

Blockchain en het recht. Een verkenning van de reguleringsbehoefte.

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

Tilburg University, juni 2019

Samenvatting

Introductie

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

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

Blockchaintechniek

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

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

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

praktisch belang. Een blockchain gebaseerd op afspraken kan wel voorzien in een mogelijkheid om oude gegevens te veranderen.

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

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

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

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

Algemene juridische aspecten

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

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

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

Smart contracts hebben diverse nadelen en risico's. Smart contracts eisen meestal betaling vooraf wat tot renteverlies en valuta-risico's leidt. Zij kunnen de gewone regels van het contractenrecht maar in beperkte mate uitvoeren: dat kan betekenen dat bescherming die een partij rechtens heeft (zoals bij overmacht) niet geëffectueerd kan worden. Bij het gebruik van menselijke 'oracles' voor de beoordeling van omstandigheden wordt het smart contract weer afhankelijk van menselijke

tussenkomenst en verloopt dan niet automatisch. Smart contracts zijn niet te begrijpen of controleren zonder specialistische kennis, en het inhuren van zulke kennis is kostbaar, terwijl het riskant is om erop te vertrouwen dat het contract doet wat de ontwikkelaar zegt. Smart contracts wijken daarnaast wezenlijk af van de gewone manier waarop mensen een contract opvatten: als een onderdeel van een intermenselijke relatie, die niet tot in detail vooraf regelt hoe er met verschillende omstandigheden moet worden omgegaan.

Smart contracts kunnen in bepaalde omstandigheden voordelen bieden ondanks de risico's. Dit lijkt met name het geval bij overeenkomsten met anonieme partijen in het buitenland, of als onderdeel van een grotere gewone overeenkomst (waarbij het smart contract wordt gebruikt als uitvoering van een deel van die overeenkomst).

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

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

Use-cases

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

Het scheepsregister

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

Schatkistbankieren ten behoeve van de nieuwbouw van scholen

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

een blockchain te realiseren. In de tweede plaats dekt een blockchain implementatie niet alle dimensies die de Auditdienst zou willen controleren af. Een blockchain maakt de Auditdienst Rijk dus niet overbodig.

Het vervoer van afvalstoffen binnen de EU

De Europese Verordening Overbrenging Afvalstoffen (EVOA Verordening) staat niet in de weg aan het digitaal uitvoeren van de relevante processen. In dit opzicht zou implementatie in een blockchain mogelijk zijn. De onmogelijkheid van het verwijderen van op de blockchain geplaatste persoonsgegevens is echter een punt van aandacht. Bovendien blijven fysieke controles nodig. Transporten die nooit ingevoerd zijn in de blockchain kent de blockchain niet. Als ingevoerde gegevens niet overeenstemmen met de werkelijkheid, kan de blockchain zelf dit niet constateren. Het is niet duidelijk wat de meerwaarde van een blockchain implementatie is ten opzichte van een traditioneel automatiseringsproces.

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

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

Synthese

Juridisch kader

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

Mensenrechten en morele waarden/beschermingsfunctie van het recht

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

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

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

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

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

Legitimiteit

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

Democratie en transparantie van het stellen van regels

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

Proportionaliteit

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

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

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

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

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