JURGEN GOOSSENS & CHARLOTTE VAN OIRSOUW
M.M.V. JULIETTE ERMERS & HELEEN ANDRIESSEN

TRANSPARANTIE IN DE BLOCKCHAIN

Een juridische verkenning van de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie

Boom juridisch

In de zomer van 2020 is Rijkswaterstaat (RWS) gestart met een strategische verkenning van de inzet van blockchain. De inzet van complexe, gedistribueerde technologie door de overheid brengt verschillende juridische en technische vraagstukken met zich mee op het vlak van transparantie en toegang tot overheidsinformatie. Op welke wijze heeft het gebruik van blockchain invloed op de verplichtingen die voortvloeien uit de Archiefwet en de Wet openbaarheid van bestuur/Wet open overheid en welke impact heeft deze wetgeving op de keuze van het blockchaindesign?

Dit boek verricht een exploratieve analyse van de dynamische relatie tussen designkeuzes en juridische verplichtingen, mede aan de hand van twee RWS blockchainpilots. De analyse heeft bijzondere aandacht voor het perspectief van de informatieverzoeker en het belang van een by-design-benadering van legal compliance.

De analyse leidt tot tien vuistregels voor het juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie. *Transparantie in de blockchain* is relevant voor iedereen die meer wil weten over de inzet van (gedistribueerde) technologie binnen de overheid of interesse heeft in toegang tot overheidsinformatie.

Jurgen Goossens is projectleider van het door NWO gefinancierd CHAIN-project over de inzet van blockchain door de overheid in de netwerksamenleving. Tot juli 2022 was hij universitair hoofddocent staats- en bestuursrecht aan Tilburg University en vanaf augustus hoogleraar staatsrecht aan de Universiteit Utrecht.

Charlotte van Oirsouw is promovenda bij het CHAIN-project. Zij voert rechtswetenschappelijk onderzoek naar de regulering van transparantie en accountability bij de inzet van algoritmische systemen door de overheid.

Juliette Ermers en **Heleen Andriessen** zijn student-onderzoeksassistenten bij het CHAIN-project.

ISBN 978-94-6212-710-4

9 789462 127104 >

Boom juridisch

Transparantie in de blockchain

Transparantie in de blockchain

Een juridische verkenning van de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie

Prof. mr. dr. Jurgen Goossens en mr. drs. Charlotte van Oirsouw,
m.m.v. Juliette Ermers en Heleen Andriessen
CHAIN research team

Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

CHAIN
Connecting Humankind through Algorithms and Information Networks

Boom juridisch
Den Haag
2022

Deze publicatie is tot stand gekomen in opdracht van het Programma Strategische Verkenningen van Rijkswaterstaat. Het onderzoek vormt onderdeel van een bredere verkenning naar de mogelijke betekenis van blockchain voor de organisatie van bepaalde typen werkprocessen en de samenwerking met relevante partners.
Het onderzoek in deze publicatie is mede tot stand gekomen in het kader van het door NWO gefinancierde interdisciplinaire onderzoek over blockchaintoepassingen van de overheid: 'Blockchain in de netwerksamenleving. Op zoek naar transparantie, vertrouwen en legitimiteit' binnen het onderzoeksprogramma 'Verantwoord Innoveren. Ontwerpen voor publieke waarden in een digitale wereld'.
Het onderzoek werd inhoudelijk afgerond op 29 oktober 2021.

Omslagontwerp en opmaak binnenwerk: Textcetera, Den Haag

ISBN 978-94-6212-710-4
ISBN 978-94-0011-166-0 (e-book)
NUR 823

www.boomjuridisch.nl

Inhoud

Samenvatting

1. *Aanleiding en doelstelling*

Rijkswaterstaat (RWS) is in de zomer van 2020 gestart met een strategische verkenning naar de mogelijke betekenis van de inzet van blockchain voor de organisatie van bepaalde typen werkprocessen en de samenwerking met partners. Het onderzoek vond plaats in het kader van het Programma Strategische Verkenningen, dat tot taak heeft om ontwikkelingen in de omgeving tijdig te signaleren en de organisatie te helpen om hierop koers te bepalen. In deze verkenning is RWS een aantal pilots gestart om meer inzicht te krijgen in de toepassingsmogelijkheden en de consequenties, met inbegrip van de juridische consequenties. Daarbij onderzoekt RWS samen met interne en externe ketenpartners of de inzet van blockchain een meerwaarde zou kunnen opleveren ten opzichte van bestaande processen. De inzet van een relatief jonge technologie zoals blockchain brengt verschillende juridische vraagstukken met zich mee waarop antwoorden in de literatuur, jurisprudentie en bestuurspraktijk nog niet zijn uitgekristalliseerd.

Op dit moment ontbreken nationale wet- en regelgeving die specifiek betrekking hebben op blockchaintechnologie. In de strategische verkenning tracht RWS bijgevolg een **pragmatische, hernieuwde interpretatie van de huidige regelgeving** te hanteren. Aangezien de pilots een oriënterend karakter hebben, hebben analyses vooralsnog enkel op abstract niveau plaatsgevonden. Desondanks tracht de strategische verkenning een kader te bieden dat bij de doorontwikkeling van deze pilots gebruikt kan worden. Bij het nadenken over de toepassing van de huidige wetgeving kwamen enkele vraagstukken naar voren op het vlak van transparantie en openbaarheid van bestuur die een combinatie van blockchainexpertise en juridische expertise vergden. Daarom identificeerde RWS de behoefte aan aanvullend juridisch opdrachtonderzoek. Het onderzoeksrapport '*Transparantie in de blockchain: een juridische verkenning van de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie*' van het interdisciplinaire onderzoeksteam CHAIN komt aan deze vraag tegemoet. Het onderzoeksrapport werd inhoudelijk afgerond op 29 oktober 2021 en werd in de lente van 2022 omgezet in boekvorm.

Dit boek beoogt een **verkennende** en **exploratieve** analyse te bieden voor de beantwoording van de juridische vraagstukken betreffende de vereisten van transparantie

en openbaarheid van bestuur in het kader van het **recht op toegang tot overheidsinformatie** bij de inzet van blockchain door de overheid, met inbegrip van de impact van het wettelijk kader op de mogelijke keuzes inzake de architectuur of het **design van de technologie**. Het boek kijkt daarbij voornamelijk naar de gevolgen van de toepassing van de **Archiefwet**, de Wet openbaarheid van bestuur (**Wob**) en de Wet open overheid (**Woo**) die vanaf 1 mei 2022 (gedeeltelijk) in werking treedt en daarmee de Wob vervangt.

Daarnaast identificeert het boek enkele andere toekomstige juridische vraagstukken die in een latere fase bij de verkenning van het gebruik van blockchain naar voren kunnen komen. Het gaat hier over de toepassing van de Algemene wet bestuursrecht (**Awb**), met inbegrip van de operationalisering van algemene beginselen van behoorlijk bestuur zoals het zorgvuldigheids- en motiveringsbeginsel, de Algemene Verordening Gegevensbescherming (**AVG**), het **mededingings- en aanbestedingsrecht**, en de Wet hergebruik overheidsinformatie (**Who**). Er wordt ook beknopt ingegaan op de mogelijke functies van blockchaingebaseerde **smart contracts**, en de kwaliteit van input via **oracles**.

2. Onderzoeksvragen en methodologie

Naast de identificatie van enkele toekomstige juridische vraagstukken die kunnen rijzen bij het gebruik van blockchain binnen processen van RWS en zijn ketenpartners, beoogt het boek vooral een basis te bieden voor de beantwoording van de volgende door RWS geïdentificeerde vragen:

*Q1: Welke consequenties heeft de **Archiefwet** op het gebruik van blockchain voor RWS, en heeft dit invloed op het **type blockchain** dat binnen RWS ingezet kan worden?*
*Q2: Op welke wijze heeft het gebruik van blockchain invloed voor RWS op de verplichtingen uit de **Wob** en de **Woo** en welke impact heeft deze wetgeving op de **keuze in het design van een blockchainnetwerk**?*

Om te komen tot een wetenschappelijk onderbouwde beantwoording van bovenstaande vragen wordt er in dit boek een rechtswetenschappelijke beschrijving en analyse verricht van de betreffende wet- en regelgeving, inclusief relevante jurisprudentie, evenals een literatuurscan (met inbegrip van rapporten en beleidsdocumenten). Deze analyse heeft algemeen betrekking op de Wob, de Woo en de Archiefwet, maar met een focus op bijdragen die specifiek betrekking hebben op de inzet van **digitale dragers en systemen**, in dit geval blockchaintechnologie en smart contracts ('als x, dan y' algoritmen). In beginsel werd voornamelijk Nederlandse literatuur geraadpleegd, en waar nodig aangevuld met internationale literatuur. Theoretische analyses over de consequenties van de inzet van blockchaintechnologie zijn een stap verder gebracht door rekening te houden met **specifieke context**. In dit boek is gekozen om de analyse van context te voorzien op basis van twee **blockchainpilots** die geëxploreerd worden binnen RWS: **grondstromen** en

zoutlogistiek. Op basis van deze twee pilots wordt in dit boek de wisselwerking onderzocht tussen de theorie en de praktijk, waarbij de concrete context de analyse op enkele punten verrijkt.

3. Bredere context: de opkomst van digital network governance

De organisatie en het functioneren van het openbaar bestuur in Nederland hebben de voorbije decennia verschillende belangrijke evoluties ondergaan. Voor het boek zijn de opkomst van digitalisering enerzijds en de opkomst van network governance anderzijds bij uitstek bijzonder relevant. RWS bevindt zich immers voor de uitoefening van zijn publieke taken geregeld in netwerken tezamen met andere overheden en private partijen. Er is vandaag de dag in de context van publieke dienstverlening dan ook geregeld sprake van netwerken, een **gedistribueerde realiteit** als het ware. RWS doet geregeld een beroep op technologie en algoritmen in een poging efficiënt te kunnen opereren in de complexe, hyper-geconnecteerde realiteit. Om **efficiëntie en betrouwbaarheid** te garanderen bij het **werken in netwerken** wordt nu ook in toenemende mate gekeken naar de mogelijke opportuniteiten die gedistribueerde technologie zoals blockchain kan opleveren. Het is deel van een zoektocht naar betrouwbare digitale netwerken, *network governance 2.0* of *digital network governance*.

4. Blockchaindesign

Blockchain is een **gedistribueerd grootboek** dat wordt onderhouden door een **peer-to-peer** (P2P) netwerk.[1] Gegevens worden hierop op **onveranderlijke** wijze geregistreerd en zijn in beginsel lastig te verwijderen. De gegevens zijn **transparant** voor de actoren die toegang en leesrechten hebben tot het netwerk respectievelijk de gegevens. Blockchaintechnologie wordt vaak ingezet tezamen met **smart contracts**. Een smart contract is een 'als x, dan y' **algoritme** of dus een set regels dat automatisch uitgevoerd wordt op het moment dat aan de vooraf vastgestelde conditie is voldaan.[2] Het gebruik van smart contracts vergroot de toepassingsmogelijkheden van blockchain enorm. In combinatie met smart contracts kan blockchain immers ingezet worden voor de automatisering van 1° de registratie van informatie, 2° waardeoverdracht en 3° het uitvoeren van regels.

Voor dit boek specifiek relevant is het feit dat toegang en leesrechten enerzijds en participatierechten anderzijds afhankelijk zijn van het blockchaindesign. Betreffende de **toegang** tot het netwerk en leesrechten kan een blockchain **publiek**, **privaat** of hybride zijn. Inzake de mogelijkheid om effectief te **participeren** in een netwerk kan een blockchain **permissionless**, **permissioned** of hybride zijn. In de praktijk zijn publieke blockchains meestal permissionless en zijn private blockchains doorgaans

1 Zie kennisclip 'What is blockchain technology', https://youtu.be/mfsK_AZPpSg.
2 Zie kennisclip 'What are smart contracts', https://youtu.be/_dvC4IRf1kA.

permissioned. Daarnaast maakt dit boek een belangrijk onderscheid in de analyse tussen **on-chain** of **off-chain registratie van gegevens**. Als gegevens op de blockchain worden geregistreerd, kunnen in beginsel alle deelnemers in het netwerk de geregistreerde gegevens bekijken. De gegevens kunnen echter ook off-chain geregistreerd worden, wat betekent dat de gegevens in een afgeschermd deel van de blockchain of apart en afgeschermd buiten de blockchain worden geregistreerd.

5. Wisselwerking tussen wettelijk kader betreffende toegang tot overheidsinformatie en blockchaindesignkeuzes

In dit boek zijn verschillende designkeuzes onderzocht die RWS heeft bij de inzet van blockchain. RWS heeft voornamelijk de keuze tussen een publieke of een private blockchain, een permissioned of een permissionless blockchain en kan opteren voor on-chain en off-chain gegevensopslag. Het boek analyseert uitvoerig de toegang tot en archivering van gegevens en informatie vanuit vier verschillende invalshoeken. Het gaat dan om gegevens en informatie die betrekking hebben op: 1° de **technische infrastructuur** (het blockchainsysteem), 2° de **gebruikers** (ketenpartners), 3° de **overheid** die een publieke taak of publiek gezag uitoefent (RWS in dit geval) en 4° de **informatieverzoeker** die zijn recht op toegang tot overheidsinformatie kan inroepen (de burger, maar bijvoorbeeld ook andere overheden dan RWS of een ketenpartner). De betrokken actoren kunnen ook meerdere posities tegelijkertijd innemen.

De toepassing van de Wob, de Woo en de Archiefwet is niet toegespitst op de inzet van een specifieke technologie, zodat de analyse inzake toegang tot en archivering van gegevens en informatie ook bij de inzet van blockchain relevant en noodzakelijk is. De **Wob** kent een **informatiestelsel**. Dit houdt in dat de verzoeker kan volstaan met een **verzoek tot openbaarmaking van informatie** over een bepaalde bestuurlijke aangelegenheid, waarna het de taak is van het bestuursorgaan om te onderzoeken of de gevraagde informatie in documenten is neergelegd. De verzoeker hoeft dus niet aan te duiden welk specifiek document hij wenst te ontvangen. De verzoeker hoeft er alleen maar voor te zorgen dat zijn verzoek ziet op een bestuurlijke aangelegenheid en voldoende concreet is om in behandeling te nemen.

Het boek identificeert onder de Wob vanuit de vier invalshoeken verschillende typen gegevens en informatie die kunnen kwalificeren als een document in de zin van de Wob en waarvoor dus Wob-verzoeken ingediend kunnen worden. Hierbij kan de **keuze voor een publieke of private blockchain invloed hebben op welke informatie in de blockchain openbaar is in de zin van de Wob**. Bij een publieke blockchain zal informatie openbaar zijn in de zin van de Wob, terwijl bij een privaat of permissioned blockchain netwerk dit in beginsel niet het geval is, tenzij RWS geen discretionaire ruimte heeft om toegang of leesrechten te weigeren aan de verzoeker. De **wijze waarop informatie wordt aangeboden** aan de ontvanger bij de

openbaarmaking in de praktijk is een **design aspect** dat bijkomende aandacht vergt, gezien de grote impact op de **toegankelijkheid** tot en **begrijpelijkheid** van informatie.

In tegenstelling tot de Wob kent de **Archiefwet** een **documentenstelsel**. Bij een dergelijk stelsel moet de verzoeker om informatie de documenten waarvan hij openbaarmaking vraagt benoemen of beschrijven. Het is daarbij niet nodig dat het gaat om een bestuurlijke aangelegenheid. Het boek identificeert vanuit de verschillende invalshoeken allerhande informatie die kan kwalificeren als een **archiefstuk** in de zin van de Archiefwet, waardoor RWS archiveringsverplichtingen heeft ook als hij blockchain inzet in zijn werkprocessen. Het is belangrijk dat RWS daarbij kan kiezen om informatie on-chain of off-chain op te slaan. Bij de **on-chain registratie van gegevens** doet zich telkens de cruciale vraag voor hoe aan de **vernietigingsplicht** onder de Archiefwet kan worden voldaan gezien het **onveranderlijke karakter van gegevens op de blockchain**. Hier dient dus voldoende aandacht voor te zijn in de design-fase.

De **Woo** maakt bestuurlijke transparantie de norm, wat het interessant zou kunnen maken voor RWS om met een **blockchainnetwerk te werken waartoe eenieder toegang heeft en eenieder informatie kan opvragen**. Het is wel cruciaal om in het achterhoofd te houden dat het toegankelijk maken van informatie niet per se impliceert dat informatie daarmee ook begrijpelijk is voor de ontvanger. Het **design van de user interface** speelt dus een belangrijke rol bij de betrachting om met de inzet van blockchain informatie daadwerkelijk transparant, toegankelijkheid en begrijpelijk te maken.

Samengevat in een notendop, laten de analyses zien dat er sprake is van een dynamische relatie tussen de **design keuzes** en de **juridische verplichtingen** voor RWS onder de Wob, de Woo en de Archiefwet. Bij het invullen van deze verplichtingen, het ontwikkelen en praktisch implementeren van beleid zal telkens voldoende aandacht moeten zijn voor de vier geïdentificeerde invalshoeken evenals voor de begrijpelijkheid van gegevens en informatie, zodat daadwerkelijk voldaan wordt aan de doelstellingen van de Wob, de Woo en de Archiefwet.

De verkennende analyse van het onderzoek mondt uiteindelijk uit in de volgende **tien vuistregels voor juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie**:

10 Vuistregels

CHAIN
Connecting Humankind through Algorithms and Information Networks

Voor juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie

Vuistregel 1

Schenk voldoende aandacht gedurende de gehele informatie-levenscyclus aan **duurzame digitale informatiehuishouding** en **toegankelijkheid van overheidsinformatie.**

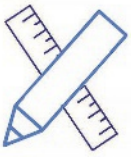
Vuistregel 2

Ontwerp de technische architectuur van de blockchain met de **Wob/Woo** en **Archiefwet** in het achterhoofd, aangezien het medium van de informatie en de opslagplaats voor de toepasselijkheid van deze wetten juridisch niet relevant zijn

Vuistregel 3

Weeg de voor- en nadelen van het blockchaindesign inzake gegevensopslag, -toegang en - bescherming af vooraleer een keuze te maken over **toegang** (publiek, privaat, hybride), **participatierechten** (permissioned of permissionless) en **gegevensopslag** (on-chain of off-chain)

Vuistregel 4



Waarborg bij het ontwerp van de technische infrastructuur '**access to information by design**' en **archiving by design**'.

Vuistregel 5

Richt **openbaarmaking** op **begrijpelijke** en **toegankelijke** wijze in en tracht toe te spitsen op de informatiebehoefte van de verzoeker.
Geef vorm aan wat begrijpelijk en toegankelijk is op basis van praktijktesten met gebruikers die **representatief** zijn voor de verschillende informatieverzoekers, zoals journalisten, burgers, bedrijven of overheden.

Vuistregel 6

Gegevens op een **publieke blockchain** die door een burger zelf te raadplegen zijn, vallen in beginsel **niet** onder de **reikwijdte van de Wob** en leiden dus niet tot te behandelen Wob-verzoeken.

Vuistregel 7

Het **design** van de blockchain architectuur en van de interface **is van groot belang** en **moet kunnen worden aangepast** in het licht van toekomstige wijzigingen in regelgeving (bv. inwerkingtreding Woo) en beleid.

Vuistregel 8

Het is aangeraden **persoonsgegevens en vertrouwelijke, concurrentiegevoelige bedrijfs- of fabricagegegevens off-chain** op te slaan.

Vuistregel 9

Maak een weldoordachte afweging welke informatie gearchiveerd wordt per proces en afhankelijk van de gevolgen van het proces, zodat een reconstructie gemaakt kan worden. **Het is aangeraden algoritmen te archiveren die een rol spelen in primaire werkprocessen.**

Vuistregel 10

Hou ook rekening met overige relevante regelgeving, zoals de Awb, de algemene beginselen van behoorlijk bestuur, de AVG, het mededingings- en aanbestedingsrecht en de Wet hergebruik overheidsinformatie.

I. Introductie

A. Aanleiding en doelstelling: strategische verkenning blockchain van Rijkswaterstaat

Rijkswaterstaat (RWS) is in de zomer van 2020 gestart met een strategische verkenning naar de mogelijke betekenis van de inzet van blockchain voor de organisatie. Het onderzoek vond plaats in het kader van het Programma Strategische Verkenningen. In deze verkenning is RWS een aantal pilots gestart samen met interne en externe ketenpartners om meer inzicht te krijgen in de toepassingsmogelijkheden en de consequenties, met inbegrip van de juridische consequenties, van de mogelijke inzet van blockchaintechnologie in de bestaande processen. In deze 'pilots' is alleen het bestaande proces herontworpen in een verkennend conceptproces geschikt voor blockchain, waarbij geen technische producten zijn ontworpen.

RWS onderzoekt in de strategische verkenning samen met interne en externe partners of de inzet van blockchain een meerwaarde zou kunnen opleveren ten opzichte van bestaande processen. Het gebruik van een relatief jonge, potentieel disruptieve gedistribueerde technologie, in dit geval blockchain, brengt verschillende juridische vraagstukken met zich mee waarop het antwoord in de literatuur, jurisprudentie en de bestuurspraktijk nog niet voldoende helder is uitgekristalliseerd. Ook is blockchain een relatief nieuwe informatietechnologie die op dit moment niet specifiek in de huidige nationale wet- en regelgeving wordt geadresseerd, wat ook bij andere nieuwe informatietechnologieën vaak nog steeds het geval is. De strategische verkenning van RWS tracht bijgevolg een **pragmatische, hernieuwde interpretatie van de huidige regelgeving** te hanteren. Omdat de RWS blockchainpilots een louter verkennend en oriënterend karakter hebben, hebben initiële analyses vooralsnog enkel op abstract niveau plaatsgevonden. Desondanks tracht de strategische verkenning een kader te bieden dat bij de doorontwikkeling van deze pilots gebruikt kan worden.

Ondanks de poging tot pragmatische interpretatie van de huidige regelgeving, kwamen uit de juridische analyse binnen RWS enkele vraagstukken naar voren waar een combinatie van blockchainexpertise en juridische expertise voor nodig is. Het gaat dan met name om de gevolgen van de toepassing van de **Archiefwet**,

de Wet openbaarheid van bestuur (**Wob**) en de Wet open overheid (**Woo**), evenals juridische vraagstukken die in een latere fase bij de verkenning van het gebruik van blockchain naar voren kunnen komen. De Archiefwet en de Woo, die vanaf 1 mei 2022 (gedeeltelijk) in werking treedt en daarmee de Wob vervangt, bevatten immers belangrijke regels voor RWS met betrekking tot toegang tot overheidsinformatie.[1] Dit wetgevende kader brengt enkele specifieke juridische vraagstukken met zich mee bij een mogelijke toekomstige toepassing van blockchain.

RWS gaf daarom aan dat er behoefte is aan aanvullend juridisch opdrachtonderzoek dat gebruikt kan worden om de verkenning verder vorm te geven. Het onderzoek in het voorliggende boek van de interdisciplinaire onderzoeksgroep CHAIN (Tilburg University en Universiteit Utrecht), die beschikt over juridische, techniek-filosofische en technische expertise, komt aan deze vraag tegemoet.[2] Het voorliggend juridisch opdrachtonderzoek beoogt op grond van een **verkennende, exploratieve analyse** een basis te bieden voor de beantwoording van enkele juridische vraagstukken betreffende vereisten van transparantie en openbaarheid van bestuur in het kader van het recht op toegang tot overheidsinformatie bij de inzet van blockchain door de overheid, met inbegrip van de impact van het wettelijke kader op de mogelijke keuzes inzake de architectuur of het design van de technologie.

Het boek heeft bijgevolg, net zoals de strategische verkenning blockchain van RWS waarbinnen het tot stand kwam, voornamelijk een verkennend, oriënterend karakter. Het beoogt RWS een basis te bieden om de materie nader uit te diepen. Uitspraken en conclusies in dit onderzoek kunnen enkel worden toegerekend aan de onderzoekers. In het boek zijn geen standpunten van RWS opgenomen. Ook wordt in het boek niet voorgesorteerd en aangestuurd op bepaalde beleidskeuzes van RWS. Daarnaast moet ook voor ogen worden gehouden dat de pilots puur verkennende scenario's zijn. Dit betekent dat de beschrijvingen van de pilots in dit boek een orienterend toekomstbeeld schetsen en dus niet de huidige werkpraktijk.

---

1 Het onderzoeksrapport voor RWS werd inhoudelijk afgerond op 29 oktober 2021. Per 1 mei 2022 treedt de nieuwe Wet open overheid (Woo) (gedeeltelijk) in werking en vervangt daarmee de Wet openbaarheid van bestuur (Wob). In de analyse is gekeken naar de Wob, maar ook naar de impact die de inwerkingtreding van de Woo met zich zou kunnen meebrengen voor de analyse.

2 Dit in opdracht van RWS opgeleverde onderzoeksrapport is mede tot stand gekomen in het kader van het door NWO gefinancierd interdisciplinair onderzoek over blockchaintoepassingen van de overheid: 'Blockchain in de netwerksamenleving. Op zoek naar transparantie, vertrouwen en legitimiteit' binnen het onderzoeksprogramma 'Verantwoord Innoveren. Ontwerpen voor publieke waarden in een digitale wereld'. De auteurs wensen tevens Annemarie Balvert (TiU) en de medewerkers van RWS te bedanken voor hun waardevolle feedback en input.

B. Structuur, onderzoeksvragen en methodologie

Het boek is als volgt opgebouwd. Na bovenstaande toelichting van de doelstelling en aanleiding van dit boek, namelijk de strategische verkenning blockchain van RWS, behandelt het **inleidende hoofdstuk (I.)** in deze sectie de structuur van het onderzoek en de methode, met inbegrip van de beperkingen inzake de omvang van het onderzoek. Vervolgens schetst het enkele bredere evoluties inzake overheidsoptreden, licht het de verkende technologie (blockchain en smart contracts) beknopt toe en tenslotte neemt het twee blockchainpilots van RWS onder de loep, namelijk de pilot zoutlogistiek en de pilot grondstromen. Vervolgens wordt het **wettelijke kader betreffende de toegang tot overheidsinformatie (II.)** op een toegankelijke manier weergegeven. Daarbij zal worden ingegaan op de Wob, de Woo en de Archiefwet. Vervolgens volgt een **korte verkenning van overige relevante juridische vraagstukken (III.)** met enkele juridische vragen die de inzet door de overheid van gedistribueerde technologie in het algemeen en blockchain specifiek met zich mee kan brengen, die in een latere fase bij de verkenning van het gebruik van blockchain naar voren kunnen komen. Het gaat hier over de toepassing van de Algemene wet bestuursrecht (Awb), met inbegrip van de operationalisering van algemene beginselen van behoorlijk bestuur zoals het zorgvuldigheids- en motiveringsbeginsel, de Algemene Verordening Gegevensbescherming (AVG), het mededingings- en aanbestedingsrecht, en de Wet hergebruik overheidsinformatie (Who). Vervolgens wordt nog beknopt ingegaan op de mogelijke functies van blockchaingebaseerde smart contracts, en de kwaliteit van input via oracles. Na een **tussenconclusie (IV.)** volgt de kern en het vernieuwende aspect van dit boek, namelijk een **verkenning van de toepassing van het wettelijk kader betreffende de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie (V.)**. Daarbij zullen eerst de soorten designkeuzes en typen informatie worden toegelicht, waarna de consequenties van het wettelijk kader op de keuzes in de architectuur van de technologie zullen worden geanalyseerd. Deze verkennende analyse zal uitmonden in **tien vuistregels voor juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie (VI.)**.

In de verkenning van de toepassing van het wettelijk kader betreffende de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie (III.) onderscheidt dit boek vier **invalshoeken** die een impact kunnen hebben op de beschikbaarheid van en toegang tot gegevens en informatie: 1° de **technische infrastructuur** (i.e. het blockchainsysteem), 2° de **gebruikers** (ketenpartners), 3° de **overheid** die een publieke taak of publiek gezag uitoefent (RWS in dit geval) en 4° de **informatieverzoeker** die zijn recht op toegang tot overheidsinformatie kan inroepen (de burger, maar ook andere overheden dan RWS of een ketenpartner bijvoorbeeld). Het gemaakte onderscheid tussen deze vier invalshoeken verrijkt de analyse. Betrokken actoren kunnen natuurlijk verschillende of meerdere posities tegelijkertijd innemen.

De analyse van het onderzoek beoogt voornamelijk een basis te bieden voor de beantwoording van de volgende door RWS geïdentificeerde deelvragen, waar telkens ook een korte toelichting vanuit RWS bij wordt geschetst:

1° Welke consequenties heeft de Archiefwet op het gebruik van blockchain voor RWS, en heeft dit invloed op het type blockchain dat binnen RWS ingezet kan worden?

Uit de strategische verkenning van RWS is gebleken dat RWS vaak te maken heeft met het verwerken van informatie in de zin van de Archiefwet. Denk bijvoorbeeld aan informatie over gebruikte conserveringen op assets, verkeersdrukte of meterstanden van rivierwater. Dit onderzoek beoogt RWS bijgevolg houvast te bieden bij het identificeren van de consequenties van het gebruik van blockchain voor de toepassing van de Archiefwet en daarnaast te beoordelen in welke mate of op welke wijze het gebruik van blockchain in overeenstemming zou zijn met deze wet. Conceptueel vertrekt de Archiefwet en -regelgeving van het principe: één waarheid op één plek, terwijl blockchaintechnologie uitgaat van een verspreide, gedistribueerde opslag waarbij de betrouwbaarheid van data en transacties in beginsel wordt geverifieerd en gegarandeerd door (een meerderheid van) het netwerk en niet door een *trusted third party*. Dit leidt tot spanning en derhalve tot nieuwe juridische en praktische uitdagingen.

Bij een *permissioned blockchain* krijgen opnieuw één of meerdere *trusted third parties* een rol toebedeeld om te bepalen wie toegang heeft tot het blockchainnetwerk, evenals wie wat juist mag doen in het netwerk.[3] Dit lijkt op het eerste gezicht mogelijk te maken dat RWS de rol van archiefvormend orgaan kan opnemen met inbegrip van de bijhorende verantwoordelijkheden. Het is dan wel van belang dat de rol en verantwoordelijkheden van RWS vooraf in de design-fase duidelijk worden vastgelegd en ingericht. In het geval van een *permissionless blockchain* is er echter geen *trusted third party* en kan RWS op het eerste gezicht moeilijk een verantwoordelijk archiefvormend orgaan zijn, tenzij de meerderheid van het netwerk de informatie over de transacties bij RWS in beheer geeft. Naast de gegevens en informatie die dan bij RWS geborgd moeten worden, dient in dat geval ook de blockchain door RWS gearchiveerd te worden als audit-trail, zodat duidelijk blijft wie wat wanneer heeft besloten.

Binnen RWS zijn specifieke bewaartermijnen opgenomen in de Selectielijst IenW die verschillen per proces en per type gegevens of informatie. Daarbij zijn tijdens de strategische verkenning blockchain van RWS al enkele concrete vragen gerezen: betekent de wettelijke plicht om gegevens te vernietigen na verloop van tijd dat deze gegevens ook fysiek verwijderd dienen te worden? Of wordt aan dit wettelijke vereiste voldaan zodra het technisch wordt ingeregeld dat de informatie niet meer door mensen of systemen te consulteren is, bijvoorbeeld door wachtwoordbeheer?

3 Zie p. 74.

In beginsel wordt informatie immers *'untraceable'* vernietigd om te voldoen aan de vernietigingsplicht. Hierbij worden enkel metagegevens van het vernietigde record vastgelegd in een vernietigingslijst, zodat aantoonbaar blijft welke informatie vernietigd is. Aangezien bij blockchain in beginsel alleen informatie kan worden toegevoegd, en dus niet gewijzigd of vernietigd, lijkt de blockchaintechnologie op gespannen voet te staan met de Archiefwet en -regelgeving. Terwijl bij blockchain informatie alleen kan worden toegevoegd en bijgevolg een hoge betrouwbaarheidsfactor heeft, is de betrouwbaarheid van informatie nu vaak gebaseerd op de partij die de informatie verstrekt, RWS bijvoorbeeld. Wanneer een *permissioned blockchain* zo zou worden ingericht dat RWS bijvoorbeeld informatie wel kan vernietigen, lijkt spanning te ontstaan met het principiële onveranderlijke karakter van blockchain. Vertrouwen wordt opnieuw gecentraliseerd in plaats van gedistribueerd. De vraag rijst dan in welke mate de inzet van blockchain meerwaarde biedt.

2° Op welke wijze heeft het gebruik van blockchain invloed voor RWS op de verplichtingen uit de Wob en de Woo en welke impact heeft deze wetgeving op de keuze in het design van een blockchainnetwerk?

Blockchain kan ondersteuning bieden bij het ontwikkelen van een transparante en betrouwbare administratie. Dit zou onder meer kunnen betekenen dat RWS eventueel sneller zou kunnen voldoen aan Wob-verzoeken die binnenkomen. Wob-verzoeken kunnen niet enkel binnenkomen van burgers, maar tevens van andere overheden, bijvoorbeeld over toegepaste grond en bagger. Daarbij worden bijvoorbeeld gegevens opgevraagd over de gedane meldingen in een bepaalde tijdsperiode, inclusief de communicatie van RWS onder meer inzake hoeveelheden, beoordeling, e-mails, toezicht en handhaving. Binnen RWS is dan ook de vraag gerezen wat de concrete impact zou zijn van het gebruik van blockchain op de transparantieverplichtingen onder de Wob. In welke mate is de informatie in de blockchain bijvoorbeeld Wob-baar en kunnen informatieverzoekers zelf informatie in de systemen opzoeken, zodat dit mogelijk het aantal Wob-verzoeken kan verminderen? Ook rijst de vraag wat de consequenties zullen zijn van de nieuwe Woo die vanaf 1 mei 2022 (gedeeltelijk) in werking treedt. Op welke wijze kan blockchain worden ingezet om overheidsinformatie transparanter te maken voor de samenleving en waar moet RWS juridisch rekening mee houden om zijn informatie beter vindbaar en uitwisselbaar te maken, goed te laten ontsluiten en te archiveren? Het kerndoel van de Wob is het reguleren van de openbaarheid van bestuur en de informatievoorziening hiervan. Tegelijkertijd kent de Wob echter ook weigeringsgronden met het oog op de bescherming van belangen van burgers, zoals privacybelangen, maar ook bedrijfsgevoelige informatie bijvoorbeeld. De vraag rijst hoe RWS deze belangen kan borgen in een blockchainnetwerk. Daarnaast is het voor de toepassing van de Wob van belang om vast te stellen bij welk bestuursorgaan een document berust en stelt zich de vraag hoe het blockchain document eruitziet gelet op de definitie van artikel 1 sub a Wob.

3° Tot welke overige, toekomstige juridische vraagstukken kan het gebruik van blockchain binnen RWS en zijn ketenpartners leiden, die in de toekomst nader onderzocht dienen te worden?

Het programma strategische verkenning van RWS streeft na om permanent alert te zijn voor nieuwe trends en ontwikkelingen die mogelijk van invloed kunnen zijn op RWS. In dat kader hebben zij geconstateerd dat nieuwe informatietechnologieën zoals blockchain leiden tot nieuwe juridische vraagstukken. Deze onderzoeksvraag is derhalve bedoeld om eventuele toekomstige juridische vraagstukken omtrent nieuwe informatietechnologieën zoals blockchain proactief te signaleren, zodat RWS daar al vroegtijdig op kan inspelen. Er wordt in **III. Korte verkenning van overige relevante juridische vraagstukken** aldus beknopt ingegaan op de Algemene wet bestuursrecht (**Awb**), met inbegrip van de operationalisering van algemene beginselen van behoorlijk bestuur zoals het zorgvuldigheids- en motiveringsbeginsel, de Algemene Verordening Gegevensbescherming (**AVG**), het **mededingings- en aanbestedingsrecht**, en de Wet hergebruik overheidsinformatie (**Who**). Er wordt ook beknopt ingegaan op de mogelijke functies van blockchaingebaseerde **smart contracts**, en de kwaliteit van input via **oracles**.

Om te komen tot een wetenschappelijk onderbouwde beantwoording van bovenstaande vragen zal het onderzoek een rechtswetenschappelijke beschrijving en analyse verrichten van de betreffende wet- en regelgeving, inclusief relevante jurisprudentie, evenals een literatuurscan (met inbegrip van rapporten en beleidsdocumenten). Deze analyse heeft algemeen betrekking op de Wob, de Woo en de Archiefwet, maar met een focus op bijdragen die specifiek betrekking hebben op de inzet van digitale dragers en systemen, in dit geval blockchaintechnologie en smart contracts (i.e. 'als x, dan y' algoritmen). In beginsel is voornamelijk Nederlandse literatuur geraadpleegd, en waar nodig internationale literatuur als aanvulling.

Het boek houdt rekening zowel met een doelpubliek van experts in een bepaald deeldomein van het onderzochte onderwerp, als een breder doelpubliek met onder meer beleidsmakers. Vakjargon zal daarom worden gebruikt, doch steeds zo goed als mogelijk worden toegelicht.

Na een **doctrinaire rechtswetenschappelijke beschrijving** van het wettelijke kader betreffende de toegang tot overheidsinformatie (II.), kan de verkenning van de toepassing van het wettelijke kader betreffende de toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie gecategoriseerd worden als **exploratief onderzoek**.[4] Het bevat dan ook een preliminaire analyse aangaande de consequenties van het wettelijk kader op de keuzes in de architectuur van de blockchaintechnologie.

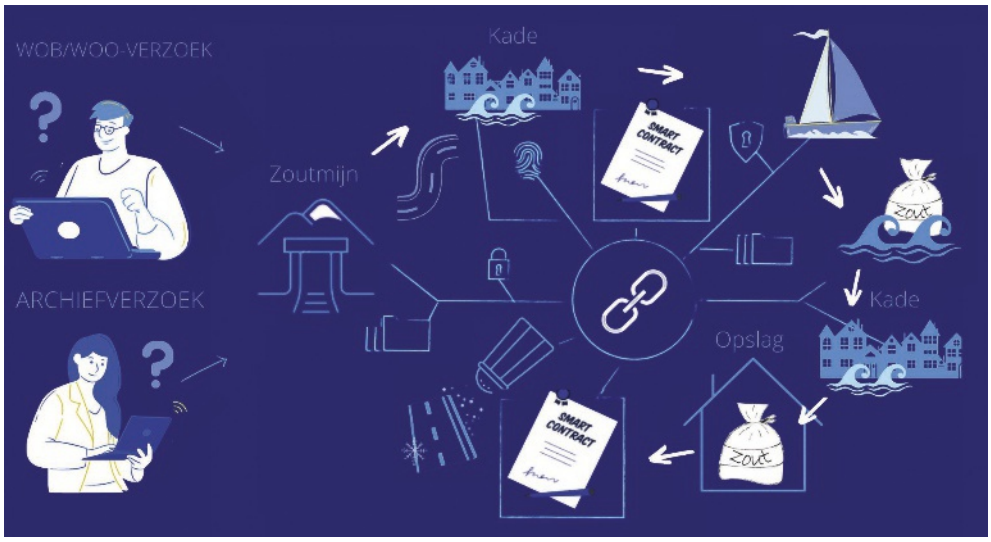
4 Zie Hirsch Ballin 2020.

De **focus** van het onderzoek ligt op de juridische rechten en verplichtingen die voortvloeien uit **de Wob, de Woo en de Archiefwet**. Bij het wettelijke kader betreffende de toegang tot overheidsinformatie (II.) worden op het einde kort en niet-exhaustief enkele overige aspecten van het juridisch kader in beeld gebracht, namelijk 1° de algemene beginselen van behoorlijk bestuur en de Algemene wet bestuursrecht, 2° de Algemene Verordening Gegevensbescherming, 3° het mededingings- en aanbestedingsrecht, 4° de Wet hergebruik overheidsinformatie. Een verdere behandeling hiervan ligt buiten de opzet en de omvang van deze onderzoeksopdracht.

Theoretische analyses inzake de consequenties van de inzet van blockchaintechnologie kunnen een stap verder worden gebracht door rekening te houden met een **specifieke context**. In dit boek is er daarom voor gekozen om de analyse van context te voorzien op basis van twee blockchainpilots die ontwikkeld zijn binnen RWS: grondstromen en zoutlogistiek (zie I. E. en zie figuren 1 en 2). Op basis van deze twee RWS blockchainpilots wordt de wisselwerking onderzocht tussen de theorie en de praktijk, waarbij de concrete context de analyse kan verrijken. De informatie betreffende deze twee pilots is het resultaat van informatie van en gesprekken met RWS.

Figuur 1 Blockchainpilot grondstromen en recht op toegang tot overheidsinformatie

Figuur 2 Blockchainpilot zoutlogistiek en recht op toegang tot overheidsinformatie



C. Bredere evoluties inzake overheidsoptreden: de opkomst van digital network governance

De organisatie en het functioneren van het openbaar bestuur in Nederland hebben de voorbije decennia voornamelijk vier belangrijke evoluties ondergaan.

– Ten eerste heeft de formele wetgever in toenemende mate regelgevende bevoegdheden toegekend aan het bestuur, met als voornaamste beweegreden dat de aanwezigheid van expertise noodzakelijk is voor het normeren van bepaalde beleidsterreinen. Aldus kan een terugtred van de wetgever worden waargenomen en is de laatste decennia een zogenaamde ***administrative state*** ontstaan.[5] Hierdoor heeft het bestuur, en dus ook RWS, een aanzienlijk takenpakket.
– Ten tweede is er binnen de overheid sprake van een toegenomen inzet van **digitalisering door het bestuur**, ook bij RWS, in combinatie met een bepaalde mate van ondoorzichtigheid van technologie (cfr. Black box), wat leidt tot belangrijke uitdagingen inzake transparantie, uitlegbaarheid en accountability. Deze digitalisering heeft tevens een belangrijke impact op de machtsevenwichten binnen de Trias Politica, waarbij de wetgever moeilijk grip krijgt op digitalisering binnen het bestuur. Zo heeft de Tweede Kamer op 2 juli 2019 de tijdelijke onderzoekscommissie 'Digitale toekomst' ingesteld om meer zicht en grip te krijgen op gewenste en ongewenste ontwikkelingen op het vlak van digitalisering door middel van de versterking van haar democratische controlefunctie.[6]

5 Lindseth 2010; Hirsch Ballin 2015.
6 Op 28 mei 2020 heeft de commissie haar eindrapport 'Update vereist – Naar meer parlementaire grip op digitalisering' overhandigd.

– Ten derde is naast bovenstaande twee belangrijke evoluties betreffende de horizontale machtenscheiding, op het vlak van de verticale machtenscheiding een **complexe, meergelaagde rechtsorde** ontstaan die gekenmerkt wordt door multilevel governance. Zo werkt ook RWS, als rijksinstelling, bijvoorbeeld samen met gemeenten, onder meer voor het inkopen van strooizout. Daarnaast dient hij bijvoorbeeld rekening te houden met Europese regelgeving onder meer inzake overheidsopdrachten en privacywetgeving.
– Ten vierde wordt in toenemende mate bestuurd via complexe publiek-private netwerken, waarbij eenzijdige gezagsuitoefening door de overheid wordt aangevuld met andersoortige sturingsmechanismen en verschillende vormen van **network governance**. Samenwerken met andere actoren is ook voor RWS een dagelijkse realiteit bij zijn taakuitoefening. Netwerkend werken is evenwel voor vele overheidsorganisaties een uitdaging, aangezien ze doorgaans niet ingericht zijn te opereren in netwerken.[7]

Voor dit boek zijn de opkomst van digitalisering enerzijds en het besturen in netwerken anderzijds bij uitstek bijzonder relevant. RWS bevindt zich voor de uitoefening van zijn publieke taken geregeld in netwerken tezamen met andere overheden en private partijen. Er is vandaag de dag in de context van publieke dienstverlening dan ook in realiteit geregeld sprake van **gedistribueerde realiteit**. Dit leidt er bijgevolg toe dat ook de overheid een beroep doet op technologie om efficiënt te kunnen opereren in een complexe, hyper-geconnecteerde realiteit. Denk aan de inzet van eenvoudige en complexe algoritmen die besluitvormings- en werkprocessen gedeeltelijk of geheel kunnen automatiseren, de opkomst van Internet of Things en Artificiële Intelligentie, met inbegrip van zelflerende systemen, geautomatiseerde feitenvaststelling, digitale platformen, én – in het kader van dit onderzoek *last but not least* – gedistribueerde technologieën zoals blockchain.

Om efficiëntie en betrouwbaarheid te garanderen bij het werken in netwerken wordt in toenemende mate geëxperimenteerd met de mogelijkheden die blockchaintechnologie als *Distributed Ledger Technology* (DLT) kan opleveren. Dit is logisch te verklaren in een wereld die steeds vaker wordt beschreven in termen zoals de platformeconomie, de informatie- en netwerksamenleving. Gedecentraliseerde en gedistribueerde technologieën, zoals blockchain, zijn deel van een zoektocht naar efficiënte, betrouwbare *digitale* netwerken, **network governance 2.0** of **digital network governance**, waarbij netwerken kunnen of moeten opereren zonder afhankelijkheid van en vertrouwen in één centrale partij. Aangezien RWS in verschillende processen zelf als centrale partij optreedt, heeft hij dan ook hierover een strategische verkenning opgezet.

7 Sedimentatie in sturing. Systeem brengen in netwerkend werken door meervoudig organiseren (2015).

D. De blockchaintechnologie

Deze sectie geeft een beknopte uitleg over wat blockchain en smart contracts zijn.[8] Blockchain is een **gedistribueerd grootboek**, een soort gedistribueerde database, en wordt onderhouden door een **peer-to-peer** (P2P) netwerk. Blockchain is een **gedistribueerd netwerk**, namelijk een computernetwerk met een gedecentraliseerde, gedistribueerde structuur in plaats van een gecentraliseerde structuur (zie figuur 3). Hierdoor is in beginsel de controle in het netwerk niet gecentraliseerd bij één centrale server of instantie, maar gedecentraliseerd en zelfs gedistribueerd onder meerdere participanten in het netwerk. Blockchain kan worden gecategoriseerd als een **distributed ledger technology (DLT)**.

Figuur 3 Gecentraliseerd, gedecentraliseerd en gedistribueerd netwerk

Een gedistribueerd blockchain netwerk bestaat uit verschillende datapunten of participanten, **nodes** genaamd. Elke node heeft een (gedeeltelijke) versie van de database die continu wordt geüpdatet. Binnen dit netwerk worden '**transacties**' uitgevoerd. In blockchain termen is een transactie niet enkel de overdracht van waarde, maar kan dit ook het registreren van gegevens en het uitvoeren van regels zijn.[9] Binnen het netwerk bestaan ook verschillende typen nodes. Zo kan een node een **full node** of een **light node** zijn. Een full node heeft een kopie van de gehele database en een light node heeft maar een deel van de kopie van de database.

De transacties in een blockchainnetwerk vinden plaats onder **pseudoniemen**. Elke deelnemer in het netwerk heeft een **publieke** en een **private sleutel**. De publieke sleutel is zichtbaar voor iedereen, de private sleutel is alleen zichtbaar voor de houder van de sleutel. Deze sleutels worden gebruikt bij het uitvoeren van transacties. Nieuwe transacties worden in blokken toegevoegd, die aan elkaar verbonden zijn

8 Voor een uitgebreidere uitleg over blockchaintechnolgie kan u bv. het volgende boek raadplegen: 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 Uitgevers 2020).

9 Zie: NEN ISO 22739.

door middel van cryptografische links, genaamd **hashes**. Ieder individueel blok bevat naast de transacties van het blok ook een **header** en tijdstempels.[10] Deze **tijdstempels** worden door het netwerk collectief gevalideerd, zodat onomstotelijk vaststaat wanneer exact een transactie in de blockchain is opgenomen en antedatering dus wordt uitgesloten.

Elke hash is uniek en verwijst naar het voorgaande blok, waardoor een *chain of blocks*, een ketting van blokken, ontstaat. Zodra er een transactie wordt toegevoegd, worden alle kopieën van de database in het netwerk geüpdatet. De transacties vinden plaats door middel van een **consensusmechanisme**, wat een set regels is waarmee overeenstemming tussen de nodes in het netwerk wordt bereikt over de geldigheid van een transactie.[11] Het consensusmechanisme is gebaseerd op crypto-economische inzichten[12] en heeft een effect op hoe miners zich in het netwerk gedragen. Miners zijn nodes die blokken 'minen' voor een vergoeding. Minen is het creëren of het valideren van blokken.[13] Twee bekende voorbeelden van een consensusmechanismen zijn *Proof of Work* en *Proof of Stake*.[14] Bij het Proof of Work (PoW) consensus mechanisme krijgt de miner die het snelste de cryptografische puzzel oplost de vergoeding. Een voorbeeld hiervan is het Bitcoin consensusmechanisme. Bij het Proof of Stake (PoS) consensusmechanisme wordt het 'recht' om het blok te minen toegekend op basis van een algoritme dat onder andere meeweegt hoeveel tokens de individuele miners hebben ingelegd (het inleggen van tokens wordt 'staken' genoemd). Een voorbeeld hiervan is het Ethereum consensus mechanisme.[15]

Deze manier van registratie van gegevens op de blockchain beoogt **onveranderlijkheid**.[16] Als gegevens eenmaal geregistreerd zijn op een blockchain, kunnen deze niet meer aangepast of verwijderd worden, omdat dit een verandering in de hash zou teweegbrengen. Er kunnen alleen maar blokken worden **toegevoegd**[17] aan de blockchain.[18] Deze eigenschap zorgt voor het behoud van data-integriteit. Dit zorgt tevens voor 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

10 Voor een voorbeeld van een blok: https://www.blockchain.com/btc/block/000000000000000000301fcfeb141088a93b77dc0d52571a1185b425256ae2fb.
11 NEN ISO 22739, artikel 3.12 en 3.11.
12 Crypto-economie is een opkomende multidisciplinaire wetenschap die gebaseerd is op economie, speltheorie en cryptografie. Crypto-economische systemen gebruiken beweegredenen of straffen om het gedrag van actoren te sturen met als doel het borgen van veiligheid en integriteit van systemen. Zie Brekke & Zuhair Alsindi 2021.
13 NEN ISO 22739, artikel 3.49.
14 Voor andere consensus mechanismen, zie: Aggarwal & Kumar 2021.
15 Wackerow 2021 & Blockgenic 2018.
16 De Engelstalige term hiervoor is 'immutability'.
17 De Engelstalige term hiervoor is 'append-only'.
18 Goossens, Verslype & Tjong Tjin Tai 2020, p. 20.

of de zorgplicht van de overheid tot het vernietigen van de daarvoor in aanmerking komende archiefbescheiden ingevolge artikel 3 Archiefwet.[19]

Als gegevens op de blockchain worden geregistreerd, dan noemt men dat ***on-chain*** registratie van gegevens, wat in beginsel betekent dat alle deelnemers in het netwerk kunnen zien dat de registratie van gegevens heeft plaatsgevonden.[20] De gegevens kunnen echter ook ***off-chain*** geregistreerd worden, wat betekent dat de gegevens in een afgeschermd deel van de blockchain of in een aparte afgeschermde ruimte geregistreerd worden.[21] De gegevens worden daarmee dus niet vastgelegd op de blockchain en staan dan in een afzonderlijke (gecentraliseerde of gedecentraliseerde) database. Gegevens die off-chain geregistreerd zijn, bezitten bijgevolg niet de eigenschappen van onveranderlijkheid en onweerlegbaarheid die on-chain registratie kenmerkend met zich meebrengen. Daarnaast zijn de off-chain geregistreerde gegevens ook niet onmiddellijk toegankelijk voor het blockchainnetwerk.

Een blockchain kan publiek (openbaar of open), privaat (afgeschermd of gesloten) of hybride zijn.[22]
- Bij een **publieke** blockchain kan iedereen *toegang* krijgen tot het netwerk. Voorbeelden hiervan zijn Bitcoin en Ethereum. Iedereen kan de blockchain dus bekijken.
- Bij een **private** blockchain, bijvoorbeeld Hyperledger, is de toegang tot het netwerk beperkt tot een bepaalde groep die is uitgenodigd of aan wie toegang is verschaft al dan niet na het voldoen aan bepaalde voorwaarden. Meestal bepaalt een centrale verwerker wie toegelaten wordt.
- Een **hybride** blockchain is dan weer een combinatie van beiden, waarbij sommige delen van het netwerk openbaar en andere afgeschermd zijn.

Een blockchain kan ook *permissionless*, *permissioned* of hybride zijn.[23] In de praktijk zijn publieke blockchains meestal permissionless en zijn private blockchains doorgaans permissioned.
- 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. In de praktijk zijn dit vaak publieke, open netwerken. Dit is tot op bepaalde hoogte te vergelijken met het internet. Iedereen met toegang tot het internet heeft in alle transparantie toegang tot de volledige blockchain en iedereen kan volwaardig participeren in het netwerk, onder meer door het

19 Zie p. 48.
20 Dit betekent niet dat de gegevens zelf ook voor iedereen kenbaar en leesbaar zijn, aangezien de gegevens ook versleuteld geregistreerd kunnen worden.
21 Zie p. 75.
22 Zie Goossens, Verslype & Tjong Tjin Tai 2020, p. 23 en 24.
23 Zie Goossens, Verslype & Tjong Tjin Tai 2020, p. 24.

uitvoeren van transacties of het bijdragen in 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 niet alleen een controlelaag die bepaalt wie toegang heeft tot het blockchainnetwerk, maar die tevens bepaalt wie wat mag doen in het netwerk. Hierdoor is er geen sprake meer van een volledig gedistribueerd netwerk. Zo kan de ene persoon bijvoorbeeld wel transacties plaatsen, maar staat deze niet in voor het veilig en operationeel houden van de blockchain. In een permissioned netwerk kennen participerende partijen elkaar of is er minstens een manier om participanten te identificeren. Zo'n blockchainnetwerk heeft vaak veel minder participanten en is eerder vergelijkbaar met een intranet van een bedrijf of consortium.
  Permissioned blockchainnetwerken zijn in beginsel energie-efficiënter en sneller omwille van het gebruikte consensusmechanisme. In tegenstelling tot permissionless netwerken zijn er meer transacties per seconde mogelijk en zijn er minder partijen betrokken bij de validatie van transacties, waardoor de mate van distributie van vertrouwen lager is. Aangezien minder partijen instaan voor de validatie, hebben deze controlerende individuele actoren relatief gezien meer zeggenschap over het netwerk dan bij volledige gedistribueerdheid, waardoor tegelijk ook de kans op manipulatie van transacties door deze actoren groter is. Hierdoor is er een hoge mate van vertrouwen in deze actoren vereist. Bij een permissioned blockchain netwerk staat een beperkt aantal entiteiten in voor het aanbieden en functioneren van het netwerk en de transacties, wat tevens ten koste gaat van vrije participatie en pseudonimiteit. Dergelijke toepassing is dus eerder gedecentraliseerd dan gedistribueerd, maar leent zich wel makkelijker voor toepassingen in een context waar bijvoorbeeld een overheid bepaalde verantwoordelijkheden en plichten heeft bij de uitoefening van publieke taken en publiek gezag.
– Er bestaan ook **hybride** netwerken, bijvoorbeeld Ripple. Iedereen kan Ripple gebruiken voor financiële transacties, maar het verwerken van transacties in de blockchain en het veilig houden van het netwerk is in handen van een beperkt aantal vaste validatoren.

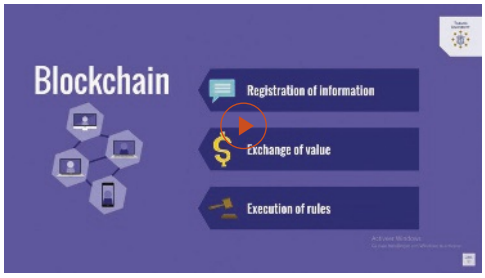
Figuur 4 Vergelijking permissionless vs. permissioned blockchain

Permissionless	Permissioned
Open voor participatie door eenieder	Controlelaag voor participatie in het netwerk
Doorgaans bijzonder energie-inefficiënt	Vaak energie-efficiënter
Trager: minder transacties en blocks per seconde	Sneller
Gedistribueerd vertrouwen	Ge(de)centraliseerd vertrouwen
Virtuele munten nodig voor transacties	Geen virtuele munten nodig voor transacties

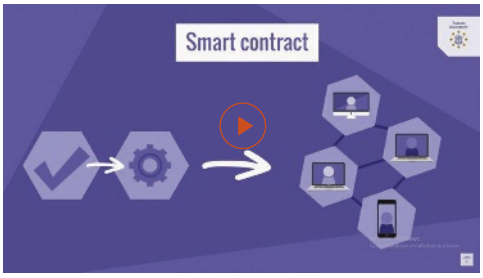
Een **smart contract** tenslotte is een simpel algoritme, namelijk een deterministische set regels die automatisch uitgevoerd worden op het moment dat aan de vooraf vastgestelde condities is voldaan. Bijvoorbeeld, *als* je je huis isoleert, *dan* ontvang je een subsidie. Het gebruik van smart contracts vergroot de toepassingsmogelijkheden van blockchain enorm. In combinatie met smart contracts kan blockchain immers ingezet worden voor de automatisering van 1° de registratie van informatie, 2° waardeoverdracht en 3° het uitvoeren van regels. Smart contracts hebben een input nodig om output te kunnen genereren, en hiertoe zijn smart contracts niet zelf in staat. Ze zijn als het ware 'doof en blind'.[24] ***Oracles*** zijn hardware of software die ervoor zorgen dat informatie die zich bevindt buiten het blockchain ecosysteem binnen het blockchainnetwerk wordt gebracht. Denk bijvoorbeeld aan een geluidsmeter of bewegingssensor. Een oracle vormt daarmee als het ware een brug tussen de wereld buiten de blockchain en het blockchainnetwerk. De inzet van oracles leidt echter tot het zogenaamde 'oracle problem', namelijk het wederom ontstaan van een afhankelijkheid ten aanzien van een centrale partij die vertrouwd dient te worden.[25]

Indien u op een visuele aantrekkelijke, toegankelijke manier kennis wil maken met blockchain en blockchaingebaseerde smart contracts, kunnen we u verwijzen naar twee kennisclips van de CHAIN onderzoeksgroep.[26]

Figuur 5 **Kennisclip 'What is blockchain technology'**



Figuur 6 **Kennisclip 'What are smart contracts'**



E. Twee blockchainpilots van Rijkswaterstaat onder de loep

1° Rijkswaterstaat

RWS is een rijksinstelling verantwoordelijk voor aanleg, beheer en onderhoud van de rijkswegen, -vaarwegen en -wateren. RWS zorgt daarmee voor een veilig, leefbaar en bereikbaar Nederland. RWS is een uitvoerend agentschap van het Ministerie

24 Goossens, Verslype & Tjong Tjin Tai 2020, p. 47-78.
25 Collins 2020.
26 Zie kennisclip 'What is blockchain technology', https://youtu.be/mfsK_AZPpSg, en kennisclip 'What are smart contracts', https://youtu.be/_dvC4IRf1kA.

van Infrastructuur en Waterstaat (IenW) en valt dus onder de ministeriële verantwoordelijkheid. De inrichting van RWS is vastgesteld in het Instellingsbesluit directoraat-generaal RWS 2013. Naast het beheren van grote wateren, het onderhouden van rijkswaterstaatswerken en het voeren van beleid met betrekking tot milieu en mobiliteit, is er aan RWS tevens een belangrijke handhavingsrol toegekend.[27] In deze rol houdt RWS zich bezig met de bescherming van de functionaliteit van waterstaatswerken door het houden van toezicht op het naleefgedrag van gebruikers van de door RWS beheerde netwerken. Door preventie, toezicht en het toepassen van bestuursrechtelijke of strafrechtelijke sancties bewerkstelligt RWS dat de geldende rechtsregels en voorschriften worden nageleefd. RWS neemt daarbij de rol in van proactieve en betrouwbare gesprekspartner voor alle netwerkgebruikers.[28]

RWS is een publiekrechtelijke overheidsorganisatie. Bij de uitvoering van zijn taken is RWS zowel gebonden aan publiekrechtelijke regels, zoals de Algemene wet bestuursrecht (Awb), de Wob, de Woo en de Archiefwet, als aan privaatrechtelijke regels, zoals de Aanbestedingswet en de Mededingingswet.

2° *Pilot Zoutlogistiek*

✓ *Beschrijving*

In de Pilot zoutlogistiek staat het verbeteren van databetrouwbaarheid centraal. RWS koopt jaarlijks grote hoeveelheden strooizout in door middel van een openbare aanbestedingsprocedure. In de praktijk is RWS al tegen een probleem aangelopen met betrekking tot de kwaliteitsborging van het strooizout. Het is voorgevallen dat het strooizout bij aankomst in Nederland niet aan de gestelde eisen voldeed. Hierbij is geconstateerd dat de kwaliteitstesten die gedurende de gunning en verscheping van het strooizout met RWS werden gedeeld, niet bleken te kloppen. Dit brengt verschillende consequenties met zich mee, niet in het minst dat het strooizout niet meteen ingezet kan worden ten behoeve van gladheidsbestrijding.

Tegen deze achtergrond is RWS de pilot zoutlogistiek gestart. De pilot onderzoekt of blockchain kan worden toegepast om de hele keten van de aanschaf van strooizout inzichtelijk en mogelijk betrouwbaarder te maken, met name voor de betrokken leveranciers (de opdrachtnemers) en voor RWS als opdrachtgever. De pilot verkent in hoeverre een *track & trace* ketensysteem op de blockchain kan worden ingezet om de kwaliteit van het strooizout gedurende de gehele zoutketen betrouwbaar en permanent te kunnen volgen en op te slaan. Het is de bedoeling om kwaliteitsinformatie over de zuiverheid, korrelgrootte en korrelverdeling onveranderlijk vast te leggen op een blockchainapplicatie, waardoor het risico dat strooizout bij aankomst niet voldoet aan de door RWS gestelde eisen zou kunnen afnemen. Dit zou tevens de mogelijkheid kunnen bieden voor leveranciers om al tussentijds actie te ondernemen

27 Besluit Handhavingsbeleidsplan Rijkswaterstaat.
28 Ibid.

wanneer blijkt dat de kwaliteit van het zout niet voldoet aan de gestelde RWS-eisen, bijvoorbeeld al op het moment dat het zout zich nog in de zoutmijn bevindt of bij het transport, en dus op een vroeger moment dan bij aankomst in de haven van Rotterdam.

✓ *Hoe werkt het?*

Figuur 7 Pilot Zoutlogistiek

De pilot verkent de volgende werking van een mogelijke blockchainapplicatie, beheerd door een consortium van zoutpartijen. Na de aanbestedingsprocedure en gunning aan de opdrachtnemer wordt het strooizout op drie momenten getest. Allereerst, indien de opdracht na gunning wordt verleend aan de opdrachtnemer, wordt het strooizout van de ketenpartner door een lokaal lab gecontroleerd. Het lokale lab registreert de batch zout en voert een controle uit die de kwaliteit en samenstelling van het strooizout inzichtelijk maakt. Dit zou worden vastgelegd op de blockchain. Vanaf dat moment kan het strooizout door middel van een *track & trace* systeem gevolgd worden. Het tweede testmoment wordt vlak voor de verscheping uitgevoerd in de haven van vertrek. Tot slot wordt het strooizout getest en gecontroleerd bij aankomst op de haven in Rotterdam. De uitkomst van deze drie controles zouden op de blockchainapplicatie worden vastgelegd. Wanneer op enig moment in de keten bij een controle blijkt dat het strooizout niet voldoet aan de kwaliteitseisen van RWS, zou dit onveranderlijk worden verankerd op de blockchain en kunnen ketenpartners al tussentijds actie ondernemen om het strooizout aan de juiste kwaliteitseisen te laten voldoen.

✓ *Beoogde voordelen voor RWS*

Het *track & trace* systeem op de blockchain maakt het voor zowel de leverancier als opdrachtnemer en RWS als opdrachtgever mogelijk om de kwaliteit van het strooizout gedurende het hele ketenproces te verifiëren en te monitoren. Ook door het toepassen en vastleggen van de kwaliteitsmonitoring van ingekocht strooizout op de blockchain kunnen problemen niet volledig worden geëlimineerd, maar deze kunnen wel eerder worden gesignaleerd en eventueel daardoor zelfs worden vermeden. Alle kwaliteitstesten die gedurende het ketenproces worden afgenomen, zouden transparant en onweerlegbaar op de blockchain worden vastgelegd. Met het transparante, onweerlegbare karakter van de blockchain wordt beoogd dat de kwaliteit van het zout bij alle ketenpartijen in het proces inzichtelijk en gegarandeerd blijft, omdat op deze wijze de mogelijkheid tot foutieve beloftes over de kwaliteit van het strooizout alsmede het eenzijdig aanpassen van kwaliteitstesten minder waarschijnlijk wordt gemaakt.

In het door RWS beoogde concept zou de blockchainapplicatie worden beheerd door een onafhankelijke derde, namelijk een consortium van verschillende zoutpartijen, die tevens instaat voor het onderhoud en de doorontwikkeling. Eventuele risico's die de werking van de technologie met zich mee zou brengen zouden dan ook voor rekening van dit consortium vallen.

✓ *Beoogde voordelen voor ketenpartners*

In de zoutketen kunnen zaken mislopen, niet alleen bij de eindleverancier waarmee RWS een contract heeft, maar zeker ook bij tussenleveranciers die betrokken worden. Er kunnen zich verschillende problemen voordoen, gaande van incorrecte beloftes over de kwaliteit van het strooizout, tot het eenzijdig aanpassen van tussentijdse kwaliteitstesten. Momenteel is het voor de ketenpartijen moeilijk te bewijzen dat de kwaliteit van het zout nog voldoende gewaarborgd was toen zij erover beschikten. Het *track & trace* systeem op de blockchain zou de kwaliteit van het strooizout in elke fase van de keten voor iedereen inzichtelijk kunnen maken, waardoor het makkelijk te traceren zal zijn of het zout bij alle ketenpartijen aan de kwaliteitseisen van RWS voldoet. Ketenpartners die aan de kwaliteitseisen (willen) voldoen, zullen zodoende niet langer geconfronteerd worden met een lastige bewijspositie. Leveranciers die verantwoordelijk zijn ten aanzien van RWS kunnen zo ook makkelijker tussenleveranciers of vervoerders aanspreken bij problemen.

3° Pilot Grondstromen

✓ *Beschrijving*

RWS is namens de Minister van Infrastructuur en Waterstaat het bevoegd gezag voor toezicht en handhaving inzake de toepassing van grond en baggerspecie in oppervlaktewaterlichamen in beheer bij het Rijk. Het grondstromenproces bestaat uit verschillende schakels, zoals het graven, vervoeren, samenvoegen, opslaan en toepassen van grond of baggerspecie. Dit is een proces waar meerdere ketenpartners,

meerdere toezichthoudende en handhavende overheden bij betrokken zijn, bijvoorbeeld de Inspectie Leefomgeving en Transport en private certificerende instellingen. Hierdoor is certificering, het houden van toezicht en handhaving binnen het grondstromenproces in de praktijk een gedeelde verantwoordelijkheid van verschillende overheidsdiensten en betrokken private actoren. Momenteel is informatie over grondstromen in diverse informatiesystemen van betrokken ketenpartners opgeslagen. Om de toezicht- en handhavingsfunctie van toezichthoudende en handhavende overheidsdiensten zoals RWS te kunnen verbeteren, is verkend hoe de gegevens die nu nog verspreid zijn in een gedistribueerde realiteit geïntegreerd kunnen worden in één informatiesysteem. De ontwikkeling van een zogenaamd 'bodempaspoort' is verkend waarmee de herkomst, de eigenschappen en het gebruik van grond in dat informatiesysteem inzichtelijk worden gemaakt, een *track & trace* systeem dus. Door middel van onderliggende blockchaintechnologie zou informatie uit diverse informatiesystemen in een 'bodempaspoort' permanent en onweerlegbaar kunnen worden vastgelegd. Hiermee wordt beoogd om de validiteit en betrouwbaarheid van informatie over de grond te vergroten, door als het ware de zandkorrel van begin tot de uiteindelijke toepassing aan het einde inzichtelijk te kunnen maken, waardoor er één betrouwbare informatieketen ontstaat over de grondstromen.

✓ *Hoe werkt het?*

Figuur 8 Pilot Grondstromen

Alle ketenpartners zouden in de blockchainapplicatie over een partij grond verschillende gegevens kunnen invullen, bijvoorbeeld over de herkomst, de kwaliteit van de grond, de capaciteit van de opslaglocatie en het aantal ton grond. Ook dient er te worden aangegeven of de grond tijdelijk moet worden opgeslagen of dat het onmiddellijk moet worden toegepast. Denk aan grond die bijvoorbeeld moet

worden toegepast voor de aanleg van een snelweg. De set van ingevoerde gegevens zou direct door betrokken toezichthouders en handhavers zoals RWS worden ontvangen.

De verkende blockchainapplicatie streefde als doel het registreren van gegevens na, zodat grondstromen gemakkelijker gevolgd en herleid kunnen worden. Gedurende de ontwikkeling van het bodempaspoort is tevens een bijkomende opportuniteit geïdentificeerd, namelijk het mogelijk invoeren van geautomatiseerde 'als x, dan y' algoritmische regels. Concreet gaat het dan bijvoorbeeld over een (rood) signaal inzake de compatibiliteit van het samenvoegen van partijen grond. De blockchainapplicatie zou na registratie van de gegevens de automatisch bepaalde 'als x dan y' regels kunnen uitvoeren. Nadat ketenpartners informatie over verschillende type grond hebben ingevoerd, zou er eventueel tevens automatisch een match kunnen plaatsvinden tussen partijen grond die dezelfde kwaliteit hebben. Partijen grond van dezelfde kwaliteit mogen immers conform bestaande regelgeving worden samengevoegd.[29] Indien een ketenpartij in het systeem zou registreren dat grond van verschillende kwaliteit zou worden samengevoegd, dan zou de applicatie er bijvoorbeeld op kunnen attenderen dat de match niet klopt. Het systeem zou dan automatisch als het ware een 'rood' signaal kunnen geven als het samenvoegen van grond niet is toegestaan, waarna de ketenpartij erop is geattendeerd dat deze niet mag overgaan tot de actie.

✓ *Beoogde voordelen voor RWS en andere toezichthoudende en handhavende overheidsdiensten*

De blockchainapplicatie zou ervoor kunnen zorgen dat RWS en de andere toezichthoudende en handhavende overheidsdiensten de herkomst en eigenschappen van grond gedurende het hele proces kan volgen. De informatie over grondstromen zou immers permanent en onweerlegbaar worden geregistreerd. De databetrouwbaarheid wordt door de blockchainapplicatie gewaarborgd, waardoor er één waarheid ontstaat over informatie aangaande grondstromen. Indien alle informatie in één systeem door alle ketenpartners zou worden geregistreerd, zijn RWS en de andere toezichthoudende en handhavende overheidsdiensten niet meer afhankelijk van de administraties van andere ketenpartners. De blockchainapplicatie zou kunnen voorkomen dat RWS en andere toezichthoudende en handhavende overheidsdiensten bij elke ketenpartner administratie moet opvragen als blijkt dat bepaalde grond niet voldoet aan de eisen uit het Besluit Bodemkwaliteit. Wanneer in het ketenproces plotseling blijkt dat er iets mis is gegaan – bijvoorbeeld wanneer bepaalde grond van verschillende kwaliteit is samengevoegd, terwijl dat niet was toegestaan – zou ingezien kunnen worden waar en door wie er fouten zijn gemaakt. De toezichthoudende en handhavende overheidsdiensten kunnen op basis van de registratie in de blockchainapplicatie vervolgens onmiddellijk een onderzoek instellen en

29 Art. 4.3.2 lid 1 onder B van de Regeling bodemkwaliteit.

waar nodig en mogelijk handhaven. De toezichthoudende en handhavende rol van overheidsdiensten zoals RWS wordt door een dergelijk systeem dus ondersteund en handmatige administratieve handelingen kunnen worden verminderd. Wel dienen er afspraken gemaakt te worden over welke informatie de toezichthoudende en handhavende overheidsdiensten uit het bodempaspoort mogen gebruiken bij het uitoefenen van hun taken. Zodoende wordt duidelijk welke onderscheidende taken en verantwoordelijkheden de diensten bezitten en wordt geborgd dat men niet op elkaars stoel gaat zitten.

✓ *Beoogde voordelen voor ketenpartners*

Deze verkende applicatie heeft niet alleen voordelen voor toezichthoudende en handhavende overheidsdiensten zoals RWS, maar ook voor de ketenpartners. Allereerst hebben ook de ketenpartners baat bij een proces waarin ze geen risico lopen dat dit langdurig wordt stilgelegd door een onderzoek van de toezichthoudende en handhavende overheidsdiensten. Daarnaast wordt de informatie eerder in de keten gedeeld, waardoor vroegtijdig actie kan worden ondernomen als bijvoorbeeld geconstateerd wordt dat partijen grond ongeoorloofd met elkaar zal worden samengevoegd. Hier hebben ketenpartners baat bij, omdat zij niet pas helemaal aan het einde van het proces hierover verwittigd worden.

II. Toegang tot overheidsinformatie: wettelijk kader

Een voldoende mate van openbaarheid en toegang tot overheidsinformatie is essentieel voor het functioneren van een democratische rechtsstaat.[1] Hoewel er geen grondrecht op overheidsinformatie is opgenomen in de Nederlandse Grondwet, zijn er in het Nederlands recht vrij omvattende wettelijke kaders vastgesteld die de toegang tot en openbaarheid van overheidsinformatie regelen. Artikel 110 Grondwet kan worden gezien als de algemene openbaarheidsbepaling: "*De overheid betracht bij de uitvoering van haar taak openbaarheid volgens regels bij de wet te stellen*".[2] In artikel 110 Grondwet is bijgevolg de plicht van de overheid tot het vaststellen van nadere wettelijke regelingen omtrent openbaarheid vastgelegd. De Wob/Woo, de Archiefwet en de Wet hergebruik van overheidsinformatie (Who) vormen de kern van het wettelijke kader dat de toegang tot en openbaarheid van overheidsinformatie nader regelt, naast onder meer enkele artikelen van de Aanbestedingswet 2012.

In de Nederlandse democratische rechtsstaat is algemeen aanvaard dat overheidsinformatie in beginsel openbaar moet zijn, tenzij er belangen zijn die zwaarder wegen dan het belang van openbaarheid.[3] De beginselplicht tot openbaarheid is gecodificeerd in artikel 110 Grondwet en is verder uitgewerkt in de Wob/Woo. Artikel 110 Grondwet houdt een **plicht** in voor de overheid om openbaarheidsregels vast te stellen, maar ziet dus niet op een **recht** op informatie van de overheid. De vraag rijst vervolgens of een dergelijk recht op toegang tot overheidsinformatie tevens in Europese of internationale wetgeving is geborgd. In het arrest van de grote Kamer van het EHRM in de zaak *Magyar Helsinki Bizzotsag t. Hongarije* is een algemeen recht op toegang tot overheidsinformatie erkend op basis van artikel 10 EVRM.[4] In artikel 10 EVRM is het recht op vrijheid van meningsuiting neergelegd, alsmede het recht om inlichtingen te ontvangen of te verstrekken. In haar arrest overweegt het EHRM dat

1 Daalder 2005, p. 12.
2 Beers & De Poorter 2021.
3 Daalder 2005, p. 2.
4 EHRM 8 november 2016, nr. 18030/11, AB 2017/1 m.nt. T. Barkhuysen & M.L. van Emmerik (*Magyar Helsinki Bizottság t. Hongarije*).

het recht op overheidsinformatie onder bepaalde voorwaarden een inherent element vormt van het recht om inlichtingen te ontvangen of te verstrekken.[5]

Artikel 10 EVRM voorziet dus in een afdwingbaar recht op toegang tot overheidsinformatie en verzoekers van overheidsinformatie kunnen onder de door het EHRM geformuleerde voorwaarden een beroep doen op dit recht. De volgende vier criteria vormen samen de drempel om dit recht te kunnen afdwingen: 1° het doel van het informatieverzoek (journalistieke activiteiten of andersoortige bijdrage aan het publieke debat), 2° de aard van de gevraagde informatie (het openbaar maken van informatie moet een publiek belang dienen), 3° de rol van de verzoeker als 'public watchdog' (alleen journalisten, ngo's en public interest groups kunnen een beroep doen op het recht), 4° de gevraagde informatie dient gereed en beschikbaar te zijn.[6] Deze voorwaarden zijn dus beperkend, zeker inzake de kring van informatieverzoekers die een beroep kunnen doen op het recht. Met betrekking tot de informatieverzoeker is het bereik van de Wob ("een ieder") in elk geval breder dan artikel 10 EVRM. De Afdeling Bestuursrechtspraak van de Raad van State (ABRvS) stelde na het Magyar-arrest dat de beperkingen in artikelen 10 en 11 Wob[7] in beginsel in overeenstemming zijn met artikel 10 EVRM, waarbij journalisten, ngo's of public interest groups uitzonderlijk wel bijzondere omstandigheden kunnen inroepen om het tegendeel aan te tonen.[8] Kortom, de Wob is in beginsel 'EHRM-proof'.[9]

In de nasleep van de toeslagenaffaire is het belang van transparantie, met inbegrip van adequate toegang tot overheidsinformatie, controleerbaarheid en accountability binnen de Nederlandse overheid bijzonder actueel. Ongetwijfeld zal er de komende jaren veel aandacht zijn voor de mate waarin overheden, en zeker ook uitvoeringsinstanties, verantwoording kunnen en moeten afleggen. De toegankelijkheid en beschikbaarheid van overheidsinformatie is daarvoor cruciaal, maar tegelijk nog geen vanzelfsprekendheid in de bestuurlijke praktijk. Onlangs, 16 jaar na het harde rapport, trok de Inspectie Overheidsinformatie en Erfgoed wederom aan de alarmbel over het ondermaatse niveau van de informatiehuishouding binnen de Nederlandse overheid.

Na 'Een dementerende overheid' waarin erop wordt gewezen dat vele overheidsorganisaties geen goede voorzieningen hebben getroffen om digitaal verantwoord te kunnen archiveren,[10] wijst de Inspectie in het rapport 'Een dementerende overheid 2.0?' op de nog steeds gebrekkige duurzame toegankelijkheid van

5 EHRM 8 november 2016, nr. 18030/11, AB 2017/1 m.nt. T. Barkhuysen & M.L. van Emmerik (*Magyar Helsinki Bizottság t. Hongarije*), par. 151.
6 Ibid., par. 157-170.
7 Zie p. 41.
8 ABRvS 25 oktober 2017, ECLI:NL: RVS:2017:2883.
9 Zie Pietermaat 2017.
10 Rijksarchiefinspectie 2005, p. 10.

overheidsinformatie. Zij geeft aan dat onder meer de kennis van informatiebeheer binnen de overheid afneemt, de ICT vaak verouderd is en 'misplaatst tech-optimisme overheerst'.[11]

Mede gelet op het risico van ondoorzichtigheid die gepaard gaat met de inzet van steeds complexer wordende technologie, waarbij het moeilijk is om grip te krijgen op digitalisering binnen het bestuur, lijken extra inspanningen dus noodzakelijk. Eerder dan het louter voldoen aan de minimumvereisten van de openbaarmakingswetgeving en het geven van een beperkte invulling aan de plicht tot openbaarmaking, lijkt het bij het inrichten van nieuwe (digitale) processen binnen overheden – eventueel dus ook bij de inzet van blockchaintechnologie – aangeraden om *by design* een adequate toegang tot overheidsinformatie te waarborgen en dat is zeker geen klus die onderschat kan worden.

A. Wet openbaarheid van bestuur (Wob)[12]

1° Doel

De Wob regelt het recht van burgers op informatie van de overheid. De Wob vloeit voort uit artikel 110 Grondwet, waarin is bepaald dat de overheid bij de uitvoering van haar taken openbaarheid betracht. Het kerndoel van de Wob is het reguleren van de openbaarheid van bestuur en het stimuleren van een goede en democratische bestuursvorming.[13] De Wob stelt burgers in staat informatie op te vragen over het handelen van de overheid, waardoor zij de bestuurlijke besluitvormingsprocessen kunnen controleren en kunnen deelnemen aan het democratisch bestel. Op een bestuursorgaan rust zowel een passieve als een actieve verplichting om overheidsinformatie te openbaren.[14]

De Wob bevat geen verplichting om documenten die openbaar worden gemaakt, toe te spitsen op de informatiebehoefte van de verzoeker. Hiervoor wordt in de praktijk geregeld wel een inspanning gedaan, eventueel in afstemming met de verzoeker, maar de uiteindelijk interpretatie van de informatie voor de beantwoording van de informatiebehoefte van de verzoeker, is diens eigen verantwoordelijkheid. De Wob heeft immers als kerndoel het openbaar maken van documenten, niet van andere zaken zoals de motivering van besluiten en beleid, feiten en aannames of conclusies die gemaakt kunnen worden op basis van de informatie in de documenten. Dit hoort eerder bij de motivering van een Awb-besluit.

---

11 Inspectie Overheidsinformatie en Erfgoed 2021, p. 4.

12 De Wet open overheid (Woo) treedt vanaf 1 mei 2022 gedeeltelijk in werking en vervangt de Wob.

13 MvT Wob, p. 29.

14 Art. 2, 3 en 8 Wob. Zie voor uitgebreide artikelsgewijze commentaar: https://www.nederlandrechtsstaat.nl/module/nlrs/script/viewer.asp?soort=commentaar&artikel=110.

2° *Passieve openbaarmaking*

De Wob bepaalt dat **eenieder** een verzoek om informatie neergelegd in documenten over een bestuurlijke aangelegenheid kan richten tot bestuursorganen die in de Wob zijn benoemd.[15] Zowel burgers als bedrijven kunnen bij een bestuursorgaan een verzoek tot openbaarmaking indienen, een zogenoemd '**Wob-verzoek**'. Wanneer een Wob-verzoek wordt ingewilligd, betekent dit dat de opgevraagde informatie voor iedereen openbaar wordt.[16]

Het kernbegrip binnen de Wob is het begrip **'document'**. Hiermee wordt bedoeld: *'een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat'*.[17] Het begrip document wordt in ruime zin uitgelegd en omvat dan ook diverse gegevensdragers.[18] In het Wob-verzoek hoeft de verzoeker geen belang te vermelden.[19] Wel moet de verzoeker duidelijk vermelden over welke **bestuurlijke aangelegenheid** de verzoeker informatie wenst te ontvangen en/of welk specifiek document de gewenste informatie bevat.[20] De Wob definieert bestuurlijke aangelegenheid als *'een aangelegenheid die betrekking heeft op beleid van een bestuursorgaan, daaronder begrepen de voorbereiding en de uitvoering ervan'*.[21] De gevraagde informatie moet daar dus betrekking op hebben. Verder is de werkingssfeer van de Wob beperkt tot documenten die bij het bestuursorgaan berusten of zouden moeten berusten. Voor de interpretatie van **'(zou moeten) berusten bij'** zal het erop neerkomen dat de inhoud van het document en/of het document bestemd is voor het bestuursorgaan.[22] In een digitale omgeving betekent dit dat het bestuursorgaan toegang moet hebben tot het medium waar de informatie zich bevindt en daar ook moet over kunnen beschikken. De opsteller van de informatie is niet van belang, zodat ook documenten opgesteld door derden onder de werkingssfeer van de Wob kunnen vallen.[23] Volgens vaste rechtspraak[24] zijn bestuursorganen evenwel niet verplicht om gegevens te vervaardigen die niet in bestaande documenten zijn neergelegd, ongeacht de mate van inspanning die dat zou kosten. Van bestuursorganen wordt dan ook niet verlangd om bepaalde gegevens uit een grote hoeveelheid op diverse plaatsen aanwezige documenten te halen en een overzicht te maken, aangezien dit gelijkgesteld kan worden met het vervaardigen van een document.[25] Als uitgangspunt moet er sprake zijn van een concreet en reeds bestaand document of gegevens in

15 Art. 3 lid 1 Wob.
16 Nieuwenhuis 2014, p. 4.
17 Art. 1 sub a Wob.
18 Schlössels, 2017, p. 438.
19 Art. 3 lid 3 Wob.
20 Art. 3 lid 2 Wob.
21 Art. 1 sub b Wob.
22 *Kamerstukken II* 1986-1987, 19 859, nr. 3, p. 21.
23 Daalder 2005, p. 112.
24 Zie o.a. ABRvS 5 juni 2013, ECLI:NL:RVS:2013:CA2102; ABRvS 26 april 2016; ECLI:NL:RVS:2016:1138.
25 ABRvS 14 februari 2018, ECLI:NL:RVS:2018:466, par. 3.1.

databestanden die simpelweg door middel van een schermafdruk verstrekt kunnen worden.[26]

3° *Actieve openbaarmaking*

Naast de passieve plicht tot het voldoen aan Wob-verzoeken, is in de Wob een algemene plicht tot actieve openbaarmaking opgenomen.[27] Bestuursorganen dienen uit eigen beweging informatie te verstrekken wanneer dit in het belang is van goed en democratisch bestuur.[28] Bestuursorganen hebben veel beoordelingsruimte bij het bepalen welke informatie openbaar gemaakt moet worden. In dit opzicht dient de informatie in beginsel tevens in begrijpelijke vorm te worden verschaft. Het perspectief van de ontvanger van informatie is hierbij immers van belang. Een burger zal bijvoorbeeld moeite hebben met het verwerken van een grote hoeveelheid aan technische of bureaucratische informatie. Het is voor de hand liggen dat het bestuursorgaan poogt om de burger op een begrijpelijke en toegankelijke manier te informeren. Desondanks is dit voorlopig niet wettelijk afdwingbaar of nader ingevuld.

4° *Uitzonderingsgronden*

Het uitgangspunt is dat bij bestuursorganen berustende documenten openbaar worden gemaakt, *tenzij* de gevraagde informatie niet geschikt is om openbaar te maken. De Wob maakt daarbij een onderscheid tussen absolute en relatieve uitzonderingsgronden.[29] De uitzonderingsgronden van artikel 10 lid 1 Wob hebben een absoluut karakter, wat inhoudt dat indien de uitzonderingsgrond zich voordoet het verzoek tot openbaarmaking *moet* worden geweigerd.[30] Er is dus volgens de Wob géén ruimte voor een afweging van belangen, als het verstrekken van informatie de eenheid van de Kroon in gevaar zou kunnen brengen, de veiligheid van de Staat zou kunnen schaden, het gaat om vertrouwelijk aan de overheid meegedeelde bedrijfs- of fabricagegegevens, of het de verwerking van bijzondere persoonsgegevens als bedoeld in hoofdstuk 2, paragraaf 2 Wet bescherming persoonsgegevens betreft, tenzij verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.

Dit is anders voor de relatieve uitzonderingsgronden van artikel 10 lid 2 Wob. Indien één van de zeven relatieve uitzonderingsgronden van artikel 10 lid 2 zich voordoet, moet het bestuursorgaan een belangenafweging maken en *kan* een verzoek tot openbaarmaking zodoende eventueel worden geweigerd. Hiervoor wordt het algemeen belang bij de openbaarmaking afgewogen tegen de door de uitzonderingsgronden

26 ABRvS 9 juni 2020, ECLI:NL:RBMNE:2020:2118, par. 9.3.
27 Art. 8 Wob.
28 Art. 8 lid 1 Wob.
29 Art. 10 lid 1 en 2 Wob.
30 Michiels e.a. 2019, p. 32.

beschermde belangen, zoals bijvoorbeeld de economische en financiële belangen van de Staat, opsporing of vervolging van strafbare feiten of de eerbiediging van de persoonlijke levenssfeer. Daarnaast kent de Wob nog een bijzondere beperking op het beginsel van openbaarheid. Op grond van artikel 11 lid 1 Wob wordt over persoonlijke beleidsopvattingen die voorkomen in documenten bestemd voor intern beraad geen informatie verstrekt. De ratio achter deze beperking is dat binnen het bestuur optimaal van gedachten moet kunnen worden gewisseld, zonder dat er een remming optreedt wegens de vrees voor het uitlekken van persoonlijke opvattingen.[31]

Voor zover een Wob-verzoek betrekking heeft op milieu-informatie, wat voor RWS dus zeker relevant kan zijn, geldt er dan weer een uitgebreider openbaarheidsregime. In uitvoering van internationale en Europese milieuverplichtingen, in het bijzonder het Verdrag van Aarhus[32] en de Europese richtlijn 2003/4/EG, zijn in de Wob uitzonderingen op de uitzonderingsgronden gemaakt voor de verstrekking van informatie die betrekking heeft op het milieu. Indien een verzoek ziet op milieu-informatie, bijvoorbeeld op lucht-, water- of bodemkwaliteit, of de verslagen en beleidsmaatregelen hierover, gelden de afwijkende eisen van artikel 10 lid 4 t/m 8 Wob.[33] Het verzoek tot openbaarmaking van milieu-informatie kan moeilijk(er) worden geweigerd, aangezien het verlenen van toegang tot informatie over de toestand van het milieu in het kader van het Verdrag van Aarhus cruciaal is.[34] Emissiegegevens nemen voorts een bijzondere positie in, omdat aan de openbaarmaking daarvan een bijzonder zwaar gewicht wordt toegekend.[35]

5° Digitale dragers

Documenten over bestuurlijke aangelegenheden vallen onder de Wob zolang ze bij een bestuursorgaan berusten. Maar wat kwalificeert in een digitale context concreet als een **document** in de zin van de Wob? Volgens de totstandkomingsgeschiedenis van de Wob[36] en vaste rechtspraak van de ABRvS[37] moet aan het begrip document een **ruime betekenis** worden toegekend. Het omvat informatie vastgelegd op **diverse gegevensdragers**. Niet alleen schriftelijke stukken, maar ook digitale

31 Schlössels 2017, p. 445.
32 Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden (Trb. 2001, 73).
33 De specifieke uitzonderingsgronden voor milieu-informatie worden in de Woo echter veralgemeniseerd: de afwijkende uitzonderingsgronden voor milieu-informatie uit de Wob worden in de Woo zo veel mogelijk opgeheven. Zie Bijlage bij MvT Wijzigingswet Woo (concept 5 juni 2020), p. 44.
34 Art. 1 Verdrag van Aarhus.
35 ABRvS 27 januari 2021, ECLI:NL:RVS:2021:153, par. 7.1.
36 *Kamerstukken II* 1986-1987, 19 859, nr. 3 (MvT).
37 Zie o.a. ABRvS, 20 maart 2019, ECLI:NL:RVS:2019:899; ABRvS mei 2019, ECLI:NL:RVS:2019:1675; Rechtbank Midden-Nederland 28 november 2017, ECLI:NL:RBMNE:2017:5979, AB 2018/34.

gegevensdragers zoals USB-sticks, videobanden, cd-roms, en elektronisch vastgelegde informatie zoals e-mailberichten, sms- en WhatsApp-berichten vallen onder het documentbegrip van de Wob. Ook data en elektronische metagegevens zijn documenten in de zin van de Wob.[38] **Een systeem** als zodanig kan **niet** worden aangemerkt als document in de zin van de Wob.[39] De **gegevens** zelf die **op een blockchain** staan, vallen in beginsel echter wel onder de Wob voor zover ze bij een bestuursorgaan berusten.

Nadat is vastgesteld of een Wob-verzoek doelt op een document zoals wordt verstaan onder de Wob, dient er te worden beoordeeld of de informatie **berust bij het bestuursorgaan**.[40] De manier waarop iets is opgeslagen, is niet bepalend voor de vraag of de Wob wel of niet van toepassing is. Uit jurisprudentie blijkt dat het niet vereist is dat een document op een harde schijf of server van het bestuursorgaan staat.[41] Bestuursorganen mogen digitale documenten opslaan op een harde schijf, een eigen server, maar ook op een externe server of in de cloud.[42] Het gaat dan nog steeds om documenten die berusten bij een bestuursorgaan.

De vorm van informatie, gedrukt of in elektronische vorm, en het medium van de drager, traditionele papierdrager of digitale drager, doet niet ter zake voor toepassing van de Wob. Voor het toepassingsbereik van de Wob zijn het **medium** van de informatie en de **opslagplaats** dus **niet relevant**.[43] Daarbij geldt evenwel dat de scheidslijn tussen de drager van gegevens en de gegevens zelf vager lijkt te worden in het digitale tijdperk.[44]

Tenslotte is het van belang dat de Wob niet van toepassing is op informatie die al openbaar is en door burgers zelf geraadpleegd kan worden.[45] Uit jurisprudentie over het Squit-systeem van de gemeente Utrecht[46] blijkt dat in een online systeem opgenomen documenten openbaar zijn in de zin van de Wob als de documenten **voor burgers toegankelijk en raadpleegbaar** zijn **via de elektronische weg**, zonder dat er door het bestuursorgaan eerst een beoordeling moet worden gemaakt of er sprake is van een uitzonderingsgrond die aan openbaarheid in de weg staat, zoals persoonsgegevens of andere gevoelige gegevens. Indien de burger onder laatstgenoemde voorwaarden zelf gegevens kan opzoeken in een online systeem en niet afhankelijk is van medewerking van het bestuursorgaan, valt het verzoek tot informatie niet onder het bereik van de Wob. Bijgevolg zullen **gegevens op een publieke**

38 ABRvS 22 mei 2019, ECLI:NL:RVS:2019:1675, par. 3.1.
39 Noot H.S. ten Cate en C.A. Geleijnse, bij ABRvS 22 mei 2019, ECLI:NL:RVS:2019:1675, par. 9.1.
40 Art. 1 onder a Wob.
41 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, r.o. 5.
42 Ibid.
43 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899.
44 ABRvS 22 mei 2019, ECLI:NL:RVS:2019:1675, m.nt. H.S. ten Cate en C.A. Geleijnse.
45 ABRvS 12 juli 2017, ECLI:NL:RVS:2017:1874, r.o. 3.1.
46 ABRvS 11 september 2019, ECLI:NL:RVS:2019:3100.

blockchain die door een burger zelf te raadplegen zijn in beginsel niet onder de reikwijdte van de Wob vallen.

B. De Wet open overheid (Woo)

1° Doel

Het initiatiefwetsvoorstel Wet open overheid (Woo) beoogt de Wob te vervangen. Na een parlementaire behandeling van maar liefst 8 jaar, is uiteindelijk de Wijzigingswet Woo op 26 januari 2021 door de Tweede Kamer en op 5 oktober 2021 door de Eerste Kamer aangenomen. Het initiatiefvoorstel vertrekt vanuit de constatering dat de huidige Wob niet voldoende expliciet is toegespitst op de digitale samenleving en te vrijblijvend is op het vlak van de actieve openbaarmakingsplicht, waardoor transparantie van de overheid in het gedrang komt.[47] Met de invoering van de Woo wordt er nagestreefd om de actieve openbaarmaking en bestuurlijke transparantie tot de norm te verheffen en toegang tot overheidsinformatie te vergroten,[48] wat in de praktijk tot grote organisatorische uitdagingen leidt.[49] Het recht van burgers op toegang tot publieke informatie is expliciet verankerd in de Woo.[50] De Woo is primair gericht op informatieverstrekking uit eigen beweging en verplicht overheidsorganisaties in dat opzicht om een aantal in de wet genoemde informatiecategorieën actief openbaar te maken.[51] Ook bevat de Woo een algemene zorgplicht voor bestuursorganen om documenten in goede, geordende en toegankelijke staat te houden evenals de zorgplicht tot het treffen van maatregelen om digitale documenten duurzaam toegankelijk te maken.[52] De Woo draagt daarmee ook bij aan de verbetering van de digitale informatiehuishouding, wat bij overheidsorganisaties nog altijd onvoldoende op orde blijkt te zijn.[53]

2° Duurzame toegankelijkheid overheidsinformatie

De digitalisering en technologische ontwikkelingen in de afgelopen decennia hebben ertoe geleid dat de informatiehuishouding en de werkwijze van de overheid drastisch zijn veranderd. Niet alleen de vorm en de hoeveelheid van informatie,

47 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 1-2.
48 Ibid.
49 De verplichtingen uit de Woo om documenten behorende tot 11 informatiecategorieën binnen 14 dagen actief openbaar te maken via PLOOI, is dan ook op 1 mei 2022 nog niet in werking getreden. PLOOI is immers nog niet klaar. De komende jaren zal de verplichting in verschillende fasen in werking treden.
50 Art. 1.1 Woo.
51 Art. 3.3 Woo.
52 Art. 2.4 en 6.1 Woo.
53 Inspectie Overheidsinformatie en Erfgoed 2021, p. 8-11.

maar ook de manier waarop overheidsorganisaties met informatie dienen om te gaan, is veranderd. Ten eerste is de hoeveelheid informatie in het digitale tijdperk explosief toegenomen.[54] Overheden beheren vele terabytes aan digitale informatie, waardoor het vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar maken én houden van alle informatie een complexe taak is geworden. De vorm van informatie is tevens veranderd. Informatie is los komen te staan van papieren gegevensdragers en raakt makkelijk versnipperd in verschillende informatiesystemen. Daarnaast is er een risico ontstaan dat digitale gegevensdragers, software en bestandsformaten verouderen of beschadigd raken, waardoor digitale informatie ontoegankelijk wordt.[55] Het belang van een goede informatiehuishouding voor het functioneren van het openbaar bestuur staat dus buiten kijf. Om te voldoen aan de wettelijke kaders van de Wob/Woo en de Archiefwet dient de overheid de duurzame toegankelijkheid van digitale documenten gedurende de **gehele levenscyclus** te waarborgen, vanaf de creatie, het bewaren en beheren, het ontsluiten tot uiteindelijk het vernietigen of preserveren.[56]

De praktijk leert dat bestuursorganen niet altijd weten welke informatie er is en niet altijd snel over de juiste informatie kunnen beschikken, waardoor het beslissen op een Wob-verzoek vaak een tijdrovend, handmatig proces is.[57] De digitalisering heeft dus serieuze uitdagingen opgeleverd. Overheidsorganisaties hebben over het algemeen meerdere informatiesystemen en vaak is niet duidelijk welke informatie zich in welk systeem bevindt. Soms ziet een Wob-verzoek zelfs op informatie die over meerdere systemen is verspreid.[58] Een systeemkoppeling tussen verschillende informatiesystemen is dan essentieel.[59]

Er is dus een acute noodzaak ontstaan om de digitale informatiehuishouding van de overheid beter op orde te brengen.[60] De Woo beoogt daarom de **digitale informatiehuishouding te verbeteren**, zodat er in de toekomst sneller over een Woo-verzoek kan worden beslist. Een goede informatiehuishouding is van essentieel belang om de doelen van de wet te bereiken. De Woo bevat een algemene **zorgplicht** voor bestuursorganen om documenten in goede, geordende en toegankelijke staat te houden en de zorgplicht tot het treffen van maatregelen om digitale documenten duurzaam toegankelijk te maken.[61] De Woo herhaalt hiermee de zorgplicht uit de

54 Archiefwet 2021 Internet Consultatieversie, p. 16.
55 Ibid.
56 Duurzaam Digitaal Databeheer bij de Rijksoverheid 2021, p. 9.
57 *Kamerstukken II* 2019/20, 35 112, nr. 9, p. 6 en Rapport: 'Verbeterpunten in de informatiehuishouding voor een tijdige en kwalitatief goede afhandeling van Wob-verzoeken' (2021).
58 'Verbeterpunten in de informatiehuishouding voor een tijdige en kwalitatief goede afhandeling van Wob-verzoeken' (2021), p. 32.
59 Ibid.
60 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 64.
61 Art. 2.4 en art. 6.1 Woo.

Archiefwet.[62] Deze zorgplicht houdt allereerst in dat bestuursorganen de verplichting hebben om bepaalde maatregelen te treffen zodat documenten te allen tijde gevonden kunnen worden en leesbaar of waarneembaar te maken zijn.[63] Digitale informatie moet in een gestructureerde vorm opgeslagen worden om de vindbaarheid en **toegankelijkheid** te waarborgen. Naast het waarborgen van de toegankelijkheid is er een zorgplicht tot het waarborgen van de **duurzaamheid**. De zorgplicht tot het waarborgen van de duurzaamheid houdt in dat bestuursorganen maatregelen dienen te treffen zodat digitale informatie door tijdsverloop niet beschadigd raakt en daardoor ontoegankelijk worden. De toegankelijkheid van informatie dient bestand te zijn tegen veranderingen van elke aard.[64] Het proces van het duurzaam toegankelijk maken van overheidsinformatie zal naar verwachting meerdere jaren duren, aangezien het fundamentele veranderingen vereist in de informatie- en applicatiesystemen van overheden.[65]

C. Archiefwet

1° Doel

Openbare archieven zijn onmisbaar voor de democratische rechtsstaat, aangezien overheidsarchieven een middel vormen tot politieke controle, participatie en emancipatie van de burger.[66] De Archiefwet schrijft daarom voor dat alle overheidsinformatie in beginsel gearchiveerd moet worden. Archiveren is het **duurzaam toegankelijk maken en houden van informatie**.[67] De Archiefwet faciliteert de borging van overheidsinformatie en maakt zodoende transparantie en verantwoording van bestuur mogelijk. Aan de hand van archieven kan namelijk achterhaald worden of er correct is gehandeld. Erfgoedbehoud is tevens een doelstelling van de Archiefwet.[68] Archieven geven immers inzicht in de geschiedenis en vormen daarmee een belangrijke bron voor cultuur-historisch onderzoek.

2° Vormen, beheren en overbrengen archiefbescheiden

De Archiefwet 1995 (hierna: Archiefwet) bevat gedetailleerde regels aangaande het vormen en beheren van het archief. In tegenstelling tot de nieuwe Archiefwet 2021, spreekt de Archiefwet 1995 anders dan de Wob niet over documenten die berusten bij bestuursorganen, maar over **archiefbescheiden** die door overheidsorganen

62 Zie p. 47.
63 Art. 20 Archiefregeling.
64 Overzicht van begrippen | Nationaal Archief.
65 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 65.
66 Ten Cate 2019, p. 1.
67 Wat betekent archiveren? | Nationaal Archief.
68 MvT Archiefwet 1995, p. 2.

worden gevormd, beheerd en ontvangen. Archiefbescheiden worden gedefinieerd als: '*bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten*' (artikel 1 onder c Archiefwet). Het uitgangspunt is dat informatie die in de context van het functioneel handelen van een overheidsorgaan wordt vastgelegd of ontvangen, valt onder het begrip 'archiefbescheid'. Hierbij is van belang dat het bescheid naar aard bestemd is om **onder het overheidsorgaan te berusten**, wat volgens de Inspectie Overheidsinformatie en Erfgoed betekent dat het **naar zijn aard gebonden moet zijn aan de werkprocessen van het overheidsorgaan**.[69] Het Nationaal Archief definieert processen als een "samenhangend geheel van stappen en procedures voor de uitvoering van een taak".[70]

De Archiefwet bevat een zorgplicht die overheidsorganisaties verplicht hun informatie in goede, geordende en toegankelijke staat te brengen en te bewaren.[71] In dit kader dienen overheidsorganisaties zorg te dragen dat het beheer van hun archiefbescheiden voldoet aan de eisen van het kwaliteitssysteem, de context en authenticiteit van de archiefbescheiden te allen tijde kan worden vastgesteld, er een samenhangend overzicht van de archiefbescheiden is, en er metagegevens worden vastgelegd.[72] Daarnaast verplicht de Archiefwet overheden om in selectielijsten te specificeren welke informatie bewaard moet worden en hoe lang.[73] Archiefbescheiden die op grond van de selectielijst blijvend bewaard dienen te worden, moeten na 20 jaar worden 'overgebracht' naar een archiefbewaarplaats.[74] De verplaatsing kan fysiek zijn, bijvoorbeeld de verplaatsing van fysieke mappen met documenten erin van een documentkast bij het bestuursorgaan naar de archiefbewaarplaats. In het geval van digitale archiefbescheiden, bijvoorbeeld mappen met daarin PDF-bestanden, dienen deze overgebracht te worden naar het *e-depot* van het Nationaal Archief.[75] Vóór overbrenging van gearchiveerde overheidsinformatie naar de archiefbewaarplaats gelden voor de openbaarheid de bepalingen uit de Wob. De overgang van de Wob naar het openbaarheidsregime van de Archiefwet vindt plaats op het moment van overbrenging naar de archiefbewaarplaats.[76]

3° Openbaarheid van archieven

De Archiefwet regelt niet alleen het vormen en beheren van archief, maar ook de openbaarheid van informatie in het archief. Na overbrenging naar de archiefbewaarplaats zijn archieven in principe voor iedereen openbaar en kosteloos te

69 Inspectie Overheidsinformatie en Erfgoed: Archiefbescheiden, wat zijn dat?
70 Proces | Nationaal Archief.
71 Art. 3 Archiefwet.
72 Art. 16-19 Archiefregeling.
73 Art. 5 Archiefwet.
74 Art. 12 lid 1 Archiefwet.
75 Zie https://www.nationaalarchief.nl/archiveren/kennisbank/digitaal-archief-overbrengen.
76 Ten Cate 2019, p. 2.

raadplegen, tenzij openbaarheid conflicteert met één van de drie in de wet genoemde beperkingsgronden: de eerbiediging van de persoonlijke levenssfeer, het belang van de Staat of onevenredige bevoordeling of benadeling van personen.[77] De Archiefwet gaat uit van het principe van volledige inzage: de gehele dossiers kunnen op verzoek ter beschikking worden gesteld. In tegenstelling tot de Wob, wordt er in beginsel geen informatie gecontroleerd, bewerkt, samengevat of weggelakt alvorens de informatie ter beschikking wordt gesteld.[78]

4° Documentenstelsel vs. informatiestelsel

De Wob heeft als grondslag een **informatiestelsel**.[79] Dit houdt in dat de verzoeker kan volstaan met een verzoek om informatie over een bepaalde bestuurlijke aangelegenheid, waarna het de taak is van het bestuursorgaan om te onderzoeken of de gevraagde informatie in documenten is neergelegd. De verzoeker hoeft dus niet aan te duiden welk specifiek document hij wenst te ontvangen. De verzoeker hoeft er alleen maar voor te zorgen dat zijn verzoek ziet op een bestuurlijke aangelegenheid en voldoende concreet is om in behandeling te nemen.[80]

De Archiefwet kent een **documentenstelsel**.[81] Bij een documentenstelsel moet de informatieverzoeker de documenten waarvan hij openbaarmaking wenst, benoemen of beschrijven.[82] Het is daarbij niet nodig om een bestuurlijke aangelegenheid te noemen.[83]

5° Vernietigingsplicht

Naast de zorgplicht tot het in goede, geordende en toegankelijke staat brengen en bewaren van archiefbescheiden, is er ook een zorgplicht tot het vernietigen van de daarvoor in aanmerking komende archiefbescheiden.[84] Onder vernietigen van informatie wordt verstaan het **blijvend ontoegankelijk** maken van informatie.[85] Voor digitale archiefbescheiden betekent dit dat het archiefbescheid een zodanige bewerking moet ondergaan, dat de informatie niet meer vindbaar, leesbaar, interpreteerbaar of te reconstrueren is. Vernietiging impliceert tevens dat digitale kopieën op back-ups of in andere systemen bij het overheidsorgaan vernietigd moeten worden zodat de informatie niet meer hersteld kan worden.[86] Zoals reeds vermeld, dienen

77 Art. 14 en 15 Archiefwet.
78 Nationaal Archief 2017, p. 42.
79 *Kamerstukken II* 1986-1987, 19 859, nr. 3, p. 9 (MvT).
80 Art. 3 lid 2 Wob.
81 Ten Cate 2019, p. 3.
82 Ibid.
83 Ibid.
84 Art. 3 Archiefwet.
85 Nationaal Archief: Wat is digitaal vernietigen?
86 Ibid.

bestuursorganen in een selectielijst te specificeren welke informatie er bewaard moet worden en hoe lang. Vernietiging geschiedt tevens aan de hand van de selectielijsten. In deze lijst wordt per informatieobject een termijn opgenomen na het verstrijken waarvan de vernietiging moet plaatsvinden. De termijn kan zo verschillen per doel en per informatieobject.

Vernietiging heeft een doel, bijvoorbeeld het voldoen aan privacyregelgeving of voorkomen dat het archief exponentieel en onbeheersbaar toeneemt. Het nagestreefde doel van vernietiging vraagt een passende vorm van vernietiging. Zo kan het in het licht van sommige doelen acceptabel zijn dat vernietigde informatieobjecten toch nog toegankelijk zijn.[87] Er zijn daarom verschillende gradaties van vernietiging mogelijk: gaande van drastische maatregelen zoals het fysiek vernietigen van de drager van het informatieobject tot het louter verbreken van de koppelingen naar het informatieobject. Afhankelijk van het object van vernietiging (document, dossier of drager), waar het object is opgeslagen of wordt beheerd (intern, extern, in de cloud of op de blockchain bijvoorbeeld) en de mogelijkheden die het informatiesysteem biedt, kan vernietiging erg complex zijn.[88] Overheidsorganen dienen na te gaan hoe het vernietigen moet worden ingericht. De reikwijdte, het niveau, de wijze en het moment van vernietigen spelen daarbij een belangrijke rol.[89]

6° Digitale dragers

De Archiefwet is volgens artikel 1 onder c van toepassing op archiefbescheiden ongeacht hun vorm. De vorm, bewaarplaats en versie hebben geen invloed op de vraag of een stuk (of data) al dan niet als archiefbescheid kan worden aangemerkt.[90] Dit betekent dat ook digitale archiefbescheiden en digitale dragers onder de Archiefwet vallen. Digitale archiefbescheiden zijn: *'archiefbescheiden die uitsluitend met behulp van besturingsprogrammatuur of toepassingsprogrammatuur geraadpleegd kunnen worden'* (Artikel 1 onder e Archiefregeling). De Archiefregeling bevat gedetailleerde regels voor het archiveren van digitale archiefbescheiden.

7° Duurzame toegankelijkheid overheidsinformatie

Het tijdperk waarin papierendossiers op een centrale plek werden gearchiveerd ligt ondertussen achter ons. Digitaal werken is inmiddels de norm geworden. Hoewel er al grootschalig digitaal gearchiveerd wordt, zijn er nog vele uitdagingen wat betreft de digitale transformatie van de informatieprocessen binnen overheden.[91]

87 Ibid. Het Nationaal Archief definieert informatieobjecten als "Een op zichzelf staand geheel van gegevens met een eigen identiteit", zie: Nationaal Archief: Informatieobject.
88 Nationaal Archief: hoe kun je digitaal vernietigen?
89 Ibid.
90 Nationaal Archief: welke informatie archiveert de overheid?
91 Erfgoedinspectie 2015, p. 6.

Een van deze uitdagingen is het duurzaam beheren en archiveren van digitale archieven. Om te voorkomen dat digitale archiefbescheiden na verloop van tijd onvindbaar of ontoegankelijk worden, dient de keten van digitaal archiveren, vanaf het ontstaan van een digitaal archiefbescheid tot en met overbrenging naar een archiefbewaarplaats, duurzaam toegankelijk ingeregeld te zijn. Het Nationaal Archief definieert het begrip duurzame toegankelijkheid als volgt: '*Toegankelijk betekent vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zolang als noodzakelijk. Duurzaam betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard*'.[92] Informatie die niet goed is bewaard, kan ook niet meer openbaar gemaakt worden. Dit maakt dat **duurzaam beheren en archiveren** een noodzakelijke randvoorwaarde is voor het recht op toegang tot overheidsinformatie. Volgens de Memorie van Toelichting van de Archiefwet is een duurzame en toegankelijke informatiehuishouding onmisbaar voor een goede democratische controle op het bestuur.[93]

Het duurzaam beheren en archiveren van digitale archiefbescheiden vergt technische en organisatorische maatregelen die complex kunnen zijn.[94] Om te kunnen voldoen aan de eis van toegankelijkheid dient informatie binnen een redelijke termijn vindbaar en met een redelijke inspanning raadpleegbaar te zijn. Overheidsorganisaties dienen overzicht te hebben van welke informatie onder de Archiefwet valt en waar deze informatie zich bevindt. Het laatste is vaak lastig omdat digitale informatie vaak verspreid is opgeslagen over meerdere informatiesystemen die niet altijd op elkaar zijn aangesloten.[95] Overheidsorganisaties dienen derhalve alle aanwezige informatiesystemen in kaart te brengen en vast te stellen of er zich in die informatiesystemen archiefbescheiden bevinden. Zo dient dus de vraag beantwoord te worden of digitale archiefbescheiden zich bevinden op een interne of externe server, in een document- of contentmanagementsysteem, in een database, in de cloud of op de blockchain. Vervolgens moeten de archiefbescheiden door middel van het toekennen van metadata worden geordend, van context voorzien en vindbaar worden gemaakt.[96] Met metagegevens kan worden aangegeven wat wel en niet openbaar gemaakt moet worden binnen welke termijn, en welke uitzonderingsgronden van toepassing zijn.[97] Metagegevens zijn onlosmakelijk verbonden met archiefbescheiden en zijn essentieel voor het waarborgen van duurzame toegankelijkheid van digitale archiefbescheiden.[98] Naast het louter toegankelijk maken van digitale archiefbescheiden, hebben overheidsorganisaties ook een belangrijke zorgplicht om digitale archiefbescheiden duurzaam toegankelijk te houden. Dit

92 Nationaal Archief: overzicht van begrippen.
93 MvT Archiefwet 1995, p. 2.
94 Erfgoedinspectie 2015, p. 12.
95 Inspectie Overheidsinformatie en Erfgoed 2021, p. 16.
96 Art. 19 Archiefregeling.
97 Duurzaam Digitaal Databeheer bij de Rijksoverheid: een verkenning (2021), p. 28.
98 Nationaal Archief: metadata.

betekent dat overheidsorganisaties ervoor dienen te zorgen dat bestandsformaten leesbaar blijven, de structuur van dossiers in stand blijven en metagegevens niet verloren gaan.[99]

Uitgangspunt voor duurzame toegankelijkheid is '**archiving by design**'.[100] Informatiesystemen en werkprocessen van overheidsorganisaties kunnen aan de voorkant zo ingericht worden dat er *by design* van meet af aan is gewaarborgd dat informatie duurzaam toegankelijk is en blijft. Vanaf het moment dat informatie wordt gevormd, moet aandacht worden besteed aan het beheer ervan. In het digitale tijdperk kan er niet gewacht worden met het effectief op orde brengen van de informatiehuishouding. Een onmiddellijke goede archivering van informatie zal ertoe leiden dat de informatie vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar is én blijft. Het informatieproces kan zo onmiddellijk worden afgestemd op de toepasselijke wet- en regelgeving. Archivering *by design* brengt het duurzaam toegankelijk maken van digitale overheidsinformatie aldus een belangrijke stap dichterbij.[101]

D. Archiefwet 2021

De regels uit de Archiefwet 1995 zijn toegespitst op het papieren tijdperk. Hoewel er destijds al werd getracht om de Archiefwet beter te laten aansluiten bij de technische ontwikkelingen, stond digitalisering toen nog in de kinderschoenen.[102] Het was toen lastig in te schatten hoe verdere technologische ontwikkelingen zouden uitpakken. Ruim 20 jaar later is een modernisering van de Archiefwet daarom noodzakelijk. Inwerkingtreding van de herziene Archiefwet 2021 is voorlopig voorzien in de loop van 2022 of 2023.

De Archiefwet 2021 beoogt beter toegespitst te zijn op het beheren en bewaren van digitale overheidsinformatie. De Archiefwet 2021 geeft een algemeen kader voor het vormgeven van een duurzame digitale informatiehuishouding en de huidige overbrengingstermijn wordt verkort van twintig jaar naar tien jaar, waardoor informatie eerder openbaar toegankelijk wordt.[103] Ook is er tegen de achtergrond van digitalisering en het ontstaan van omvangrijke databestanden bij overheidsorganisaties een ontheffingsmogelijkheid voor de overbrengingsverplichting opgenomen, het zogenaamd "bewaren bij de bron".[104] De Archiefwet 2021 laat daarnaast het begrip archiefbescheiden los en spreekt van documenten, waarbij wordt aangesloten bij het

99 Art. 20 Archiefregeling.
100 Zie: Rapport: 'Duurzaam Digitaal Databeheer bij de Rijksoverheid: een verkenning' (2021); en Vereniging van Nederlandse Gemeenten, 'Archiveren by Design' (2021).
101 Zie ook VNG, Handreiking voor archiveren van algoritmes gepubliceerd (2021).
102 MvT Archiefwet 1995, p. 4.
103 Art. 4.3 Archiefwet 2021.
104 Art. 4.5 Archiefwet 2021.

documentbegrip dat is opgenomen in de Wob en de Woo. Op het eerste gezicht leiden deze veranderingen niet tot fundamenteel afwijkende conclusies op de verdere analyse van de relatie tussen Archiefwet en blockchain.

III. Beknopte verkenning van overige relevante juridische vraagstukken

Hierna volgt niet-limitatief een beknopte toelichting van overige wet- en regelgeving die op het eerste gezicht ook specifiek relevant kunnen zijn in het licht van toegang tot overheidsinformatie en de gevolgen daarvan, mede voor de keuzes in het blockchaindesign. Nader onderzoek dient op dit vlak in de toekomst nog gevoerd te worden. In de volgende paragrafen wordt aldus beknopt ingegaan op de Algemene wet bestuursrecht (Awb) en de algemene beginselen van behoorlijk bestuur, de Algemene Verordening Gegevensbescherming (AVG), het mededingings- en aanbestedingsrecht en de Wet hergebruik overheidsinformatie (Who). Tenslotte wordt ook nog beknopt ingegaan op de mogelijke functies van blockchaingebaseerde smart contracts, en de kwaliteit van input via oracles.

A. Algemene beginselen van behoorlijk bestuur en de Algemene wet bestuursrecht

RWS is een bestuursorgaan en zijn handelingen zijn bestuurlijk van aard. RWS is bij de uitvoering van zijn taken dan ook gebonden aan sectorale wet- en regelgeving, evenals de algemenere regels van het bestuursrecht in de Algemene wet bestuursrecht (Awb). Het handelen van RWS wordt genormeerd door de algemene beginselen van behoorlijk bestuur (abbb). Een deel van deze beginselen is gecodificeerd in de Awb, zoals het zorgvuldigheidsbeginsel, het motiveringsbeginsel of het evenredigheidsbeginsel. Ook zijn er ongeschreven abbb, zoals het vertrouwens- en het rechtszekerheidsbeginsel, die in jurisprudentie nader zijn uitgewerkt. De Awb normeert het optreden van bestuursorganen evenals de verhouding tussen overheid en burger. De algemene regels in de Awb hebben ook betrekking op de uitvoeringsgebieden. RWS is bij de uitvoering van zijn sectorspecifieke opdrachten bijgevolg gebonden aan de in de Awb opgenomen algemene beginselen van behoorlijk bestuur, zoals het zorgvuldigheids- en motiveringsbeginsel, en aan de procedurele waarborgen van de Awb, tenzij daarvan in bijzondere wetgeving rechtmatig is van afgeweken.

De Awb ziet voornamelijk op besluiten. Artikel 1:3 lid 1 Awb definieert een besluit als: *'een schriftelijke beslissing van een bestuursorgaan, inhoudende een publiekrechtelijke*

rechtshandeling'. Doorgaans verrichten bestuursorganen echter ook feitelijke handelingen ter voorbereiding en uitvoering van besluiten. Denk hierbij bijvoorbeeld aan de rol van RWS als toezichthouder in de toepassing van grond. De toezichthandelingen die RWS tijdens dit proces uitvoert zijn feitelijk van aard. Pas wanneer RWS een overtreding constateert, wordt er een besluit tot het opleggen van een sanctie genomen. RWS is op basis de schakelbepaling van artikel 3:1 lid 2 Awb ook bij het uitvoeren van feitelijke handelingen gehouden te handelen conform de in afdeling 3.2 tot en met 3.4 gecodificeerde abbb. Niet alleen bij het nemen van besluiten dient RWS de abbb dus in acht te nemen, maar ook het feitelijk handelen van RWS kan getoetst worden aan de abbb.

De context is steeds in sterk mate bepalend voor de concrete invulling van de abbb. Gezien de inzet van een nieuwe technologie een nieuwe context betekent, doet dit pertinente vragen rijzen over de concrete invulling van deze beginselen. In het kader van nieuwe technologieën in zijn algemeenheid wordt in de literatuur gediscussieerd of de huidige abbb voldoende geschikt zijn om de juridische uitdagingen die nieuwe technologieën met zich meebrengen te adresseren. Hierover bestaat onenigheid.[1] Specifiek in relatie tot blockchain noemen Goossens, Verslype en Tjong Tjin Tai dat de interpretatie van de abbb een uitdaging kunnen vormen, en dat het discutabel is of de huidige wettelijke vereisten van legaliteit, transparantie en controleerbaarheid voldoende effectief zijn om risico's te adresseren waar blockchaingebaseerde smart contracts ingezet worden voor besluitvorming in de zin van de Awb.[2] Schemkes e.a. constateren dat de inzet van blockchain onder de Awb mogelijk is in de communicatie tussen burger en overheid, omdat de Awb elektronisch berichtenverkeer toelaat. Ze benoemen verder dat er ook bij de inzet van blockchain behoefte zal bestaan te voldoen aan de algemene beginselen van behoorlijk bestuur. Hierbij wijzen zij erop dat het belangrijk is in het achterhoofd te houden dat de openbaarheid van een smart contract niet noodzakelijk ook rechtens voldoende transparantie biedt.[3]

1 Zie Kulk & van Deursen 2020; Uylenburg 2019; Wolswinkel 2020; van Eck, Bovens & Zoudiris 2018; van Ettekoven 2019; van Eck, Peeters & Widlak 2021.
2 Goossens, Verslype & Tjong Tjin Tai 2020.
3 Schemkes e.a. 2019.

B. Algemene Verordening Gegevensbescherming (AVG)

Er kan binnen een blockchain sprake zijn van het verwerken van persoonsgegevens. Om deze reden wordt in deze paragraaf beknopt maar niet-limitatief ingegaan op enkele vraagstukken betreffende de Algemene Verordening Gegevensbescherming (AVG). In de literatuur over blockchain en de AVG zijn onder meer de volgende frequent terugkerende thema's te onderscheiden: toepassingsgebied, rollen van verwerker en verwerkingsverantwoordelijke, dataminimalisatie en het recht op vergetelheid.[4]

1° Toepassingsgebied

Met betrekking tot het **materieel toepassingsgebied** is de AVG van toepassing op geheel of gedeeltelijk geautomatiseerde verwerking, evenals de **verwerking van persoonsgegevens** die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[5] De AVG is evenwel niet van toepassing op de verwerking van persoonsgegevens in bepaalde gevallen beschreven in artikel 2 lid 2 AVG.

Artikel 4 lid 1 AVG definieert persoonsgegevens als: *"Alle informatie over een geïdentificeerde of identificeerbare natuurlijk persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*". Zodra gegevens geanonimiseerd zijn, is de AVG niet meer van toepassing. Volgens de Artikel 29-Werkgroep (nu de European Data Protection Board) zijn gegevens pas geanonimiseerd als het niet meer mogelijk is om de identiteit te achterhalen van een persoon.[6] In de literatuur[7] wordt het volgende onderscheid gemaakt tussen verschillende type gegevens in relatie tot de AVG:

4 Schemkes e.a. 2019.
5 Art. 1 lid 1 AVG.
6 Article 29 Data Protection Working Party 2014. In dit rapport wordt de objectieve leer aangehouden, aangezien dit niet tot non-compliance leidt indien de rechtspraak zich oriënteert richting de relatieve leer, terwijl dit andersom wel het geval is. Zie: Laan & Rutjes 2017.
7 Laan & Rutjes 2017; Berberich & Steiner 2016.

Figuur 9 Type gegevens in relatie tot de AVG

Type gegeven	Relatie tot de AVG
In het blok geregistreerde transactiegegevens	Versleutelde transactiedata zijn gepseudonimiseerde data, omdat deze ontsleuteld kunnen worden.[8] Het hashen of versleutelen van persoonsgegevens leidt in het algemeen slechts tot pseudonimisering en dus niet anonimisering. De header en de inhoud van het block kunnen persoonsgegevens bevatten.[9]
Public key	De publieke sleutel bevat gepseudonimiseerde data, omdat de identiteit van de persoon achterhaald kan worden door gebruik te maken van andere informatie, zoals een IP adres.[10] De public key *kan* een persoonsgegeven zijn als deze herleidbaar is tot een natuurlijke persoon.[11]
Private key	De private key kan een persoonsgegeven worden als de private key te herleiden is naar een natuurlijke persoon. De private key wordt echter doorgaans niet op de blockchain verwerkt.[12]
Smart contract	Een smart contract kan een persoonsgegeven zijn, indien er persoonsgegevens in een smart contract zijn opgenomen.[13]

Er moet dus telkens voldoende aandacht zijn voor wat wel of niet op de blockchain bewaard wordt, welke additionele informatiegegevens op de blockchain kunnen leiden tot de identificatie van een natuurlijk persoon, wie die additionele informatie kent en hoe die additionele informatie beveiligd is. Soms kunnen zelfs op erg subtiele wijze persoonsgegevens afgeleid worden uit metadata op de blockchain. Indien er – al dan niet gepseudonimiseerde – persoonsgegevens op de blockchain bewaard worden, is de AVG in elk geval van toepassing. Na pseudonimiseren is informatie nog steeds herleidbaar en is bijgevolg de AVG van toepassing is. Oplossingen hiervoor zijn het off-chain opslaan van persoonsgegevens met daarbij een link naar on-chain gegevens.[14] De gegevens die on-chain zijn opgeslagen, kunnen weliswaar eventueel nog steeds gekwalificeerd worden als persoonsgegevens.[15] Soms is dus

8 Schemkes e.a. 2019, p. 69.
9 Van Heukelom-Verhage e.a. 2019, par. 2.2.13, 2.3.1-2.3.3.
10 Schemkes e.a. 2019, p. 69.
11 Van Heukelom-Verhage e.a. 2019, par. 2.3.3.
12 Ibid., par. 2.3.4.
13 Ibid., par. 2.3.4.
14 Schemkes e.a. 2019; Van Heukelom-Verhage e.a. 2019.
15 Zoals de hash en de cryptografische sleutel. Schemkes e.a. 2019, p. 69 en 70.

inderdaad de enige oplossing om geen persoonsgegevens in de blockchain op te nemen en deze buiten de blockchain op te slaan, of deze te anonimiseren vooraleer ze worden opgenomen.[16] Daarnaast kunnen ook technieken zoals zero-knowledge-proofs[17] ingezet worden als extra maatregelen.[18]

Met betrekking tot het **territoriaal toepassingsgebied** is de verordening van toepassing op de verwerking van persoonsgegevens:[19]

1. *bij de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking al dan niet in de Unie plaatsvindt;*
2. *van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:*
   a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of
   b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt;
3. *door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is.*

Voor toepassing van de AVG is het dus vooral van belang dat de **vestiging van de verwerker of de verwerkingsverantwoordelijke in de Europese Unie** gelegen is, ongeacht of de verwerking zelf binnen de Unie plaatsvindt. De kwalificatie van participanten in een blockchain als verwerkers of verwerkingsverantwoordelijken is dus van belang om te bepalen of de AVG van toepassing is.[20]

In het geval de AVG van toepassing is *'op de buiten de EU gevestigde beheerder van een node, gebruiker of eigenaar van een blockchain die verantwoordelijke of verwerker is, mits de verwerkingen betrokkenen in de EU betreffen en verband houden met a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt'* stellen de auteurs van het rapport *Blockchain en het recht* terecht vragen over de handhaafbaarheid van de AVG, aangezien het kan gaan om grote aantallen nodes en die nodes zich buiten de EU kunnen bevinden.[21] In het rapport *Blockchain in de zorg* trekken de auteurs de conclusie dat al snel aan de territoriale eisen voor de

16 Goossens, Verslype & Tjong Tjin Tai 2020, p. 133-135; Laan & Rutjes 2017.

17 Dit is een cryptografische methode om te bewijzen dat je een bepaalde waarde ('een geheim') kent, zonder evenwel verdere informatie over die waarde prijs te geven. Dankzij deze technologie kan je dus een statement over gegevens bewijzen zonder dat de gegevens zelf gedeeld worden. Een voorbeeld is een digitale handtekening, waarbij men bewijst eigenaar te zijn van een private sleutel, zonder die sleutel zelf prijs te geven. J. Goossens, K. Verslype & E. Tjong Tjin Tai 2020, p. 130.

18 Schemkes e.a. 2019, p. 70.

19 Art. 3 AVG.

20 Goossens, Verslype & Tjong Tjin Tai 2020, p. 132 en 133.

21 Schemkes e.a. 2019, p. 69.

AVG zal zijn voldaan.[22] Wanneer een blockchain beheerd wordt in Nederland maar wel toegankelijk is voor buitenlandse gebruikers moet naar de concrete omstandigheden van het geval gekeken worden.[23]

2° *Rollen verwerkingsverantwoordelijke en verwerker*

Artikel 4 lid 7 AVG bepaalt dat de **verwerkingsverantwoordelijke** *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; (…)'* is. Het louter lezen van persoonsgegevens in een blok vormt al een verwerking van persoonsgegevens en het is dus irrelevant of een actor ook schrijfrechten heeft.[24] Het gedistribueerde karakter van blockchain kan het lastig maken om een partij aan te wijzen die zeggenschap heeft over de doelen en de middelen van de verwerking,[25] maar vaak zal het uiteindelijk mogelijk zijn om toch een centrale partij aan te wijzen die kan functioneren als verwerkingsverantwoordelijke, zelfs in een permissionless blockchain. Het is echter wel zo dat het lastig is om deze verantwoordelijkheid vorm te geven op een adequate manier zonder een duidelijke governance structuur. In het geval van een private permissioned blockchain is dit minder problematisch dan in het geval van een publieke permissionless blockchain, aangezien een private permissioned blockchain een bepaalde vorm van governance structuur heeft.[26]

Het rapport *Blockchain in de Zorg* concludeert dat (de nodes van) geautoriseerde gebruikers[27] verwerkingsverantwoordelijke zijn voor de persoonsgegevens die zij op de blockchain plaatsen en ten aanzien van de persoonsgegevens waarvan zij geautoriseerd zijn om ze te raadplegen, wijzigen of verwijderen.[28] Bij een groot aantal verwerkingsverantwoordelijken zal het nodig zijn om een super user aan te wijzen.[29]

De **verwerker** definieert artikel 4 lid 8 AVG als *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'*. Hierbij speelt bij een permissionless blockchain de vraag of (full) nodes die persoonsgegevens verwerken, maar niet als verwerkingsverantwoordelijke aangewezen kunnen worden, gelden als

22 Van Heukelom-Verhage e.a. 2019, par. 2.4.2-2.4.7.
23 Ibid, par. 2.4.4, 2.4.5.
24 Van Heukelom-Verhage e.a. 2019 par. 3.1.2.
25 Ibid., par. 3.3.5.
26 Schemkes e.a. 2019, p. 64-68.
27 Dit definieert het rapport als volgt: "De geautoriseerde gebruiker van de blockchain is een gebruiker die zelfstandig bepaalt of hij persoonsgegevens op de blockchain verwerkt en voor welke doelen hij dat doet." Zie: Van Heukelom-Verhage e.a. 2019, par. 3.3.9.
28 Ibid., par. 3.3.8.
29 Van Heukelom-Verhage e.a. 2019, par. 3.3.18.

verwerker en handelen 'namens' de verantwoordelijke.[30] Het is mogelijk dat nodes als verwerkers optreden als zij persoonsgegevens verwerken in een private permissioned blockchain.[31] Indien nodes persoonsgegevens verwerken namens de verwerkingsverantwoordelijke, dan zal een verwerkersovereenkomst opgesteld moeten worden.[32] In het geval van een publieke permissionless blockchain is het lastig om verwerkersovereenkomsten te sluiten, wat er in beginsel toe leidt dat alle individuele nodes als verantwoordelijke kunnen worden aangemerkt. Dit roept belangrijke vragen op in het licht van transparantie, omdat er veel verschillende verantwoordelijkheden verspreid zijn over een groot aantal partijen.[33]

3° Dataminimalisatie en het recht op gegevenswissing

De registraties van gegevens op de blockchain zijn bedoeld om onveranderlijk te zijn. In relatie tot de AVG roept dit onder meer vragen op met betrekking tot het principe van minimale gegevensverwerking en rechten van de betrokkene zoals het recht op gegevenswissing (ook recht op 'vergetelheid' genoemd), omdat het verwijderen van gegevens lastig is.[34] Voornamelijk als het permissionless blockchains betreft kan dit moeilijkheden opleveren, aangezien de persoonsgegevens van alle nodes verwijderd dienen te worden en er vaak geen coördinatie is tussen de onderlinge nodes. Daarnaast maakt het crypto-economisch protocol het onaantrekkelijk voor nodes om tegen de regels van het protocol, zoals onveranderlijkheid, in te gaan.[35]

Artikel 5 lid 1 AVG omschrijft het beginsel van **dataminimalisatie** als dat persoonsgegevens *'toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking")'*. Dit beginsel roept belangrijke vragen op in een blockchain context, omdat elke node in beginsel een (volledige) kopie van het grootboek bezit terwijl gegevensverwerking beperkt moet zijn tot hetgeen wat strikt noodzakelijk is op basis van het beginsel van dataminimalisatie. Daarnaast is de registratie van transactiegegevens in een blockchain onveranderlijk en roept dit bijgevolg vragen op over hoe gegevens verwijderd kunnen worden op het moment dat het niet meer noodzakelijk is dat deze op de blockchain verwerkt worden. Bij dergelijk append-only-mechanisme kunnen alleen maar blokken toegevoegd worden maar niet verwijderd, zodat er enkel meer gegevens worden verwerkt.[36]

30 Schemkes e.a. 2019, p. 68.
31 Van Heukelom-Verhage e.a. 2019, par. 3.6.7.
32 Ibid.
33 Schemkes e.a. 2019, p. 68.
34 Schemkes e.a. 2019; Van Heukelom-Verhage e.a. 2019; Berberich & Steiner, 2016; Millard 2018; Laan & Rutjes 2017.
35 Schemkes e.a. 2019, p. 71.
36 Van Heukelom-Verhage e.a. 2019, par. 5.4.7-5.4.10; Laan & Rutjes 2017, p. 1.

Het **recht op gegevenswissing**[37] is neergelegd in artikel 17 AVG. Dit is het recht van de betrokkene om "*van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen*" indien een van de gevallen genoemd in sub a-f van het eerste lid zich voordoet. Op dit recht zijn uitzonderingen mogelijk ingevolge artikel 23 AVG. Martini & Weinzierl zijn van oordeel dat het houden van openbare registers, zoals genoemd in overweging 73 VG, een uitzonderingsmogelijkheid kan vormen voor blockchains die openbare registers bevatten.[38] Het rapport *Blockchain in het Recht* noemt hierbij nog de Manni-zaak[39] en oordeelt dat blockchains die publieke registers bevatten "*kunnen profiteren van een lidstaatrechtelijke bepaling als bedoeld in art. 23 AVG. Op basis van de Manni zaak is aan te nemen dat de wezenlijke inhoud van grondrechten en fundamentele vrijheden (als genoemd in art. 23 aanhef AVG) inderdaad onverlet kan blijven bij een lidstaatrechtelijke beperking van het recht op wissing ten behoeve van openbare registers, mits de openbaar te maken persoonsgegevens beperkt blijven.*"[40]

Het rapport *Blockchain in de Zorg* benadrukt dat een verwerkingsverantwoordelijke onder andere technische maatregelen zal moeten nemen om ervoor te zorgen dat eenmaal registreerde persoonsgegevens verwijderd kunnen worden. De maatregelen die daarbij genomen moeten worden, zijn afhankelijk van het ontwerp van de blockchain.[41] Aan dit probleem kan onder meer tegemoet worden gekomen door enkel gepseudonimiseerde gegevens op de blockchain te plaatsen die aan een natuurlijk persoon kunnen gekoppeld worden met behulp van aanvullende gegevens die elders bewaard worden. Door middel van procedures moet het daarbij mogelijk zijn om de additionele informatie te verwijderen die nodig is om die gepseudonimiseerde gegevens te herleiden naar een natuurlijk persoon. Op dat moment is er immers niet langer sprake van gepseudonimiseerde, maar van anonieme gegevens waardoor de AVG niet langer van toepassing is.[42]

C. Mededingings- en aanbestedingsrecht

1° Mededingingsrecht

De inzet van blockchain als faciliterende technologie door RWS kan mededingingsrechtelijke en aanbestedingsrechtelijke vragen en risico's met zich meebrengen.

37 Ook wel het recht op vergetelheid genoemd.
38 Martini & Weinzierl 2017.
39 HvJ 9 maart 2017, zaak C-398/15 (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce tegen Salvatore Manni*).
40 Schemkes e.a. 2019, p. 70 en 71.
41 Van Heukelom-Verhage e.a. 2019, par. 5.4.42 ev. Zie voor een aantal oplossingsrichtingen ook: Schemkes e.a. 2019, p. 72 en 73.
42 Goossens, Verslype & Tjong Tjin Tai 2020, p. 137.

Zowel voor het mededingings- als aanbestedingsrecht zijn de mogelijke vraagstukken en risico's afhankelijk van de blockchaindesignkeuzes. Hierna worden voor beide beknopt een aantal van deze vraagstukken en risico's aangestipt.

Voor de mededingingsrechtelijke vraagstukken en risico's zijn de toegankelijkheid van informatie en de mogelijkheid om smart contracts op te zetten voor gebruikers van belang. In een blockchain waarbij concurrentiegevoelige informatie binnen het blockchain ecosysteem wordt geregistreerd en openbaar is voor concurrerende partijen, bestaat de mogelijkheid op samenzwering tussen partijen op basis van deze informatie. Het registreren van informatie op de blockchain versterkt hiermee de cohesie tussen partijen, zowel in het geval van publieke als private blockchains,[43] en samenzwering wordt hiermee een minder risicovolle uitkomst voor partijen.[44] Doordat informatie op de blockchain staat, wordt het daarnaast ook makkelijker voor partijen om afwijkend gedrag te monitoren, wat kartels mogelijk duurzamer maakt.[45] Dit **risico op strategisch gedrag** kan mogelijk **verkleind worden als concurrentiegevoelige informatie off-chain bewaard wordt**, waardoor het niet toegankelijk is voor concurrenten.[46] Bovendien gelden **vertrouwelijk aan de overheid meegedeelde bedrijfs- of fabricagegegevens** als **absolute uitzonderingsgrond** ex artikel 10 lid 1 **Wob**, wat inhoudt dat het verzoek tot openbaarmaking moet worden geweigerd.[47] Verder is het belangrijk om op te merken dat ook eenzijdige, eigen communicatie van concurrentiegevoelige informatie, bijvoorbeeld via het sturen van een e-mail, het risico met zich mee kan brengen dat de mededinging verzwakt raakt, aangezien het openbaar maken van deze informatie immers onzekerheid op de markt vermindert.[48] Denk bijvoorbeeld aan het eenzijdig kenbaar maken van de productie van zout in de pilot zoutlogistiek middels de blockchain waardoor concurrenten weten hoeveel ieder produceert en zich strategisch zouden kunnen gedragen. In het licht van designkeuzes is het risico op vervalsing van de concurrentie volgens Lianos waarschijnlijker in een private blockchain dan in een publieke blockchain.[49]

Verder bestaan in een permissionless blockchain geen restricties op de acties die gebruikers uit kunnen voeren, waardoor gebruikers zelf ook smart contracts kunnen opzetten. Smart contracts kunnen onder meer gebruikt worden om afspraken tussen partijen vast te leggen en automatisch uit te voeren, maar zouden bijvoorbeeld ook gebruikt kunnen worden om op voorhand een sanctie in het systeem in te bouwen waardoor partijen minder geneigd zijn om af te wijken van een gemaakte

43 Schrepel 2019, p. 141 en 142.
44 Pike & Capobianco 2020, hoofdstuk 4.
45 Schrepel, 2019, p. 145.
46 OECD 2018, p. 7.
47 Zie p. 41.
48 Eenzijdige communicatie kan daarmee onder artikel 101 VWEU vallen indien er voldoende bewijs is van kartelvorming. Zie: Guidelines on the Applicability of Article 101 TFEU to Horizontal Cooperation Agreements [2011] OJ C11/1, par. 62 en Lianos 2019, p. 66-68.
49 Lianos 2019, p. 66-68.

concurrentievervalsende afspraak. Stel: partij A en partij B hebben een prijsafspraak gemaakt waarbij ze gebruik maken van een smart contract dat automatisch een geldelijke sanctie oplegt als de prijsafspraak niet wordt nageleefd. Als een partij toch besluit van deze prijsafspraak af te wijken, wordt het smart contract automatisch uitgevoerd en wordt automatisch het afgesproken bedrag van de geldelijke sanctie overgemaakt van de afwijkende partij naar de andere partij. Afwijken van de prijsafspraak zal bijgevolg alleen lucratief zijn voor een partij indien de opbrengsten voor het afwijken van de prijsafspraak groter zijn dan de geldelijke sanctie die vastgelegd is in het smart contract. Om dit te voorkomen, zouden partij A en partij B de geldelijke sanctie in het smart contract dusdanig hoog kunnen maken dat het voor beide partijen bij voorbaat niet lucratief is om afwijkend gedrag te vertonen, zodat ze de prijsafspraak blijven naleven. Dit voorbeeld laat zien dat door de inzet van automatische sancties door middel van smart contracts concurrentievervalsend gedrag mogelijk langer in stand kan blijven.[50]

2° *Aanbestedingsrecht*

Binnen de pilot zoutlogistiek wordt zout aanbesteed, wat betekent dat het aanbestedingsrecht ook mogelijke juridische uitdagingen met zich mee kan brengen. Het aanbestedingsrecht is grotendeels van de EU afkomstig en de Nederlandse implementatie van deze regels is te vinden in de Aanbestedingswet 2012. Binnen het aanbestedingsrecht geldt dat in beginsel alle relevante partijen mee moeten kunnen doen bij aanbestedingsprocedures om marktverstoringen te voorkomen.[51]

Er bestaat nog weinig Nederlandstalige aanbestedingsrechtelijke literatuur die betrekking heeft op het gebruik van blockchain. Internationale publicaties hebben zich al kort verdiept in mogelijke juridische uitdagingen die zich voor kunnen doen bij de inzet van blockchain in publieke aanbestedingen.[52] Hierbij worden onder andere de onveranderlijkheid van blockchain en de versterking van de samenwerking van concurrerende partijen (*bid rigging*) als uitdagingen genoemd. De onveranderlijkheid van blockchain kan mogelijk uitdagingen opleveren omdat er bij aanbestedingen vaak een bepaalde mate van flexibiliteit nodig is, bijvoorbeeld als zich bijzondere omstandigheden voordoen waardoor het contract gewijzigd dient te worden. Daarnaast is een van de doelen van aanbestedingen dat mededinging zich ontwikkelt voor publieke contracten,[53] zodat publiek geld zo efficiënt mogelijk gespendeerd wordt.[54] Zoals al eerder is uitgelegd, kan de inzet van blockchain echter risico's met zich mee brengen voor de mededinging.

50 Schrepel 2019 p. 142-144.
51 Schlössels & Zijlstra 2017, nr. 604.
52 Carvalho 2019; Nin Sanchez 2019.
53 HvJ EU 15 oktober 2009, C-1 38/08 ECLI:EU:C:2009:627 (*Hochtief*), par. 47.
54 Europese Commissie 2011.

Over het meest geschikte blockchaindesign in het licht van aanbestedingen signaleert Sanchez dat de inzet van private blockchains het meest geschikt is in het aanbestedingsproces, omdat private blockchain makkelijker op maat gemaakt kunnen worden en daarmee aansluiting vinden bij de bijzonderheden van het aanbestedingsproces.[55] Ook Carvalho oordeelt dat een permissioned blockchain geschikter is om tegemoet te komen aan de complexiteit van het aanbestedingsrecht.[56]

In beginsel heeft een aanbestedende dienst ruimte om de scope van een opdracht vast te stellen. Dit geldt ook voor het opnemen van een eis van technische specificaties.[57] Deze technische specificaties hebben zeer snel een mededingingsrechtelijk aspect en zijn mededingingsgevoelig, waarbij men niet vergaand een bepaalde methode mag voorschrijven. Een technische eis mag dan ook niet disproportioneel of te beperkend zijn. Ook moet een gelijkwaardige oplossing worden geaccepteerd. De vraag hoe dit kan worden geregeld bij het (vereiste) gebruik van blockchain en in hoeverre sturing mogelijk is op de blockchain keuze zijn interessante vragen voor verder onderzoek, die buiten de scope van dit boek vallen. Het zal sowieso afhangen van het blockchaindesign of een dergelijke eis tot gebruik van blockchain in de opdracht kan worden uitgevraagd.

D. Wet hergebruik overheidsinformatie (Who)

1° Who en RWS

Open data dragen bij aan transparantie en accountability van de overheid binnen de democratische rechtsstaat. RWS verzamelt dagelijks grote hoeveelheden data. RWS meet bijvoorbeeld waterstanden, de verkeersintensiteit en de windsnelheid. RWS spant zich in om het hergebruik van open datasets te bevorderen door deze data toegankelijk te maken in een eigen dataregister.[58] Wie bepaalde data zoekt, kan in het register zien of de data beschikbaar is voor hergebruik. Het actief ter beschikking stellen van open datasets past in een beleid gericht op digitaal en transparant bestuur.

2° Who en open data

Uit het voorgaande blijkt dat RWS zich inspant met betrekking tot het realiseren van hergebruik van overheidsinformatie. RWS beoogt hiermee te voldoen aan de EU regelgeving over open data en hergebruik van overheidsinformatie. De huidige Europese regels voor het hergebruik van overheidsinformatie staan in de richtlijn

55 Sanchez 2019.
56 Carvalho 2019.
57 Art. 2:76 Aanbestedingswet.
58 Data Rijkswaterstaat.

2013/37/EU, ook wel bekend als de '*PSI Directive*'.[59] De richtlijn 2013/37/EU is inmiddels herzien en is per 17 juli 2021 vervangen door de Europese richtlijn inzake open data en hergebruik van overheidsinformatie.[60]

Met de Wet hergebruik overheidsinformatie (Who), in werking getreden sinds 1 juli 2021, is de Europese richtlijn voor het hergebruik van overheidsinformatie geïmplementeerd. De Who regelt dat eenieder een publieke instelling[61] kan verzoeken openbare overheidsinformatie te leveren in een vorm die hergebruik mogelijk maakt. In de Who wordt onder 'hergebruik' verstaan: "*het gebruik van informatie, neergelegd in documenten berustend bij een met een publieke taak belaste instelling, voor andere doeleinden dan het oorspronkelijke doel binnen de publieke taak waarvoor de informatie is geproduceerd*" (artikel 1 onder b Who). De Who heeft als doel natuurlijke personen en rechtspersonen in staat te stellen om openbare overheidsinformatie te hergebruiken als grondstof voor commerciële of niet-commerciële doeleinden.[62] Overheidsinformatie vertegenwoordigt immers vaak een substantiële economische waarde en kan derhalve door burgers of bedrijven worden hergebruikt voor innovatieve doeleinden, anders dan waarvoor de informatie in eerste instantie is geproduceerd. Het begrip overheidsinformatie wordt niet in de Who gedefinieerd, maar het wordt aangenomen dat daaronder alle informatie valt die overheidsorganisaties met een bepaald doel produceren en verzamelen om hun publieke taak te kunnen vervullen.[63] De reikwijdte van de Who is groot. Het toepassingsbereik strekt zich uit tot documenten die toegankelijk zijn op grond van de Archiefwet of op grond van regelgeving inzake openbare registers.[64] Het gaat dus om informatie die al algemeen openbaar is.

Onder het documentbegrip van de Who vallen zowel fysieke als digitale informatie.[65] Digitale documenten kunnen ook digitaal opgeslagen datasets of gegevens bevatten.[66] Het uitgangspunt van de Who is dat alle openbare overheidsinformatie zo gemakkelijk mogelijk beschikbaar moet zijn.[67] De Who stelt eisen hoe deze informatie beschikbaar moet worden gesteld. Instellingen moeten voor hergebruik beschikbare informatie verstrekken "*zoals de informatie bij de met een publieke taak*

59 De oorspronkelijke richtlijn stamt uit 2003 (2003/98/EC) en was geïmplementeerd in de Wob. Na herziening van de richtlijn en met de inwerkingtreding van de Who zijn de artikelen in de Wob vervallen.
60 Richtlijn (EU) 2019/1024.
61 Een publieke instelling wordt gedefinieerd als een openbaar lichaam als bedoeld in artikel 2 lid 1 Richtlijn 2003/98/EG. In richtlijn 2013/37/EU is de reikwijdte uitgebreid met musea, bibliotheken en archieven.
62 MvT Who, p. 3.
63 Handreiking VNG, 'Wet gebruik van overheidsinformatie (Who)', p. 7.
64 Zie MvT Who. Denk aan bijvoorbeeld meteorologische data of verkeersgegevens uit registers van het KNMI of CBS.
65 MvT Who, p. 8.
66 Ibid.
67 Handreiking VNG, 'Wet gebruik van overheidsinformatie (Who)', p. 6.

belaste instelling aanwezig is en voor zover mogelijk langs elektronische weg, in een open en machinaal leesbaar formaat, samen met de metadata, waarbij het formaat en de metadata voor zover mogelijk voldoen aan formele open standaarden" (artikel 5 lid 1 Who). Het is niet de bedoeling dat de informatie door de overheidsinstelling wordt bewerkt alvorens de gevraagde informatie ter beschikking wordt gesteld. Verstrekking dient "*as is*" plaats te vinden in een bestandsformaat met een zodanige structuur dat softwaretoepassingen eenvoudig gegevens in het document kunnen identificeren, herkennen en extraheren.[68] Overheidsorganisaties dienen hun informatiehuishouding dus zodanig te organiseren dat zij aan verzoeken tot hergebruik kunnen voldoen.

Een verzoek tot hergebruik dient in beginsel te worden gehonoreerd, tenzij er sprake is van één van de limitatief omschreven uitzonderingen uit artikel 2 lid 1 Who. Het mag bijgevolg niet gaan om informatie die nog niet openbaar is, er mogen geen rechten van derden op rusten en verstrekking van de informatie is niet toegestaan als deze persoonsgegevens bevat die niet zijn bedoeld voor hergebruik.

De herziene Europese richtlijn inzake open data en hergebruik van overheidsinformatie (Richtlijn (EU) 2019/1024), ook wel bekend als de Europese Open Data Richtlijn, zal op enkele punten een aanpassing van de Who vereisen. De aanleiding voor de herziening is de bredere datastrategie van de EU. Data moet door alle sectoren heen vrij kunnen stromen en de belemmeringen voor het hergebruik van data zouden door de nieuwe richtlijn moeten worden weggenomen.[69] In de richtlijn zijn bepalingen opgenomen over het beschikbaar stellen van dynamische gegevens en real-time data via *Application Programme Interfaces* (API's). Dit kunnen bijvoorbeeld gegevens of onderzoeksdata zijn die instellingen verzamelen via sensoren. Daarnaast is de reikwijdte van het begrip 'open data' uitgebreid. Het begrip omvat nu ook publieke informatie van overheidsbedrijven en onderzoeksdata die met overheidsmiddelen gefinancierd werden.[70] De inzet van blockchain zou een bijdrage kunnen leveren aan het uitvoeren van de Who, maar vanzelfsprekend is dit afhankelijk van de blockchaindesignkeuzes die gemaakt worden.

3° Who en Wob

Er zijn enkele verschillen tussen een Wob-verzoek en een Who-verzoek. Een Wob-verzoek ziet enkel op openbaarmaking van informatie, en impliceert niet tevens een verzoek tot hergebruik.[71] De Who gaat verder dan de Wob, in die zin dat het herbruikbaar ter beschikking stellen van informatie verder gaat dan het louter openbaar maken. Een instelling heeft namelijk een inspanningsverplichting om de informatie in een herbruikbare vorm aan te bieden, namelijk in een open en

68 MvT Who, p. 7.
69 VNG, 'Data delen en open maken', Brief aan de leden van 23 november 2020.
70 Art. 1 lid 1 Richtlijn (EU) 2019/1024.
71 Rijksoverheid, 'Handleiding Wet hergebruik van overheidsinformatie' (2016), p. 9.

machinaal leesbaar formaat.[72] Daarnaast mogen er, anders dan bij een Wob-verzoek, op de ter beschikking gestelde informatie geen auteursrechten van derden berusten.[73]

Ook de doelstelling achter een Wob- en Who-verzoek verschilt. Bij een Wob-verzoek wenst de verzoeker enkel kennis te nemen van de inhoud van een document, terwijl bij een Who-verzoek de verzoeker de informatie daadwerkelijk wil gebruiken voor andere doeleinden. Zowel de Wob als de Who beogen transparantie van overheidshandelen te bevorderen, maar de Who ziet daarnaast ook op het vrij hergebruik van informatie voor het creëren van economische waarde.

Wob- en Who-verzoeken staan niet op gespannen voet met elkaar en afhandeling van beide verzoeken kan gelijktijdig plaatsvinden.[74] Wanneer er een Who-verzoek om hergebruik wordt gedaan ten aanzien van informatie die nog niet openbaar is, kan er gelijktijdig een afweging over de openbaarmaking plaatsvinden.[75] De gebruikelijke Wob-toets moet dan worden uitgevoerd. Als blijkt dat er sprake is van de weigeringsgronden van de Wob en de informatie zich dus niet leent voor openbaarmaking, dient het Who-verzoek te worden afgewezen.

4° Who en Archiefwet

Op grond van de Who kan ook een verzoek tot hergebruik worden ingediend met betrekking tot informatie die zich in een archiefbewaarplaats bevindt. In de Archiefwet is bepaald dat onder 'gebruik' ook hergebruik wordt verstaan in de zin van richtlijn 2003/98/EG. In de Archiefwet zijn enkele artikelen van de Who van overeenkomstige toepassing verklaard, namelijk artikelen 5, 6 en 9 Who.[76] De Archiefwet is aangevuld met regels over het ter beschikking stellen van de informatie in een machinaal leesbaar formaat, de voorwaarden voor hergebruik en de tarifering onder de Who.

De Who verplicht niet tot het bewaren van informatie specifiek met hergebruik tot doel. De Who staat zodoende niet op gespannen voet met de vernietigingsplicht uit de Archiefwet.

72 Art. 5 lid 1 Who.
73 Art. 2 lid 1 onder b Who.
74 Rijksoverheid, 'Handleiding Wet hergebruik van overheidsinformatie' (2016) p. 10.
75 Ibid. p. 11.
76 Zie art. 17 lid 1 en art. 19 Archiefwet.

E. Smart contracts: functies

Een smart contract is een simpel 'als x, dan y' algoritme, namelijk een deterministische set regels die automatisch uitgevoerd worden op het moment dat aan de vooraf vastgestelde condities is voldaan. Het gebruik van smart contracts vergroot de toepassingsmogelijkheden van blockchainapplicaties enorm. In combinatie met smart contracts kan blockchain immers ingezet worden voor de automatisering van 1° de registratie van informatie, 2° waardeoverdracht en 3° het uitvoeren van regels. In een permissionless blockchain kunnen partijen zelf smart contracts opzetten.

Smart contracts kunnen dus drie functies vervullen. Allereerst het **registreren van feiten**, bijvoorbeeld het registreren van stappen in een ketenproces. Ten tweede het **transfereren van waarde** of een representatie daarvan via een token, bijvoorbeeld de koop van een huis met een cryptomunt. Ten derde het **automatisch uitvoeren van regels**, bijvoorbeeld een automatische betaling van boetes of belastingen. Meestal worden deze functies gecombineerd en het combineren van deze functies vergroot de toepassingsmogelijkheden van blockchain aanmerkelijk. In het licht van deze drie functies kan over de pilots van RWS het volgende geobserveerd worden.

Op het moment van schrijven van dit boek maken de pilots enkel gebruik van de eerste functie van smart contracts, namelijk het registreren van feiten. In de pilot zoutlogistiek werd alleen verkend of gegevens over het ketenproces in de blockchain geregistreerd konden worden. Een automatische executie van regels was niet in de pilot meegenomen, zoals een automatische boete bij zout met ondermaatse kwaliteit. Er vond ook geen transfer van waarde plaats middels de blockchain, bijvoorbeeld voor de aankoop van het zout. In de pilot grondstromen werd alleen verkend of gegevens over de samengevoegde grond geregistreerd konden worden. De mogelijke inzet van een (rood) signaal algoritme over het samenvoegen van partijen grond zou in de toekomst ontworpen kunnen worden als een algoritme dat automatisch een regel uitvoert en daar een consequentie aan verbindt, zoals een automatische boete bij het verkeerd samenvoegen van grond. Verder vindt er ook geen transfer van waarde plaats middels de blockchain, bijvoorbeeld betaling middels een token voor de koop van grond.

In de toekomst zouden de pilots de inzet van de andere twee functies kunnen **exploreren**, aangezien het inzetten van een combinatie van verschillende functies van smart contracts de toepassingsmogelijkheden van de blockchainpilots kan vergroten. Het gaat dan in casu vooral om de mogelijke **automatische uitvoering van regels**. Hierbij zal dan aandacht moeten worden besteed aan de juridische consequenties van het inzetten van deze andere functies, zoals **gevolgen voor rechtsbescherming bij de (gedeeltelijke) automatisering van besluitvorming**.

F. Oracles: garbage in, garbage out

Verder is het belangrijk op te merken dat het feit dat gegevens in de blockchain geregistreerd zijn geen garantie vormen voor de correctheid van die gegevens.[77] Zo kunnen gegevens afkomstig van oracles onbetrouwbaar zijn, omdat oracles uiteindelijk entiteiten zijn die vertrouwd moeten worden aangaande de juistheid van hun input in de blockchainapplicatie. Dit probleem wordt het "*oracle problem*" genoemd.[78] Risico's die het gebruik van oracles met zich mee brengen zijn bijvoorbeeld het (opzettelijk) invoeren van foutieve gegevens of dat het oracle onveilig is en daarmee gevoelig voor cyber-aanvallen. Foutieve invoer van gegevens is onwenselijk, want op het moment dat het oracle geen goede input geeft aan een smart contract, zal het smart contract ook geen verwachtte output kunnen genereren. Daarenboven liggen de foutieve gegevens onveranderlijk vast op de blockchain. Verder is het interessant om op te merken dat vanuit spel theoretisch oogpunt de kans hierop hoger wordt naarmate de waarde waar de transactie over gaat hoger wordt.[79]

Een overheid die publiek gezag uitoefent dient zich echter onder meer te houden aan het zorgvuldigheidsbeginsel. Op basis van artikel 3:2 Awb dient het bestuursorgaan bij de voorbereiding van een besluit de nodige kennis te vergaren omtrent de relevante feiten (en de af te wegen belangen). Het ligt dus voor de hand dat een bestuursorgaan er zich zal moeten van vergewissen dat er een juiste input via oracles heeft plaatsgevonden. Daarnaast moet op basis van de AVG informatie die gekwalificeerd wordt als persoonsgegevens ook correct zijn.

77 Schemkes e.a. 2019, p. 27 en 28.
78 Caldarelli 2020, p. 5.
79 Sztorc 2017.

IV. Tussenconclusie

Het recht op toegang tot overheidsinformatie is fundamenteel voor een goede werking van onze democratische rechtsstaat. Uit het wettelijk kader betreffende de toegang van overheidsinformatie blijkt dat geen grondrecht op overheidsinformatie is opgenomen in de Nederlandse Grondwet, maar dat de toegang tot en openbaarheid van overheidsinformatie in verschillende wetten is gewaarborgd.

De Wob/Woo en de Archiefwet vormen samen het belangrijkste wettelijke kader. Zowel de Wob als de Archiefwet hanteren het uitgangspunt dat overheidsinformatie voor eenieder openbaar is, tenzij openbaarheid conflicteert met een in de wet genoemde uitzonderingsgrond. Overheden dienen bij het beheer, de verwerking en ontsluiting van overheidsinformatie de vereisten van de Wob en de Archiefwet in acht te nemen. Onder de reikwijdte van de juridische begrippen 'document' uit de Wob en 'archiefbescheiden' uit de Archiefwet ('documenten' in de Archiefwet 2021) vallen niet alleen papieren documenten, maar ook digitale informatiedragers, elektronische gegevens en data.[1] **Voor het toepassingsbereik van de Wob en de Archiefwet zijn de vorm en het medium van de informatie niet relevant**.[2] De Wob en de Archiefwet zijn dus onverkort van toepassing op digitale vormen van informatie. **Gegevens op een blockchain** zullen logischerwijs dus ook **onder de reikwijdte van de Wob en de Archiefwet** vallen.

Door de sterk toegenomen inzet van steeds complexer wordende technologieën hebben overheden **onvoldoende grip op de digitale informatiehuishouding**. Overheden hebben moeite met het beheren van grote hoeveelheden digitale informatie waardoor de toegankelijkheid en beschikbaarheid van overheidsinformatie geen vanzelfsprekendheid is in de bestuurlijke praktijk. Er is een acute noodzaak om de digitale informatiehuishouding van de overheid op orde te brengen, en mede tegen die achtergrond vervangt de Woo vanaf 1 mei 2022 de Wob. De **Woo** beoogt een noodzakelijke cultuuromslag teweeg te brengen bij de overheid, door **het recht**

---

1 Vlg. ABRvS 26 april 2016, ECLI:NL:RVS:2016:1138, AB 2016/233, m.nt. P.J. Stolk, JG 2016/40, m.nt. T. Barkhuysen & A. Span; ABRvS 22 mei 2019 ECLI:NL:RVS:2019:1675, m.nt. H.S. ten Cate en C.A. Geleijnse; Duurzaam Digitaal Databeheer bij de Rijksoverheid (2021).

2 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899.

op toegang tot overheidsinformatie ten opzichte van de Wob te **versterken** en **actieve openbaarmaking van overheidsinformatie** tot de **norm** te verheffen.[3] Het op zodanige wijze inrichten van informatiesystemen en werkprocessen dat er ***by design*** een adequate toegang tot overheidsinformatie is gewaarborgd, zal binnen overheden meer dan ooit van belang worden. Ook bij de inzet van blockchaintechnologie zullen overheden bij de designkeuze het belang van een effectieve toegang tot overheidsinformatie voorop moeten stellen.

Niet alleen de Wob en de Archiefwet, maar ook de Who stelt eisen met betrekking tot de toegang tot overheidsinformatie. De Who is het wettelijk kader voor **het voor hergebruik beschikbaar stellen van overheidsinformatie** en stelt randvoorwaarden aan het formaat waarin de informatie dient te worden verstrekt. Dit vraagt van overheden om informatiesystemen en werkprocessen zodanig in te richten dat aan verzoeken tot hergebruik conform de Who kan worden voldaan. Bij het ontwerp van nieuwe informatiesystemen of de inzet van blockchaintechnologie zal dus ook rekening gehouden moeten worden met de vereisten van de Who.

Voorts blijkt uit de korte schets van het overige wettelijk kader dat de toegang tot overheidsinformatie mede ten gevolge van de **AVG** niet onbegrensd is. Er is een spanningsveld tussen de openbaarheid van overheidsinformatie enerzijds, en de bescherming van persoonsgegevens anderzijds. De AVG is erop gericht om persoonsgegevens tegen onnodige verwerking en openbaarmaking te beschermen. Overheden zullen bij een mogelijke inzet van blockchainapplicaties dus tevens privacy *by design* moeten waarborgen. De inzet van blockchaintechnologie brengt gegevensbeschermingsrechtelijke uitdagingen met zich mee en heeft consequenties met betrekking tot designkeuzes bij een eventuele inzet van blockchaintechnologie binnen de overheid. Indien er – al dan niet gepseudonimiseerde – persoonsgegevens op de blockchain bewaard worden, is de AVG in elk geval van toepassing. Meestal is de meest voor de hand liggende oplossing het off-chain opslaan van persoonsgegevens.

Verder roept de inzet van blockchain ook **mededingings- en aanbestedingsrechtelijke vragen** op. Ook hier is het specifieke blockchaindesign de meest relevante factor. Zo kan transparantie positieve of negatieve effecten hebben voor zowel de mededinging als aanbestedingen, is het belangrijk te overwegen of commerciële partijen ook smart contracts kunnen opzetten in het licht van het mededingingsrecht en kan flexibiliteit van het design van belang zijn in het aanbestedingsproces. Het risico op strategisch gedrag kan mogelijk verkleind worden als **concurrentiegevoelige informatie off-chain bewaard** wordt, waardoor het niet toegankelijk is voor concurrenten. Bovendien gelden **vertrouwelijk aan de overheid meegedeelde**

3 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 1-2.

bedrijfs- of fabricagegegevens als **absolute uitzonderingsgrond** ex artikel 10 lid 1 Wob, wat inhoudt dat het verzoek tot openbaarmaking moet worden geweigerd.

De bevindingen van dit hoofdstuk vormen de basis voor de verkenning van de Wob en de Archiefwet in het volgende hoofdstuk. Hierbij wordt ingegaan op de toepasselijkheid en de consequenties van deze wetten op de inzet van blockchain en het blockchaindesign.

V. Verkenning: toepassing van wettelijk kader toegang tot overheidsinformatie bij de inzet van gedistribueerde technologie

A. Soorten designkeuzes en typen informatie

1° Designkeuzes

Bij de inzet van blockchain staat RWS voor verschillende keuzes in design of architectuur van het systeem. Het gaat voornamelijk om keuzes met betrekking tot toegang (publiek, privaat, hybride), autorisaties of participatierechten voor gebruikers (permissioned of permissionless) en gegevensopslag (on-chain of off-chain). Wat deze keuzes precies inhouden, is behandeld in sectie I.D van dit boek.[1] Elke designkeuze gaat gepaard met verschillende voor- en nadelen. Alvorens in te gaan op de juridische consequenties van de designkeuzes worden hieronder niet-limitatief enkele voor- en nadelen inzake gegevensopslag, -toegang en -bescherming samengevat weergegeven die een invloed hebben op de keuze tussen publieke, private of hybride blockchains.[2] In de praktijk zijn publieke blockchains meestal permissionless en zijn private blockchains doorgaans permissioned.

1 Zie p. 28-29.
2 Deels gebaseerd op VNG Realisatie 2019, hoofdstuk 11.

Figuur 10 Enkele voor- en nadelen van het blockchaindesign inzake gegevensopslag, -toegang en -bescherming

Soort blockchain	Voordelen	Nadelen
Publiek	– Netwerk waarborgt de integriteit van geregistreerde gegevens en alle actoren in het netwerk kunnen de gegevens verifiëren – Alle actoren kunnen transacties verifiëren – Broncode en eventueel code van toepassingen zijn openbaar	– Mogelijk spanning met de AVG indien sprake is van verwerking van persoonsgegevens – Weinig controle mogelijk op de governance van het platform
Privaat	– Gegevensbescherming is makkelijker te borgen – Toegangsrechten zijn beheersbaar – Software is beheersbaar	– Partijen buiten het netwerk hebben geen toegang, wat transparantievraagstukken kan opleveren
Hybride	– Privacy- of bedrijfsgevoelige gegevens kunnen worden opgeslagen en beheerd in het besloten deel	– Weinig controle op governance in het open deel van de blockchain
Permissioned	– In beginsel een heldere governance structuur aanwezig – Rollen van actoren onder de AVG zijn makkelijker in te regelen – Meer invloed mogelijk op design van de technische architectuur – Geschikter voor aanbestedingsprocedures wegens grotere flexibiliteit	– Afhankelijk van de specifieke blockchain: in mindere mate of niet gedecentraliseerd – Zeggenschap over de regels voor het technologische design ligt bij selecte groep – Kans op samenzwering van actoren in het netwerk
Permissionless	– Mededingingsrechtelijke vraagstukken indien partijen zelf concurrentiebeperkende smart contracts op kunnen zetten	– Duidelijke governance structuur afwezig – Rollen van actoren onder de AVG zijn lastiger te regelen

Wijze van gegevensopslag	Voordelen	Nadelen
On-chain gegevensopslag in blockchain	– Onveranderlijke en fraudebestendige vastlegging van gegevens – Afhankelijk van soort blockchain: geregistreerde gegevens zijn mogelijk zichtbaar voor partijen binnen het netwerk	– Spanning met o.m. het recht op vergetelheid onder de AVG – Eenmaal geregistreerde gegevens zijn lastig te verwijderen – Mededingingsrechtelijke vraagstukken bij on-chain registratie van concurrentiegevoelige informatie – Aanbestedingsrechtelijke vraagstukken
Deel van de gegevens off-chain opslaan in een andere (mogelijk centrale) database	– Gegevensbescherming is makkelijker te borgen in een centrale database – Beheer en huishouding van data is makkelijk te regelen	– Kwetsbare gegevensbeveiliging: hacken van het centraal systeem is voldoende om toegang te krijgen tot de gegevens

2° *Gegevens en informatie*

Vanuit juridisch-analytisch oogpunt is het nuttig om een onderscheid te maken tussen volgende **vier invalshoeken** die een impact kunnen hebben op de beschikbaarheid van en toegang tot gegevens en informatie: 1° de technische infrastructuur (i.e. het blockchainsysteem), 2° de gebruikers (ketenpartners), 3° de overheid die een publieke taak of publiek gezag uitoefent (RWS in dit geval) en – voor dit boek bijzonder relevant – 4° de informatieverzoeker die zijn recht op toegang tot overheidsinformatie kan inroepen (de burger, maar ook andere overheden dan RWS of een ketenpartner bijvoorbeeld).[3] Betrokken actoren kunnen ook verschillende of meerdere posities tegelijkertijd innemen. RWS is bijvoorbeeld gebruiker van en ketenpartner in een mogelijke blockchainapplicatie, maar heeft tevens bijkomende verantwoordelijkheden bij het uitoefenen van een publieke taak of publiek gezag, bijvoorbeeld in zijn rol als toezichthouder. De invulling van deze invalshoeken zal dus afhangen van het concreet geval. Het is tevens denkbaar dat RWS zelf de rol van informatieverzoeker inneemt indien hij informatie opvraagt binnen een blockchainapplicatie van een ander bestuursorgaan.

De eerste invalshoek is het **blockchainsysteem**. Hier zijn verschillende gegevens denkbaar, bijvoorbeeld de code van het consensusmechanisme of het smart contract, de locatie van nodes, of gegevens over oracles. Het gaat hier om ***hard- en software***. Voorbeelden van informatie over het blockchainsysteem zijn informatie over hoe

3 Deze vier invalshoeken zijn natuurlijk slechts deel van een vereenvoudigde indeling met het doel om tot een heldere analyse te kunnen komen. Bijkomende invalshoeken zijn denkbaar.

het consensusmechanisme of andere algoritmen binnen het systeem werken. Vanuit juridisch oogpunt is het daarnaast interessant om tussen deze verschillende soorten gegevens en informatie waar mogelijk een onderscheid te maken tussen onderdelen van het systeem die al dan niet deel uitmaken van een besluitvormingsproces dat leidt tot een Awb-besluit. Dit onderscheid is onder meer van belang voor de toegang tot en rechtsbescherming door de bestuursrechter. Een voorbeeld hiervan is een algoritme dat (gedeeltelijk) geautomatiseerd besluiten in de zin van de Awb neemt.

De tweede invalshoek is de **gebruiker** die zelf gegevens in het systeem invoert, bijvoorbeeld welke typen grond de gebruiker heeft samengevoegd. Het gaat hier dus om ***inputgegevens*** zelf. Daarnaast bestaan er ***gegevens die door het gebruik van het systeem ontstaan***, zoals de transacties die in het gedistribueerde grootboek staan.[4] Verder bestaan er ook nog ***gegevens van gebruikers***, zoals de pseudoniemen waaronder transacties in het systeem plaatsvinden.

Verder bestaan er vanuit de invalshoek van de **overheid die een publieke taak of publiek gezag uitoefent (RWS)** gegevens over hoe RWS het systeem gebruikt, bijvoorbeeld gegevens over hoe vaak RWS de gebeurde transacties bekeken heeft, onder meer met het oog op zijn toezichtfunctie.[5] Daarnaast bestaat er ook informatie over hoe RWS omgaat met het systeem, bijvoorbeeld het beleid van RWS met betrekking tot hoe hij omgaat met een (rood) signaal inzake de compatibiliteit van het samenvoegen van partijen grond in de grondstromen pilot. RWS heeft als bestuursorgaan tevens allerhande verplichtingen die onder meer voortvloeien uit de Wob, de Woo en de Archiefwet.

Tenslotte is er de invalshoek van de **informatieverzoeker**. Een beslissing op een verzoek tot informatie is een besluit in de zin van artikel 1:3 lid 1 Awb.[6] Met deze beslissing wordt tevens nieuwe overheidsinformatie gecreëerd waartoe openbaarheid verzocht kan worden. Het gaat hier om ***informatieverzoekers die in beginsel zelf geen participanten zijn in het blockchainnetwerk***, want participanten die binnen het blockchainnetwerk actief zijn hebben doorgaans toegang tot de informatie op de blockchain. Eenieder kan een verzoek tot informatie indienen, bijvoorbeeld burgers, bedrijven, NGO's, journalisten of overheden. Er dient te worden opgemerkt dat deze verschillende actoren bij het verzoek tot informatie verschillende informatiebehoeften hebben.[7]

---

4 Zie ook: Lemieux, Hofman, Batista & Joo 2019, tabel 1.

5 Dit geldt natuurlijk enkel voor zover het design van het systeem zo is vormgegeven dat deze gegevens worden opgeslagen.

6 Damen, Albers, de Graaf, Klap, Klingenberg, Marseille, Nicolaï, Olivier, Tolsma en Vermeer 2013, p. 303.

7 De Fine Licht & Naurin 2016.

Onderstaande tabel geeft het bovenstaande nogmaals schematisch weer aan de hand van de pilot grondstromen. Er moet wel worden vermeld dat in de pilot geen technische concepten en geen technisch blockchaindesign zijn uitgewerkt. De voorbeelden benoemd in onderstaande tabel zijn dus hypothetisch en louter bedoeld om de invalshoeken en typen gegevens te verduidelijken.

Figuur 11 Enkele voor- en nadelen van het blockchaindesign inzake gegevensopslag, -toegang en -bescherming

Invalshoeken en typen gegevens/ informatie	Pilot grondstromen
1° **Blockchainsysteem**	
Informatie over de architectuur van het systeem	Informatie over de verschillende bouwstenen van het systeem, zoals de hardware of de softwarecode.
Informatie over de werking van het systeem	Informatie over hoe bijvoorbeeld het (rood) signaal zou kunnen werken bij het samenvoegen van grond en welke output bij een bepaalde input verwacht kan worden. Dit zou informatie kunnen inhouden in het kader van besluitvorming in de zin van de Awb. Deze informatie is afhankelijk van de design- en beleidskeuzes die betrokken ketenpartners maken en kan bijvoorbeeld zijn neergelegd in een handleiding.
2° **Gebruikers**	
Gegevens die de gebruiker invoert	Bijvoorbeeld welke typen grond samengevoegd worden, kwaliteit van de grond, capaciteit van de opslaglocatie, aantal ton grond, PDF's.
Gegevens die gegenereerd worden bij het gebruik van het systeem	Hashes, transacties, of het grootboek (als een set van gegevens) waarop alle eerdere transacties staan.
Gegevens over de gebruikers	Pseudoniemen waaronder transacties plaatsvinden en mogelijk andere persoonsgegevens.[8]

8 Zie p. 55 e.v. van dit rapport; Voor een uitgebreide analyse van persoonsgegevens binnen een blockchain, zie Van Heukelom-Verhage e.a. 2019.

Invalshoeken en typen gegevens/ informatie	**Pilot grondstromen**
3° **Overheid (RWS)**	
Gegevens over hoe RWS het systeem gebruikt	Metagegevens, bijvoorbeeld de tijdstippen wanneer toezichthoudende en handhavende overheidsinstellingen zoals RWS een bepaalde transactie heeft bekeken om te checken of en hoe vaak er sprake is van een rood signaal ten behoeve van hun rol van als toezichthouder en/of handhaver.
Informatie over hoe RWS blockchain gebruikt	Beleid over hoe toezichthoudende en handhavende overheidsinstellingen zoals RWS het blockchainsysteem inzet bij zijn toezicht- en handhavende houdende taak op grondstromen, documentatie over beleidsvorming, en documentatie van het testproces van de ontwikkeling van de pilot grondstromen.[9]
4° **Informatieverzoeker**	
Beslissing op informatieverzoek	Hypothetisch voorbeeld: Een onderzoeker is geïnteresseerd naar de historische ontwikkeling van een stuk grond en dient daartoe een Wob-verzoek in. De onderzoeker doet onderzoek naar het bredere natuurgebied en de ontwikkelingen ervan, waardoor hij naast de grond die momenteel aanwezig is ook geïnteresseerd is in de informatie over de grond die is weggehaald maar nu niet meer aanwezig is. De onderzoeker dient een Wob-verzoek in en hierop volgt een beslissing van RWS om alle documenten over het stuk grond openbaar te maken. Met deze informatie kan de onderzoeker een beeld schetsen van de historische ontwikkeling.

3° *Verhouding van gegevens en informatie tot Wob en Archiefwet*

De toepassing van de Wob, de Woo en de Archiefwet is **niet toegespitst op de inzet van een specifieke technologie**, zodat de analyse van dit wettelijke kader inzake toegang tot en archivering van gegevens en informatie ook bij de inzet van blockchain van belang is.[10] De Wob is een informatiestelsel, terwijl de Archiefwet een documentenstelsel kent.[11] Het **informatiestelsel** van de **Wob** houdt in dat de verzoeker kan volstaan met een verzoek tot openbaarmaking van informatie over een bepaalde bestuurlijke aangelegenheid, waarna het de taak is van het bestuursorgaan om te onderzoeken of de gevraagde informatie in documenten is neergelegd. De verzoeker hoeft dus niet aan te duiden welk specifiek document hij wenst te ontvangen. De verzoeker hoeft er alleen maar voor te zorgen dat zijn verzoek ziet op een bestuurlijke aangelegenheid en voldoende concreet is om in behandeling te nemen.

9 Zie Helwig 2020.
10 Zie p. 69.
11 Zie p. 48.

Bij het **documentenstelsel** van de **Archiefwet** daarentegen moet de informatieverzoeker de documenten waarvan hij openbaarmaking vraagt benoemen of beschrijven. Het is daarbij niet nodig dat het gaat om een bestuurlijke aangelegenheid.

De volgende secties behandelen gegevens en informatie vanuit de vier geïdentificeerde perspectieven in het licht van de Wob en de Archiefwet.

✓ *Wob*

Informatie kan "gewobt" worden zodra het gaat om informatie die is neergelegd in documenten over een bestuurlijke aangelegenheid. Onder de Wob rust er geen plicht op het bestuursorgaan om een document met de gevraagde elektronische gegevens aan te maken als dit niet al in een bestaand document staat, ongeacht de mate van inspanning.[12] Zolang RWS bovengenoemde typen gegevens niet vastlegt in documenten, zal een Wob-verzoek naar informatie niet slagen en heeft RWS geen verplichting om dit Wob-verzoek te beantwoorden. Neem als hypothetisch voorbeeld het niet registreren van het signaal dat afgegeven wordt bij typen grond die niet samengevoegd mogen worden in de pilot grondstromen. In dit geval zal een Wob-verzoek naar deze informatie in beginsel niet slagen. Hierbij is het relevant om op te merken dat het registreren van deze informatie interessant kan zijn voor RWS in zijn rol als toezichthouder, omdat dit als bewijs kan dienen dat de gebruiker van het systeem er bewust van diende te zijn dat bepaalde partijen grond niet samengevoegd mochten worden. Het vastleggen van deze informatie in documenten, in de pilot grondstromen eventueel in de blockchain, kan daarmee de effectiviteit van RWS als toezichthouder (en andere betrokken toezichthoudende en handhavende overheidsinstellingen) verhogen. De vraag welke informatie in een blockchain moet worden opgenomen, is dus zeker niet alleen een juridisch vraagstuk. Het is ook een uitvoeringsvraag, een bestuurlijke vraag en kan mogelijk zelfs een politieke beleidsvraag worden in het licht van de ministeriële verantwoordelijkheid en de democratische controle van de volksvertegenwoordiging op rechtmatig en efficiënt overheidsoptreden.

Volgens de Wob is een document "*een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat*" (artikel 1 onder a Wob). Dit begrip omvat twee elementen, namelijk "een schriftelijk stuk of ander materiaal dat gegevens bevat" en "berusten bij". Hierna wordt ingegaan op deze twee verschillende elementen en wordt behandeld welke typen gegevens en informatie kunnen worden beschouwd als documenten in de zin van de Wob in het geval van een blockchaintoepassing. Bij de individuele behandeling van deze twee elementen wordt voor deze analyse aangenomen dat aan het andere criterium is voldaan. Zo wordt bij de behandeling van het element "schriftelijk stuk of ander materiaal dat gegevens bevat" aangenomen

12 ABRvS 5 juni 2013, ECLI:NL:RVS:2013:CA2102, par. 3.1.

dat, indien hiervan te spreken is, het document berust of behoort te berusten[13] bij het bestuursorgaan, en andersom.

Schriftelijk stuk of ander materiaal dat gegevens bevat
In een uitspraak van 20 maart 2019 oordeelde de ABRvS dat het begrip document in ruime zin moet worden uitgelegd en dat ook andere soorten gegevensdragers onder dit begrip kunnen vallen.[14] Het is dan ook vaste rechtspraak van de ABRvS dat elektronisch vastgelegde gegevens documenten zijn in de zin van de Wob.[15] Het is echter niet zo dat een systeem als zodanig een document is in de zin van de Wob.[16] Hoewel de Wob is geschreven toen de blockchaintechnologie nog niet bestond, zullen bepaalde gegevens en informatie die zijn neergelegd in een blockchainsysteem dat RWS inzet kunnen kwalificeren als "ander materiaal dat gegevens bevat" en dus mogelijk als Wob-baar "document". Dit wordt toegelicht aan de hand van de pilot grondstromen.

Met de pilot grondstromen beoogde RWS een grondstromenpaspoort te genereren dat inzichtelijk maakt wat de herkomst, eigenschappen en het gebruik van grond zijn. Gebruikers krijgen een interface te zien waarbij ze zelf gegevens in kunnen vullen over grond. Een van de functionaliteiten is dat gebruikers verschillende typen grond in kunnen voeren, waarna ze een eventueel (rood) signaal zouden kunnen krijgen, wat weergeeft dat partijen grond niet samengevoegd mogen worden.

Vanuit de **invalshoek van het systeem** bestaan twee typen materialen, namelijk gegevens van het systeem zoals de hardware- en de softwarecode en informatie over het systeem, zoals een handleiding. Bij analoge toepassing van de vaste rechtspraak van de ABRvS[17] zullen de gegevens van het **systeem zelf** hoogstwaarschijnlijk **niet** kwalificeren als een **document in de zin van de Wob** en het blockchainsysteem als zodanig is daarmee geen document in de zin van de Wob. Zo zal bijvoorbeeld de code van het consensusmechanisme in beginsel niet Wob-baar zijn. Naarmate de relatie tussen informatiesystemen en de bestuurlijke aangelegenheid nauwer wordt, zou dit echter kunnen veranderen. Verder zal de informatie die is vastgelegd in andere materialen of schriftelijke stukken, zoals (delen van) een handleiding over hoe het systeem werkt wel te kwalificeren zijn als een document in de zin van de Wob.

---

13 Als documenten onder het bestuursorgaan hadden behoren te berusten, dan mag van het bestuursorgaan worden verwacht dat het al het redelijkerwijs mogelijke doet om deze documenten alsnog te achterhalen. Zie ABRvS 30 September 2009, ECLI:NL:RVS:2009:BJ8916, r.o. 2.6.1.
14 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, r.o. 5.
15 ABRvS 21 december 2011, ECLI:NL:RVS:2011:BU8863.
16 Noot bij H.S. ten Cate en C.A. Geleijnse ABRvS 22-05-2019, ECLI:NL:RVS:2019:1675, par. 9.1.
17 Zie p. 42 e.v. Zie in het bijzonder: ABRvS 22 mei 2019, ECLI:NL:RVS:2019:1675 (*PRIS*).

Het is daarnaast van belang op te merken dat ingevolge de **AERIUS** uitspraken van de ABRvS[18], waarbij een **toetsingskader voor algoritmische besluitvorming** werd geïntroduceerd door een recht op informatie en uitleg te ontwikkelen, toegang tot informatie over de werking van de algoritmen binnen het blockchainsysteem verzocht zou kunnen worden ter voorkoming van een ongelijkwaardige procespositie. Een gebrek aan inzicht in de gemaakte keuzes en de gebruikte gegevens en aannames kan volgens de ABRvS immers de inzichtelijkheid en controleerbaarheid van (deels) geautomatiseerde besluitvorming belemmeren.[19] Op basis van de AERIUS I uitspraak geldt volgende verplichting, namelijk dat:

> "gemaakte **keuzes** en de gebruikte **gegevens** en **aannames volledig, tijdig en uit eigen beweging openbaar** te **maken op een passende wijze** zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen".[20]

Hierbij moet op basis van de AERIUS II uitspraak een onderscheid gemaakt worden tussen maatwerk en standaard invoergegevens. **Standaard invoergegevens** hoeven alleen openbaar gemaakt te worden indien belanghebbenden daartoe verzoeken.[21] Hierbij valt bijvoorbeeld te denken aan het (rood) signaal algoritme dat partijen grond niet samengevoegd mogen worden, als dit algoritme dusdanig ontworpen en ingezet wordt dat het gaat om (deels) geautomatiseerde besluitvorming die onder het besluitbegrip van artikel 1:3 Awb valt. **Maatwerk-invoergegevens** moeten echter wel uit eigen beweging op papier of anderszins waarneembaar worden overgelegd. 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 maatwerk invoergegevens.

Vanuit de **invalshoek van de gebruiker** zal informatie die de gebruikers zelf invullen, gekwalificeerd worden als een document in de zin van de Wob gezien het vaste rechtspraak is dat elektronisch vastgelegde gegevens documenten zijn in de zin van de Wob. Deze informatie wordt immers elektronisch vastgelegd op het moment dat de gebruiker het invoert. Daarnaast zullen binnen het blockchainsysteem andere gegevens zoals de individuele transacties, pseudoniemen die de transacties aangaan, hashes of het grootboek, die het blockchainsysteem genereert doordat deze gegevens door de gebruiker zijn ingevoerd elektronisch worden vastgelegd ook

18 ABRvS 17 mei, ECLI:NL:RVS:2017:1259 en ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454.
19 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, par. 14.3.
20 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259, par. 14.4, eigen nadruk toegevoegd.
21 ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454, par. 23.5.

kwalificeren als een document in de zin van de Wob.[22] Bij de pilot grondstomen zullen bijvoorbeeld de ingevoerde gegevens over de samengevoegde grond, het grootboek waar alle transacties opstaan en de individuele transacties (zijnde het registreren van gegevens door pseudoniemen) gelden als documenten in de zin van de Wob.

Vanuit de **invalshoek van de overheid (RWS) die een publieke taak of publiek gezag uitoefent**, bestaan er gegevens over hoe RWS gebruikmaakt van het blockchainsysteem, bijvoorbeeld hoe vaak RWS de transacties inziet of wat ze verder doet met de gegenereerde informatie in het kader van de uitoefening van zijn publieke taak. Als deze gegevens worden vastgelegd door het blockchainsysteem, zullen deze elektronisch vastgelegde gegevens kwalificeren als een document in de zin van de Wob. Daarnaast bestaan er ook nog gegevens buiten het blockchainsysteem die schriftelijk of elektronisch vastgelegd kunnen worden, bijvoorbeeld documentatie over het ontwikkelde beleid rondom de pilot grondstromen of documentatie over de ontwikkeling van de techniek, aangezien dit kan bijdragen aan uitlegbaarheid, auditeerbaarheid, verantwoording en toetsbaarheid.[23]

De **informatieverzoeker** zal dus gegevens geïdentificeerd vanuit de bovenstaande drie invalshoeken op basis van een Wob-verzoek op kunnen vragen indien ook aan de andere eisen voor een Wob-verzoek is voldaan.

Berusten bij een bestuursorgaan
In tegenstelling tot gecentraliseerde technologieën werkt blockchain gedistribueerd, wat betekent dat documenten in de zin van de Wob zich tegelijkertijd op verschillende locaties bij verschillende nodes (participanten) bevinden. Deze eigenschap is niet uniek voor blockchaintechnologie en doet zich ook voor bij andere gedistribueerde systemen.

Voor het element "berusten bij" is bij de toepassing van de Wob de techniek van opslaan niet bepalend. Het gaat om documenten "van" het bestuursorgaan. Hierbij is niet alleen de fysieke aanwezigheid van het document van belang, maar ook het feit dat het document is bestemd voor het bestuursorgaan als zodanig.[24] In het geval van Whatsapp- en sms-berichten is hiervan bijvoorbeeld sprake indien de inhoud van het bericht een bestuurlijke aangelegenheid betreft. Daarnaast is de toepassing van de Wob niet afhankelijk van de concrete gegevensdrager.[25] Bij analoge toepassing van de rechtspraak van de ABRvS **maakt het dus niet uit of RWS blockchain inzet, wat het design van deze blockchain is, of dat de documenten in de zin van de Wob ook fysiek bij RWS berusten**.

---

22 Zie p. 26 e.v. voor een uitleg over deze gegevens.
23 Helwig 2020.
24 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, par 5 en *Kamerstukken II* 1986-1987, 19 859, nr. 3, blz. 21.
25 ABRvS 20 maart 2019, ECLI:NL:RVS:2019:899, r.o. 5.

Dit betekent echter niet dat alle documenten die in een blockchainsysteem staan ook onder RWS berusten puur omdat RWS toegang heeft tot het netwerk. Zo geldt bijvoorbeeld ook niet dat alle informatie die op het internet staat berust bij een bestuursorgaan louter omdat ambtenaren daartoe toegang hebben.[26] Dit is echter wel anders indien informatie van het internet gehaald wordt en gebruikt wordt door het bestuursorgaan.[27] Voor RWS impliceert dit dat de informatie die in het blockchainecosysteem staat waar zij deel vanuit maakt niet gelijk ook onder RWS berust. **Als RWS bijvoorbeeld opteert voor het gebruik van een (bestaande) publieke blockchain, zal niet alle informatie die te vinden is binnen het blockchainecosysteem bij RWS berusten. Gegevens die onlosmakelijk verbonden zijn met informatie over een bestuurlijke aangelegenheid vallen echter wél onder de Wob.** Dit geldt ook voor gegevens die zich bevinden in het grootboek van een publieke blockchain. Niet alle individuele transacties op een grootboek zullen sowieso te maken hebben met een bestuurlijke aangelegenheid van RWS, terwijl het grootboek an sich wel als dusdanig met een bestuurlijke aangelegenheid van RWS verbonden lijkt te kunnen zijn zodat het onder de Wob kan vallen, aangezien het grootboek een bewijs is van de geldigheid en betrouwbaarheid van documenten die *wel* bij RWS berusten of zou moeten berusten.

✓ *Archiefwet*

De Archiefwet is van toepassing op archiefbescheiden. Dit bescheid kan zowel ontvangen als opgemaakt worden door het bestuursorgaan en de vorm maakt hierbij niet uit. Hierdoor kunnen ook digitale data en informatie over onderliggende algoritmes kwalificeren als bescheiden onder de Archiefwet.[28] Het is wel van belang dat het archiefstuk bestemd is om onder het bestuursorgaan te berusten, wat volgens de Inspectie Overheidsinformatie en Erfgoed betekent dat het archiefstuk naar zijn aard gebonden moet zijn aan de werkprocessen van het bestuursorgaan.[29]

Op het **niveau van het systeem** kunnen algoritmen die van belang zijn voor de werking van het systeem kwalificeren als archiefbescheiden.

Helwig beargumenteert in haar essay dat het tot aanbeveling strekt om in ieder geval algoritmen die een rol spelen in de primaire werkprocessen een plaats te geven in het archief. Dit **vraagt van overheidsorganisaties dat een afweging gemaakt moet worden welke informatie gearchiveerd wordt zodat een reconstructie gemaakt kan worden**. Hierbij noemt zij het volgende voorbeeld om een onderscheid te maken tussen welke algoritmen wel en niet gearchiveerd moeten worden:

---

26 ABRvS 22 mei 2019, ECLI:NL:RVS:2019:1675, m.nt. H.S. ten Cate en C.A. Geleijnse, r.o. 4.

27 ABRvS 16 augustus 2006, ECLI:NL:RVS:2006:AY6317, AB 2006/337, m.nt. E.J. Daalder; Gst. 2007/29 m.nt. R. Kooper, JB 2006/289, m.nt. M. O-V), par 2.6.

28 Duurzaam Digitaal Databeheer bij de Rijksoverheid: een verkenning [2021], p. 16, en P. Helwig, 'Rekenen en rekenschap: algoritmes en de Archiefwet', TvT 2020, p. 4.

29 Inspectie Overheidsinformatie en Erfgoed: Archiefbescheiden, wat zijn dat?

> "Voor het algoritme dat de lift in een overheidskantoorgebouw efficiënt naar de juiste verdieping stuurt, geldt misschien een andere afweging dan voor een algoritme dat beslist of voorstelt een instelling of bedrijf nader te inspecteren, of dat individuele personen categoriseert."[30]

Het antwoord **wat gearchiveerd wordt, zal dus verschillen per proces en vooral mede afhangen van de gevolgen die intreden door de output van het proces**, zoals het samenvoegen van grond of een bodemonderzoek. Daarnaast zal ook de **complexiteit van het algoritme** een rol spelen bij wat mogelijk en wenselijk is om te archiveren. Wat complexiteit betreft, zijn smart contracts computerinstructies die simpele 'als x, dan y' regels (algoritmes) op geautomatiseerde wijze uitvoeren. Hierbij zullen de gemaakte keuzes in het algoritme in beginsel af te leiden zijn uit wet- of regelgeving of beleid en valt het normaal ook te achterhalen hoe de software werkt door de regels te bestuderen.[31] Opslag zou dus geen probleem mogen vormen.

Deze punten laten zich goed illustreren aan de hand van de pilot grondstromen en de pilot zoutlogistiek.

– De pilot grondstromen had in eerste instantie als doel het registreren van gegevens te verkennen. Later in de pilot werd de mogelijkheid geïdentificeerd om ook een (rood) signaal af te geven aan gebruikers, zowel aan ketenpartners als aan RWS, over de compatibiliteit van het samenvoegen van verschillende typen grond. In het concept werd de mogelijkheid verkend tot inzet van het algoritme dat een (rood) signaal geeft, wat invloed zou kunnen hebben op de werkprocessen van RWS en andere toezichthoudende en handhavende overheidsinstellingen. Bij een (rood) signaal als mogelijke output kan RWS bijvoorbeeld besluiten een bodemonderzoek uit te voeren. Het signaal zou een algoritme zijn dat volgens ons in ieder geval een plaats in het archief verdient, aangezien dit algoritme bepalend is voor het belangrijke oordeel of grond samengevoegd mag worden of niet. De gemaakte keuzes voor dit algoritme – wanneer het algoritme een (rood) signaal geeft – zullen af te leiden zijn uit het Besluit bodemkwaliteit waarin is vastgelegd welke grond wel of niet samengevoegd mag worden. Voor de archivering van andere algoritmen binnen het systeem zal het erop neerkomen wat de invloed is van deze algoritmen op de betrouwbaarheid van geregistreerde gegevens en de werkprocessen van toezichthoudende en handhavende overheidsinstellingen zoals RWS. Hierbij verdient het aanbeveling telkens de vraag te stellen welke informatie nodig is om een reconstructie te maken.
– Het doel van de pilot zoutlogistiek is het vastleggen van gegevens om daarmee de logistieke keten van strooizout betrouwbaar en efficiënt vast te leggen. Hiermee kunnen in de eerste plaats de hoofdaannemers (inclusief onderaannemers) en in de laatste plaats RWS als opdrachtgever de kwaliteit van het strooizout monitoren, waarbij de hoofdaannemer eindverantwoordelijk blijft voor de

30 Helwig 2019, p. 57.
31 Ibid.

kwaliteit ervan. Ook hier zal de keuze voor het archiveren van verschillende algoritmes binnen het systeem neerkomen op wat de rol is van deze algoritmen voor de werkprocessen van RWS en de mogelijkheid tot reconstructie daarvan. Dit is afhankelijk van het design dat een zoutconsortium van verschillende zoutpartijen zou kiezen als mogelijk blockchainsysteem. Als bijvoorbeeld besloten wordt om met een permissioned blockchain te werken, dan heeft dit invloed op hoe "de waarheid binnen het systeem" bereikt wordt omdat het consensusprotocol omschrijft wie transacties kan valideren en daarmee de waarheid vast kan leggen. Aangezien er commerciële belangen betrokken zijn bij de controle op de kwaliteit van het strooizout en de mogelijkheid op strategisch gedrag wordt vergroot bij de toegankelijkheid van meer informatie, zou het inderdaad aangeraden kunnen zijn om vast te leggen welke partijen in het blockchainsysteem bepaalde autorisaties hebben. Daarnaast kan ook gedacht worden aan het archiveren van de partijen die op verschillende momenten fungeerden als controlerende *oracles* voor de zoutkwaliteit en daarmee degenen waren die informatie over de kwaliteit van het zout uit de buitenwereld in het blockchainecosysteem brachten.

In het geval van RWS zullen op het niveau van het systeem dus niet alle algoritmen die deel uitmaken van het blockchainsysteem gearchiveerd hoeven te worden, maar het is wel te aan te raden de algoritmen te archiveren die een rol spelen in de primaire werkprocessen, zoals het algoritme dat een (rood) signaal geeft in de pilot grondstromen. Bij analoge toepassing hoeft het consensusmechanisme bijvoorbeeld niet gearchiveerd te worden als het op de primaire werkprocessen van RWS geen invloed heeft.[32]

Op het **niveau van de gebruiker** zijn er verschillende (input)gegevens die kunnen kwalificeren als archiefstuk. De gegevens die door gebruikers aangeleverd worden in het systeem worden door RWS ontvangen en spelen vervolgens een rol in de werkprocessen van RWS, onder meer in zijn rol als toezichthouder. Hierbij zullen in de praktijk waarschijnlijk niet de individuele ingevoerde gegevens als archiefstuk worden aangemerkt, maar eerder de set van gegevens zoals gebruikers die invoeren. De rol van deze gegevens laat zich goed illustreren aan de hand van twee voorbeelden:

– In de pilot grondstromen zouden gebruikers van de blockchainapplicatie na het inloggen in het systeem bij een scherm komen waar zij gegevens kunnen invullen, bijvoorbeeld over de grond die ze van plan zijn samen te voegen, het vaknummer, het aantal ton en een aantal PDF-documenten. Deze set van ingevoerde gegevens worden door toezichthoudende en handhavende overheidsinstellingen als RWS ontvangen. Deze toezichthoudende en handhavende instellingen kunnen

32 Hierbij dient RWS wel duidelijk voor ogen te hebben wat in hun werking als 'primair werkproces' te categoriseren valt.

vervolgens deze gegevens gebruiken voor hun toezichthoudende taak, bijvoorbeeld door na te gaan of de grond correct samengevoegd is en of de geüploade PDF-documenten een voldoende betrouwbaar bewijs vormen.
– In de pilot zoutstromen wordt bij een aanbesteding het zout door een (lokaal) lab gecontroleerd. Het lokaal lab registreert de batch en het kwaliteitsrapport dat het heeft opgemaakt na zijn onderzoek. Het was de bedoeling dat dit zou worden vastgelegd in een blockchainapplicatie van het zoutconsortium, aangezien de ketenpartners (opdrachtnemers) verantwoordelijk zijn voor de kwaliteit van het zout. De registratie van de batch en het kwaliteitsrapport worden door RWS ontvangen als een geheel van gegevens. Deze gegevens gebruikt RWS vervolgens om te controleren en te besluiten of de batch aanbesteed wordt en of de kwaliteit van de levering gegarandeerd is.

Met betrekking tot het grootboek en de transacties die in het grootboek staan kan RWS zelf beslissen hoe hij informatie beheert en hoe hij dit indeelt als informatieobjecten. Meestal gebeurt dit aan de hand van hoe de informatie beheerd en gebruikt wordt.[33] Dit zal ook zo zijn op het moment dat RWS zelf besluit blockchain in te zetten of besluit deel te nemen aan andere blockchainapplicaties. RWS zou er bijvoorbeeld voor kunnen kiezen om het gehele grootboek als informatieobject aan te merken of om de individuele blokken of transacties als informatieobjecten aan te merken.[34]

Volgens de inspectie Overheidsinformatie en Erfgoedkunnen kunnen databases aangemerkt worden als archiefbescheiden.[35] **Gezien het grootboek bij een blockchainapplicatie te vergelijken is met een – weliswaar in dit geval gedistribueerde – database lijkt het grootboek ook te kwalificeren als een archiefstuk in de zin van de Archiefwet. Het grootboek wordt echter continu geüpdatet door de toevoeging van nieuwe transacties en blokken, wat de vraag doet rijzen wat precies de "grenzen" van het archiefstuk zijn op het moment dat het archiefstuk overgebracht moet worden.** Blockchain heeft zowel elementen van een *continuum model* als een *lifecycle model* voor het managen van documenten. Gezien geen van deze beiden modellen goed de realiteit van blockchain weergeeft, vraagt dit mogelijk om een herijking van de archiveringspraktijk.[36]

De beantwoording van de vraag wat de "grenzen" van het archiefstuk zijn op het moment dat het archiefstuk overgebracht moet worden, is afhankelijk van hoe RWS besluit het grootboek in te delen als informatieobject. Indien RWS het gehele grootboek als informatieobject aanmerkt, kunnen onduidelijkheden ontstaan over hoe

33 Zie p. 46.
34 Individuele records kunnen gelden als informatieobjecten, maar geaggregeerde records kunnen ook één record vormen. Zie: Lemieux, Hofmann, Batista, & Joo 2019, p. 30.
35 Inspectie Overheidsinformatie en Erfgoed: Archiefbescheiden, wat zijn dat?
36 Zie Lemieux, Hofmann, Batista, & Joo 2019, hoofdstuk 3.

het oude deel van het grootboek overgebracht moet worden zonder dat het nieuwe deel van het grootboek (het deel dat jonger is dan 20 jaar) ook mee overgebracht wordt, tenzij RWS continu aparte kopieën bewaart van het grootboek, zodat dit onderscheid gemaakt kan blijven worden. Dit zou van RWS echter veel opslagcapaciteit vergen als veel informatie op het grootboek staat.

Daarnaast kunnen **individuele blokken** ook als informatieobject aangemerkt worden. In dit geval zijn de "grenzen" van het archiefbescheid duidelijker. Het is bij archivering van de aparte blokken echter wel van belang dat er een link gemaakt wordt met de transacties geregistreerd in de blokken. Een blok kan bijvoorbeeld de on-chain geregistreerde transactie bevatten die de (mogelijk off-chain opgeslagen) ingevoerde gegevens door een partij in de pilot zoutstromen vastlegt. Zonder deze link kan de geldigheid van de ingevoerde gegevens worden betwist en is de geregistreerde transactie in het blok een set gegevens die niet veel meer zegt dan dat een transactie heeft plaatsgevonden. Zonder deze link vermindert dus zowel de betrouwbaarheid van de transactie in het blok als de ingevoerde gegevens door de gebruiker, wat een betrouwbare reconstructie kan belemmeren. Verder kunnen ook de **individuele transacties** als informatieobjecten aangemerkt worden, maar als er veel transacties per tijdseenheid uitgevoerd worden, kan dit mogelijk tot hoge inspanningen leiden bij het overbrengen.

De gegevens aangaande de gebruikers zullen op zichzelf staand niet kwalificeren als individueel archiefstuk omdat deze niet een apart bescheid zijn maar onlosmakelijk deel uitmaken van de transacties op het grootboek.

Vanuit de **invalshoek van RWS als overheid die een publieke taak of publiek gezag uitoefent**, zijn verschillende informatieobjecten denkbaar, bijvoorbeeld documentatie over het beleid inzake de inzet van blockchain in de werkprocessen van RWS, documentatie over testprocessen van de pilots of Wob-verzoeken.

B. Consequenties van het wettelijk kader voor gemaakte keuzes in architectuur

Deze paragraaf behandelt de consequenties van het wettelijk kader inzake toegang tot overheidsinformatie op de keuzemogelijkheden die RWS heeft betreffende het blockchaindesign. Hierbij wordt telkens eerst de Wob en daarna de Archiefwet besproken. Er wordt ingegaan op de volgende drie designkeuzes: publieke, private of hybride blockchain, permissioned of permissionless blockchain, en on-chain en off-chain registratie van gegevens. Na bespreking van deze designkeuzes, vindt er nog een korte bespreking plaats van de rol die smart contracts en oracles spelen binnen een blockchainapplicatie. Tenslotte wordt een conclusie getrokken over het

maken van keuzes betreffende het meest geschikte blockchaindesign in het licht van de geanalyseerde wet- en regelgeving.[37]

1° Publieke of private blockchain

✓ *Wob*

De Wob heeft een wezenlijke invloed op de keuze voor een publieke, private of hybride blockchain en op de keuze voor een permissioned of een permissionless blockchain. RWS zou kunnen overwegen blockchain in te zetten om informatie uit het blockchainsysteem op actieve of passieve wijze openbaar te maken. De impact van de Wob op blockchain designkeuzes zal hierna worden bekeken op basis van een behandeling van de toegang tot en de rechten van actoren binnen het netwerk.

Actieve openbaarmaking

Allereerst is van belang te herhalen dat Wob-verzoeken niet ingediend kunnen worden voor informatie die al openbaar is[38] en de Wob niet van toepassing is op openbare registers die burgers zelf kunnen raadplegen.[39] In een uitspraak van 20 oktober 2010 van de ABRvS ging het bijvoorbeeld om het verzoeken van informatie uit het KvK en informatie uit het BIG-register. De ABRvS oordeelde dat informatie hier al openbaar was omdat de verzoeker de informatie zelf kon opvragen in het openbare handelsregister. In deze zaak ging het ook om modellen die bij het inschrijven voor een aanbesteding toegezonden werden aan de aanvragers en die de aanvragers vervolgens moesten invullen. De openbaarheid van deze modellen werd betwist omdat deze modellen niet op internet stonden. De ABRvS oordeelde dat deze modellen al openbaar waren, aangezien eenieder die daarom verzocht de modellen toegestuurd kreeg.[40] Als een bestuursorgaan een openbaarmakingsverzoek ontvangt dat betrekking heeft op informatie die een informatieverzoeker zelf kan raadplegen, kan worden volstaan met een brief waarin aan de verzoeker wordt meegedeeld dat de Wob niet op zijn verzoek van toepassing is.

Analoog aan deze uitspraak zal informatie die in een **publieke blockchain** staat **openbaar** zijn **in de zin van de Wob, omdat in principe eenieder deze informatie op kan vragen in het publiek raadpleegbare blockchainregister**. Een publieke

37 Bij de analyse wordt de mogelijke aanwezigheid van uitzonderingsgronden onder de Wob en de Archiefwet buiten beschouwing gelaten.

38 ABRvS 20 oktober 2010, ECLI:NL:RVS:2010:BO1165, r.o. 2.6.2 en ABRvS 12 juli 2017, ECLI:NL:RVS:2017:1874, r.o. 3.1.

39 Alle stukken die naar hun aard al openbaar zijn vallen buiten de reikwijdte van de Wob, ongeacht of het informatie betreft die in registers staat. Zie ABRvS 18 juli 2007, ECLI:NL:RVS: 2007:BA9793, r.o. 2.4. De feitelijke invulling van openbaarheid doet daar niet aan af: ook informatie die bijvoorbeeld maar tijdelijk openbaar is, kan worden aangemerkt als reeds openbaar en behoeft dus niet meer openbaar gemaakt te worden. Zie: ABRvS 12 juli 2017, ECLI:NL:RVS:2017:1874, r.o. 3.1. Zie ook: ABRvS 9 mei 2018, ECLI:NL:RVS:2018:1540, r.o. 2, ABRvS 16 mei 2018, ECLI:NL:RVS:2018:1636.

40 ECLI:NL:RVS:2010:BO1165, r.o. 2.6-2.6.3.

permissionless blockchain is in die zin te vergelijken met het internet, aangezien iedereen toegang heeft en iedereen leesrechten heeft. Een publieke blockchain zou in dit geval te vergelijken zijn met een register zoals het KvK waarbinnen gebruikers zelf op zoek kunnen gaan naar informatie, mits dit technisch zo ingeregeld wordt in de user interface. Gebruikers moeten wel daadwerkelijk zelf de informatie op *kunnen* zoeken en de **user interface mag dus niet onnodig technisch gecompliceerd zijn**. Indien RWS gegevens in het blockchain ecosysteem registreert die ertoe strekken eenieder te informeren, zullen dit ook openbare documenten zijn in de zin van de Wob.[41] In het geval van een private blockchain zou RWS kunnen beslissen het beleid te voeren eenieder die daartoe een verzoek indient de informatie waartoe toegang verzocht wordt te laten bekijken. Deze informatie zal openbare informatie zijn als dit informatie is die naar aard voor eenieder bedoeld is en als iedereen leesrechten krijgt die daartoe verzoekt. RWS **kan dus bij analoge toepassing van deze uitspraken een publieke blockchain – maar ook een private blockchain indien iedereen die om toegang verzoekt het grootboek kan bekijken – inzetten voor actieve openbaarmaking**. Indien een openbaarmakingsverzoek wordt ingediend naar informatie die al te vinden is via het blockchainsysteem, dan heeft RWS nog de verantwoordelijkheid om het verzoek te beantwoorden met een brief waarin vermeld wordt dat de Wob niet van toepassing is. Verder is het belangrijk hierbij op te merken dat informatie die eenmaal openbaar is, openbaar blijft.[42] De informatie die openbaar gemaakt is middels een publieke blockchain mag dus niet meer door RWS bewerkt of aangepast worden.

RWS heeft ruime beoordelingsruimte met betrekking tot welke informatie zij actief besluit openbaar te maken, wat wel zal veranderen met de inwerkingtreding van de Woo.[43] Daarbij geldt niet dat het wenselijk is dat RWS zomaar alle informatie openbaar maakt via de blockchain. De MvT bij de Wob deelt het volgende mee over informatieverstrekking, namelijk dat:

> "De informatieverstrekking uit eigen beweging zal zo gericht mogelijk moeten geschieden. Ongerichte informatieverstrekking kan namelijk de waarde van de voorlichting als zodanig schaden. Wanneer burgers aangeboden informatie als overbodig ervaren, kan dat een negatieve invloed hebben op hun oordeel over het nut van voorlichting in het algemeen. Dit doet zich ook voor indien de informatieverstrekking leidt tot verwarring bij hen tot wie de voorlichting is gericht. Het is daarom van groot belang dat bij de voorlichting met nadruk wordt gewezen op de betekenis en de status van de informatie in het kader van de bestuurlijke aangelegenheid of de daarop betrekking hebbende bestuursvoering."[44]

41 ABRvS 12 juli 2017, ECLI:NL:RVS:2017:1874, r.o. 3.1.

42 Zie ABRvS, 20 april 2000, ECLI:NL:RVS:2000:AA5845, r.o. 2.7 en Rb. Arnhem, 19 mei 2011, ECLI:NL:RBARN:2011:BQ7669, r.o. 3.

43 Zie p. 44.

44 *Kamerstukken II* 1986-1987, 19 859, nr. 3, p. 30-31 (MvT). Eigen nadruk toegevoegd.

Hierbij geldt wel dat de informatie in een voor de informatieverzoeker begrijpelijke vorm moet worden verschaft.[45] **Voldoende aandacht voor de toegankelijkheid tot het (blockchain)systeem en dus het design van de interface, evenals leesbaarheid en begrijpbaarheid van de informatie voor de informatieverzoeker zijn van wezenlijk belang. Het louter toegang bieden tot de achterliggende data of code is onvoldoende.**[46] De Wob vereist geen volledige transparantie in de zin dat *alle* informatie actief openbaar gemaakt wordt. Sterker nog, dit zou in het licht van transparantie – evenals in het licht van het gegevensbescherming- en mededingingsrecht, averechts kunnen werken. Om informatie effectief actief openbaar te maken, is het dus belangrijk hoe de informatie gepresenteerd wordt aan de verzoeker. Hierbij speelt de user interface een grote rol, bijvoorbeeld door het bieden van handleidingen over het zoeken van informatie, makkelijk hanteerbare zoekfuncties en gebruiksvriendelijke designs. Verder kan de informatiebehoefte per verzoeker verschillen. Zo is het bijvoorbeeld denkbaar dat een journalist of onderzoeker op zoek is naar andere informatie dan een bedrijf of een burger. Het kan afhangen van de betrokkene of informatie bijvoorbeeld wel of niet als "overbodig" of "onbegrijpelijk" wordt ervaren. Daarbij is het mogelijk dat bijvoorbeeld per pilot de typen informatieverzoekers verschillen. Bij de pilot zoutlogistiek kan bijvoorbeeld verwacht worden dat voornamelijk bedrijven, zoals zout-, logistieke en transportbedrijven, informatieverzoekers zullen zijn, terwijl het bij de pilot grondstromen te verwachten is dat ook burgers en andere (toezichthoudende en handhavende) overheden geïnteresseerd zullen zijn in de informatie die in het blockchainsysteem staat. Indien RWS blockchain besluit in te zetten om aan informatie op actieve wijze openbaar te maken, dan is het raadzaam om eerst empirisch onderzoek uit te voeren naar wat als begrijpelijk wordt beschouwd voor de verschillende doelgroepen die gebruik gaan maken van het systeem. Hierbij moet in het achterhoofd worden gehouden dat de doelgroepen kunnen veranderen in de tijd, net als wat "begrijpelijk" precies inhoudt.[47] Beslissingen hieromtrent kunnen ook verschillen per casus. Daarnaast is het technisch inrichten van de **mogelijkheid om het design aan te passen in het licht van toekomstige wijzigingen in wet- en regelgeving en beleid** tevens een uitermate belangrijk aandachtspunt. Denk bijvoorbeeld aan de inwerkingtreding van de Woo.

De "openbaarheid" van informatie verandert zodra er toegang tot de informatie verleend moet worden door RWS door de keuze voor een private blockchain. Bij een **private blockchain** geldt dat alleen een bepaalde groep toegang krijgt tot het netwerk. Bij een permissioned blockchain geldt daarenboven dat alleen een bepaalde groep participatierechten krijgt binnen het netwerk. **Als RWS de keuze maakt voor een publieke blockchain of private blockchain en daarover vervolgens het beleid voert dat niet eenieder toegang krijgt om het grootboek te bekijken die**

45 Zie ook Nationale Ombudsman (2021).
46 Van Heukelom 2018.
47 Bijvoorbeeld naarmate de inzet van blockchaintechnologie gangbaarder en daarmee "begrijpelijker" wordt.

daarom verzoekt, dan is de informatie in het netwerk geen openbare informatie. De informatie voor personen buiten het netwerk is immers niet toegankelijk. In dat geval moet een informatieverzoeker een Wob-verzoek indienen om tot deze informatie toegang te krijgen.

Daarnaast bestaat nog het scenario waarbij RWS een private blockchain inzet en beoordelingsruimte heeft met betrekking tot het bieden van toegang aan informatieverzoekers om het grootboek te bekijken. In dit scenario kan eenieder informatie opzoeken onder de voorwaarde dat toegang door RWS verschaft wordt. RWS is hier als het ware een gatekeeper met betrekking tot informatie die op de blockchain staat. In het geval van een gebonden bevoegdheid waarbij RWS geen beoordelingsruimte heeft om een verzoek tot informatie te honoreren, *moet* RWS toegang of leesrechten verlenen tot eenieder. In dit laatste geval blijft er een afhankelijkheid bestaan tussen de RWS en de verzoeker. Voordat toegang verschaft wordt, wordt namelijk eerst nog een beoordeling gemaakt. Een gelijkaardige situatie deed zich voor in de al eerder genoemde Squit uitspraak van de ABRvS van 11 september 2019. Zo oordeelde de ABRvS dat informatie die te raadplegen was via het Squit systeem niet openbaar was in de zin van de Wob, omdat er eerst nog een beoordeling moest plaatsvinden door een ambtenaar in verband met de bescherming van persoonsgegevens.[48] In het geval van discretionaire ruimte met betrekking tot het verlenen van toegang tot informatie is bijgevolg geen sprake van openbaarheid in de zin van de Wob. In het geval dat RWS beslist te allen tijde toegang te verlenen op een verzoek, geldt de informatie als openbare informatie onder de Wob. In dit opzicht is het juridische aldus meer doorslaggevend dan het blockchaindesign. Volgens Balvert kan dit in de toekomst nog veranderen in het licht van technologische ontwikkelingen, aangezien er ruimte voor debat is over wat "openbaarheid" precies inhoudt en het kan betwist worden dat openbaarheid sowieso ook toegankelijkheid impliceert.[49]

In het geval van een **hybride** blockchain zullen de bovengenoemde analyses inzake publiek en private blockchains gelden voor de respectievelijke publieke en private onderdelen van het netwerk.

Passieve openbaarmaking
Artikel 7 lid 1 Wob regelt dat bij passieve openbaarmaking het bestuursorgaan de informatie verstrekt met betrekking tot de documenten die de verlangde informatie bevatten door:

48 Zie de uitspraak ABRvS 11 september 2019 ECLI:RVS:2019:3100, par 5.1.
49 Zie: Balvert 2020, p. 66.

"a. kopie ervan te geven of de letterlijke inhoud ervan in andere vorm te verstrekken,
b. kennisneming van de inhoud toe te staan,
c. een uittreksel of een samenvatting van de inhoud te geven, of
d. inlichtingen daaruit te verschaffen."

De informatieverstrekking moet gebeuren in de vorm die de informatieverzoeker verzoekt, tenzij dit niet redelijkerwijs gevergd kan worden of tenzij de informatie al in een gemakkelijk toegankelijke vorm beschikbaar is voor het publiek.[50] Hieronder wordt de pilot zoutlogistiek als voorbeeld gehanteerd om een concrete invulling van deze wijzen van informatieverstrekking te illustreren. De voorbeelden benoemd in onderstaande tabel zijn dus hypothetisch en louter bedoeld om de invalshoeken en typen gegevens te verduidelijken. De opsomming is derhalve niet limitatief bedoeld; er zijn meerdere voorbeelden denkbaar.

Figuur 12 Wijze van informatieverstrekking

Wijze van informatieverstrekking	Voorbeeld
Kopie of de letterlijke inhoud ervan in andere vorm	RWS verstrekt een (digitale) kopie van bijvoorbeeld de certificaten met betrekking tot de kwaliteit van het zout die door partijen in het blockchainsysteem zijn ingevoerd.
Kennisneming van de inhoud toestaan	RWS geeft toegang aan de informatieverzoeker om kennis nemen van de informatie over de zoutketen op de blockchain en helpt de verzoeker met informatie opzoeken in het blockchainsysteem.[51]
Een uittreksel of samenvatting van de inhoud geven	RWS geeft een samenvatting van de transacties on-chain en de geregistreerde gegevens (mogelijk off-chain) die plaats hebben gevonden in de logistieke keten bij de aanbesteding van zout.
Inlichtingen daaruit verschaffen	RWS geeft uitleg over het consensusalgoritme dat in de pilot wordt ingezet.

Ingevolge artikel 7 lid 2 Wob kan informatieverstrekking ook op een andere wijze plaatsvinden dan op de manieren in artikel 7 lid 1 Wob opgesomd. Dit is relevant indien het verstrekken van de informatie op de verzochte wijze niet redelijkerwijs van RWS gevergd kan worden (artikel 7 lid 2 sub a Wob) of indien de informatie al in een toegankelijke vorm beschikbaar is voor het publiek (artikel 7 lid 2 sub b Wob). Het verstrekken van informatie in een andere vorm dan dat de informatieverzoeker

50 Art. 7 lid 2 sub a en b Wob.
51 ABRvS 23 maart 2011, m.nt. P.J. Stolk.

wenst, is aanvaardbaar zolang dezelfde informatie wordt verstrekt als bij verstrekking in de gewenste vorm.[52]

De mogelijke invulling van een alternatieve wijze indien op basis van artikel 7 lid 2 sub a Wob de verzochte wijze niet redelijkerwijs verwacht kan worden van RWS bij de inzet van blockchain, is naar de huidige stand van zaken in de pilots nog lastig in te schatten gezien de variabelen die nog openstaan in het blockchaindesign. Een voorbeeld van wat in ieder geval *niet* redelijkerwijs van een bestuursorgaan gevergd mag worden, deed zich bijvoorbeeld voor in de uitspraak van de ABRvS op 1 juli 2009 over het verstrekken van fotokopieën.[53] Hier oordeelde de ABRvS dat een extra tijdsinspanning van 29 uur om de informatie in de verzochte vorm te verstrekken niet redelijk was en dat daarom met een vorm anders dan de verzoeker verzocht kon worden volstaan.

Met betrekking tot de situatie waarin de informatie al in een toegankelijke vorm beschikbaar is voor het publiek (artikel 7 lid 2 sub b) noemt de MvT van de Wob het volgende:

> "Bestuursorganen mogen uitgaan van datgene dat redelijkerwijs van een aanvrager verlangd kan worden. Zo geldt dat, indien de betreffende informatie op een andere reguliere wijze voor het publiek beschikbaar is gesteld (te denken valt aan terinzagelegging bij het bestuursorgaan of aan beschikbaarstelling via elektronische weg zoals het Internet), bestuursorganen in beginsel mogen aannemen dat deze vorm van beschikbaarheid afdoende is in het licht van artikel 7, tweede lid, onderdeel b. Dat komt anders te liggen als de verzoeker aangeeft dat voor hem de informatie niet gemakkelijk toegankelijk is."[54]

Hierbij is het telkens aan de verzoeker om aan te geven of de informatie gemakkelijk toegankelijk is. Er rust geen verplichting op het bestuursorgaan om dit na te gaan.[55] Het blijft evenwel onduidelijk wat geldt als "regulier" en of met name beschikbaarstelling voor het publiek middels blockchain als "regulier" kan worden beschouwd, aangezien blockchain nog een relatief jonge en volop in ontwikkeling zijnde technologie is. Daarnaast wordt beschikbaarstelling middels de "reguliere" weg beïnvloed door de keuzes die RWS zou maken in het blockchaindesign, bijvoorbeeld of de blockchainecosystemen in de pilots te raadplegen zijn via de website van RWS, of dat gebruikers voor toegang tot de informatie nog software moeten downloaden. In ieder geval zal de verantwoordelijkheid bij de verzoeker blijven liggen om aan te

52 ABRvS 11 februari 2009, AB 2009/148, m.nt. P.J. Stolk. Informatie kan alleen weggelaten worden als er sprake is van een weigeringsgrond of een beperking, zie: ABRvS 23 september 2015, AB 2015/409 (m.nt. P.J. Stolk); Gst. 2015, 126 (m.nt. C.N. van der Sluis).

53 ABRvS 01-07-2009, ECLI:NL:RVS:2009:BJ1122, m.nt. P.J. Stolk. Eigen nadruk toegevoegd.

54 MvT Wob, p. 9-10.

55 Ibid.

geven dat de informatie niet gemakkelijk toegankelijk. RWS heeft geen juridische verplichting om dit zelf na te gaan.

✓ *Archiefwet*
De Archiefwet heeft in beginsel geen wezenlijke consequenties voor de keuze tussen een publieke of private blockchain.

2° Permissioned of permissionless

✓ *Wob*
De Wob heeft in beginsel geen wezenlijke consequenties voor de keuze tussen een permissioned of permissionless blockchain, een keuze die te maken heeft met het verlenen van participatierechten in het netwerk. Het moet wel in herinnering worden gebracht dat publieke blockchains doorgaans permissionless zijn en private blockchains doorgaans permissioned.

✓ *Archiefwet*
Conceptueel vertrekt de Archiefwet en -regelgeving van het principe: één waarheid op één plek, terwijl blockchaintechnologie uitgaat van een verspreide, gedistribueerde opslag op verschillende locaties waarbij de betrouwbaarheid van data en transacties in beginsel wordt geverifieerd en gegarandeerd door (een meerderheid van) het netwerk en niet door een *trusted third party*. Opslag via blockchain kan bijgevolg aanleiding geven tot spanning met het 'één waarheid op één plek'-principe. Anderzijds is het net een van de hoofddoelstellingen van blockchain om de betrouwbaarheid en onwijzigbaarheid van geregistreerde data en transacties te garanderen.

Bij een permissioned blockchain wordt opnieuw aan één of meerdere *trusted third parties* een rol gegeven om te bepalen wie toegang heeft om te participeren in het blockchainnetwerk en te bepalen wie wat precies mag doen in het netwerk. **De keuze voor een permissioned blockchain lijkt zich op het eerste gezicht dus beter te verhouden tot de rol van RWS als archiefvormend orgaan met inbegrip van de bijhorende verantwoordelijkheden dan een permissionless blockchain.** Het is wel van belang dat de rol en verantwoordelijkheden van RWS vooraf in de designfase duidelijk worden vastgelegd en ingericht.

In het geval van een permissionless blockchain is er geen *trusted third party* die participatierechten in de blockchain toekent of weigert. RWS kan dan ook moeilijker zijn verantwoordelijkheid als archiefvormend orgaan uitvoeren, omdat RWS slechts één van vele participerende actoren is in het netwerk. Bij de mogelijke inzet van een permissionless blockchain blijven de verantwoordelijkheden van RWS onder de Archiefwet bestaan. Naast de archiefbescheiden die bij RWS bewaard moeten worden, dient dus in dat geval ook de gehele blockchainwerking door RWS gearchiveerd te worden als audit-trail, zodat duidelijk blijft wie wat wanneer heeft besloten.

3° *On-chain vs. off-chain gegevensopslag*

RWS heeft niet alleen keuzes te maken met betrekking tot het type en de hoeveelheid gegevens, maar ook de plaats waar het de gegevens opslaat.[56] RWS kan ervoor kiezen om de gegevens on-chain of off-chain te registreren. Zodra gegevens on-chain geregistreerd zijn, kunnen deze door het onveranderlijke karakter van blockchain in beginsel niet meer worden verwijderd. Er dient nog vermeld te worden dat er tevens voor zou kunnen worden geopteerd om een gedistribueerde on-chain opslag uiteindelijk ook bijkomend centraal op te slaan, wat sowieso dient te gebeuren op het moment van archivering.

Allereest speelt bij **on-chain** registratie de vraag hoe archiefbescheiden vernietigd kunnen worden zodra de bewaartermijn verstreken is gezien het onveranderlijke karakter van blockchain. Vernietiging impliceert ook dat digitale kopieën of back-ups van archiefbescheiden moeten worden vernietigd.[57] Een tweede vraag is dus hoe vernietiging plaats kan vinden bij on-chain registratie van gegevens bij de inzet van blockchain gelet op het gedistribueerde karakter van de gegevensopslag op verschillende locaties.

Om te beginnen kan RWS zelf bepalen middels de selectielijsten welke archiefbescheiden wel of niet vernietigd dienen te worden na het verstrijken van de bewaartermijn. Daarnaast heeft RWS de keuze om naast de transactiegegevens (hash, pseudoniem, tijdstip van transactie etc.) nog andere informatieobjecten on-chain op te slaan, zoals PDF-bestanden die de gebruikers moeten uploaden bij de pilot zoutlogistiek of de ingevoerde gegevens bij de pilot grondstromen. Er bestaan ook verschillende vormen van vernietiging, waarbij de gepaste vorm van vernietiging bepaald wordt door het doel dat de vernietiging dient.[58] Zo bestaan er verschillende gradaties van digitaal vernietigen[59] en verschillende alternatieven voor digitaal vernietigen.[60] Hierbij kan gedacht worden aan administratieve vernietiging, waarbij de verwijzingen naar het te vernietigen informatieobject verwijderd worden. Een alternatief voor vernietigen is bijvoorbeeld het verbreken van koppelingen waarbij de verwijzingen naar informatieobjecten verwijderd worden en de informatieobjecten toegankelijkheid, context en informatiewaarde verliezen. De informatieobjecten zelf blijven echter nog wel bestaan. Een ander alternatief is het beëindigen van het beheer.[61] Voor de eenmaal on-chain geregistreerde informatie blijft echter telkens gelden dat dit niet verwijderd kan worden door middel van overschrijving of het

56 Lemieux, Hofman, Batista & Joo 2019, p. 22.
57 Nationaal Archief: Wat is digitaal vernietigen?
58 Nationaal Archief: Wat is digitaal vernietigen?
59 Nationaal Archief: Wat is digitaal vernietigen?
60 Nationaal Archief: Wat is digitaal vernietigen?
61 Nationaal Archief: Wat is digitaal vernietigen?

verbreken van koppelingen vanwege het design van een blockchainsysteem, tenzij een meerderheid van het netwerk instemt met het handelen van RWS.

Verder kan RWS de keuze maken om de blockchain te gebruiken ter verificatie van geregistreerde gegevens en de rest van de informatieobjecten **off-chain** bewaren. Voor de informatieobjecten die off-chain bewaard worden, gelden de "reguliere" regels van vernietiging bij digitale bestanden. De on-chain gegevens die nog resteren zijn de gegevens die geregistreerd zijn bij de transactie, bijvoorbeeld de hash van de transactie, het pseudoniem en andere metadata. Deze set van gegevens kan echter ook op zichzelf kwalificeren als een informatieobject, gezien het "een op zichzelf staand geheel van gegevens met een eigen identiteit"[62] betreft. Bij deze keuzemogelijkheid kan vernietiging van de off-chain geregistreerde gegevens plaatsvinden door deze bijvoorbeeld administratief te verwijderen en de link met de transactie on-chain te verbreken. Dit neemt echter niet weg dat de **transactie on-chain *niet* vernietigd wordt. RWS doet er in dit scenario dus verstandig aan om de on-chain transacties op te nemen in de selectielijst waarin hij besluit deze informatie niet te vernietigen.**

4° Uitzonderingsgronden: bedrijfs- en fabricagegegevens en persoonsgegevens

Een type van ondoorzichtigheid in algoritmische systemen is bewuste afwezigheid van transparantie, waarbij informatie verborgen blijft voor commerciële redenen.[63] Als er sprake is van vertrouwelijk aan de overheid meegedeelde bedrijfs- en fabricagegegevens in de zin van de Wob, dan is dit een absolute uitzonderingsgrond op basis van artikel 10 lid 1 Wob. Dit betekent dat een verzoek tot openbaarmaking moet worden geweigerd. Hiervan kan bijvoorbeeld sprake zijn als RWS met een private partij in zee gaat voor het ontwikkelen van het blockchainsysteem. Idealiter is contractueel met de private partij geregeld wat wel of niet openbaar gemaakt kan worden en is dit dus ook *by design* geregeld, alvorens een Wob-verzoek ingediend wordt door een informatieverzoeker en is deze vraag eventueel niet langer aan de orde, bijvoorbeeld bij open source contracting.

Er is sprake van bedrijfs- of fabricagegegevens:

> "indien en voor zover uit die gegevens wetenswaardigheden kunnen worden afgelezen of afgeleid met betrekking tot de technische bedrijfsvoering of het productieproces dan wel met betrekking tot de afzet van de producten of de kring van afnemers en leveranciers. Ook gegevens die uitsluitend de financiële bedrijfsvoering betreffen, kunnen onder omstandigheden als bedrijfsgegevens worden aangemerkt".[64]

62 Informatieobject | Nationaal Archief

63 Dit wordt ook wel '*intentional opacity*' genoemd, zie: Cobbe, Sengh Ah Lee & Singh 2021; Danaher 2016; Burell 2016.

64 Zie onder andere ABRvS 29 april 2008, ECLI:NL:RVS:2008:BD0771, par. 2.6.

Indien er sprake is van bedrijfs- of fabricagegegevens, dient de absolute uitzonderingsgrond van artikel 10 lid 1 aanhef en onder c Wob restrictief te worden uitgelegd. Een voorbeeld van een succesvol beroep op deze uitzonderingsgrond biedt inzicht in de uitleg hiervan. In de uitspraak van de ABRvS van 8 februari 2017[65] werd deze uitzonderingsgrond ingeroepen bij handleidingen waarin bedrijfs- en fabricagegegevens zouden staan. De ABRvS was het eens met de minister dat de uitzonderingsgrond gold en er delen van de handleiding niet openbaar gemaakt konden worden omdat er concurrentiegevoelige informatie in stond van de producenten van meetsystemen. Zo stond in de handleidingen het volgende beschreven:

- In detail hoe de systemen werken en wat de mogelijkheden en beperkingen van de systemen zijn.
- Hoe verschillende onderdelen van het systeem beveiligd zijn.
- Schermafbeeldingen van het programma waarmee de gegevens worden verwerkt.

Daarnaast waren de gegevens vertrouwelijk meegedeeld en de producten slechts voor een beperkte groep bestemd.[66] Algemene gegevens kunnen daarnaast ook onder de uitzonderingsgrond vallen "*Wanneer de bedrijfs- en fabricagegegevens zodanig zijn verweven met andere, meer algemene informatie dat het niet mogelijk is die vertrouwelijke bedrijfsgegevens te anonimiseren of weg te lakken, staat de Afdeling toe dat ook de algemene gegevens niet worden verstrekt*".[67]

Bij analoge toepassing van deze uitspraak zal de uitzonderingsgrond waarschijnlijk opgaan als de volgende informatie aan RWS vertrouwelijk is meegedeeld:

- Bedrijfs- of fabricage gegevens die door partijen zijn ingevoerd in het blockchainsysteem. Voor de bedrijven die dit invullen, is dit mogelijk concurrentiegevoelige informatie. Zo kan bijvoorbeeld in de pilot zoutlogistiek de ingevulde informatie mogelijk iets zeggen over de prijs, afzet of het productieproces. Of er uiteindelijk sprake is van concurrentiegevoelige informatie blijft natuurlijk uiteindelijk afhankelijk van de informatie die RWS zou besluiten op te vragen bij partijen.
- De hard- en software van het blockchainsysteem, omdat dit iets kan zeggen over het "productieproces" van de leverancier van het blockchainsysteem. Niet alle algoritmes die deel uitmaken van het gehele systeem zullen hier echter onder vallen.
- Gegevens die algemeen van aard zijn, maar onlosmakelijk verweven zijn met informatie die is toevertrouwd aan RWS dat het niet mogelijk is om het weg te lakken.
- Delen van handleidingen over het blockchainsysteem die algemene gegevens bevatten indien deze delen zodanig verweven zijn met vertrouwelijke

65 ABRvS 8 februari 2017, ECLI:NL:RVS:2017:344, m.nt. P.J. Stolk.
66 ABRvS 8 februari 2017, ECLI:NL:RVS:2017:344, m.nt. P.J. Stolk, r.o. 10.
67 ABRvS 20 juni 2018, ECLI:NL:RVS:2018:2045, r.o. 4.2.

bedrijfs- en fabricagegegevens dat deze algemene gegevens niet geanonimiseerd of weggelakt kunnen worden.

Een verzoek tot informatie over de inzet en de toepassing van het blockchainsysteem door RWS zal wel openbaar gemaakt kunnen worden met een Wob-verzoek; een uitzondering gaat hier in beginsel niet op. Hierbij valt onder andere te denken aan informatie over hoe RWS blockchain inzet bij zijn toezichthoudende taak. Bijvoorbeeld in de pilot grondstomen zou dit informatie kunnen zijn over hoe vaak RWS de ingevoerde informatie in het blockchainsysteem checkt, of welke gevolgen RWS verbindt aan een (rood) signaal inzake het samenvoegen van partijen grond.

Het verstrekken van informatie onder de Wob dient achterwege te blijven indien het gaat om de verwerking van bijzondere persoonsgegevens als bedoeld in hoofdstuk 2, paragraaf 2 Wet bescherming persoonsgegevens, tenzij verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt (artikel 10 lid 1 sub d Wob). Indien het belang van het verstrekken van informatie daarnaast niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer, kan de informatie ook niet worden verstrekt. Het betreft hier een relatieve uitzonderingsgrond en er dient dus eerst een belangenafweging te worden gemaakt.

Daarnaast kan het verwerken van persoonsgegevens ook een rol spelen bij beperkingen op de openbaarheid van archieven. Artikel 15 lid 1 (a) Archiefwet noemt namelijk de eerbiediging van de persoonlijke levenssfeer als een van de uitzonderingsgronden. Afhankelijk van het feit of RWS persoonsgegevens op de blockchain zou zetten, kan deze uitzonderingsgrond dus relevant zijn.[68]

5° Woo

Met de inwerkingtreding van de Woo is het de bedoeling dat actieve openbaarmaking en bestuurlijke transparantie de norm worden.[69] In het licht hiervan zou het interessant kunnen zijn voor RWS om met een **publieke blockchain** te werken waartoe eenieder toegang heeft en waarbij eenieder informatie kan bekijken. Hierbij is echter van belang in het achterhoofd te houden dat het **toegang geven tot de informatie niet per se de informatie ook transparanter en "toegankelijker" maakt**, gezien een veelheid aan informatie ook kan leiden tot ondoorzichtigheid.[70] In dit opzicht zal het design van de user interface een belangrijke rol spelen, bijvoorbeeld door te werken met zoekbalken of informatiefilters. Het verdient dan ook aandacht om goed na te denken over de designkeuzes die hier gemaakt worden,

68 Voor een uitspraak van de ABRvS waar de beperkingsgrond eerbiediging van de persoonlijke levenssfeer aan de orde was, zie: ABRvS 8 maart 2017, ECLI:NL:RVS:2017:620.

69 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 1-2.

70 Dit is wat Stohl en Leonardi *inadvertent opacity* noemen. Zie Stohl & Leonardi 2016.

aangezien de user interface een keuzearchitectuur is die ook eigen (gedrags)normen met zich kan meebrengen. Het design van de user interface kan immers beïnvloeden hoe mensen zich gedragen, bijvoorbeeld omdat je bepaalde acties wel of niet kan uitvoeren.[71]

Daarnaast bevat de Woo voor RWS ook een zorgplicht om bepaalde maatregelen te treffen zodat **documenten te allen tijde gevonden kunnen worden en leesbaar of waarneembaar te maken zijn**.[72] Bovendien moet RWS maatregelen treffen om zijn documenten duurzaam toegankelijk te maken door ervoor te zorgen dat informatie via openbaar toegankelijke voorzieningen ontsloten kan worden.[73] Voor RWS betekent dit voornamelijk dat hij rekening moet houden met de manier waarop alle aanwezige overheidsinformatie in het blockchainsysteem ingedeeld, leesbaar en waarneembaar gemaakt wordt. Hierbij kunnen de vaardigheden van verschillende informatieverzoekers uiteenlopen, wat van belang is bij de invulling van wat "leesbaar" of "waarneembaar" voor verschillende informatieverzoekers betekent. Voor een techneut bijvoorbeeld zou softwarecode eventueel wel "leesbaar" kunnen zijn, terwijl dat voor een leek niet zo is. Een begin van oplossing hiervoor zou kunnen zijn dat bij het archiveren van de code er ook een geschreven uitleg over de softwarecode gearchiveerd wordt, of een verwijzing naar waar deze beschrijving gevonden kan worden, zodat verschillende typen informatieverzoekers met de overheidsinformatie in het archief uit de voeten kunnen.

71 Koops 2007, p. 2.
72 Art. 2.4 en art. 6.1 Woo jo. Art. 20 Archiefregeling.
73 Geconsolideerde artikelsgewijze toelichting bij de Wet open overheid zoals gewijzigd door de verwerking van de Wijzigingswet Woo, p. 65.

VI. Tien Vuistregels voor juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie

10 Vuistregels

Voor juridisch verantwoord ontwerpen van blockchaintechnologie inzake toegang tot overheidsinformatie

CHAIN
Connecting Humankind through Algorithms and Information Networks

Vuistregel 1

Schenk voldoende aandacht gedurende de gehele informatie-levenscyclus aan **duurzame digitale informatiehuishouding** en **toegankelijkheid van overheidsinformatie**.

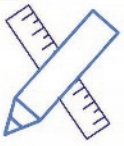
Vuistregel 2

Ontwerp de technische architectuur van de blockchain met de **Wob/Woo** en **Archiefwet** in het achterhoofd, aangezien het medium van de informatie en de opslagplaats voor de toepasselijkheid van deze wetten juridisch niet relevant zijn

Vuistregel 3

Weeg de voor- en nadelen van het blockchaindesign inzake gegevensopslag, -toegang en - bescherming af vooraleer een keuze te maken over **toegang** (publiek, privaat, hybride), **participatierechten** (permissioned of permissionless) en **gegevensopslag** (on-chain of off-chain)

Vuistregel 4



Waarborg bij het ontwerp van de technische infrastructuur '**access to information by design**' en **archiving by design**'.

Vuistregel 5

Richt **openbaarmaking** op **begrijpelijke** en **toegankelijke** wijze in en tracht toe te spitsen op de informatiebehoefte van de verzoeker.
Geef vorm aan wat begrijpelijk en toegankelijk is op basis van praktijktesten met gebruikers die **representatief** zijn voor de verschillende informatieverzoekers, zoals journalisten, burgers, bedrijven of overheden.

Vuistregel 6

Gegevens op een **publieke blockchain** die door een burger zelf te raadplegen zijn, vallen in beginsel **niet** onder de **reikwijdte van de Wob** en leiden dus niet tot te behandelen Wob-verzoeken.

Vuistregel 7

Het **design** van de blockchain architectuur en van de interface **is van groot belang** en **moet kunnen worden aangepast** in het licht van toekomstige wijzigingen in regelgeving (bv. inwerkingtreding Woo) en beleid.

Vuistregel 8

Het is aangeraden **persoonsgegevens en vertrouwelijke, concurrentiegevoelige bedrijfs- of fabricagegegevens off-chain** op te slaan.

Vuistregel 9

Maak een weldoordachte afweging welke informatie gearchiveerd wordt per proces en afhankelijk van de gevolgen van het proces, zodat een reconstructie gemaakt kan worden. **Het is aangeraden algoritmen te archiveren die een rol spelen in primaire werkprocessen.**

Vuistregel 10

Hou ook rekening met overige relevante regelgeving, zoals de Awb, de algemene beginselen van behoorlijk bestuur, de AVG, het mededingings- en aanbestedingsrecht en de Wet hergebruik overheidsinformatie.

VII. Literatuurlijst

Abels 2017
B.J. Abels, *Open, openbaar, organiseren? Digitalisering en openbaarheid archieven* (Den Haag: Ministerie van Onderwijs, Cultuur en Wetenschappen / Nationaal Archief 2017).

Aggarwal & Kumar 2021
S. Aggarwal & N. Kumar, 'Chapter Eleven – Cryptographic consensus mechanisms', *Advances in Computers* 2021, 121, p. 211-226.

Article 29 Data Protection Working Party 2014
Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 2016, WP 216.

Balvert 2020
A. Balvert, 'Noot bij ABRvS, 11 september 2019 (Wob verzoek Utrecht)', *Mediaforum* 2020, 20 (2), p. 65-66.

Beers & De Poorter
A.A.L. Beers & J.C.A. de Poorter, 'Commentaar op artikel 110 van de Grondwet', in E.M.H. Hirsch Ballin en G. Leenknegt (red.), *Artikelsgewijs commentaar op de Grondwet* (webeditie 2021), http://www.Nederlandrechtsstaat.nl.

Berberich & Steiner 2016
M. Berberich & M. Steiner, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers', *European Data Protection Law Review* 2016, 2 (3), p. 422-426.

Blockgenic 2018
Blockgenic, 'Different blockchain consensus mechanisms', *Hackernoon* 10 november 2018, https://hackernoon.com/different-blockchain-consensus-mechanisms-d19ea6c3bcd6.

Bovens 2007
M. Bovens, 'Analysing and assessing accountability', *European Law Journal* 2007, 4 (13), p. 447-468.

Brekke & Zuhair Alsindi 2021
J. K. Brekke & W. Zuhair Alsindi, 'Cryptoeconomics', *Internet Policy Review* 2021, 10 (2).

Burell 2016
J. Burrell, 'How the machine "thinks": Understanding opacity in machine learning algorithms', *Big Data & Society* 2016, 3(1).

Caldarelli 2020
G. Caldarelli, 'Understanding the blockchain Oracle Problem: A Call for Action', *Information* 2020, 11 (11), 509.

Carvalho 2019
Raquel Carvalho, 'Blockchain and public procurement', *Journal of Comparative Law and Governance* 2019, 6 (2), p. 187-225.

Cobbe, Sengh Ah Lee & Singh 2021
J. Cobbe, M. Sengh Ah Lee & J. Singh, 'Reviewable Automated Decision-Making: A framework for accountable systems', *ACM Conference on Fairness, Accountability, and Transparency (FAccT 21), March 2021, Virtual Event, Canada*, p. 598-609.

Collins 2020
P. Collins, What is a blockchain oracle?, 2 september 2020, https://betterprogramming.pub/what-is-a-blockchain-oracle-f5ccab8dbd72.

Damen e.a. 2013
L.J.A. Damen, C.L.G.F.J. Albers, K.J. de Graaf, J.H. Jans, A.P. Klap, A.M. Klingenberg, A.T. Marseille, P. Nicolaï, B.K. Olivier, H.D. Tolsma & F.R. Vermeer, *Bestuursrecht 1* (Den Haag: Boom juridisch, 2013, vierde druk).

Danaher 2016
J. Danaher, 'Three Types of Algorithmic Opacity', *Algocracy and the Transhumanist Project*, 5 maart 2016, https://algocracy.wordpress.com/2016/03/05/three-types-of-algorithmic-opacity.

De Fine Licht 2014
J. de Fine Licht, *Magic wand or Pandora's box? How transparency in decision-making affects public perceptions of legitimacy* (diss. University of Gothenburg, University of Gothenburg: Department of Political Science 2014).

De Fine Licht & Naurin 2016
J. de Fine Licht & D. Naurin, 'Transparency', in Christopher Ansell and Jacob Torfing (eds.) *Handbook on Theories of Governance* (Cheltenham: Edward Elgar Publishing 2016).

Enthoven e.a. 2021
G. Enthoven, H. Spanninga, C. Pino & A. Spruit, *Verbeterpunten in de informatiehuishouding voor een tijdige en kwalitatief goede afhandeling van Wob-verzoeken* (Berenschot-advies in opdracht van Rijksprogramma voor Duurzaam Digitale Informatiehuishouding 2021).

Erfgoedinspectie 2012
Erfgoedinspectie, *Beperkt houdbaar? Duurzame toegankelijkheid in een digitale omgeving bij de rijksoverheid* (Den Haag: Erfgoedinspectie 2012).

Erfgoedinspectie 2015
Erfgoedinspectie, *Onvoltooid Digitaal: de kwaliteit van de digitale archieven bij de organisaties van de Rijksoverheid* (Den Haag: Ministerie van Onderwijs, Cultuur en Wetenschap 2015).

Erfgoedinspectie 2018
Erfgoedinspectie, *Wel digitaal, nog niet duurzaam* (Den Haag: Erfgoedinspectie 2018).

Erkkilä 2012
T. Erkkilä, *Government Transparency: Impacts and Unintended Consequences* (Basingstoke: Palgrave Macmillan 2012).

European Union Agency For Fundamental Rights & Council of Europe 2018
Handbook European Data protection law: 2018 edition (Luxembourg: Publications Office of the European Union 2018).

Europese Commissie 2011
European Commission, 'Green Paper on the Modernization of EU Public Procurement Policy – Towards a More Efficient European Procurement Market', COM (2011) 15 final.

Goossens, Verslype & Tjong Tjin Tai 2020
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 Uitgevers 2020).

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

Helwig 2020
P. Helwig, 'Rekenen en rekenschap: algoritmes en de Archiefwet', *Tijdschrift voor Toezicht* 2020, nr. 1, p. 54-59.

Hirsch Ballin 2015
E.M.H. Hirsch Ballin, 'De constitutie van het bestuursprocesrecht', in A.T. Marseille, A.C.M. Meuwese, F.C.M.A. Michiels & J.C.A. de Poorter (red.), *Behoorlijk bestuursprocesrecht, Opstellen aangeboden aan prof. mr. B.W.N. de Waard over grondslagen, beginselen en vernieuwingen van het bestuursprocesrecht* (Den Haag: Boom juridisch, 2015, p. 19-30).

Hirsch Ballin 2020
E.M.H. Hirsch Ballin, *Advanced introduction to legal research methods*, Elgar Advanced Introductions (Cheltenham, UK / Northampton MA, USA: Edward Elgar, 2020).

Inspectie Overheidsinformatie en Erfgoed
Inspectie Overheidsinformatie en Erfgoed, 'Archiefbescheiden, wat zijn dat?', https://www.inspectie-oe.nl/onderwerpen/archiefbescheiden.

Inspectie Overheidsinformatie en Erfgoed 2021
Inspectie Overheidsinformatie en Erfgoed, *Een dementerende overheid 2.0?* (Den Haag: Inspectie Overheidsinformatie en Erfgoed 2021).

Koops 2007
B.-J. Koops, 'Criteria for Normative Technology', (2007) *TILT Law & Technology Working Paper* No. 005/2007 version 0.4 & *Tilburg University Legal Studies Working Paper* No. 007/2007.

Laan & Rutjes 2017
V.I. Laan & A. Rutjes, 'Privacy Issues bij blockchain: Hoe voorkom of minimaliseer je die?', *Computerrecht* 2017, 253.

Lemieux, Hofman, Batista & Joo 2019
V.L. Lemieux, D. Hofman, D. Batista, A. Joo, *Blockchain Technology & Recordkeeping* (ARMA International Educational Foundation, 2019).

Lianos 2019
I. Lianos, 'Blockchain Competition – Gaining Competitive Advantage in the Digital Economy: Competition Law Implications', in P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich, (red.) *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford: Oxford University Press 2019).

Lindseth 2010
P.L. Lindseth, *Power and Legitimacy: Reconciling Europe and the Nation-State* (New York: Oxford University Press, 2010).

Martini & Weinzierl 2017
M. Martini & Q. Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden', *Neue Zeitschrift für Verwaltungsrecht* 2017, 36 (8), p. 1251-1259.

Millard 2018
C. Millard, 'Blockchain and law: Incompatible codes?', *Computer Law & Security Review* 2018, 34, p. 843-846.

Nationaal Archief, Digitaal archief overbrengen
Nationaal Archief, 'Digitaal archief overbrengen', https://www.nationaalarchief.nl/archiveren/kennisbank/digitaal-archief-overbrengen.

Nationaal Archief, Hoe kun je digitaal vernietigen?
Nationaal Archief, 'Hoe kun je digitaal vernietigen?', https://www.nationaalarchief.nl/archiveren/kennisbank/hoe-kun-je-digitaal-vernietigen.

Nationaal Archief, Informatieobject
Nationaal Archief, 'Informatieobject', https://www.nationaalarchief.nl/archiveren/kennisbank/informatieobject.

Nationaal Archief, Metadata
Nationaal Archief, 'Metadata', https://www.nationaalarchief.nl/archiveren/kennisbank/metadata.

Nationaal Archief, Overzicht van begrippen
Nationaal Archief, 'Overzicht van begrippen', https://www.nationaalarchief.nl/archiveren/kennisbank/overzicht-van-begrippen.

Nationaal Archief, Wat betekent archiveren?
Nationaal Archief, 'Wat betekent archiveren?', https://www.nationaalarchief.nl/archiveren/kennisbank/wat-betekent-archiveren.

Nationaal Archief, Wat is digitaal vernietigen?
Nationaal Archief, 'Wat is digitaal vernietigen?', https://www.nationaalarchief.nl/archiveren/kennisbank/wat-is-digitaal-vernietigen.

Nationaal Archief, Welke informatie archiveert de overheid?
Nationaal Archief, 'Welke informatie archiveert de overheid?', https://www.nationaalarchief.nl/archiveren/kennisbank/welke-informatie-archiveert-de-overheid.

Nationale Ombudsman 2021
Nationale Ombudsman, *Een burger is geen dataset: Ombudsvisie op behoorlijk gebruik van data en algoritmen door de overheid*, Rapportnr. 2021/021 (Den Haag: Nationale Ombudsman 2021).

Nieuwenhuis 2014
P. Nieuwenhuis, *Open overheid, open vizier*, Rapport van de Rekenkamer Lelystad van 10 juni 2014 voor de gemeente Lelystad, (Lelystad: Rekenkamer Lelystad 2014).

Nin Sanchez 2019
S. Nin Sanchez, 'The Implementation of Decentralised Ledger Technologies for Public Procurement: Blockchain Based Smart Public Contracts', *European Procurement & Private Partnership Law Review* 2019, 14 (3) p. 180-196.

OECD 2018
Organization for Economic Co-operation and development, 'Summary of Discussion – Blockchain and Competition Policy', DAF/COMP/M(2018)1/ANN5/FINAL, 2019.

Ouwerkerk e.a. 2021
R. Ouwerkerk, S. Heirbaut, M. Bos, A. Moen, P. Berkers, E. Vullings, J. Hoeven, L. de Vries, C. de Haas, W. Zandvliet, E. Mettes, K. Groeneveld & G. Enthoven, *Archiveren by Design* (Den Haag: Vereniging van Nederlandse Gemeenten 2021).

PBLQ 2021
Duurzaam digitaal databeheer bij de Rijksoverheid: een verkenning (PBLQ eindrapport in opdracht van Rijksprogramma voor Duurzaam Digitale Informatiehuishouding 2021).

Pietermaat 2017
E. Pietermaat, 'De Wob is EHRM-proof, tenzij...', *Blogbestuursrecht* 5 december 2017, https://blogbestuursrecht.nl/wob-is-ehrm-proof/.

Pike & Capobianco, 2020
C. Pike & A. Capobianco, 'Antitrust and the trust machine', *OECD Blockchain Policy Series* 2020 http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

Purtova 2018
N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology* 2018, 10 (1), p. 40-81.

Rijksarchiefinspectie 2005
Rijksarchiefinspectie, *Een dementerende overheid? De risico's van digitaal beheer van verantwoordingsinformatie bij de centrale overheid* (2005).

Rijksoverheid 2016
Handleiding Wet hergebruik van overheidsinformatie (Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2016).

Rijkswaterstaat, Data Rijkswaterstaat
'Data Rijkswaterstaat', https://rijkswaterstaatdata.nl/.

Schemkes e.a. 2019
F. Schemkes, E. Tjong Tjin-Tai, M. Schellekens, W. Kaufmann & R. Leenes, *Blockchain en het recht: Een verkenning van de reguleringsbehoefte* (Tilburg: Tilburg University 2019).

Schlössels & Zijlstra 2017
R.J.N. Schlössels en S.E. Zijlstra, *Onderwijseditie Bestuursrecht in de sociale rechtsstaat* – Band 1 (Deventer: Wolters Kluwer 2017).

Schrepel 2019
T. Schrepel, 'Collusion by blockchain and smart contracts', *Harvard Journal of Law & Technology*, 2019/33, (1), p. 117-166.

Stohl & Leonardi 2016
C. Stohl, M. Stohl & P.M. Leonardi, 'Managing opacity: information visibility and the paradox of transparency in the digital age', *International Journal of Communication Systems* 2016, 10, p. 123-137.

Sztorc 2017
P. Sztorc, 'Blockchain: The Oracle Problems', *QCON London* March 8 2017, https://www.infoq.com/presentations/blockchain-oracle-problems/.

Ten Cate 2019
H.S. ten Cate, De verhouding tussen de Archiefwet en de Wob: cohesie of conflict', *Gemeentestem* 2019/134, afl. 7495, p. 670-680.

Van Heukelom 2018
S. van Heukelom, 'Responsieve rechtsstaat en digitale overheid: blockchain en smart contracts', *Nederlands Tijdschrift voor Bestuursrecht* 2018/39, afl. 5, p. 28-46.

Van Heukelom-Verhage e.a. 2019
Van Heukelom-Verhage, van Graafeiland, Gillhaus & Van Mechelen, *Blockchain in de zorg in relatie tot de AVG* (Pels Rijcken en Ledger Leopard rapport in opdracht voor Zorginstituut Nederland 2019).

Vereniging van Nederlandse Gemeenten 2018
Handreiking: Wet hergebruik van overheidsinformatie (Den Haag: Vereniging van Nederlandse Gemeenten 2018).

Wackerow 2021
P. Wackerow, 'Consensus Mechanisms', *Ethereum.org* 30 juli 2021, https://ethereum.org/en/developers/docs/consensus-mechanisms/.

Wieringa 2020
M.A. 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, Barcelona*.