 RWS, 'Strategische Verkenning Blockchain. Hoe blockchain kan zorgen voor beter strooizout', *Rijkswaterstaat &*, 3 september 2021, <https://www.magazinesrijkswaterstaat.nl/zakelijkeninnovatie/2021/03/strategische-verkenning-blockchain>.

77 Zie J. Goossens & C. van Oirsouw 2021.

gearchiveerd, en hoe kan RWS bij een blockchainapplicatie op technisch vlak voldoen aan de wettelijke plicht om gegevens te vernietigen na verloop van tijd?

- Wat is vervolgens de invloed van de blockchainedesignkeuzes in de use cases op de beantwoording van de twee voorgaande vragen, namelijk designkeuzes inzake de toegang tot het netwerk (publieke of private blockchain), de participatierechten in het netwerk (permissionless of permissioned blockchain) en on-chain of off-chain registratie van gegevens?

Uit ons lopend onderzoek naar de Rode Knop en afgerond onderzoek naar de twee RWS-blockchain use cases blijkt dat een afdoende beantwoording van bovenstaande vragen over de operationalisering van transparantie en accountability geregeld een analyse vergt van de praktische toepassing van de specifieke blockchainapplicatie in een concrete context.

6. Het belang van onderzoek naar praktische toepassingen in een concrete context

Op basis van de vorige paragraaf blijkt dat onderzoek naar de inzet van blockchain in een overheidscontext tot het inzicht leidt dat het van belang is om ook (kwalitatief) onderzoek te doen naar praktische toepassingen in een concrete context om na te kunnen gaan hoe binnen het huidige juridische kader transparantie en accountability kunnen worden geborgd én geoperationaliseerd op het moment dat overheden blockchain inzetten om het uitvoeren van publieke taken binnen een netwerkomgeving te automatiseren. Hierna gaan we dieper in op drie fundamentele redenen waarom dergelijk onderzoek naar de concrete praktijk van belang is: 1° gebrek aan informatie, 2° de invloed van context op transparantie en accountability, 3° effectiviteit van regulering.

6.1 Gebrek aan informatie

Allereerst is blockchain nog steeds een relatief jonge, zich volop ontwikkelende technologie. De inzet van blockchain en smart contracts door overheden is dan ook een nieuw fenomeen, waardoor (vooralsnog) specifieke wetgeving en jurisprudentie, evenals best practices ontbreken. Hierdoor is er een gebrek aan informatie waaruit relevante inzichten opgedaan kunnen worden. Een situatie waarin er geen specifieke wetgeving of jurisprudentie is, betekent natuurlijk geenszins dat de inzet van blockchain en smart contracts daardoor ongereguleerd is en zich in een juridisch vacuüm zou bevinden.⁷⁸ Bestaande constitutionele beginselen en algemene beginselen van behoorlijk bestuur, de Awb en andere toepasselijke regelgeving, zoals de Wob of de AVG vormen tezamen het regelgevend kader dat transparantie en accountability borgt, ook wanneer een overheid blockchain en smart contracts inzet bij de oefening van publiek

gezag in netwerken. Substantiële theoretische en praktische kennis over hoe dit regelgevende kader moet worden geïnterpreteerd, geïmplementeerd en geoperationaliseerd in een concrete context ontbreekt echter. Desondanks is deze kennis noodzakelijk voor overheden om op betrouwbare en legitieme wijze te kunnen innoveren met blockchain. Er is op zijn minst nood aan een (her)interpretatie van het huidige juridisch kader toegespitst op deze nieuwe context, waardoor onderzoek naar deze context bij praktische toepassingen onontbeerlijk is.

6.2 Invloed van context op transparantie en accountability

Ten tweede blijkt uit een bestudering van de brede literatuur over transparantie en accountability, alsmede de impact van deze rechtstatelijke waarden op de legitimiteit van overheidsoptreden, dat deze concepten grotendeels bepaald worden door de context waarin zij geborgd en geoperationaliseerd worden. Als men met deze bevinding in het achterhoofd kijkt naar de huidige literatuur in het Nederlandse staats- en bestuursrecht over de inzet van blockchain en smart contracts in een overheidscontext, is er echter amper onderzoek naar mogelijke concrete praktijktoepassingen. Huidig onderzoek behoudt doorgaans een bepaalde afstand ten aanzien van de concrete praktijk en heeft daarmee een hoog niveau van abstractie met betrekking tot de kennis en inzichten die daaruit voortvloeien. Hierna volgen enkele voorbeelden ter illustratie.

In het rapport *Blockchain en het Recht* uitgevoerd in opdracht van het WODC analyseren Schemkes, Tjong Tjin Tai, Schellekens, Kaufmann en Leenes de aanvaardbaarheid van de verschillende manieren waarop blockchain ingezet kan worden aan de hand van de criteria voor het analyseren van normatieve technologieën ontwikkeld door Koops.⁷⁹ Volgens hen is blockchain een normatieve technologie die de verhoudingen tussen betrokken partijen opnieuw beoogt te definiëren, wat kan leiden tot veranderingen in bestaande verhoudingen in de samenleving en met als risico het onder druk zetten van waarden en belangen. Zij identificeren verschillende kansen en risico's die gepaard gaan met de inzet van blockchain. De gedistribueerde aard van een blockchain kan het bijvoorbeeld moeilijk maken om aan de eisen van de AVG te voldoen, onder meer omdat het lastig is om een verwerkingsverantwoordelijke aan te wijzen en om deze verantwoordelijkheid vorm te geven aangezien de coördinatie tussen verwerkers lastig kan zijn. Daarnaast komt de autonomie van de gebruiker onder druk door de rigiditeit ten gevolge van het vatten van processen in code, de onveranderlijkheid van gegevens op de blockchain en de onduidelijkheid van informatieplichten jegens de gebruikers. Naast vragen inzake democratische legitimatie, vereist legitimiteit binnen een blockchain ook dat er waarborgen worden ingebouwd om de gebruiker niet over te leveren

⁷⁸ Zie ook J. Oster, 'Code is code and law is law – The law of digitization and the digitization of law', *International Journal of Law and Information Technology* 2021, afl. 29, p. 102.

⁷⁹ F. Schemkes, E. Tjong Tjin Tai, M. Schellekens, W. Kaufmann, & R. Leenes 2019.

aan de willekeur van de bouwer of de blockchain zelf.⁸⁰ De auteurs gaan in dit rapport in op een viertal use cases om voorgaande en andere juridische knelpunten in kaart te brengen, maar gaan niet in op de impact in de praktijk van de concrete, bestaande normen, wat natuurlijk niet onlogisch is wegens de verkennende aard van het onderzoeksrapport.

Ten opzichte van het WODC-rapport is Van Heukelom-Verhage optimistischer over de inzet van blockchain en smart contracts door de overheid in haar preadvies over maatwerk binnen het bestuursrecht en digitalisering. Zij beargumenteert dat de inzet van blockchain kan bijdragen aan de doelen van een responsieve overheid, onder andere omdat de inzet van blockchain tot meer transparantie en maatwerk kan leiden. In haar preadvies biedt zij een overzicht hoe de contextspecifieke invulling van algemene beginselen van behoorlijk bestuur langzaam vorm krijgt.⁸¹ Uit het preadvies valt echter te concluderen dat we aan het begin staan van een ontwikkeling en dat er dus nog veel kennis op te halen is over de contextspecifieke invulling van de algemene beginselen van behoorlijk bestuur. Zij gaf eerder al aan dat er nog verschillende te beantwoorden vraagstukken zijn, zoals de vraag of een blockchainapplicatie nog herkend kan worden als een publieke service of de vraag hoe bestuursrechters smart contracts zullen beoordelen.⁸²

Verder concludeert het rapport 'Blockchain in de zorg in relatie tot de AVG'⁸³ met betrekking tot transparantie het volgende. De inzet van blockchain brengt in het licht van de eis van rechtmatigheid, behoorlijkheid en transparantie van artikel 5 (1) (a) AVG geen onoverkomelijke gegevensbeschermingsrechtelijke problemen met zich mee, maar de gebruikers moeten wel afdoende afspraken met elkaar maken, zodat de AVG in acht kan worden genomen.⁸⁴ Daarnaast concludeert het rapport dat overheidsorganen die gebruikmaken van een blockchain moeten controleren of zij persoonsgegevens vastleggen in archiefbescheiden waarvoor op grond van de Archiefwet een bewaartermijn geldt.⁸⁵ Goossens, Verslype en Tjong Tjin Tai signaleren op hun beurt dat het borgen van de algemene beginselen van behoorlijk bestuur, zoals onder andere het zorgvuldigheidsbeginsel, het motiveringsbeginsel en de hoorplicht, een

uitdaging kunnen vormen bij de inzet van blockchain en smart contracts.⁸⁶

Aangezien het aantal publicaties dat specifiek gaat over de inzet van blockchain door de overheid en het Nederlandse staats- en bestuursrechtelijke kader beperkt is, loont het om ook te kijken naar publicaties die in het algemeen gaan over *network governance* en de inzet van algoritmen. Op basis van een literatuurstudie dienaangaande blijkt echter dat ook hier onderzoek naar de concrete implementatie, interpretatie en operationalisering van het huidige juridische kader vaak achterwege blijft. Publicaties gaan doorgaans over een van de volgende twee vraagstukken: of het huidige recht op andere wijze geconceptualiseerd en geïnterpreteerd moet worden; of dat het recht fundamenteel uitgedaagd wordt door de inzet van nieuwe technologieën.⁸⁷ Door het stellen van dergelijke meer abstracte vragen, houdt ook de beantwoording een bepaald niveau van abstractie aan. Daarnaast wordt methodologisch vaak afstand behouden van de concrete praktijk, aangezien de meeste publicaties een juridisch-dogmatische methode hanteren en geen aanvullend empirisch onderzoek verrichten.⁸⁸

Zo signaleert de literatuur vaak juridische knelpunten of uitdagingen, waarna vervolgens abstracte aanbevelingen worden gedaan over het borgen van transparantie en accountability. Het gaat dan bijvoorbeeld om het signaleren van een digitale informatiele disbalans binnen de trias,⁸⁹ uitdagingen inzake een effectieve rechtelijke controle,⁹⁰ behoefte aan betere democratische controle en rechtsbescherming bij publiek-private samenwerkingen⁹¹ en de rol van softwareontwikkelaars,⁹² de constitutionele kwalificatie van de uitoefening van bevoegdheden bij volledig geautomatiseerde besluitvorming in de vorm van delegatie of mandaat,⁹³ de vraag of de Awb en de huidige set algemene beginselen van behoorlijk bestuur voldoende accountability mechanismen bieden om het bestuur te normeren bij

80 Ibid.

81 S. van Heukelom-Verhage, 'Maatwerk bieden in een gedigitaliseerde en datagedreven samenleving; #HoeDan?', in: L. van den Berge, M.F. Vermaat, M. Lurks, N.A. van Renssen & S. van Heukelom-Verhage (red.), *Maatwerk in het Bestuursrecht*, Preadviezen VAR-reeks nr. 164, Den Haag: Boom Juridisch 2020, paragraaf 4.2.

82 S. van Heukelom-Verhage, 'Responsieve rechtsstaat en digitale overheid: blockchain en smart contracts', *NTB* 2018/39.

83 S. van Heukelom-Verhage, M. van Graafeiland, T. Gillhaus & J. van Mechelen, 'Blockchain in de zorg in relatie tot de AVG', onderzoeksrapport in opdracht van Zorginstituut Nederland 2019.

84 S. van Heukelom-Verhage, M. van Graafeiland, T. Gillhaus & J. van Mechelen 2019, sectie 5.3.4, 5.4.4.

85 S. van Heukelom-Verhage, M. van Graafeiland, T. Gillhaus & J. van Mechelen 2019, sectie 5.3.32.

86 J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 43-44.

87 Zie ook: J. Oster 2021, p. 102.

88 Voor een aantal voorbeelden van uitzonderingen hierop, zie: M. van Eck, *Geautomatiseerde ketenbesluiten & rechtsbescherming: een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming* (diss. Tilburg), Tilburg 2018; S. Kulk & S. van Deursen, *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*, (Rapport in opdracht van het WODC) Den Haag: WODC 2020; A. Widlak, M. van Eck & R. Peeters, 'Towards principles of good digital administration: Fairness, Accountability and Proportionality in Automated Decision Making', in: M. Schuilenberg en R. Peeters (red.), *The Algorithmic Society. Technology, power and knowledge*, Oxfordshire: Routledge 2021.

89 R.H.T. Jansen, 'Digitalisering, machtenscheiding en transparantie', Montesquieu Instituut 16 april 2020, www.montesquieuinstituut.nl/id/vl7vdo9fojsr/; C. Prins, 'Digitale (dis)balans binnen de trias', *NJB* 2016/682; R. Passchier, 'Digitalisering en de (dis)balans binnen de trias politica', *Ars Aequi* 2020, p. 916-927.

90 J. de Poorter & J. Goossens 2019.

91 L. van den Berge 2020, par. 6.3.

92 M. van Eck, M. Bovens & S. Zouridis, 'Algoritmische rechtstoepassing in de democratische rechtsstaat', *NJB* 2018/2101, p. 2107.

93 J. Goossens, E.M.H. Hirsch Ballin & E.Y. van Vught, 'Algoritmische beslisseregels vanuit constitutioneel oogpunt - Tweedeling tussen algemene regels en concrete toepassing onder druk', *TvCR* 2021, (afl.) 12 (1) 4-19. Zie ook: J. Cobbe 2019, p. 636-655.

de inzet van algoritmen in hun algemeenheid⁹⁴ of bij de verwerking van persoonsgegevens in het bijzonder.⁹⁵ Voorbeelden van aanbevelingen zijn onder andere het besteden van meer aandacht aan transparantie en de neutraliteit van algoritmen, waarbij het de vraag blijft hoe dit vormgegeven kan worden,⁹⁶ het openbaar maken van algoritmen op transparante wijze,⁹⁷ transparantie en uitlegbaarheid *by design* om een effectieve rechtsbescherming te garanderen⁹⁸ of de introductie van aanvullende elementen voor beginselen die van toepassing zijn op geautomatiseerde ketenbesluiten, zoals een centrale mogelijkheid tot correctie van fout geregistreerde gegevens als aanvulling op het proportionaliteitsbeginsel.⁹⁹

Yang geeft aan dat het ontwikkelen van een goed begrip van de betekenis en de functies van accountability bijvoorbeeld bijzonder belangrijk is wanneer onderzoekers een nieuwe context analyseren. Hij haalt in dit opzicht uitdrukkelijk partnerschappen en netwerken aan. Zo wijst hij erop dat ondanks het toenemende belang van *network governance* de traditionele invulling van accountability is gebaseerd op aparte, autonome, hiërarchische organisaties. Aangezien accountability in netwerken echter niet kan worden afgeleid van accountability in een organisatie, roept Yang op verkennend onderzoek uit te voeren op basis van inductieve en kwalitatieve methoden. Hij geeft ook aan dat kwalitatief onderzoek bij uitstek geschikt is om de door de tijd wijzigende dynamieken inzake accountability te bestuderen. Ten slotte wijst hij erop dat het manifesteren en implementeren van accountability samenhangt met de waarden, percepties, interpretaties en strategische reacties van betrokken actoren, zodat degelijk onderzoek daar ook rekening mee moet houden.¹⁰⁰

Ten slotte is het bij het ontwikkelen van technologische applicaties van belang om voldoende aandacht te besteden aan

het perspectief van de burger¹⁰¹ die wordt geconfronteerd met vormen van digitaal besturen in netwerken, met inbegrip van de ondoorzichtigheid en complexiteit die daarmee gepaard kunnen gaan. In dit opzicht is ook de toegankelijkheid van de interface van technologische toepassingen van cruciaal belang, bijvoorbeeld wanneer een burger de digitale, blockchain-gebaseerde Rode Knop zou willen indrukken om in het geval van een gemeentelijk schuldhulpverleningstraject het automatisch verhogen van boetes door het CJIB stop te zetten en de inning op te schorten. Hiervoor is contextspecifiek onderzoek nodig naar de ervaring van de burger.

Algemeen kan dus worden gesteld dat het vaak nog steeds onvoldoende duidelijk is hoe het huidige juridisch kader inzake transparantie en accountability in een concrete context moet worden geoperationaliseerd. Daarnaast is het ook onduidelijk of het huidige juridisch kader in de praktijk voldoende houvast biedt en voldoende effectief is om de waarden van transparantie en accountability te borgen, wanneer overheden besturen in netwerken en algoritmen inzetten, en al zeker wanneer overheden innoveren met blockchain en smart contracts als vorm van *digital network governance*. Er ligt dus op dit vlak nog heel wat werk op de plank voor de publiekrechtelijke Nederlandse academische gemeenschap.

6.3 Effectiviteit van regulering

Ten derde kan onderzoek naar zowel de theorie als de praktijk het risico van overregulering of inadequate regulering verminderen door theorie en praktijk beter op elkaar te laten aansluiten, wat bijdraagt aan de effectiviteit van regulering.¹⁰² Uiteindelijk bepaalt het recht of en onder welke voorwaarden de inzet van nieuwe technologieën wel of niet wordt toegelaten.¹⁰³ Het risico van overregulering of inadequate regulering kan als impact hebben dat de mogelijke voordelen die de inzet van technologie, in dit geval blockchain, door de overheid te bieden heeft, mogelijk niet behaald kunnen worden, en dat negatieve gevolgen, zoals gebrekkige handhaving, kunnen optreden.¹⁰⁴ Het uitblijven van effectieve regulering kan ervoor zorgen dat mogelijke voordelen niet behaald worden, omdat actoren die willen experimenteren met blockchain zich in een juridische grijze zone bevinden en dus worden geconfronteerd met rechts-onzekerheid.¹⁰⁵ Door te onderzoeken hoe het huidige juridisch kader bij de inzet van blockchain door de overheid in de praktijk wordt geïnterpreteerd, geïmplementeerd en geoperationaliseerd, kunnen naderhand onderbouwde

94 Over het antwoord bestaat onenigheid in de literatuur, zie: S. Kulk & S. van Deursen 2020; M. van Eck, M. Bovens & S. Zouridis 2019; R. Uylenburg, 'Rechterlijke Toetsing van Digitale Besluiten', in: T. Barkhuysen, W. den Oudem & R. Schlössels (red.), *25 Jaar Awb – In eenheid en verscheidenheid*, Deventer: Wolters Kluwer 2019, p. 759-769; C. Adriaanz, 'De Rechtmatigheid van algoritmische besluitvorming in het licht van het zorgvuldigheidsbeginsel en het motiveringsbeginsel', *NTB 2020/100*; J. Wolswinkel, 'AR meets AI: Een bestuursrechtelijk perspectief op een nieuwe generatie besluitvorming', *Computerrecht 2020/4*, afl. (1), p. 22-29; A. Widlak, M. van Eck & R. Peeters 2021.

95 F. Çapkurt & Y.E. Schuurmans, 'Blinde vlek in de Awb: data', in: T. Barkhuysen, W. den Ouden & R. Schlössels (red.), *25 Jaar Awb – In eenheid en verscheidenheid*, Deventer: Wolters Kluwer 2019, p. 253-265; zie ook J. Cobbe 2020.

96 M. Vetzo, J. Gerards & R. Nehmelan, *Algoritmes en Grondrechten*, Den Haag: Boom Juridisch 2018, p. 188, p. 189; M. Vetzo & J. Gerards, 'Algoritme-gedreven technologieën en grondrechten', *Computerrecht 2019/3* (afl.) 1, p. 1-48.

97 R. van Male, 'Digitalisering van discretionaire bevoegdheden', in: B.A. Beijen, A.M.M.M. Bots, J.A.F. Peeters & R.J.N. Schlössels (red.), *In het nu... Over toekomstig bestuursrecht* (Serie Staat en Recht), Deventer: Wolters Kluwer 2018.

98 J. de Poorter & J. Goossens 2019.

99 A. Widlak, M. van Eck & R. Peeters 2021.

100 K. Yang, 'Qualitative analysis', in: M.A.P. Bovens, T. Schillemans & R.E. Goodin (red.), *The Oxford Handbook of Public Accountability*, Oxford: Oxford University Press 2014, p. 161-162.

101 Nationale ombudsman, 'Een burger is geen dataset. Ombudsvisie op behoorlijk gebruik van data en algoritmen door de overheid', Rapportnummer: 2021/021, 2 maart 2021.

102 M. Partington, 'Empirical Legal Research and Policy-Making', in: P. Crane & M. Kritzer (red.), *The Oxford Handbook of Empirical Legal Research*, Oxford: Oxford University Press 2010, p. 2.

103 Zie ook: J. Oster 2021, p. 114.

104 A. Zwitter & J. Hazenberg, 'Decentralized network governance: blockchain technology and the future of regulation', *Frontiers in blockchain 2020*, afl. 3(12), p. 7; P. de Filippi & A. Wright 2018, p. 189.

105 P. de Filippi & A. Wright 2018, p. 209.

conclusies en aanbevelingen worden gedaan inzake de huidige effectiviteit van het regelgevende kader om transparantie en accountability te borgen, en kan daarmee ook de vraag worden beantwoord of er behoefte is aan een aanpassing van het juridische kader of zelfs aan een geheel nieuw regelgevend kader.

7. Conclusie

De inzet van blockchain door de overheid kan in bepaalde gevallen van *network governance* en een gedistribueerde realiteit leiden tot voordelen, maar brengt zeker ook juridische uitdagingen met zich mee inzake het borgen en operationaliseren van transparantie en accountability. Om te beoordelen of de toepassing en (her)interpretatie van het huidige juridische kader afdoende is in dit opzicht, dient het doorgaans abstracte niveau van huidig onderzoek te worden overstegen en te worden aangevuld met kwalitatief onderzoek naar de concrete praktijk. Zo is onderzoek nodig naar innovatie door de inzet van blockchain door de overheid gelet op de toename van digital network governance, bijvoorbeeld door onderzoek te verrichten naar een specifieke blockchaintoepassing, zoals de Rode Knop. Ons lopend onderzoek naar de Rode Knop leidde bijvoorbeeld tot de concrete vraag of, en zo ja, hoe bij een intakegesprek voor schuldhulpverlening aan de burger moet worden uitgelegd hoe de onderliggende blockchaintechnologie werkt bij het indrukken van de Rode Knop.

Bij het uitvoeren van zulk onderzoek naar de toepassing van nieuwe, opkomende technologieën is het dus belangrijk om op basis van kwalitatief onderzoek naar het verantwoord ontwikkelen van technologische toepassingen na te gaan hoe fundamentele rechtsstatelijke vereisten zoals transparantie en accountability *by design* kunnen worden geborgd. In het geval van een *by design*-benadering wordt rekening gehouden met deze rechtsstatelijke waarborgen in het technologische design en dus bij het ontwikkelen van de technologische applicaties zelf, in plaats van enkel achteraf te onderzoeken of bij de inzet van een technologische oplossing transparantie en accountability wel afdoende zijn geborgd. Een *by design*-benadering waarbij normen zoals transparantie en accountability in het technologische ontwikkelingsproces uitdrukkelijk worden betrokken, kan worden aanbevolen. Het is vaak immers onmogelijk om de gevolgen van de gevolgen van de toepassing van technologie achteraf terug te draaien zodra de technologie is ontwikkeld en wordt gebruikt. Om in zo'n geval achteraf de vraag te stellen of een bepaalde technologie al dan niet acceptabel is, is te laat.¹⁰⁶ Het voorzien van '*transparency and accountability by design*' is dan ook uiterst belangrijk,¹⁰⁷ waarbij uiteindelijk ook de

vraag zal moeten worden beantwoord of er in dit opzicht ook nood is aan optreden van de wetgever.¹⁰⁸

¹⁰⁶ B.J. Koops 2007.

¹⁰⁷ M. Veale, M. van Kleek & R. Binns, 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 2018, p. 440.

¹⁰⁸ R. van den Hoven van Genderen, 'Algoritmen en AI: distopische black box of glazen bol? Is een wettelijk kader voor transparantie van algoritmen mogelijk en wenselijk?', *Computerrecht* 2020, 5.