KU LEUVEN
FACULTEIT RECHTSGELEERDHEID
Academiejaar 2017-2018

Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR

Promotor: Prof. Dr. P. Valcke
Co-promotor: J. Schroers
Woordenaantal: 15 290

Masterscriptie ingediend door
Justine SIMAL
Bij het eindexamen voor de graad van
MASTER IN INTELLECTUELE EIGENDOM EN ICT RECHT

KU LEUVEN
FACULTEIT RECHTSGELEERDHEID
Academiejaar 2017-2018

Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR

Promotor: Prof. Dr. P. Valcke
Co-promotor: J. Schroers
Woordenaantal: 15 290

Masterscriptie ingediend door
Justine SIMAL
Bij het eindexamen voor de graad van
MASTER IN INTELLECTUELE
EIGENDOM EN ICT RECHT

Ik bevestig dat deze masterscriptie mijn eigen werk is, dat alle ideeën die vervat liggen in de masterscriptie worden uitgedrukt in mijn eigen woorden en dat ik niet letterlijk of quasi-letterlijk zaken heb overgenomen uit andere teksten, behalve fragmenten die worden aangehaald tussen aanhalingstekens waarvoor ik volledige en nauwkeurige bibliografische gegevens heb voorzien.

Justine Simal

ABSTRACT

DOEL – Het doel van dit onderzoek is nagaan of en in hoeverre blockchaintechnologie en de GDPR verzoenbaar zijn. Verwacht wordt dat enkele basiseigenschappen van blockchaintechnologie in aanvaring zullen komen met bepalingen van de GDPR.

RELEVANTIE – Blockchaintechnologie wordt beschouwd als een disruptieve technologie die een grote impact zal hebben in tal van sectoren en die zicht leent tot tal van toepassingen. Daarnaast wordt verwacht dat de GDPR zal zorgen voor een nieuwe standaard op vlak van de bescherming en verwerking van persoonsgegevens. Aangezien vele overheden en ondernemingen experimenteren met blockchaintechnologie, is het antwoord op de vraag of blockchaintechnologie en een correcte toepassing van de GDPR verzoenbaar zijn, zeer relevant.

METHODE – In een eerste stap werd nagegaan wat de basiseigenschappen zijn van blockchaintechnologie. Deze basiseigenschappen werden nadien afgetoetst aan de bepalingen van de GDPR om op die manier de knelpunten aan het licht te brengen.

RESULTATEN – Het versleutelde karakter van blockchaintechnologie stelt geen problemen. Het gedecentraliseerde karakter zorgt voor moeilijkheden bij het bepalen van de verwerkingsverantwoordelijke, wat op zijn beurt het waarborgen van een heel aantal rechten van de betrokkene onmogelijk maakt. Het gedistribueerde karakter vereist een hoge mate van transparantie, wat botst met het beginsel van gegevensbescherming door ontwerp en standaardinstellingen. Het permanente karakter tot slot verhindert de mogelijkheid tot het waarborgen van verschillende rechten van de betrokkene en botst met een groot aantal algemene beginselen.

AANBEVELINGEN – Geavanceerde encryptietechnieken, *obfuscation* en *off-chain* opslag zijn voorbeelden van technieken en methoden die door ontwikkelaars kunnen worden gebruikt om persoonsgegevens in de blockchain extra te beveiligen. Deze zouden eventueel in de toekomst kunnen worden aanvaard als technieken die kunnen leiden tot anonimisering van de desbetreffende blockchain, wat betekent dat de GDPR geen toepassing meer zal vinden, of als technieken die leiden tot een blockchain die conform is aan de vereisten gesteld door de GDPR.

BESLUIT – Blockchaintechnologie zoals initieel ontworpen door Nakamoto, is op vandaag niet verzoenbaar met de GDPR. Een lex specialis als aanvulling op de GDPR die zorgt voor een soepelere interpretatie wanneer het gaat over distributed ledgers en blockchains, kan ertoe leiden dat blockchains zullen kunnen worden ontwikkeld zonder twijfel omtrent hun legaliteit.

DANKWOORD

Met het schrijven van dit dankwoord leg ik de laatste hand aan mijn masterproef, het sluitstuk van mijn opleiding aan de KU Leuven en van mijn rechtenopleiding in zijn geheel. Graag neem ik even de tijd om iedereen te bedanken op wie ik kon rekenen in de loop van dit proces.

Eerst en vooral wil ik mijn promotor Prof. Dr. Peggy Valcke en co-promotor mevrouw Jessica Schroers bedanken voor het enthousiast onthalen van mijn onderzoeksplan, de raadzame opmerkingen en de nuttige feedback. Ik heb de kans gekregen om een masterproef te schrijven die volledig aansluit bij mijn interesses en waarmee ik vaardigheden en kennis heb vergaard die mij zeker verder van pas zullen komen in mijn toekomstige carrière.

Vervolgens bedank ik graag mijn ouders en mijn vriend voor hun niet-aflatende steun, liefde, begrip en geduld. In het bijzonder dank aan mijn papa voor het nalezen en voor de suggesties in de zoektocht naar de juiste woorden.

Tot slot ook dank aan mijn grootouders, die gedurende de afgelopen jaren mijn meest trouwe supporters waren. Het gezegde dat grootouders zilver in hun haar en goud in hun hart hebben, is in mijn geval meer dan waar.

INHOUDSOPGAVE

INLEIDING

Tijdens een interview in 2014 aan The Washington Post zei Marc Andreessen, ondernemer, investeerder en software-ingenieur, die het best bekend is als co-auteur van Mosaic, de eerste veel gebruikte webbrowser, dat hij *"er alle vertrouwen in heeft dat we het over 20 jaar hebben over blockchaintechnologie zoals we vandaag over het internet praten."*[1]

Blockchaintechnologie is veelbelovend en dit niet enkel binnen de financiële wereld: ook ver daarbuiten wordt verwacht dat blockchaintechnologie een grote impact zal hebben. Zo schatte IDC in 2016 dat 20% van alle *Internet of Things*-toepassingen een basisniveau van blockchaintechnologie zullen hanteren[2] en wordt verwacht dat blockchaintechnologie in de toekomst een grote sociale invloed zal hebben, waaronder ook in ontwikkelingslanden.[3] Blockchaintechnologie biedt een ongezien potentieel: de toepassingen zijn eindeloos en ondernemingen en overheden zijn dan ook volop aan het onderzoeken wat blockchaintechnologie voor hen kan betekenen.

Op het eerste zich lijken blockchains niks dan voordelen te bieden. Toch is waakzaamheid geboden, en dan in het bijzonder op het vlak van privacy. Blockchains kunnen een grote hoeveelheid persoonsgegevens verwerken. Hier dient logischerwijs zorgvuldig mee te worden omgesprongen én op een manier die conform is aan de Europese regelgeving omtrent de bescherming van persoonsgegevens, beter bekend als de GDPR. De vraag die centraal staat in dit onderzoek is of dit laatste mogelijk is: zijn blockchaintechnologie en de GDPR verzoenbaar? Zo nee, waar wringt het schoentje?

Het eerste hoofdstuk geeft een introductie tot blockchaintechnologie. In het tweede hoofdstuk worden de vormende elementen van blockchaintechnologie getoetst aan de GDPR en wordt nagegaan of blockchaintechnologie en de GDPR verzoenbaar zijn. Het derde hoofdstuk omvat aanbevelingen waarin methoden en technieken worden besproken om blockchains op zo'n manier te ontwikkelen dat deze zo conform mogelijk aan de GDPR. Tot slot volgt een conclusie waarin alle bevindingen en aanbevelingen worden samengevat.

---

[1] B. FUNG, "Marc Andreessen: In 20 years, we'll talk about Bitcoin like we talk about the Internet today", 21 mei 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/?utm_term=.1252983fa32e

[2] IDC, "IDC Futurescape: Worldwide Internet of Things 2017 Prediction", november 2016, https://www.idc.com/research/viewtoc.jsp?containerId=US40755816

[3] HESSEKIEL, D., "The Future of Social Impact is… Blockchain", 3 april 218, https://www.forbes.com/sites/davidhessekiel/2018/04/03/the-future-of-social-impact-is-blockchain/#4ca3ddc9c3fd

1. Een introductie tot blockchaintechnologie

1.1. Het ontstaan en het doel van blockchaintechnologie

Blockchaintechnologie is de technologie achter de digitale munt Bitcoin en werd in het jaar 2008 ontwikkeld door de man, vrouw of groep van personen die schuilgaat achter de naam Satoshi Nakamoto. De bedoeling van Nakamoto was om een *"purely peer-to-peer version of electronic cash"* te ontwikkelen *"[which] would allow online payments to be sent directly from one party to another without going through a financial institution"*.[4]

Het doel van blockchaintechnologie zoals deze werd ontwikkeld door Nakamoto is om de nood aan een tussenpersoon uit te schakelen en partijen rechtstreeks met elkaar te laten communiceren en handelen zonder dat er een derde partij aan te pas moet komen. Als we het hebben over geldtransacties, staat dat in schril contrast met de manier waarop dit vandaag gebeurt. Wanneer men een overschrijving uitvoert, passeert het geld langs één of twee banken, afhankelijk van of beide partijen klant zijn bij dezelfde bank of bij twee verschillende banken. De tussenkomst van een tussenpersoon, namelijk de bank, zorgt voor het nodige vertrouwen: zonder de bank ben je aangewezen op de eerlijkheid van de tegenpartij, die je mogelijks niet kent.

Welnu, Bitcoin lost dit anders op. Wanneer men handelt in Bitcoin vertrouwt men niet op een derde partij zoals bijvoorbeeld de bank, maar op de werking van de zogenaamde blockchain, een gedecentraliseerde en gedistribueerde databasetechnologie die volledig is onderbouwd door wiskundige encryptie of versleuteling. Dat is meteen de reden waarom Bitcoin een *cryptocurrency* wordt genoemd. Het creëren van vertrouwen zonder dat je een tussenpersoon nodig hebt, is het basisidee achter blockchaintechnologie.

Een andere bekende blockchain is de Ethereumblockchain. Een belangrijk verschil met Bitcoin is dat Ethereum een programmeerbare blockchain is die zich leent tot verschillende types van blockchainapplicaties, inclusief maar niet beperkt tot cryptocurrencies. Later wordt dieper ingegaan op de Ethereumblockchain.[5]

[4] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[5] Ethereum Homestead Documentation, "What is Ethereum?", 2016, http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

Ontwikkeld als de technologie achter Bitcoin, wordt vaak gedacht dat blockchaintechnologie zich louter situeert in de wereld van de *fintech*[6] en zich enkel of op z'n minst hoofdzakelijk leent voor geldtransacties. Niets is echter minder waar. De blockchain achter Bitcoin legt inderdaad geldtransacties vast, maar er bestaan nog tal van andere blockchains waarin gegevens worden bewaard. Zo bestaan er bijvoorbeeld blockchains waarin auteursrechten worden vastgelegd.[7] Sinds 2014 maken verschillende start-ups actief gebruik van blockchaintechnologie om intellectuele eigendomsrechten vast te leggen. Op deze manier wordt er een bestendige link gelegd tussen het beschermde werk en de auteur met daarbovenop een time stamp.[8] Maar er zijn nog vele andere toepassingen denkbaar. Zo gebruikt winkelketen Walmart blockchaintechnologie om de voedselveiligheid van hun voedingswaren te kunnen opvolgen en waarborgen[9], en testen India en Zweden of blockchaintechnologie kan worden gebruikt om eigendomsregisters te bewaren.[10]

Het mag duidelijk zijn dat er naast de Bitcoinblockchain nog zeer veel andere blockchains bestaan en dat vele ondernemingen en overheden de afgelopen jaren met blockchaintechnologie aan de slag gingen. Een Belgisch voorbeeld is Juru, een platform gebouwd met blockchaintechnologie dat je toelaat zelf je online-identiteit te beheren en te bepalen met wie je welke informatie deelt.[11] "*Op die manier wordt het Juru-account het centrale punt van je online identiteit*" aldus oprichter Dimitri Verhelst.[12]

In wat volgt wordt dieper ingegaan op hoe blockchaintechnologie precies in elkaar zit, welk onderscheid er kan worden gemaakt tussen verschillende soorten blockchains en wat de belangrijkste technische aspecten zijn.

---

[6] Staat voor 'financial technology' of 'financiële technologie' en verwijst naar technologische innovaties in de financiële sector. N.Y. Times beschrijft het als een label voor *"almost any start-up that is trying to use technology to solve some financial problem, and that can mean everything from insurance brokering to data analytics to budgeting software."* Zie N.Y. Times, "Ranking the Top Fintech Companies", N.Y. Times, 6 april 2016, https://www.nytimes.com/interactive/2016/04/07/business/dealbook/The-Fintech-Power-Grab.html

[7] B. CLARK, "Blockchain and IP law: a match made in crypto heaven?", februari 2018, *WIPO Magazine*, http://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html

[8] D. DE JONGHE en V.I. LAAN, "Blockchain in de realiteit", *Computerrecht* 2017, Afl. 6, p.347-353

[9] **R.** AITKEN, "IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com", 14 december 2017, https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#a653e867d9c5

[10] S. BALAJI, "India's blockchain revolution goes beyond banks into land records and private firms", 28 december 2017, https://www.forbes.com/sites/sindhujabalaji/2017/12/28/indias-blockchain-revolution-goes-beyond-banks/#2e9ce9aa4123; J.I. WONG, "Sweden's blockchain-powered land registry is inching towards reality", 3 april 2017, https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality

[11] M. VAN STEENKISTE, "Antwerpse start-up laat je je online identiteit beheren met blockchain", 7 augustus 2017, http://datanews.knack.be/ict/start-ups/antwerpse-start-up-laat-je-je-online-identiteit-beheren-met-blockchain/article-normal-885539

[12] *Ibid.*

1.2. De werking van blockchaintechnologie

Blockchaintechnologie zorgt ervoor dat er vertrouwen wordt gecreëerd door middel van slimme codering, namelijk de blockchain. Op abstracte wijze kan een blockchain worden omschreven als een gedecentraliseerde en gedistribueerde database van gegevens die permanent worden opgeslagen en moeilijk tot niet kunnen worden gewijzigd, waarbij het geheel wordt beveiligd door asymmetrische encryptie en gehandhaafd door een consensusmechanisme. [13]

De database is gedistribueerd, wat betekent dat ze niet wordt bewaard op één centrale server maar op alle computers van de deelnemers aan het netwerk (*nodes* genoemd). Elke deelnemer bewaart dus een kopie van de blokchain op zijn computer. De database is ook gedecentraliseerd, wat betekent dat er niet één centraal beheer is maar dat elke node eigen beslissingen neemt die achteraf door het systeem zelf worden gevalideerd. Het permanente en zo goed als onwijzigbare karakter van de gegevens in de blockchain wordt verkregen via cryptografische hasfuncties. Wat deze precies inhouden wordt verderop omstandig toegelicht. Ook asymmetrische encryptie wordt verderop verduidelijkt, maar in het kort kan al worden vermeld dat het een manier is om ervoor te zorgen dat acties in de blockchain worden ondernomen door de persoon die is wie hij zegt te zijn. Een consensusmechanisme, tot slot, is een mechanisme dat de integriteit van de blockchain bewaart doordat de deelnemers aan de blockchain consensus bereiken over de nieuw toegevoegde gegevens.[14]

De gegevens in de blockchain, worden vastgelegd in blokken, vandaar de 'block' in blockchain. Elk blok van gegevens wordt gekoppeld aan het vorige blok zodat ze als het ware een ketting vormen, vandaar de 'chain'.[15] De aaneenkoppeling van een nieuw blok aan het vorige blok, vindt plaats wanneer alle deelnemers aan het netwerk consensus bereiken omtrent de authenticiteit van het nieuwe blok en dit blok willen aanvaarden.[16] Consensus kan op verschillende manieren worden bereikt, namelijk doormiddel van het gebruik van verschillende consensusmechanismen. Aaneenkoppeling vindt plaats wanneer een *miner* (dit is een deelnemer aan het netwerk die zich actief bezighoudt met het koppelen van blokken omdat hij

[13] E.W. VERHELST, "Blockchain aan de ketting van de Algemene Verordeningen Gegevensbescherming?", *Privacy & Informatie* 2017, Afl. 1, p.17-23 ; M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 2017, p.1

[14] Learncryptography.com, "Proof of Work System", 2017, https://learncryptography.com/cryptocurrency/proof-of-work-system

[15] J. LINNEMAN, "Juridische aspecten van (toepassingen van) blockchain", *Computerrecht* 2016, Afl. 6, p.319-324

[16] Learncryptography.com, "Proof of Work System", 2017, https://learncryptography.com/cryptocurrency/proof-of-work-system

hiervoor een *incentive* krijgt) *Proof of Work* aflevert.[17] Proof of Work is het consensusmechanisme dat wordt gebruikt in de Bitcoinblockchain en de Ethereumblockchain.[18] In andere blockchains worden soms andere consensusmechanismen worden gebruikt, zoals bijvoorbeeld Proof of Stake.[19]

De werking van het consensusmechanisme Proof of Work is als volgt. Proof of Work wordt verkregen na de oplossing van een wiskundig vraagstuk.[20] Een vraagstuk waarbij men, in tegenstelling tot een klassiek vraagstuk, niet aan de hand van de gegevens en een formule tot de oplossing kan komen, maar moet werken via trial en error.[21] Dit verplicht de miner om telkens random combinaties uit te proberen tot hij, per toeval, op de correcte waarde stuit.[22] Wanneer een miner de oplossing vindt, kan hij Proof of Work afleveren aan de rest van het netwerk. Door dit Proof of Work bereikt het netwerk consensus omtrent de authenticiteit van de gegevens vervat in het blok.[23]

De blokken worden nu aan elkaar gekoppeld, waarbij telkens een deel van de gegevens die vervat liggen in het vorige blok, wordt geïntegreerd in het nieuwe blok. Dit zorgt ervoor dat, wanneer iemand de gegevens in een bepaald blok zou willen wijzigen, hij ook de gegevens in alle volgende blokken moet wijzigen.[24] Dit is praktisch en technisch bijna onmogelijk.

Voor het aaneenkoppelen ontvangt de miner een beloning.[25] Bij de blockchain achter Bitcoin is dit logischerwijs een vergoeding in Bitcoin, maar bij andere blockchains zijn andere beloningen denkbaar. De beloning is de incentive om je computerkracht ter beschikking te stellen van de opbouw van de blockchain.[26]

Daarnaast wil de beloning er ook voor zorgen dat nodes hun computerkracht ter beschikking stellen van de 'goede zaak', namelijk het opbouwen en veilig houden van de blockchain, en

[17] *Ibid.*
[18] Ethereumontwikkelaars plannen wel een overgang van Proof-of-Work naar Proof-of-Stake in de toekomst. Zie Ethereum Homestead Documentation "What's the future of Ethereum?", http://ethdocs.org/en/latest/frequently-asked-questions/frequently-asked-questions.html
[19] V. BUTERIN, "What Proof of Stake Is And Why It Matters", 26 augustus 2013, https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/
[20] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.40
[21] Learncryptography.com, "Bitcoin Mining", 2017, https://learncryptography.com/cryptocurrency/bitcoin-mining
[22] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[23] Learncryptography.com, "Proof of Work System", 2017, https://learncryptography.com/cryptocurrency/proof-of-work-system
[24] *Ibid.*
[25] *Ibid.*
[26] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.40

deze computerkracht niet aanwenden voor het ondermijnen van de blockchain.[27] In principe is het zo dat, wanneer één node meer computerkracht kan inzetten dan alle andere nodes samen, deze ene node ook meer Bitcoin verkrijgt dan alle andere nodes samen.[28] Het principe is dus dat het inzetten van veel computerkracht voor de opbouw en beveiliging van de blockchain, veel Bitcoin kan opleveren. Hierdoor zal de desbetreffende node worden aangemoedigd om eerlijk te handelen in plaats van zich te focussen op het terug stelen van zijn eigen gedane betalingen, aangezien dit het systeem en dus ook zijn eigen rijkdom zou ondermijnen.[29]

Wanneer één node over meer computerkracht zou beschikken dan alle andere nodes samen, bestaat namelijk de mogelijkheid dat er corrupt wordt gehandeld door middel van een zogeheten *51% attack*.[30] Dit omdat deze node geen andere nodes nodig heeft om het netwerk consensus te laten bereiken en hij dus zelf autonoom beslissingen kan nemen. Consensus wordt namelijk bereikt wanneer meer dan de helft van het netwerk akkoord is met de handeling en deze aanvaardt. Deze ene node, die op zichzelf de helft van de computerkracht van het netwerk beslaat, zou op deze manier de macht hebben om te (proberen) beslissen welke transacties worden aanvaard en welke niet.[31] Via dit systeem van beloningen worden de nodes aangemoedigd om eerlijk te handelen.

Na de aaneenkoppeling van de blokken door de miners zijn de gegevens zo goed als permanent in de blockchain vastgelegd op versleutelde wijze en bevindt zich gedistribueerd op de computers van alle deelnemers aan het netwerk, dezelfde versie van deze blockchain.

De eerste en ook de meest bekende blockchain die ooit werd ontwikkeld, is deze achter Bitcoin, maar zoals reeds vermeld is ook Ethereum een grote speler in de wereld van blockchaintechnologie. De Ethereumblockchain werd bedacht en gesticht door Vitalik Buterin en heeft naast cryptocurrency nog andere toepassingen.[32] De Ethereumblockchain maakt namelijk de uitvoering van zogenaamde *smart contracts* mogelijk. Deze term werd voor het eerst gebruikt eind de jaren ’90 door Nick Szabo en werd door hem gedefinieerd als *“a set of promises, specified in digital form, including protocols within which the parties perform on these promises”*.[33] Smart contracts bestonden dus reeds lang voor er sprake was van

[27] S. NAKAMOTO, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, https://bitcoin.org/bitcoin.pdf.
[28] *Ibid.*
[29] *Ibid.*
[30] Learncryptography.com, “51% Attack”, 2014, https://learncryptography.com/cryptocurrency/51-attack
[31] *Ibid.*
[32] Ethereum Homestead Documentation, “What is Ethereum?”, http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html
[33] N. SZABO, “Formalizing and Securing Relationships on Public Networks”, *First Monday* 1997, Afl. 9, http://ojphi.org/ojs/index.php/fm/article/view/548/469

blockchaintechnologie. Toegepast op blockchaintechnologie zijn smart contracts software applicaties die meteen op de blockchain worden geïnstalleerd – en niet op een centrale server – en die overeenkomsten en engagementen bevatten die automatisch worden uitgevoerd wanneer de voorwaarden vervuld zijn.[34] Deze voorwaarden zijn vastgelegd in de software zelf, waardoor de vervulling van deze voorwaarden geheel automatisch aanleiding geeft tot de uitvoering van de overeenkomst. Smart contracts laten toe dat er software wordt ontwikkeld die zeer dicht in de buurt komt van contractuele bepalingen die partijen effectief kunnen binden.[35] Volgend voorbeeld geeft iets meer duiding. Denk bijvoorbeeld aan een overeenkomst tussen A en B voor een voedingswarentransport waarbij de voorwaarde is dat tijdens het transport de temperatuur in de koelwagen steeds lager dan 8°C moet zijn. Het smart contract bevat dan de overeenkomst en de voorwaarden. Dit wordt dan in code gegoten in de vorm van een reeks 'als, dan' verklaringen.[36] Vereenvoudigd komt het voorbeeld dan hierop neer:

> als de temperatuur in de koelwagen onder 8°C blijft
> dan betaalt A het bedrag van €50 000 aan B
> als de temperatuur in de koelwagen stijgt tot 8°C of hoger
> dan betaalt B het bedrag van €2500 als schadevergoeding aan A

Smart contracts tussen partijen die elkaar kennen, bieden transparantie en zekerheid, onmiddellijke uitvoering en een mindere mate van afhankelijkheid van derde partijen zoals bijvoorbeeld rechtbanken.[37] Daarnaast kunnen kosten en mogelijke fouten in de uitvoering worden beperkt. Er zijn uiteraard ook nadelen, bijvoorbeeld dat het niet eenvoudig is om complexe overeenkomsten om te zetten in code, aangezien dit vereist dat men vooraf alle mogelijkheden vastlegt in de code.[38] Wanneer onverwachte gebeurtenissen zich voordoen, zou een automatische uitvoering of net het gebrek eraan, gecombineerd met het permanente karakter van de transactie, ongewenste resultaten met zich mee kunnen brengen. Daarnaast is het ook mogelijk om smart contracts af te sluiten met tegenpartijen die niet gekend zijn. Dergelijke smart contracts brengen logischerwijs uitdagingen met zich mee op vlak van tenuitvoerlegging.[39]

---

[34] A. DE BACKER en V. DE BOE, "Smart contracts in de financiële sector: grote verwachtingen en regulatoire uitdagingen", *Computerrecht* 2017, Afl. 6, p.355-363

[35] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.73

[36] C. BURNISKE, "Bitcoin and Ethereum: How smart contracts work", 29 mei 2016, https://ark-invest.com/research/smart-contracts-work

[37] A. DE BACKER en V. DE BOE, "Smart contracts in de financiële sector: grote verwachtingen en regulatoire uitdagingen", *Computerrecht* 2017, Afl. 6, p.355-363

[38] *Ibid.*

[39] Stel dat er bijvoorbeeld een rechtszaak zou dienen te worden ingesteld, wordt de tenuitvoerlegging van het vonnis enorm bemoeilijkt. Zie P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.85

Blockchaintechnologie wordt regelmatig voorgesteld als een 'nieuwe' technologie. Het is belangrijk om hier een kleine kanttekening bij te maken. Blockchaintechnologie op zich was inderdaad ongezien vóór Bitcoin. De verschillende eigenschappen van blockchaintechnologie (waarop verder dieper wordt ingegaan) zoals bijvoorbeeld *distributed ledger* technologie (DLT) en asymmetrische encryptie, werden daarentegen reeds voor het bestaan van blockchaintechnologie apart ontworpen en gebruikt.[40] Nakamoto heeft deze eigenschappen samengebracht en ontwierp zo de Bitcoinblockchain.

1.3. Publieke en private blockchains

De werking van de blockchain zoals deze hier wordt besproken, is de werking hoe deze oorspronkelijk werd bedacht door Nakamoto, namelijk een publieke, of in het Engels *permissionless*, blockchain: een open en publiek toegankelijke blockchain waar geen voorafgaande toestemming vereist is en waarin iedereen kan participeren.[41] Deze blockchain is *open-source* en *open-access*, wat betekent dat iedereen een Bitcoin adres kan aanmaken, de nodige software kan installeren en een node kan worden.

Een variant op de publieke blockchain is de private, of in het Engels *permissioned*, blockchain. Dit soort blockchain bevindt zich op een privaat netwerk, zoals een intranet of VPN. Het verschil tussen beide heeft betrekking op wie deel kan uitmaken van het netwerk: een private blockchain is afgeschermd en een deelnemer moet uitgenodigd en goedgekeurd worden.[42] Wanneer dit gebeurd is, kan de nieuwe toetreder acties uitvoeren in de blockchain (tot op het niveau waarvoor hij toestemming heeft gekregen) en zal hij zijn bijdrage leveren aan in het in stand houden van de blockchain.

Bij private blockchains wordt in het merendeel van de gevallen geen consensusmechanisme gebruikt omdat er ofwel wordt vertrouwd op het collectieve goede gedrag van de nodes, ofwel bepaalde nodes worden aangeduid als verantwoordelijke voor de verificatie van transacties.[43]

Publieke blockchains zijn het meest vernieuwend en brengen ook de meeste privacy-uitdagingen met zich mee. Om die reden ligt de focus in de volgende hoofdstukken op publieke blockchains.

---

[40] M. FINCK, "Blockchains and Data Protection in the European Union", 30 november 2017, *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 2017, p.3
[41] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[42] A. BERKE, "How safe are blockchains? It depends", *Harvard Business Review,* 7 maart 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends
[43] *Ibid.*

1.4. De technische aspecten van naderbij bekeken

1.4.1. Cryptografische hashfuncties

Bij blockchaintechnologie staan de zogenaamde cryptografische hashfuncties centraal. Dit zijn wiskundige berekeningen die een invoer van willekeurige omvang omzetten in een uitvoer van een vaste lengte (die meestal kleiner is dan de invoer), namelijk een reeks hexadecimale tekens met een specifieke lengte (256 bit bijvoorbeeld). De uitvoer noemt men een hash of hashwaarde.[44] Wanneer je over een reeks originele gegevens beschikt, is het eenvoudig om hier een hash van te berekenen.

Het achterhalen van de invoer die een bepaalde hash als resultaat gaf, is een voorbeeld van een wiskundig vraagstuk waarbij men, zoals hierboven beschreven, aan de hand van trial en error moet zien te ontdekken wat de oplossing is. De miners zullen proberen nagaan welke invoer de desbetreffende hash als resultaat heeft gegeven en zullen op deze manier Proof-of-Work leveren aan de rest van het netwerk opdat consensus kan worden bereikt omtrent de transactie. In principe is een hash one-way: het is namelijk redelijkerwijs onhaalbaar om uit de hash af te leiden welke gegevens ingevoerd werden om de hash te verkrijgen. Let wel, het is onhaalbaar, maar dus niet onmogelijk, anders zou het leveren van Proof of Work ook onmogelijk zijn. Het is de overeengekomen incentive die de miners ertoe aanzet om toch de inspanning te doen om de invoer van de hash te berekenen, via trial en error zoals gezegd.[45]

Er zijn verschillende redenen waarom gegevens in de blockchain niet zomaar als tekst worden opgeslagen en waarom hashfuncties worden gebruikt. Een eerste belangrijke reden is dat wanneer alle gegevens louter als tekst zouden worden bewaard, alles in de blockchain zomaar leesbaar zou zijn voor iedereen die het bestand opent. Vanuit privacyoogpunt is dit niet wenselijk. Een tweede belangrijke reden is dat het opslaan van gegevens als tekstbestanden zeer veel opslagruimte vergt, wat vanuit economisch oogpunt dan weer niet wenselijk is.[46]

Een cryptografische hashfunctie heeft vier belangrijke eigenschappen. Zoals reeds gezegd moet het ten eerste onhaalbaar zijn om de invoer af te leiden uit de uitvoer. Een tweede eigenschap is dat een hashfunctie liefst weinig tot geen 'botsingen' of conflicten mag veroorzaken.[47] Dit

[44] Learncryptography.com, "What are hash functions", 2017, https://learncryptography.com/hash-functions/what-are-hash-functions
[45] *Ibid.*
[46] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.10
[47] J. LINNEMAN, "Juridische aspecten van (toepassingen van) blockchain", *Computerrecht* 2016, Afl. 6, p.319-324

betekent dat het in de praktijk haast onhaalbaar moet zijn om dezelfde uitvoer te vinden voor verschillende invoer.[48] Verschillende invoer moet dus leiden tot verschillende uitvoer. Hieruit volgt een derde eigenschap: dezelfde invoer moet ook leiden tot dezelfde uitvoer. Iedereen die over dezelfde gegevens beschikt, bekomt dezelfde hash als uitkomst. Dezelfde input zorgt dus steeds voor dezelfde output en de hash is uniek voor de gegevens die erin vervat zitten.[49] Tot slot is het bij een hashfunctie steeds zo dat de kleinste wijziging in de invoer, bijvoorbeeld slechts één letter of cijfer, leidt tot een totaal verschillende hash. Het is dus niet zo omdat je bijvoorbeeld slechts één teken wijzigt in de invoer, dat de nieuwe hash ook slechts één teken zal verschillen.

Elk blok in de blockchain bevat een hash. Daarnaast bevat elk blok ook een timestamp en de transactiegegevens.[50] De hash wordt berekend aan de hand van de gegevens en de hash in het vorige blok. Wanneer je de inhoud van een blok in de blockchain zou proberen wijzigen, verander je daarmee de hash van dat blok. Aangezien de hash van het volgende blok steeds wordt berekend aan de hand van de hash van het vorige blok, zou je alle volgende blokken moeten wijzigen om je wijziging door te voeren. Zoals reeds gezegd is dit niet mogelijk: het systeem zal geen consensus bereiken voor dergelijke niet toegelaten acties aangezien het weinig waarschijnlijk is dat meer dan de helft van de nodes hiermee akkoord zouden gaan.[51] Dit is de reden waarom een blockchain permanent wordt genoemd en waarom het wijzigen van gegevens in een blockchain bijna niet mogelijk is.

1.4.2. Een gedistribueerd en gedecentraliseerd grootboek

Blockchaintechnologie is een vorm van *distributed ledger* technologie. Dit is een technologie waarbij een gedistribueerd grootboek, een soort van database, verspreid wordt over alle nodes, dus over alle computers die deelnemen aan het netwerk.[52] Men kan een blockchain vergelijken met een spreadsheet waarvan op duizenden verschillende computers die deelnemen aan het netwerk een kopie terug te vinden is die regelmatig wordt geüpdatet.

Een blockchain is een soort gedistribueerd grootboek, maar niet elk gedistribueerd grootboek is een blockchain. Een blockchain onderscheidt zich door zijn opbouw, namelijk een ketting

[48] *Ibid.*
[49] Learncryptography.com, "What are hash functions", 2017, https://learncryptography.com/hash-functions/what-are-hash-functions
[50] A. NARAYANAN, J. BONNEAU, S. GOLDFEDER, A. MILLER, E.W. FELTEN en E. FELTEN, *"Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"*, Princeton, Princeton University Press, 2016
[51] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.36
[52] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 2017, p.2-6

van blokken die wordt beveiligd door cryptografie en waarin wijzigingen zo goed als onmogelijk zijn.

Blockchaintechnologie is naast gedistribueerd ook gedecentraliseerd: de nodes zijn niet verbonden met één centrale server maar zijn daarentegen allemaal onderling verbonden. Er is dus geen sprake van één centraal bestuur of beheer, wat in principe de norm is en ook de vorm van beheer of bestuur die het vaakst wordt gekozen.[53] Gedecentraliseerde platformen hebben de afgelopen jaren aan populariteit gewonnen. Een belangrijke oorzaak van deze stijgende populariteit is de groeiende centralisatie van (persoons)gegevens door enkele grote online spelers.[54] Dit zorgt voor een verstoord machtsevenwicht. Als tegenreactie kiezen ontwikkelaars er daarom steeds vaker voor om (persoons)gegevens decentraal op te slaan, al is dit uiteraard niet zonder gevolgen. Aangezien het aspect decentralisatie zowel interessant als nuttig is in dit kader, zeker indien het wordt bekeken vanuit een privacystandpunt, gaan we hier dieper op in.

Decentralisatie brengt verschillende gevolgen met zich mee, waaronder het feit dat toezicht en controle (door bijvoorbeeld een overheid) veel moeilijker wordt.[55] Er is namelijk niet één entiteit die de informatiestroom beheert en controleert. Het succes van bijvoorbeeld TOR (The Onion Router) toont aan dat mensen overal ter wereld op zoek zijn naar mogelijkheden om te ontsnappen aan het toezicht door een overheid of het *tracken* door commerciële websites.[56] Dit zeker niet enkel om duistere praktijken te verdoezelen: denk bijvoorbeeld aan journalisten die op deze manier contact kunnen houden met klokkenluiders of slachtoffers van partnergeweld die op deze manier lotgenotenfora kunnen bezoeken. Dit alles zonder dat iemand hun online activiteiten kan volgen.

Tegenover de beperkte mogelijkheid tot toezicht en controle door een centrale entiteit, staat dat een decentrale database veel opener en transparanter is dan een centrale database.[57] Dit is noodzakelijk: aangezien het hele netwerk samen moet zorgen voor het beheer, los van een centrale tussenpersoon, moet ook het hele netwerk toegang hebben tot alle informatie om op die manier gecoördineerd de juiste beslissingen te kunnen nemen en zo consensus te kunnen

[53] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.43
[54] K. ABERER en M. HAUSWIRTH, "An Overview of Peer-to-Peer Information Systems", *WDAS* 2002, p. 171-188
[55] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/
[56] Zie voor meer informatie: Tor, "Overview", https://www.torproject.org/about/overview.html.en
[57] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/

bereiken.[58] Wanneer er wel een centraal beheer of bestuur is, neemt deze tussenpersoon of tussenpersonen de beslissingen en is het niet noodzakelijk om alle informatie te delen met heel het netwerk. Om op een effectieve wijze alle activiteiten te kunnen coördineren tussen de verschillende nodes, vereisen gedecentraliseerde databases dus een hogere mate van transparantie dan gecentraliseerde databases.[59]

Daarnaast zorgt transparantie er ook voor dat alle nodes eerlijk blijven handelen: aangezien alle informatie beschikbaar is voor alle nodes en deze ook samen moeten beslissen over het aanvaarden van een transactie, reguleert het decentrale netwerk op deze manier zichzelf.[60] Men zou kunnen stellen dat, hoe meer gedecentraliseerd een systeem is, hoe minder vertrouwen (op tussenpersonen) er nodig is maar des te meer transparantie.[61] Het blijft de vraag of deze transparantie, die ervoor zorgt dat er geen tussenpersonen nodig zijn, opweegt tegen een potentieel verminderde privacy van de betrokkenen.[62] (zie *infra*, '2.2.2 Gedecentraliseerd en gedistribueerd')

Het is natuurlijk niet zo dat transparantie betekent dat alle gegevens in de blockchain letterlijk 'leesbaar' zijn voor iedereen. Zoals reeds werd vermeld, worden de transactiegegevens in een blockchain opgeslagen in de vorm van een hash. Dit betekent dat de hash eerst moet worden 'ontcijferd' vooraleer de gegevens leesbaar zijn. Daarnaast wordt er ook gebruik gemaakt van encryptie (zie *infra*). Aan het 'probleem' van de transparantie wordt dus tegemoetgekomen door gebruik te maken van hashing en encryptie, al blijven de desbetreffende persoonsgegevens wel publiekelijk beschikbaar voor alle nodes.[63] Dit is ook zo bij smart contracts: zowel het smart contract als de code zelf wordt doorheen het hele netwerk verspreid en is zichtbaar voor alle nodes.[64] Dit betekent dat de identiteit van de contractspartijen mogelijks kan worden achterhaald, wat in het geval van smart contracts zeer onwenselijk kan zijn.[65]

Een gedecentraliseerde database kent geen formele hiërarchische structuur is. Hierdoor is het mogelijk dat derden proberen het netwerk te manipuleren of over te nemen, waardoor

[58] K. ABERER en M. HAUSWIRTH, "An Overview of Peer-to-Peer Information Systems", *WDAS* 2002, p. 171-188
[59] A.R. GALLOWAY, *"Protocol: How control exists after decentralization"*, Cambridge, MIT Press, 2004
[60] D. BRADBURY, "The problem with Bitcoin", *Computer Fraud and Security* 2013, Afl. 11, p. 5-8
[61] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/
[62] *Ibid.*
[63] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.36
[64] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.83
[65] A. KOSBA, A. MILLER, E. Shi, Z. Wen en C. Papamanthou, 'Hawk: The Blockchain Model of Cryptography and Privacy Preserving Smart Contracts", *IEEE Symposium on Security and Privacy* 2016, p.839-858

onofficiële clusters kunnen ontstaan en het niet meer duidelijk is waar de controle over het netwerk zich nu precies bevindt.[66] Deze onofficiële en onzichtbare controle over het netwerk kan een probleem zijn aangezien de nodes geen inzicht hebben in hoe deze controle eruit ziet of wat de concrete gevolgen kunnen zijn. Wanneer we kijken naar de Bitcoinblockchain, zien we dat het mijnen van Bitcoin steeds meer gecentraliseerd wordt: het netwerk wordt ondertussen gecontroleerd door vier grote *mining pools* die sinds december 2017 samen meer dan 50% van de Bitcoinblockchain controleren.[67] Indien ze samenwerken, zouden ze eenvoudig het netwerk kunnen overnemen met een 51% attack.[68]

Een laatste belangrijk punt om aan te halen, is dat decentralisatie zorgt voor een groot zelfbeschikkingsrecht over de eigen (persoonsgegevens).[69] Het is logisch dat het zelfbeschikkingsrecht over de eigen gegevens groter is wanneer dit mede zelf kan worden beheerd en niet enkel wordt beheerd vanuit een centraal bestuur. Dit zelfbeschikkingsrecht betekent bijvoorbeeld dat de betrokkenen zelf de keuze hebben om te beslissen over welke gegevens ze met welke partijen delen.[70] Een ander voorbeeld is dat betrokkenen ervoor kunnen kiezen om hun persoonsgegevens op een bepaalde manier doorheen het netwerk te verspreiden, zodat het onmogelijk is om informatie omtrent deze persoonsgegevens te verkrijgen wanneer je niet over alle delen beschikt.[71]

We kunnen besluiten dat decentralisatie enkele interessante gevolgen en misschien ook uitdagingen met zich meebrengt. Het feit dat een blockchain decentraal en gedistribueerd is, zorgt ervoor dat, wanneer er consensus is bereikt in het netwerk, elke node nadien beschikt over een identieke gesynchroniseerde kopie. Gedistribueerde en gedecentraliseerde databases zorgen ervoor dat partijen die elkaar niet volledig vertrouwen overeenstemming kunnen bereiken omtrent het bestaan en de status van een set gedeelde gegevens.

---

[66] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/

[67] Blockchain.info, "Hashrate Distribution", https://blockchain.info/pools

[68] J.A. KROLL, I.C. DAVEY en W. FELTEN, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries", *WEIS* 2013

[69] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/

[70] De Antwerpse start-up Juru die hierboven reeds werd vermeld, is hier een voorbeeld van.

[71] G. ZYSKIND, O. NATHAN en A. PENTLAND, "Enigma: Decentralized Computation Platform with Guaranteed Privacy", 2015

1.4.3. Asymmetrische encryptie

Een blockchain wordt beveiligd door asymmetrische encryptie.[72] Dit is een geavanceerde encryptietechniek die ervoor zorgt dat de bron vanwaar de actie afkomstig is, rechtmatig is en dat je gegevens kan versleutelen waardoor deze enkel leesbaar zijn voor de rechtmatige persoon.[73]

Wanneer je gebruik maakt van asymmetrische encryptie, werk je met een sleutelpaar dat bestaat uit een publieke sleutel en een private of geheime sleutel. Je publieke sleutel deel je met iedereen en is je 'adres', je geheime sleutel hou je vanzelfsprekend geheim. Beide sleutels staan in relatie tot elkaar, aangezien je de publieke sleutel gebruikt om gegevens te versleutelen en de private sleutel om deze gegevens te kunnen lezen.

Wanneer je een bewerking wilt uitvoeren in de blockchain, bijvoorbeeld een Bitcointransactie, kan je de transactie digitaal ondertekenen met je geheime sleutel.[74] Iets digitaal ondertekenen komt op hetzelfde neer als een document ondertekenen: door het ondertekenen geef je de toestemming dat een bepaalde actie mag plaatsvinden, in dit geval een Bitcointransactie.

Na het ondertekenen wordt je transactie verstuurd naar de miners die via je publieke sleutel, waar iedereen toegang toe heeft, kunnen controleren of je wel degelijk bent wie je zegt te zijn, namelijk de persoon die de transactie wilt uitvoeren.[75] Wanneer de miners hebben kunnen verifiëren dat je effectief bent wie je zegt te zijn, kunnen de desbetreffende gegevens aan het volgende blok worden gekoppeld en kan de actie, in dit geval de Bitcointransactie, worden uitgevoerd. Encryptie is dus *two-way*: wanneer gegevens versleuteld zijn, kan je deze met de juiste sleutel eenvoudig ontcijferen en leesbaar maken.[76]

Dit systeem werkt natuurlijk slechts naar behoren wanneer je je geheime sleutel effectief geheimhoudt: wanneer je hem deelt met iemand of verliest, kan iedereen hem gebruiken om zich voor te doen als iemand anders. Om deze reden is het niet abnormaal om voor elke transactie of na een bepaald aantal transacties, een nieuw sleutelpaar te genereren. Dit wordt

[72] Vaak wordt ook de Engelse term *public key cryptography* gebruikt.
[73] D. DRESCHER, *"Blockchain Basics: A non-technical introduction in 25 steps"*, New York, Apress, 2017, p96-101
[74] Zie A. NARAYANAN et al., *"Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"*, Princeton, Princeton University Press, 2016
[75] D. DRESCHER, *"Blockchain Basics: A non-technical introduction in 25 steps"*, New York, Apress, 2017, p96-108
[76] Dit is het grote verschil met hashfuncties: wanneer gegevens gehasht zijn, is het onhaalbaar om nog te achterhalen wat de oorspronkelijke input was. Wanneer gegevens versleuteld zijn, is het met de juiste sleutel zeer eenvoudig om de oorspronkelijke input te verkrijgen.

ook aangeraden door Nakamoto zelf: *"As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner."*[77]

Wanneer gegevens, stel een hoeveelheid Bitcoin, overgaan naar iemand anders, verschuiven deze van het ene 'adres' naar het andere. Je adres wordt gegenereerd aan de hand van je publieke sleutel.[78] Je adres is eigenlijk je pseudoniem via hetwelk je volledige transactiegeschiedenis kan worden teruggevonden.[79] Je kan het vergelijken met het schrijven van boeken onder een pseudoniem: niemand weet dat jij het bent, maar als één iemand erin slaagt om het pseudoniem naar jou terug te linken, weet iedereen dat alle boeken die je ooit onder dat pseudoniem geschreven hebt, van jouw hand zijn. Dit betekent dat privacy in de blockchain gewaarborgd is tot op het moment dat iemand de link maakt tussen een persoon en zijn of haar pseudoniem.[80] Wanneer voldoende gegevens beschikbaar zijn op de blockchain, is het mogelijk om heel de transactiegeschiedenis te achterhalen.[81] Hieruit volgt dat hoe vaker een adres wordt gebruikt, hoe meer informatie er zichtbaar wordt. Blockchains worden dus gekenmerkt door pseudonimiteit en niet door anonimiteit.[82]

1.5. Besluit

De slimme codering achter blockchaintechnologie laat partijen toe betrouwbare transacties uit te voeren waarvan de authenticiteit wordt vastgesteld door massale samenwerking tussen verschillende deelnemende computers aan het netwerk die worden gedreven door een collectief eigenbelang, en niet door één of meerdere tussenpersonen. Het vertrouwen dat wordt gecreëerd door het systeem zelf, los van een tussenpersoon die voor het nodige vertrouwen moet zorgen, is nieuw.[83]

Wanneer we kijken naar de opbouw en de kenmerken van een blockchain, leren we dat een blockchain een gedecentraliseerde en gedistribueerde database is van gegevens die permanent worden opgeslagen, waarbij het geheel wordt beveiligd door asymmetrische encryptie. Een

---

[77] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[78] *Ibid.*
[79] P. DE FILIPPI, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/
[80] M. MOSER, "Anonymity of Bitcoin transactions", Münster Bitcoin Conference 2013
[81] A. NARAYANAN en V. SHMATIKOV, "Robust Deanonymization of Large Sparse Datasets", *IEEE Symposium on Security and Privacy* 2008, p.111-125
[82] F. REID en M. HARRIGAN, "An Analysis of Anonimity in the Bitcoin System", *IEEE International Conference on Privacy, Security, Risk, and Trust* 2011*, and IEEE International Conference on Social Computing* 2011, p.1318-1326
[83] D. TAPSCOTT en A. TAPSCOTT, "*Blockchain revolution: how the technology behind bitcoin is changing money, business and the world*", New York, Portfolio Penguin, 2016, p.5

blockchain bestaat uit een grote hoeveelheid blokken die door miners aan elkaar worden gekoppeld zodat ze een ketting vormen. Het aaneenkoppelen gebeurt nadat deze miners Proof of Work hebben geleverd waardoor het systeem consensus bereikt en de authenticiteit van de gegevens vervat in het blok, wordt aanvaard. Wanneer de blokken gekoppeld zijn, kunnen de gegevens in het blok bijna onmogelijk worden gewijzigd. Een permanente versie van de blockchain die continu geüpdatet wordt, bevindt zich nu op elke computer van de deelnemers aan het netwerk.

Een blockchain verkrijgt zijn permanente karakter via cryptografische hashfuncties, de wiskundige berekeningen waar het bij blockchain allemaal rond draait. Daarnaast is blockchaintechnologie is een vorm van distributed ledger technology: technologie waarbij een gedistribueerd grootboek, een soort van database, verspreid wordt over alle computers die deelnemen aan het netwerk en waarbij er geen centraal beheer is. Tot slot wordt er bij blockchaintechnologie gebruik gemaakt van asymmetrische encryptie. Deze techniek zorgt ervoor dat elke actie die wordt ondernomen, op pseudonieme wijze plaatsvindt. Hieruit kunnen de belangrijkste vormende elementen van blockchaintechnologie worden afgeleid: een blockchain is gedecentraliseerd en gedistribueerd, permanent en versleuteld.

In het volgende hoofdstuk worden deze hoofdeigenschappen verder besproken en wordt dieper ingegaan op hoe deze eigenschappen zich verhouden tot de Algemene Verordening Gegevensbescherming (AVG), beter bekend als General Data Protection Regulation of GDPR.

2. Blockchaintechnologie en de GDPR

In het vorige hoofdstuk maakten we kennis met blockchaintechnologie en al zijn technische aspecten. We konden vaststellen dat een blockchain over drie belangrijke vormende elementen beschikt: een blockchain is gedecentraliseerd en gedistribueerd, permanent en versleuteld.

In wat volgt wordt nagegaan in hoeverre deze vormende elementen verenigbaar zijn met de geldende regelgeving omtrent de bescherming van persoonsgegevens, namelijk de General Data Protection Regulation. Aangezien natuurlijke personen en ondernemingen die zich bevinden in de Europese Unie, en natuurlijke personen en ondernemingen die persoonsgegevens verwerken van burgers van de Europese Unie, aan deze regelgeving zijn onderworpen, is het noodzakelijk dat zij persoonsgegevens verwerken op een manier die conform is aan deze regelgeving. Indien blijkt dat deze regelgeving niet kan worden nageleefd indien een onderneming gebruik maakt van blockchaintechnologie om persoonsgegevens te verwerken, stelt zich uiteraard een probleem en is het de vraag of blockchaintechnologie een legale technologie is om te gebruiken voor de verwerking van persoonsgegevens.

Eerst volgt een korte bespreking van de General Data Protection Regulation. Nadien worden de vormende elementen getoetst aan deze regelgeving om na te gaan of deze verenigbaar zijn. Tot slot volgt een conclusie waarin wordt uiteengezet of, en in welke mate, blockchaintechnologie verzoenbaar is met deze geldende regelgeving omtrent de bescherming van persoonsgegevens.

2.1. General Data Protection Regulation

De General Data Protection Regulation[84] (hierna: GDPR) is de Europese verordening omtrent de bescherming van persoonsgegevens die op 25 mei 2018 in werking trad. Deze verordening tracht burgers van de Europese Unie meer controle te geven over hun persoonsgegevens. Er vindt ook een modernisering en uniformisering van de regels plaats aangezien de GDPR één enkel pakket regels voor heel de EU invoert.

De GDPR versterkt de bestaande rechten en creëert ook nieuwe rechten zoals onder meer gemakkelijker toegang tot persoonsgegevens, een recht op gegevensoverdraagbaarheid, een recht op gegevenswissing en een recht om te weten wanneer persoonsgegevens zijn gehackt.

[84] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming)

Ook het recht op rectificatie, het recht op beperking van de verwerking en het beginsel van minimale gegevensverwerking zijn opgenomen in de GDPR.

Daarnaast komen er ook nieuwe regels en verplichtingen voor ondernemingen zoals bijvoorbeeld het aanstellen van een functionaris voor gegevensbescherming, het gebruik van privacyvriendelijke technieken zoals pseudonimisering, effectbeoordelingen en het bijhouden van een register van de verwerkingsactiviteiten. Ondernemingen die persoonsgegevens verwerken, vallen nog steeds onder de titel 'verwerkingsverantwoordelijke' of 'verwerker', afhankelijk van welke partij de middelen en doeleinden van de verwerking bepaalt.[85]

De huidige gegevenseconomie wordt gekenmerkt door *platform power*, waarbij grote spelers zoals Google en Amazon over enorme hoeveelheden gegevens beschikken.[86] De GDPR werd dan ook ontworpen met dergelijke verwerkers van persoonsgegevens in het achterhoofd. Het doel is om deze gecentraliseerde beheerders van grote hoeveelheden persoonsgegevens een halt toe te roepen en hen verantwoordelijkheden en verplichtingen op te leggen.

In wat volgt wordt telkens aangenomen dat de persoonsgegevens waarvan eventueel sprake is, worden opgeslagen ín de blockchain. Het is daarentegen belangrijk om te weten dat naast het '*on-chain'* opslaan van persoonsgegevens ook de mogelijkheid bestaat om persoonsgegevens buiten de blockchain ('*off-chain'*) op te slaan, in een andere versleutelde database. Het gebruik van een extra database zal er in de meeste gevallen voor zorgen dat men opnieuw dient te vertrouwen op een derde partij, waardoor er natuurlijk grotendeels wordt voorbijgegaan aan het opzet van blockchaintechnologie, namelijk het uitschakelen van tussenpersonen. Let wel, de mogelijkheden om gegevens off-chain op te slaan zonder te moeten vertrouwen op derden, worden volop onderzocht en enkele toepassingen zijn reeds gekend.[87]

Het zal blijken dat verschillende technische aspecten van blockchaintechnologie niet steeds eenvoudig te verzoenen zijn met de geldende wetgeving omtrent de bescherming van persoonsgegevens. Er werd met dergelijke vorm van opslag namelijk geen rekening gehouden bij het vormgeven van de GDPR. Dit sluit evenwel niet uit dat in de toekomst nieuwe vormen van blockchaintechnologie kunnen worden ontwikkeld waarbij wel tegemoet wordt gekomen aan de objectieven van de GDPR, aangezien blockchains, net zoals de GDPR, ook kunnen

[85] Artikel 4(7) en (8) GDPR
[86] Zie O. LYNSKEY, "Regulating 'platform power', 21 februari 2017, *LSE Law, Society and Economy Working Papers*, No. 1/2017, 31 pp.
[87] J. Eberhardt en S. Tai hebben een reeks vormen van off-chain opslag ontworpen waarbij er geen nood is aan een derde partij. Zie J. EBERHARDT en S. TAI "On or Off the Blockchain? Insights on Off-Chaining Computation and Data", *Springer International Publishing, Lecture Notes in Computer Science* 2017, *LNCS-10465*, p.3-15

streven naar meer controle over persoonsgegevens voor de betrokkene.[88] Dit evenwel op andere manieren dan deze die werden voorzien door de GDPR.[89]

2.2. Toetsing van de vormende elementen van blockchaintechnologie aan de GDPR

2.2.1. Versleuteld

§ 1. De verwerking van persoonsgegevens

De GDPR is regelgeving omtrent de bescherming van persoonsgegevens, wat betekent dat ze slechts toepassing kan vinden indien er sprake is van persoonsgegevens. Daarom is het belangrijk om vooraf na te gaan of we te maken hebben met de verwerking van persoonsgegevens in het geval van blockchaintechnologie.

De GDPR gaat over de verwerking van persoonsgegevens. Het begrip 'verwerking' wordt in de wettekst gedefinieerd als: *"Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."*[90] Het behoeft geen betoog dat de bewerkingen en transacties die plaatsvinden op de blockchain, vallen onder het begrip 'verwerking'.

'Persoonsgegevens' wordt in de GDPR gedefinieerd *als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke 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."*[91] Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens.[92] In wat volgt wordt

[88] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 2017, p.2
[89] *Ibid.*
[90] Artikel 4(2) GDPR
[91] Artikel 4(1) GDPR
[92] Artikel 2, artikel 4, leden 1 en 5 en overwegingen 14, 15, 26, 27, 29 en 30 GDPR; Advies 4/2007 van de Artikel 29 Werkgroep over het begrip persoonsgegevens (01248/07/NL, WP 136)

nagegaan of de gegevens die worden verwerkt in een blockchain, al dan niet als persoonsgegevens in de zin van de GDPR kunnen worden beschouwd.

§ 2. Pseudonimisering

Persoonsgegevens die zijn versleuteld of gepseudonimiseerd**,** maar die kunnen worden gebruikt om iemand opnieuw te identificeren, blijven persoonsgegevens en vallen binnen het toepassingsgebied van de GDPR.[93] Dit omdat gepseudonimiseerde gegevens steeds kunnen herleid worden naar de persoon erachter. In de GDPR wordt pseudonimisering gedefinieerd als *"het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld".*[94]

Persoonsgegevens die op zo'n wijze zijn geanonimiseerd dat de betrokkene niet of niet langer kan worden geïdentificeerd, worden niet meer als persoonsgegevens aanzien. Gegevens zijn pas echt geanonimiseerd als de anonimisering onomkeerbaar is en er op geen enkele manier kan worden teruggekeerd naar de oorspronkelijke gegevens.[95]

In het vorige hoofdstuk werd reeds uitgelegd dat een blockchain wordt versleuteld via asymmetrische encryptie en dat hiervoor een set van twee sleutels wordt gebruikt, namelijk een private en een publieke sleutel, waarbij de publieke sleutel fungeert als het adres of pseudoniem van de betrokkene. De publieke sleutel wordt hier beschouwd als persoonsgegeven aangezien deze sleutel fungeert als pseudoniem aan de hand waarvan de transactiegeschiedenis in de blockchain kan worden teruggevonden wanneer iemand de link maakt tussen deze publieke sleutel en de persoon erachter. Versleuteling door middel van asymmetrische encryptie is steeds een vorm van pseudonimisering, aldus de Artikel 29 Werkgoep.[96]

Daarnaast werd ook reeds vermeld dat transactiegegevens in de blockchain worden opgeslagen als een hash. De Artikel 29 Werkgroep heeft uitdrukkelijk bevestigd dat hashing een vorm van pseudonimisering is. Dit omdat een hash nog steeds kan terugleiden naar de oorspronkelijke

[93] Advies 4/2007 over het begrip persoonsgegevens (01248/07/NL, WP 136)
[94] Artikel 4(5) GDPR
[95] Advies 05/2014 van de Artikel 29 Werkgroep over anonimiseringstechnieken
[96] *Ibid.*

gegevens.[97] In een blockchain kan de hash dus in principe terugleiden naar de transactiegegevens die erin vervat liggen.

Voorlopig dienen we dus te stellen dat transactiegegevens die opgeslagen zijn onder de vorm van een hash, nog steeds persoonsgegevens zijn. Daarnaast is ook de publieke sleutel een persoonsgegeven.

Pseudonimisering is een aspect van blockchaintechnologie dat in hoge mate verzoenbaar is met de GDPR. Meer nog, de GDPR moedigt pseudonimiseringsmaatregelen ten zeerste aan. Zo staat er in de verordening te lezen dat *"de toepassing van pseudonimisering op persoonsgegevens kan de risico's voor de betrokkenen verminderen en de verwerkingsverantwoordelijken en de verwerkers helpen om hun verplichtingen inzake gegevensbescherming na te komen."*[98] Het gebruik van een digitale handtekening en asymmetrische encryptie zorgen ervoor dat men deel kan uitmaken van het netwerk, informatie kan delen en transacties kan uitvoeren zonder dat de echte identiteit gekend hoeft te zijn.[99] Of zoals Narayanan et al. het stellen met betrekking tot de Bitcoinblockchain: *"There are no real-world identities required to participate in the Bitcoin protocol. Any user can create a pseudonymous key pair at any moment, any number of them."*[100]

Cryptografische hashfuncties en versleuteling door middel van asymmetrische encryptie zijn beide inherente eigenschappen van blockchaintechnologie.[101] Dit betekent dat een blockchain steeds pseudoniem is. Toch is het belangrijk om te benadrukken dat er verschillende types van blockchains bestaan en dat sterke versleuteling geen inherente eigenschap is van blockchaintechnologie.[102] Het is de keuze van de ontwikkelaar van de blockchain hoe sterk de versleutelingsprotocollen zijn die worden gebruikt.

Het is niet ondenkbaar dat de Artikel 29 Werkgroep, de Europese Toezichthouder voor Gegevensbescherming of de Europese hoven en rechtbanken na verloop van tijd een ander standpunt innemen omtrent pseudonimisering.[103] Dit zou het geval kunnen zijn wanneer van bepaalde cryptografische processen wordt aangenomen dat deze in staat zijn om gegevens te

---

[97] *Ibid.*
[98] Overweging 28 GDPR
[99] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.38
[100] A. NARAYANAN et al., *"Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"*, Princeton, Princeton University Press, 2016
[101] *Ibid.*
[102] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.8
[103] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.11

anonimiseren. Zo bestaan er bijvoorbeeld op vandaag al geavanceerde versleutelingstechnieken die door velen worden beschouwd als technieken die leiden tot anonimiteit.[104]

Voorlopig is het standpunt van de Artikel 29 Werkgroep dat de nieuwste en meest geavanceerde encryptietechnieken kunnen verzekeren dat persoonsgegevens een zeer hoog beveiligingsniveau genieten, maar dat dit niet steeds resulteert in anonimisering.[105] Zolang de sleutel of de oorspronkelijke gegevens beschikbaar zijn, is volgens de Artikel 29 Werkgroep de mogelijkheid tot identificatie niet uitgesloten. Het is om die reden dan ook belangrijk om elke zaak afzonderlijk te beoordelen.

We kunnen besluiten dat blockchains op heden worden beschouwd als pseudoniem, zowel in de literatuur als door de Artikel 29 Werkgroep. In het licht van de GDPR is het gebruik van pseudonimiseringstechnieken een positief punt. Indien de gebruikte versleutelingstechnieken in dergelijke mate geavanceerd zouden worden dat er geen sprake meer is van pseudonieme maar louter van anonieme gegevens, zal de GDPR geen toepassing meer vinden aangezien *"de gegevensbeschermingsbeginselen derhalve niet van toepassing [dienen] te zijn op anonieme gegevens, namelijk […] persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is."*[106]

2.2.2. Gedecentraliseerd en gedistribueerd

In wat vooraf ging werd reeds uitgelegd dat blockchaintechnologie een vorm is van distributed ledger technologie, waarbij een soort van database gedistribueerd wordt over alle nodes. Daarnaast is een blockchain ook gedecentraliseerd omdat een blockchain geen centraal beheer kent.

In wat volgt wordt nagegaan in hoeverre deze eigenschappen van blockchaintechnologie te verzoenen zijn met de GDPR. Verwacht wordt dat omtrent beide eigenschappen problemen zullen rijzen. Zoals reeds werd verduidelijkt, werd de nieuwe wetgeving namelijk niet ontworpen met gedecentraliseerde databases in het achterhoofd, maar had deze gecentraliseerde databases in gedachten.[107]

---

[104] E. BEN SASSON, A. CHIESA, C. GARMAN, M. GREEN, I. MIERS, E. TROMER en M. VIRZA, "Zerocash: Decentralized Anonymous Payments from Bitcoin*", IEEE Symposium on Security and Privacy* 2014, p.459-474; P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.67

[105] Advies 05/2014 van de Artikel 29 Werkgroep over anonimiseringstechnieken

[106] Overweging 26 GDPR

[107] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 2017, p.27

§ 1. Verwerkingsverantwoordelijke

In de GDPR is een centrale rol voorbehouden aan de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is de "*natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*."[108]

De verwerkingsverantwoordelijke is degene die eindverantwoordelijkheid draagt voor het gehele proces van de verwerking van persoonsgegevens.[109] Dit is wat de GDPR de verantwoordingsplicht noemt. Hij moet toezicht houden op een conforme interne verwerking en dient er ook voor te zorgen dat de verwerking door externe verwerkers conform aan de GDPR gebeurt. Het is de verwerkingsverantwoordelijke die aansprakelijk is voor de schade die wordt veroorzaakt door niet-conforme verwerking.

Het is daarnaast ook de taak van de verwerkingsverantwoordelijke om de rechten die de GDPR creëert voor betrokkenen, te waarborgen. Indien een betrokkene bijvoorbeeld een verzoek tot inzage van zijn of haar gegevens indient, is het de taak van de verwerkingsverantwoordelijke om dit verzoek in te willigen.[110]

De aandachtige lezer merkt reeds op dat het gedecentraliseerde karakter van blockchaintechnologie een struikelblok kan vormen wanneer we willen bepalen wie de verwerkingsverantwoordelijke is. Aangezien we niet kunnen spreken van een centraal beheer, is het moeilijk om één verwerkingsverantwoordelijke aan te duiden.

We zouden drie hypotheses kunnen onderscheiden omtrent wie kwalificeert als verwerkingsverantwoordelijke: een eerste hypothese is dat alle nodes kwalificeren als (gezamenlijke) verwerkingsverantwoordelijke, in een tweede hypothese kwalificeren de miners als gezamenlijke verwerkingsverantwoordelijke en in een derde hypothese kwalificeert de betrokkene zelf als verwerkingsverantwoordelijke.

[108] Artikel 4(7) GDPR
[109] Artikel 5, tweede lid GDPR
[110] Artikel 15 GDPR

(1) Alle nodes kwalificeren als (gezamenlijke) verwerkingsverantwoordelijke

Er kan worden beargumenteerd dat alle nodes kwalificeren als verwerkingsverantwoordelijke omdat elke node autonoom handelt, geen externe instructies opvolgt en zelf bepaalt welke acties worden ondernomen in de blockchain.[111]

Wanneer we deze hypothese zouden aanvaarden, rijzen er enkele problemen. Eerst en vooral hebben nodes geen vat hebben op hoe het systeem precies functioneert en dienen ze zich te schikken naar de werking van de blockchain. Daarnaast zien alle nodes hetzelfde in de blockchain, namelijk gehashte data, waaraan ze daarenboven geen wijzigingen kunnen aanbrengen.[112] Nodes bepalen dus verre van het verloop van de verwerking, wat wel wordt verwacht van een verwerkingsverantwoordelijke.

Kwalificeren ze dan als gezamenlijke verwerkingsverantwoordelijken? Het begrip gezamenlijke verwerkingsverantwoordelijken wordt gedefinieerd als volgt: *"Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast […] door middel van een onderlinge regeling […]."*[113]

Ook wanneer we deze hypothese zouden willen volgen, rijzen er enkele moeilijkheden. Nodes bepalen namelijk niet samen de doeleinden en de middelen voor de verwerking. Ze stellen ook niet samen op duidelijke wijze hun respectieve verantwoordelijkheden vast.[114] Integendeel, nodes zijn vrij om te beslissen of ze al dan niet deel willen uitmaken van het netwerk.

Er kan worden geconcludeerd dat nodes gedecentraliseerde entiteiten zijn die moeilijk in staat kunnen worden geacht om aan de verantwoordelijkheden en verplichtingen die de GDPR oplegt aan – centrale – verwerkingsverantwoordelijken, te voldoen. Het wordt hierdoor dan ook moeilijk om nodes te beschouwen als (gezamenlijke) verwerkingsverantwoordelijken.

[111] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.16-18
[112] *Ibid.*
[113] Artikel 26 GDPR
[114] M. BERBERICH en S. MALGORZATA, "Blockchain technology and the GDPR: How to reconcile privacy and distributed ledgers", *European Data Protection Law Review* 2016, Volume 2, Afl.3, p.422 - 426

(2) De miners kwalificeren als gezamenlijke verwerkingsverantwoordelijke

Een tweede hypothese stelt dat de miners kunnen worden beschouwd als gezamenlijke verwerkingsverantwoordelijken. De miners zijn bepaalde nodes die de transacties valideren en de blokken van gegevens aan elkaar vastmaken waardoor de desbetreffende gegevens permanent worden vastgelegd in de blockchain. Op grond hiervan zouden ze kunnen worden beschouwd als gezamenlijke verwerkingsverantwoordelijke.[115]

Toch rijzen ook hier moeilijkheden. Het zijn namelijk de computers op zich die deze taken automatisch uitvoeren, zonder dat er een echte beslissing voor nodig is. De miners zelf zijn zich in principe niet bewust van de inhoud die circuleert via de computer in kwestie, wat betekent dat ze louter een technische rol vervullen en geen effectieve beslissingen (kunnen) nemen.

Het zal op grond van bovenstaand argument dan ook moeilijk worden aanvaard dat miners kunnen worden beschouwd als gezamenlijke verwerkingsverantwoordelijken.

(3) De betrokkene zelf kwalificeert als verwerkingsverantwoordelijke

Een laatste hypothese is deze waarbij de betrokkene zelf kwalificeert als verwerkingsverantwoordelijke. Het kan worden aanvaard dat, wanneer de betrokkene zelf eigen persoonsgegevens hasht en toevoegt aan de blockchain, deze kan kwalificeren als betrokkene én als verwerkingsverantwoordelijke.[116] De betrokkene bepaalt namelijk zelf welke middelen hij gebruikt voor de verwerking, aangezien hij zelf beslist welke software en hardware hij gebruikt. Daarnaast bepaalt de betrokkene in vele gevallen ook zelf waarom hij beroep doet op de desbetreffende blockchain, wat betekent dat hij zelf beslist omtrent de doeleinden van de verwerking. Om deze twee redenen zou de betrokkene zelf kunnen kwalificeren als verwerkingsverantwoordelijke, al is het steeds noodzakelijk om dit geval per geval te onderzoeken.[117] Het is dus niet mogelijk om algemeen te concluderen dat de betrokkene in elk geval, in elke blockchain als verwerkingsverantwoordelijke zou kunnen worden beschouwd.

We kunnen besluiten dat het zeer moeilijk is om te bepalen welke partij(en) de verwerkingsverantwoordelijke is in een publieke blockchain omdat het niet duidelijk is welke partij(en) nu precies het doel en de middelen van de verwerking bepaalt. Het meest plausibele antwoord is dat alle nodes verwerkingsverantwoordelijken zijn, maar dit stelt uiteraard

[115] J. CZARNECKI "Blockchains and Personal Data Protection Regulations explained", 29 april 2017, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/
[116] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.16-18
[117] *Ibid.*

problemen wanneer betrokkenen hun rechten willen laten gelden, aangezien er vaak ontelbaar veel nodes zijn en het onmogelijk is om hen allen te identificeren en te adresseren.[118]

In wat volgt zal niet telkens worden teruggekomen op de moeilijkheid van het aanduiden van een verwerkingsverantwoordelijke. Het is evident dat het bij het waarborgen van alle rechten en algemene beginselen die naderhand worden besproken, telkens een probleem zal stellen dat het voor de betrokkene moeilijk tot onmogelijk is om de verwerkingsverantwoordelijke aan te duiden. Het gebrek aan duidelijkheid omtrent de verwerkingsverantwoordelijke leidt er *de facto* toe dat de betrokkene louter beschikt over rechten op papier.

§ 2. Recht van inzage

Het recht van inzage wordt gewaarborgd door artikel 15 van de GDPR en geeft aan de betrokkene het recht om van de verwerkingsverantwoordelijke *"uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie: (a) de verwerkingsdoeleinden, (b) de betrokken categorieën van persoonsgegevens, (c) de ontvangers of categorieën van ontvangers, (d) indien mogelijk, de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen, (e) […], (f) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit, (g) […], (h) het bestaan het geautomatiseerde besluitvorming met inbegrip van […] profilering en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene."*[119]

Het recht van inzage valt uiteen in een heel aantal deelrechten waarbij het meteen duidelijk is dat het moeilijk wordt om aan deze rechten tegemoet te komen. Bij blockchaintechnologie is er geen sprake van één centrale verwerkingsverantwoordelijke die dergelijke verzoeken kan behandelen. Geen enkele van de nodes heeft de mogelijkheid of bevoegdheid om deze informatie na te gaan of op te vragen en deze dan door te geven aan de node die hierom verzoekt. Wanneer bepaalde nodes in de toekomst zouden kunnen kwalificeren als verwerkingsverantwoordelijke en de node die om inzage verzoekt, slaagt erin de juiste nodes te identificeren en contacteren, blijft het zo dat nodes enkel een versleutelde of gehashte versie

[118] *Ibid.*
[119] Artikel 15, eerste lid GDPR

van de blockchain en dus van persoonsgegevens zien, waardoor ze nog steeds in de onmogelijkheid zijn om het verzoek in te willigen.[120]

De verwerkingsverantwoordelijke is daarnaast ook verplicht om een kopie van de persoonsgegevens te verstrekken aan de betrokkene.[121] Gezien het feit dat elke node beschikt over een volledige en actuele versie van de blockchain op zijn eigen computer, zou kunnen worden beargumenteerd dat hier aan wordt voldaan. Hier kunnen echter vraagtekens bij worden geplaatst aangezien deze versie van de blockchain waarover de betrokkene (en alle andere nodes) beschikt, een versleutelde en gehashte versie is, wat betekent dat het bestand zonder de juiste sleutels onleesbaar is.[122]

Ook om aan het recht van inzage tegemoet te komen, kan off-chain opslag van persoonsgegevens grotendeels voor een oplossing zorgen.

Tot slot waarborgt artikel 15 GDPR ook het recht van de betrokkene om in kennis te worden gesteld omtrent de passende waarborgen die worden voorzien wanneer zijn gegevens worden doorgegeven aan een land of internationale organisatie buiten de Europese Unie.[123] Op deze doorgifte aan landen buiten de Europese Unie gaan we meteen dieper in.

Het gebrek aan een duidelijke verwerkingsverantwoordelijke, leidt er toe dat er niet tegemoet kan worden gekomen aan het recht op inzage. Ook het waarborgen van andere rechten zoals bijvoorbeeld het recht op gegevenswissing[124], het recht op rectificatie[125] of het recht op beperking van de verwerking[126] komen hierdoor onder druk te staan. Omdat deze drie rechten nog meer in strijd zijn met een ander vormend element van blockchaintechnologie, namelijk het permanente karakter, worden ze in het volgend hoofdstuk verder besproken (zie *infra*, '2.2.3 Permanent').

§ 3. Gegevensbescherming door ontwerp en door standaardinstellingen

De verwerkingsverantwoordelijke is verplicht om, "*zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische*

[120] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.22-23
[121] Artikel 15, tweede lid GDPR
[122] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.22-23
[123] Artikel 15, tweede lid GDPR
[124] Artikel 17 GDPR
[125] Artikel 16 GDPR
[126] Artikel 18 GDPR

maatregelen te treffen" om op die manier de gegevensbeschermingsbeginselen "*op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen*."[127] Hierbij mag de verwerkingsverantwoordelijke rekening houden met *"de stand van de techniek, de uitvoeringskosten en de aard, de omvang, de context en het doel van de verwerking, alsook met de […] risico's voor de rechten en vrijheden van natuurlijke personen"*.[128]

Daarnaast dient de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen "*om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.*"[129] Het gaat met name over "*de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan*."[130] Het doel van deze maatregelen is ervoor zorgen dat "*persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt*."[131]

Het beginsel van gegevensbescherming door ontwerp en standaardinstellingen wil ontwikkelaars, verwerkers en verwerkingsverantwoordelijken van in het begin doen nadenken over de bescherming van persoonsgegevens. *"Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen de producenten […] te worden gestimuleerd om bij de ontwikkeling en de uitwerking […] rekening te houden met het recht op bescherming van persoonsgegevens […]."*[132] Het kan dan onder meer gaan over *"het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, transparantie met betrekking tot de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en uit het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren."*[133]

Men kan er moeilijk om heen dat het niet eenvoudig is om blockchaintechnologie zoals deze werd ontwikkeld door Nakamoto, waaronder met name het gedistribueerde karakter, te

[127] Artikel 25, eerste lid GDPR
[128] *Ibid.*
[129] Artikel 25, tweede lid GDPR
[130] *Ibid.*
[131] Artikel 25, tweede lid in fine GDPR
[132] Overweging 78 GDPR
[133] *Ibid.*

verzoenen met het beginsel van gegevensbescherming door ontwerp en door standaardinstelling. Nakamoto heeft deze nu eenmaal niet ontworpen met de GDPR in het achterhoofd, aangezien hier in 2008, wanneer Nakamoto de Bitcoinblockchain op de wereld losliet, nog lang geen sprake van was. Het gedistribueerde karakter van blockchains, dat ervoor zorgt dat alle informatie met hele hele netwerk wordt gedeeld, lijkt moeilijk verzoenbaar met het beginsel van gegevensbescherming door ontwerp. Ook het doel dat de maatregelen nastreven die in dit kader worden genomen, namelijk dat "*persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt"*[134] lijkt zeer problematisch.

In de toekomst zal blijken hoe streng dit beginsel wordt geïnterpreteerd en of de verwerkingsverantwoordelijke de soort technologie die wordt gebruikt in rekening mag brengen om af te wegen of de verwerking gerechtvaardigd is of niet. Dit naar analogie met het feit dat de verwerkingsverantwoordelijke rekening mag houden met *"de stand van de techniek, de uitvoeringskosten en de aard, de omvang, de context en het doel van de verwerking, alsook met de […] risico's voor de rechten en vrijheden van natuurlijke personen"*.[135]

§ 4. Doorgifte aan landen buiten de Europese Unie of internationale organisaties

Wanneer persoonsgegevens worden doorgegeven aan landen buiten de Europese Unie of aan internationale organisaties gelden er extra voorwaarden en waarborgen.[136] Dit omdat de Europese wetgever wil dat het beschermingsniveau waarvan de betrokkene in de Unie verzekerd is, gewaarborgd wordt.[137]

Een doorgifte kan geschieden op basis van een adequaatheidsbesluit[138] of op basis van passende waarborgen[139]. Een adequaatheidsbesluit houdt in dat de Europese Commissie de beslissing neemt dat het land of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt.[140] Wanneer geen dergelijke beslissing werd genomen door de Europese Commissie, is een doorgifte slechts toegestaan wanneer passende waarborgen worden geboden en betrokkenen beschikken over afdwingbare rechten en doeltreffende rechtsmiddelen.[141]

---

[134] Artikel 25, tweede lid in fine GDPR
[135] *Ibid.*
[136] Artikel 44 GDPR
[137] Overweging 101 GDPR
[138] Artikel 45 GDPR
[139] Artikel 46 GDPR
[140] Artikel 45, eerste lid GDPR
[141] Artikel 46, eerste lid GDPR

Bij open en publieke blockchains kunnen nodes zich over de hele wereld bevinden. Het gedistribueerde karakter van de blockchain zorgt ervoor dat exemplaren van de blockchain zich dus ook op computers over de hele wereld bevinden. Daarbovenop zorgt het gedecentraliseerde karakter ervoor dat beslissingen omtrent transacties ook over de hele wereld worden genomen. Dit brengt met zich mee dat nodes in vele gevallen zorgen voor doorgiften van persoonsgegevens naar derde landen. Nodes hebben evenwel op geen enkele manier zicht op of controle over waar de andere nodes zich bevinden, wat betekent dat het zeer moeilijk wordt om te voldoen aan de vereisten die de GDPR stelt op vlak van doorgiften naar landen buiten de Europese Unie. Dit omdat een node nooit kan weten of het gaat om een doorgift en zo ja, naar welk land. Zonder deze informatie is het voor een node namelijk onmogelijk om na te gaan of er een adequaatheidsbesluit bestaat of, indien dit niet het geval is, het land in kwestie passende waarborgen biedt en aan de betrokkene afdwingbare rechten en doeltreffende rechtsmiddelen verleent.

§ 5. Grensoverschrijdende verwerking

Om het hoofdstuk over het gedecentraliseerde en gedistribueerde karakter af te ronden, wordt ter volledigheid het begrip 'grensoverschrijdende verwerking' besproken. De GDPR definieert dit begrip als volgt: "*(a) [een verwerking] van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of (b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden".*[142]

De GDPR is van toepassing op de verwerking van persoonsgegevens door ondernemingen die gevestigd zijn binnen de EU, ongeacht waar de verwerking precies plaatsvindt.[143] Elke onderneming binnen de EU die persoonsgegevens verwerkt, is dus onderworpen aan de GDPR. Deze verplichting zorgt ervoor dat ondernemingen hun verwerkingsactiviteiten niet toevertrouwen aan landen buiten de EU om op die manier aan hun verplichtingen te ontsnappen.

Daarnaast is de GDPR ook van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de EU bevinden, los van de plaats waar de

[142] Artikel 4(23) GDPR
[143] Artikel 3, eerste lid GDPR

verwerkingsverantwoordelijke of verwerker gevestigd is, indien er goederen of diensten worden aangeboden of indien het gedrag van de betrokkene wordt gemonitord.[144] Dit betekent dat, wanneer een onderneming, los van de plaats van vestiging, persoonsgegevens verwerkt van personen die zich bevinden binnen de EU, deze onderneming verplicht is de GDPR na te leven.

Dit zal er voor zorgen dat wanneer een onderneming een open en publieke blockchainapplicatie lanceert, de GDPR toepassing vindt vanaf het moment dat een node die zich in de EU bevindt, beslist om deel uit te maken van de blockchain. Een gevolg hiervan zal zijn dat de GDPR ook toepassing zal vinden op transacties die weinig tot geen link hebben met de EU.[145]

2.2.3. Permanent

Het permanente karakter van een blockchain wordt gecreëerd via cryptografische hashfuncties en wijst op het feit dat gegevens, eenmaal deze in een blok zijn gegoten en zijn vastgekoppeld aan het vorige blok, nog slechts zeer moeilijk kunnen worden gewijzigd. Men noemt dit ook het *append-only* mechanisme.[146] Dit betekent dat wanneer iets wordt opgeslagen in de blockchain, het er definitief in opslagen is, met een zeer beperkte mogelijkheid tot wijziging achteraf.

In theorie bestaat de mogelijkheid dat gegevens alsnog kunnen worden gewijzigd. Let wel, in de praktijk zal dit bijna onhaalbaar zijn. De enige mogelijkheid om alsnog gegevens te wijzigen is door medewerking van de meerderheid van de nodes waarbij deze opnieuw consensus dienen te bereiken omtrent de desbetreffende transactie en alle daaropvolgende transacties, ditmaal van achter naar voren, waarbij de hele blockchain vanaf het desbetreffende block moet 'losgemaakt' worden en nadien terug vastgemaakt.[147] Dit zou een enorme computerkracht vergen en daarnaast ook de samenwerking van meer dan de helft van de nodes, wat praktisch niet haalbaar is.[148] Ondertussen is de hele blockchain ook geblokkeerd wat betekent dat er ondertussen geen transacties kunnen plaatsvinden.[149] Dit is vanuit operationeel oogpunt niet wenselijk.

---

[144] Artikel 3, tweede lid GDPR
[145] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.19
[146] Zie K. HEINES, "The Risks and Rewards of Blockchain Technology", *Risk Management* 2016, *Afl. 4, p.6-7;* D. DRESCHER, "*Blockchain basics: a non-technical introduction in 25 steps*", New York, Apress, 2017, 255 p.
[147] M. BERBERICH en S. MALGORZATA, "Blockchain technology and the GDPR: How to reconcile privacy and distributed ledgers", *European Data Protection Law Review* 2016, Volume 2, Afl.3, p.422 - 426
[148] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.36
[149] J. TENNISON, "What is the impact of blockchains on privacy?", Open Data Institute, 12 november 2015, https://theodi.org/blog/impact-of-blockchains-on-privacy

Wanneer we deze eigenschap van blockchaintechnologie bekijken in het licht van de GDPR, lijkt het meteen duidelijk dat deze zou kunnen botsen met enkele algemene beginselen en rechten die worden gewaarborgd in de GDPR. Deze algemene beginselen en rechten worden naderhand apart verder besproken.

§ 1. Recht op gegevenswissing

Het recht op gegevenswissing wordt ook wel eens het 'recht om vergeten te worden' of het 'recht op vergetelheid' genoemd en werd erkend door het Hof van Justitie in 2014 in de *Google Spain* zaak.[150]

Artikel 17 van de GDPR versterkt dit recht zoals erkend door het Hof in 2014 door aan elke betrokkene het recht te geven om van de verwerkingsverantwoordelijke wissing van de hem betreffende persoonsgegevens te verkrijgen onder bepaalde voorwaarden, namelijk wanneer (a) de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld, (b) de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking is, (c) de betrokkene bezwaar maakt tegen de verwerking en er geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking zijn, (d) de persoonsgegevens onrechtmatig zijn verwerkt, (e) de persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting of (f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.[151]

Het recht op gegevenswissing is geen absoluut recht: wanneer de verwerkingsverantwoordelijke verplicht is om bepaalde persoonsgegevens te wissen, *"neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen (...)."*[152] Deze bepaling zou zo kunnen worden geïnterpreteerd dat er in het geval van blockchaintechnologie een alternatieve oplossing mag worden gezocht, aangezien in het geval van blockchaintechnologie meer dan redelijke maatregelen noodzakelijk zijn.

Al het bovenstaande is niet van toepassing voor zover verwerking nodig is voor (a) het uitoefenen van het recht op vrije meningsuiting en informatie, (b) het nakomen van een wettelijke verplichting, het vervullen van een taak van algemeen belang of het uitoefenen van openbaar gezag, (c) redenen van algemeen belang op het gebied van volksgezondheid, (d)

[150] HvJ 13 mei 2014, nr. C131/12, ECLI:EU:C:2014:317, 'Google Spain'
[151] Artikel 17, eerste lid GDPR; Overweging 65 GDPR
[152] Artikel 17, tweede lid GDPR

archiveringsdoeleinden of (e) het instellen, uitoefenen of onderbouwen van een rechtsvordering.[153]

Het is meteen duidelijk dat het waarborgen van dit recht problematisch kan zijn. Het permanente karakter van de blockchain verhindert het zomaar wissen van gegevens: eens deze zijn vastgelegd, zijn ze blijvend opgeslagen en praktisch onmogelijk te verwijderen.

Wanneer we kijken naar artikel 17, eerste lid (a) GDPR, lezen we dat het recht op gegevenswissing onder meer van toepassing is wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze werden verzameld. De manier waarop een blockchain technisch functioneert, zou kunnen worden gebruikt als argument om aan te geven dat de persoonsgegevens in kwestie nog steeds nodig zijn voor de doeleinden waarvoor ze werden verzameld.[154] Een blockchain is namelijk technisch ontworpen als een ketting die permanent is en steeds langer wordt, wat betekent dat de persoonsgegevens die erin vervat liggen nog steeds noodzakelijk zijn.

Een andere mogelijkheid die in de toekomst misschien werkelijkheid kan worden, is de volgende. Zoals reeds vermeld, bevat artikel 17, eerste lid (b) het recht om gegevenswissing te verkrijgen wanneer de betrokkene de toestemming intrekt en er geen andere rechtsgrond is voor de verwerking. Het zou kunnen dat de kern van het technisch functioneren van een technologie in de toekomst aanvaard wordt als rechtsgrond die verdere verwerking toch kan rechtvaardigen.[155]

Persoonsgegevens off-chain opslaan kan een oplossing bieden, aangezien er dan geen wijzigingen dienen te gebeuren aan de blockchain zelf maar enkel aan de externe database. Let wel, dit biedt louter een oplossing voor de transactiegegevens; de publieke sleutel dient steeds opgeslagen te blijven in de blockchain.[156] Zoals reeds werd vermeld, gaat dit in sommige gevallen wel voorbij aan het idee achter blockchaintechnologie, namelijk het overbodig maken van een tussenpersoon. Dit omdat deze externe database wel een centraal beheer kan kennen. Indien dit zo is, stelt zich opnieuw hetzelfde probleem.

Er kan worden besloten dat het recht op gegevenswissing praktisch zeer moeilijk kan worden afgedwongen. Dit vanwege het feit dat blockchaintechnologie werd ontwikkeld met het totaal

[153] Artikel 17, derde lid GDPR; Overweging 65 GDPR
[154] M. BERBERICH en S. MALGORZATA, "Blockchain technology and the GDPR: How to reconcile privacy and distributed ledgers", *European Data Protection Law Review* 2016, Volume 2, Afl.3, p.422 - 426
[155] *Ibid.*
[156] *Ibid.*

omgekeerde principe aan de basis, namelijk een database met een *append-only* mechanisme waarin gegevens aanpassen zeer moeilijk tot onmogelijk is.[157] Het recht op gegevenswissing, dat een aanpassing van bepaalde blokken van gegevens vergt, staat hier haaks op. In de tekst van de GDPR zoals deze op vandaag bestaat, kunnen moeilijk oplossingen worden gevonden. Het valt daarentegen niet uit te sluiten dat toekomstige interpretaties van de tekst het mogelijk kunnen maken dat blockchaintechnologie alsnog voldoet aan de eisen die de wetgeving stelt op vlak van gegevenswissing. Daarnaast is het ook mogelijk om persoonsgegevens off-chain op te slaan en om op die manier te voldoen aan de vereisten die de wetgeving stelt.

§ 2. Recht op rectificatie

Het recht op rectificatie wordt gewaarborgd in artikel 16 van de GDPR en stelt dat "*de betrokkene [het recht heeft] om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken*."[158]

Het recht op rectificatie is tweeledig en wil aan de betrokkene het recht verschaffen om incorrecte gegevens te wijzigen en wil daarnaast ook waarborgen dat een betrokkene ten allen tijd onvolledige gegevens kan aanvullen. Dit artikel hangt ook nauw samen met het algemeen beginsel van juistheid dat stelt dat *"persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren."*[159] Dit kadert volledig in het verhaal dat de Europese Unie wil brengen met deze regelgeving, namelijk meer controle over persoonsgegevens geven aan de betrokkene zelf.

Het is op grond van de GDPR voor de betrokkene dus mogelijk om een aanpassing van zijn of haar persoonsgegevens te vragen aan de verwerkingsverantwoordelijke. In wat voorafging werd reeds duidelijk dat het niet eenvoudig is om te bepalen wie de verwerkingsverantwoordelijke is. Wat wel duidelijk is, is dat het niet over één entiteit gaat, wat betekent dat er ontelbaar veel entiteiten moeten worden geïdentificeerd en geadresseerd, wat praktisch onmogelijk is.[160] Stel

[157] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[158] Artikel 16 GDPR; Overweging 65 GDPR
[159] Artikel 5, eerste lid (d) GDPR
[160] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.21-22

dat dit toch zou lukken en een betrokkene slaagt erin om zijn verzoek te richten naar alle nodes, dan zijn de nodes technisch niet in staat om de gevraagde wijzigingen door te voeren. Een blockchain is immers permanent, wat betekent dat gegevens zeer moeilijk tot onmogelijk kunnen worden gewijzigd.

Een zinsnede uit artikel 16 kan misschien toch een oplossing bieden. Er staat te lezen dat *"de betrokkene het recht [heeft] vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken."*[161] Dit laatste zou kunnen betekenen dat het recht op rectificatie kan worden gewaarborgd indien de foutieve informatie wordt gecorrigeerd door middel van correcte, aanvullende informatie in een nieuw blok.[162] Het append-only mechanisme staat hieraan niet in de weg, maar de foutieve gegevens zijn hierdoor uiteraard niet verwijderd uit de blockchain. Het is een stap in de goede richting, maar ook deze mogelijkheid zorgt niet voor het volledig waarborgen van het recht op rectificatie.

Ook hier kan persoonsgegevens off-chain opslaan een oplossing bieden, aangezien de wijzigingen dan buiten de blockchain zelf kunnen plaatsvinden. Zoals reeds gezegd is dit enkel een oplossing voor de transactiegegevens en niet voor de publieke sleutel.

De combinatie van een moeilijke tot onmogelijke identificatie van de verwerkingsverantwoordelijke en het append-only mechanisme staat een vlotte uitvoering van het recht op rectificatie in de weg. Off-chain opslag kan voor wat de transactiegegevens betreft, deels een oplossing bieden.

§ 3. Recht op beperking van de verwerking

Artikel 18 van de GDPR bevat het recht op beperking van de verwerking en geeft de betrokkene het recht om van de verwerkingsverantwoordelijke in bepaalde gevallen de beperking van de verwerking te verkrijgen.[163] Het gaat om gevallen waarin (a) de juistheid van de persoonsgegevens wordt betwist, (b) de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen van de persoonsgegevens, (c) de verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft maar de betrokkene wel, namelijk voor het instellen, uitoefenen of onderbouwen van een rechtsvordering, (d) de betrokkene bezwaar heeft gemaakt

[161] Artikel 16 GDPR
[162] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.21-22
[163] Artikel 18, eerste lid GDPR

tegen de verwerking en een antwoord afwacht op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder doorwegen.[164]

In de gevallen waarin de verwerking is beperkt, worden persoonsgegevens, behalve de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor het instellen, uitoefenen of onderbouwen van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang.[165]

Voor een goed begrip geef ik nog graag de definitie van 'verwerking' mee zoals deze beschreven staat in de GDPR: *"Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens"*.[166]

Stel dat onjuiste persoonsgegevens worden opgenomen in een blockchain. Of dit per ongeluk of moedwillig gebeurt, heeft geen belang. In dergelijk geval heeft de betrokkene het recht om beperking van de verwerking te vragen aan de verwerkingsverantwoordelijke. Dit betekent dat de gegevens opgeslagen mogen blijven, maar dat er verder niets mag gebeuren met de gegevens. Dit houdt ook in dat telkens, automatisch, een nieuwe kopie maken die wordt opgeslagen op de computer van een nieuwe deelnemer aan het netwerk, niet toegestaan is. Ook het telkens opnieuw updaten van de volledige blockchain, betekent dat de persoonsgegevens blijvend opnieuw worden verwerkt.

Ook hier botst de GDPR botst met het permanente karakter van de blockchain. Het is namelijk onmogelijk om de desbetreffende persoonsgegevens eruit te halen en niet verder te verwerken. De persoonsgegevens kunnen niet worden gewist, wat betekent dat ze telkens opnieuw zullen worden verwerkt voor het berekenen van hashwaarden en dat ze telkens opnieuw zullen worden gekopieerd en geüpdatet. Wanneer persoonsgegevens worden opgeslagen op de blockchain, kan het recht op beperking van de verwerking niet worden gewaarborgd. Off-chain opslag zou ook in dit geval een oplossing kunnen bieden voor het beperken van de verwerking van transactiegegevens.

[164] *Ibid.*
[165] Artikel 18, tweede lid GDPR
[166] Artikel 4(2) GDPR

§ 4. Gegevensbescherming door ontwerp en door standaardinstellingen

Dit beginsel werd reeds besproken in het vorige hoofdstuk; een uitgebreide bespreking is daar terug te vinden (zie *supra*, 2.2.2 Gedecentraliseerd en gedistribueerd, § 3. Gegevensbescherming door ontwerp en standaardinstellingen). Het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen is echter ook hier van belang. Het permanente karakter van blockchaintechnologie valt namelijk moeilijk tot zelfs helemaal niet te verzoenen met het beginsel van gegevensbescherming door ontwerp. Ervoor kiezen om persoonsgegevens permanent te bewaren zonder mogelijkheid tot verwijderen van deze gegevens, strookt niet met het beginsel van gegevensbescherming door ontwerp.

§ 5. De algemene beginselen van minimale gegevensverwerking en van opslagbeperking

Het beginsel van minimale gegevensverwerking stelt dat *persoonsgegevens "toereikend [moeten] zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt."* [167] Dit houdt onder meer in dat het noodzakelijk is *dat "ervoor wordt gezorgd dat de opslagperiode […] tot een strikt minimum wordt beperkt."*[168]

Daarnaast definieert de GDPR nog eens apart het algemeen beginsel van opslagbeperking, dat inhoudt *dat "persoonsgegevens [moeten] worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt, noodzakelijk is"*.[169] Er wordt een uitzondering voorzien voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of de verwerking voor statistische doeleinden.

Een blockchain is per definitie een ketting van blokken die steeds langer wordt.[170] Het groeiende karakter van de blockchain in combinatie met de gedistribueerde opslag staat haaks op het beginsel van minimale gegevensverwerking, dat van de verwerkingsverantwoordelijke verlangt dat hij geen gegevens verwerkt die niet toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is.[171]

Tijdens de eerste en oorspronkelijke transactie zijn de persoonsgegevens beperkt tot wat noodzakelijk is voor de doeleinden van de verwerking. Er worden geen overbodige

[167] Artikel 5, eerste lid (c) GDPR
[168] Overweging 39 GDPR
[169] Artikel 5, eerste lid (e) GDPR
[170] S. NAKAMOTO, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, https://bitcoin.org/bitcoin.pdf.
[171] M. FINCK, "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper*, No. 18-01, 2017, p.20-21

persoonsgegevens gevraagd om een transactie mogelijk te maken. Toch is dit na deze eerste oorspronkelijke transactie niet meer het geval. Aangezien deze persoonsgegevens steeds opnieuw en blijvend worden verwerkt door het maken van kopieën en updates, kan worden beargumenteerd dat de persoonsgegevens in kwestie vanaf dan verwerkt worden buiten wat noodzakelijk is voor de doeleinden van de verwerking.

Ook het beperken van de opslagperiode wordt in een blockchain niet gerespecteerd. Persoonsgegevens blijven per definitie opgeslagen tot op het moment dat de blockchain ophoudt te bestaan en wanneer dit moment plaatsvindt, valt niet vooraf met zekerheid te zeggen.[172] Er zijn geen mechanismen in werking die zorgen voor een beperking van de opslagperiode.

Daarnaast lijkt ook het algemeen beginsel van opslagbeperking niet te worden gerespecteerd, aangezien er geen moment is waarop alle persoonsgegevens in de blockchain worden geanonimiseerd. Alles blijft pseudoniem opgeslagen. De vraag kan natuurlijk worden gesteld of deze opslag noodzakelijk is. Wanneer men beargumenteert dat het wel degelijk noodzakelijk is voor het technisch functioneren van de blockchain dat persoonsgegevens niet worden geanonimiseerd maar pseudoniem bewaard blijven, zou men kunnen stellen dat dit algemeen beginsel niet wordt geschonden door persoonsgegevens pseudoniem in de plaats van anoniem op te slaan.

Wanneer persoonsgegevens off-chain zouden worden opgeslagen, wordt er wat betreft de transactiegegevens, verholpen aan deze problemen. Off-chain bestaat namelijk wel de mogelijkheid om bepaalde verwerkingen te stoppen of om persoonsgegevens na een bepaalde termijn te wissen of anonimiseren. De publieke sleutel dient zoals steeds opgeslagen te blijven op de blockchain zelf, wat betekent dat er wat betreft de publieke sleutel niet aan het probleem wordt verholpen.

Toekomstige interpretaties van de wet, of eventuele additionele wetgeving gericht op distributed ledger technologieën en blockchaintechnologie, zullen uitwijzen of en hoe aan deze knelpunten kan worden verholpen.

[172] *Ibid.*

2.3. Besluit

Na een grondige toetsing van de vormende elementen van blockchaintechnologie aan de vereisten die worden gesteld door de GDPR, kwamen enkele knelpunten aan het licht. Het werd zeer duidelijk dat de GDPR niet werd ontworpen met decentrale opslag van persoonsgegevens in het achterhoofd, waardoor de wetgeving dan ook niet is aangepast aan deze vorm van opslag en op sommige punten onvermijdelijk botst met blockchaintechnologie.

Het versleutelde karakter van blockchaintechnologie stelt geen problemen en is integendeel zelfs een kenmerk van de technologie dat ten zeerste in lijn is met de geest en de bepalingen van de GDPR, die pseudonimisering aanmoedigt. Het is daarentegen wel belangrijk om te onthouden dat de ontwikkelaar van de blockchain zelf beslist hoe sterk de mate van versleuteling is die hij implementeert. Sommige blockchains zullen daardoor zeer sterk versleuteld tot zelfs anoniem kunnen zijn, andere blockchains zullen op dit punt minder waarborgen bieden. Of een blockchain voldoende waarborgen biedt, zal steeds geval per geval en dus per blockchain moeten worden onderzocht.

Het gedecentraliseerde en gedistribueerde karakter van de blockchain, geeft wel aanleiding tot enkele moeilijkheden. De grootste uitdaging stelt zich op het vlak van de verwerkingsverantwoordelijke. Het blijkt onhaalbaar om een verwerkingsverantwoordelijke aan te wijzen in het geval van een open en publieke blockchain. Er worden drie hypotheses aangehaald en uitgewerkt (de nodes, de miners of de betrokkene zelf zouden kunnen kwalificeren als verwerkingsverantwoordelijke), maar geen van deze drie hypotheses kan voldoende overtuigen. Dit leidt ertoe dat het waarborgen van verschillende rechten, zoals bijvoorbeeld het recht op inzage, onder druk komen te staan aangezien er geen verantwoordelijke kan worden aangeduid die hiervoor moet instaan. Het gedecentraliseerde karakter leidt er ook toe dat een hoge mate van transparantie noodzakelijk is om het netwerk consensus te laten bereiken. Het feit dat alle gegevens zichtbaar zijn voor iedereen, toch in de blockchain zoals deze oorspronkelijk werd bedacht, kan vanuit privacyoogpunt als onwenselijk worden beschouwd. Tot slot worden ook de regels omtrent doorgiften aan landen buiten de Europese Unie en grensoverschrijdende verwerkingen aangehaald omdat het gedistribueerde karakter ertoe leidt dat deze regels toepassing vinden.

Het derde en laatste vormend element dat wordt besproken is het permanente karakter van blockchaintechnologie. Deze eigenschap van blockchaintechnologie leidt ertoe dat het onhaalbaar is om gegevens te wijzigen in een blockchain en zorgt voor de meeste

moeilijkheden. Het leidt ertoe dat het recht op gegevenswissing, het recht op rectificatie en het recht op beperking van de verwerking niet kunnen worden gewaarborgd. Daarnaast is het ook in strijd met de algemene beginselen van minimale gegevensverwerking en van opslagbeperking en met het principe van gegevensbescherming door ontwerp en door standaardinstellingen. Het permanent bewaren van persoonsgegevens, ook wanneer deze voor geen enkel doeleinde nog noodzakelijk blijken, valt niet te verzoenen met de geest en de bepalingen van de GDPR.

De mogelijkheid tot off-chain opslag van persoonsgegevens of het gebruik van geavanceerde encryptietechnieken kan oplossingen bieden. Deze mogelijkheden worden dan ook verder uitgediept in het volgende hoofdstuk. Hierin worden aanbevelingen geformuleerd, gericht aan de ontwikkelaars van blockchains, die kunnen helpen om een zo hoog mogelijke mate van pseudonimiteit of zelfs anonimiteit te bereiken.

Toekomstige interpretaties van de GDPR, of een eventuele *lex specialis* gericht op distributed ledger technologieën en blockchaintechnologie, zullen aantonen of en op welke manier aan deze onverenigbaarheden kan worden tegemoetgekomen.

3. Aanbevelingen voor een GDPR-conforme blockchain

Er werd aangetoond dat de GDPR en blockchaintechnologie op bepaalde punten botsen. In wat volgt worden verschillende aanbevelingen gedaan voor het implementeren van maatregelen die de bescherming van persoonsgegevens verhogen. Implementatie van deze maatregelen zou in de toekomst eventueel kunnen leiden tot het aanvaarden van blockchains als een manier om persoonsgegevens conform de GDPR te verwerken, of zou de toepassing van de GDPR kunnen ontwijken door te slagen in volledige anonimisering. De tijd zal uitwijzen in welke richting de interpretatie van de GDPR en blockchaintechnologie beiden evolueren.

Een eerste stap voorafgaand aan het ontwikkelen van een nieuwe blockchain waarin persoonsgegevens worden verwerkt, is het uitvoeren van een gegevensbeschermingseffect-beoordeling. De GDPR verplicht de verwerkingsverantwoordelijke om, *"wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, vóór de verwerking een beoordeling uit [te voeren] van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens."*[173] Deze beoordeling zal noodzakelijk zijn om na te gaan of de rechten van de betrokken op vlak van bescherming van persoonsgegevens al dan niet worden geschonden.[174]

Het is belangrijk om vooraf duidelijk te stellen dat er geen perfecte oplossing bestaat en dat het voor ontwikkelaars een dagelijkse zoektocht blijft naar goede methodes en technieken. Of zoals Vitalik Buterin het zegt: *"with privacy, as we see, there is no magic bullet. While there are partial solutions for specific use cases, and often these partial solutions offer a high degree of flexibility, the abstractions that they present are quite different from what developers are used to."*[175]

Onderstaande lijst van aanbevelingen en illustraties is niet extensief en dient louter om aan te tonen dat ontwikkelaars verschillende paden kunnen, en mijn inziens, dienen te bewandelen om een zo hoog mogelijk niveau van bescherming van persoonsgegevens te realiseren.

---

[173] Artikel 35, eerste lid GDPR

[174] J. TENNISON, "What is the impact of blockchains on privacy?", Open Data Institute, 12 november 2015, https://theodi.org/blog/impact-of-blockchains-on-privacy

[175] V. BUTERIN, "Privacy on the blockchain, 15 januari 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain

3.1. Geavanceerde encryptietechnieken

Geavanceerde encryptietechnieken kunnen zorgen voor een toenemende mate van pseudonimiteit en in de toekomst misschien leiden tot anonimiteit. De Artikel 29 Werkgroep benadrukt dat het feit of een encryptietechniek al dan niet zorgt voor anonimisering, steeds geval per geval moet worden bekeken.[176] Het is belangrijk om vooraf duidelijk te stellen dat het niet mogelijk is om te zeggen welke geavanceerde encryptietechnieken voldoende waarborgen bieden en welke niet. Dit moet steeds voor elke blockchain apart en in het licht van de andere maatregelen worden bekeken. Enkel zo kan een correcte beoordeling worden gemaakt.

In wat volgt worden twee voorbeelden gegeven van blockchains die gebruik maken van geavanceerde encryptietechnieken die leiden tot een zeer hoge mate van pseudonimisering en volgens sommigen zelfs anonimisering [177]. Blockchains zoals Zcash en Monero verhogen de privacy van de gebruikers door de oorsprong, bestemming en inhoud van een transactie te verbergen.[178]

De geavanceerde encryptietechnieken die in deze blockchains worden gebruikt zijn *zero-knowledge proofs* bij Zcash en *ring signatures* en *stealth addresses* bij Monero.[179] Zero-knowledge proofs[180] is een methode waarbij één partij kan bewijzen aan de andere partij dat ze iets weet, zonder daarbij enige andere informatie te ontsluiten en waarbij de andere partij dit aanvaardt.[181] De sterke garanties die Zcash kan bieden op vlak van privacy komen voort uit het feit dat het netwerk erin slaagt consensus te bereiken, ook al zijn de gegevens volledig

[176] Advies 05/2014 van de Artikel 29 Werkgroep over anonimiseringstechnieken
[177] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.67; E. BEN SASSON et.al., "Zerocash: Decentralized Anonymous Payments from Bitcoin*", IEEE Symposium on Security and Privacy* 2014, p.459-474
[178] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.67
[179] E. BEN SASSON et.al., "Zerocash: Decentralized Anonymous Payments from Bitcoin*", IEEE Symposium on Security and Privacy* 2014, p.459-474; A. MACKENZIE, S. NOETHER en het Monero Core Team: "Improving Obfuscation in the Cryptonote Protocol", 26 januari 2015, https://lab.getmonero.org/pubs/MRL-0004.pdf
[180] Wikipedia, "Zero-knowlegde proof", https://en.wikipedia.org/wiki/Zero-knowledge_proof
[181] Een eenvoudig voorbeeld om dit te duiden, is het volgende. Stel je hebt een rode en een groene bal die voor de rest identiek zijn, en een kleurenblinde vriend. Jij ziet het verschil in kleur, je vriend uiteraard niet: in zijn ogen zijn beide ballen identiek. Je wil aan hem bewijzen dat beide ballen verschillend zijn, maar niet prijsgeven welke bal groen is en welke rood. Het systeem werkt als volgt. Je geeft beide ballen aan je vriend en vraagt hem om deze achter zijn rug te houden. Daarna toont hij één van beide ballen en verbergt deze nadien terug achter zijn rug. Vervolgens kan hij kiezen om de ballen achter zijn rug om te wisselen, of niet. Hij zal dan vragen of je denkt dat hij de ballen heeft omgewisseld of niet. Je hoeft niet te gokken, want je kan duidelijk zien of de groene of de rode bal getoond wordt. Dit wordt zo vaak herhaald als nodig is om je vriend te overtuigen dat jij weet dat de ballen inderdaad een verschillende kleur hebben. Wanneer je dit tientallen keren herhaalt, is de kans dat je er steeds op goed geluk in slaagt om het antwoord juist te hebben, zo goed als onbestaande. Het bewijs dat je geleverd hebt is *zero-knowledge*, aangezien je vriend nooit te weten komt welke bal welke kleur heeft of hoe deze kunnen worden onderscheiden. Hij vergaart dus geen kennis, hij weet enkel dat jij deze kennis wel hebt.

versleuteld, hierbij gebruik makend van *zk-SNARK proofs*.[182] Dit acroniem staat voor *"Zero-Knowledge Succinct Non-Interactive Argument of Knowledge"* en verwijst naar een constructie waarbij iemand het beschikken over bepaalde correcte informatie kan aantonen (de *prover*), bijvoorbeeld een private sleutel of een hashwaarde, zonder deze informatie te moeten onthullen aan een ander (de *verifier*) en zonder interactie tussen beide partijen.[183] Omdat deze informatie niet onthuld moet worden, moet ze niet publiekelijk op de blockchain worden geplaatst, wat betekent dat Zcash de identiteit van gebruikers, de inhoud van transacties en de balans van de accounts kan afschermen.[184] Enkel het tijdstip waarop een transactie plaatsvond, zal zichtbaar zijn. De encryptietechniek van zero-knowledge proofs is veelbelovend en kan de toepassingen waarvoor blockchaintechnologie kan worden gebruikt, aanzienlijk verhogen.[185]

Monero gebruikt onder meer ring signatures en stealth adresses als privacyverhogende maatregelen.[186] Een ring signature is een digitale handtekening die kan worden uitgevoerd door eender welk lid van een groep gebruikers die elk over bepaalde sleutels beschikken. De belangrijkste eigenschap van ring signatures is dat het onhaalbaar moet zijn om te bepalen welke sleutel van welk groepslid werd gebruikt om de transactie te ondertekenen.[187] Dit betekent dat ring signatures ervoor zorgen dat niet kan worden achterhaald wie de zender van een transactie is.[188]

Om af te schermen wie de ontvanger is, worden stealth addresses gebruikt. Deze adressen staan toe en vereisen dat de afzender voor elke transactie willekeurige eenmalige adressen aanmaakt namens de ontvanger. De ontvanger kan ervoor kiezen om slechts één adres te publiceren, maar al zijn inkomende betalingen gaan naar unieke adressen op de blockchain, waar ze niet kunnen worden gelinkt aan het gepubliceerde adres van de ontvanger of de adressen van andere transacties.[189] Door het gebruik van stealth-adressen kunnen enkel de afzender en ontvanger bepalen waar een betaling naartoe is gestuurd.[190]

---

[182] E. BEN SASSON et.al., "Zerocash: Decentralized Anonymous Payments from Bitcoin*", IEEE Symposium on Security and Privacy 2014*, p.459-474
[183] *Ibid.*
[184] *Ibid.*
[185] V. BUTERIN, "Privacy on the blockchain, 15 januari 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain
[186] A. MACKENZIE, S. NOETHER en het Monero Core Team: "Improving Obfuscation in the Cryptonote Protocol", 26 januari 2015, https://lab.getmonero.org/pubs/MRL-0004.pdf
[187] Wikipedia, "Ring signature", https://en.wikipedia.org/wiki/Ring_signature
[188] Monero, "Ring Signature", https://getmonero.org/resources/moneropedia/ringsignatures.html
[189] Monero, "Stealth Address", https://getmonero.org/resources/moneropedia/stealthaddress.html
[190] *Ibid.*

Het bedrag van de transactie wordt verborgen door het gebruik van *ring confidential transactions*, wat een methode van *obfuscation* is.[191] Hier wordt in het volgende hoofdstuk dieper op ingegaan (zie *infra*).

De besproken technieken verhogen de privacy op de blockchain en kunnen in de toekomst misschien leiden tot anonieme blockchains waarop de GDPR ofwel niet van toepassing zal zijn, of die ofwel worden aanvaard door de Europese regelgever.

3.2. *Obfuscation*

Naast de mogelijkheid om gebruik te maken van geavanceerde encryptietechnieken, kunnen ontwikkelaars van blockchains ook gebruik maken van *obfuscation* om persoonsgegevens te verbergen op de blockchain. In het Nederlands betekent obfuscation zoveel als 'versluieren' of 'verduisteren' en in deze context betekent het dat ontwikkelaars *"misleidende, dubbelzinnige en plausibele maar verwarrende informatie opnemen in hun code om bepaalde zaken te verbergen"*.[192] Hierdoor wordt het lezen van de werkelijke inhoud van een bepaalde transactie of communicatie erg bemoeilijkt. Het is niet ondenkbaar dat blockchains in anonieme netwerken kunnen veranderen wanneer obfuscation wijdverspreid en massaal wordt toegepast.[193]

CoinJoin, een vorm van *mixing*[194], is een methode die valt onder obfuscation[195] en die wordt gebruikt door gebruikers van de Bitcoinblockchain om hun identiteit te verbergen.[196] Een gebruiker die CoinJoin wil gebruiken, gaat opzoek naar een ander gebruiker die, net zoals hij, een transactie wilt 'vermengen'. Ze starten dan samen een *joint transaction*. Het verzendingsadres wordt beschouwd als input, het adres van de ontvanger als output. CoinJoin versluiert de transactie door meerdere inputs en meerdere outputs te combineren of te vermengen, waardoor slechts één transactie wordt opgenomen in de blockchain. Op deze manier is het niet mogelijk om de inputs en outputs te combineren.[197] Stel dat Alice een betaling

[191] S. NOETHER, A. MACKENZIE en het Monero Core Team: "Ring Confidential Transactions", februari 2016, https://lab.getmonero.org/pubs/MRL-0005.pdf
[192] F. BRUNTON en H. NISSENBAUM, "Political and ethical perspectives on data obfuscation", *Privacy, Due Process and the Computational Turn* 2013, p.164-188.
[193] P. DE FILIPPI en A. WRIGHT, *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, p.39
[194] In het geval van *mixing* worden transacties vermengd, waardoor het zeer moeilijk wordt om na te gaan wie de verzender en wie de ontvanger van een transactie is.
[195] A. NARAYANAN en M. MÖSER, "Obfuscation in Bitcoin: Techniques and Politics", *International Workshop on Obfuscation: Science, Technology, and Theory* 2017
[196] G. MAXWELL, "CoinJoin: Bitcoin privacy for the real world", 22 augustus 2013, https://bitcointalk.org/index.php?topic=279249
[197] *Ibid.*

doet aan Bob, Carol een betaling doet aan Dave en Eve een betaling doet aan Frank. Zonder het gebruik van CoinJoin, worden er drie aparte transacties opgenomen in de blockchain. Door gebruik te maken van CoinJoin wordt slechts één transactie opgenomen. Er zal te lezen staan dat Alice, Carol en Eve een betaling hebben gedaan en dat Bob, Dave en Frank een betaling hebben ontvangen, maar wie aan wie betaald heeft, zal niet kunnen worden afgeleid uit de informatie die opgeslagen is op de blockchain.[198] Ondertussen zijn er reeds verschillende implementaties gekend, waarvan Dark Wallet de meest bekende is.

Het gebruik van deze methode werkt privacyverhogend, maar er is wel een combinatie met andere technieken nodig, aangezien het bedrag van de transactie de identiteit eenvoudig kan onthullen. Stel dat Alice 1 Bitcoin heeft betaald een Bob en Carol 2 Bitcoin heeft betaald aan Dave, en nadien is zichtbaar op de Blockchain dat Bob 1 Bitcoin meer heeft dan ervoor en Dave 2 Bitcoin meer heeft dan voor de transactie, dan hoeft men geen genie te zijn om te achterhalen wie de zender van de transactie was. CoinJoin kan dus enkel zonder additionele maatregelen werken indien alle zenders exact hetzelfde bedrag overmaken aan de ontvanger. Is dit niet zo, dan moet bovenop het mixen gebruik worden gemaakt van *confidential signatures*, die het bedrag verbergen.[199] Bij Monero wordt er bijvoorbeeld gebruik gemaakt van *ring confidential signatures* om het bedrag van de transactie te verbergen.[200] Hierbij wordt er net genoeg informatie vrijgegeven zodat het netwerk de authenticiteit kan valideren en consensus kan bereiken, maar blijft het bedrag van de transactie verborgen.

Obfuscation kan op verschillende manieren bereikt en toegepast worden. Het is een techniek die de bescherming van persoonsgegevens aanzienlijk kan verhogen en waar best rekening mee wordt gehouden bij het ontwikkelen van een nieuwe blockchain. Net zoals bij geavanceerde encryptietechnieken zou een hoge mate van obfuscation misschien kunnen leiden tot een anonieme blockchain waarop de GDPR niet op van toepassing zal zijn of een blockchain die wordt aanvaard als conform de wetgeving. De tijd zal dit uitwijzen.

[198] Investopedia.com, “Coinjoin”, https://www.investopedia.com/terms/c/coinjoin.asp
[199] A. BACK, “Bitcoins with homomorphic value (validatable but encrypted)”, 1 oktober 2013, https://bitcointalk.org/index.php?topic=305791.0
[200] S. NOETHER, A. MACKENZIE en het Monero Core Team: “Ring Confidential Transactions”, februari 2016, https://lab.getmonero.org/pubs/MRL-0005.pdf

3.3. Off-chain opslag van persoonsgegevens

Off-chain opslag van (persoons)gegevens betekent zoveel als het verhuizen van gegevens van de blockchain naar een andere opslaglocatie, server of derde partij.[201] Dit gebeurt in de meeste gevallen om de blockchain te ontlasten, aangezien het aantal transacties dat een blockchain kan verwerken per seconde, beperkt is.[202] Men noemt dit het schaalbaarheidsprobleem van blockchains.[203] Daarnaast worden per transactie op de blockchain, transactievergoedingen aangerekend door de miners.[204] Door transacties buiten de blockchain te laten plaatsvinden, vermijdt men het betalen van deze vergoedingen. Een derde belangrijke reden tot slot om gebruik te maken van off-chain opslag is om meer privacywaarborgen te creëren, aangezien alle gegevens op de blockchain doelbewust transparant zijn. Off-chain transacties vinden niet op de blockchain plaats, wat maakt dat ze niet zichtbaar zijn voor iedereen. Dit is vanuit privacyoogpunt zeer interessant.

Wanneer men off-chain opslag overweegt, is het belangrijk om ervoor te zorgen dat de fundamentele eigenschappen van blockchaintechnologie niet worden ondergraven en dat het systeem zonder vertrouwen kan blijven, wat betekent dat er geen vertrouwen in anderen noodzakelijk is om toch veilig gebruik te kunnen maken van het systeem.[205]

Off-chain opslag zorgt er dus voor dat persoonsgegevens verhuizen naar een andere locatie. Dit zou betekenen dat de GDPR niet meer van toepassing is op blockchains waarin geen persoonsgegevens worden verwerkt. De GDPR zal dan wel van toepassing zijn op deze andere

---

[201] J. EBERHARDT en S. TAI "On or Off the Blockchain? Insights on Off-Chaining Computation and Data", september 2017, *Springer International Publishing, Lecture Notes in Computer Science, LNCS-10465*, p.2

[202] De Bitcoinblockchain kan momenteel tot maximaal 7 transacties per seconde verwerken, de Ethereumblockchain tot 15 transacties per seconde. Wanneer we dit bekijken in het licht van andere betalingsplatformen zoals bijvoorbeeld Visa, dat gemiddeld 24.000 transacties per seconde kan verwerken, met soms zelfs pieken tot 47.000 transacties per seconde, kunnen we de snelheid waaraan een blockchain transacties verwerkt, beschouwen als zeer gelimiteerd. Zie Blockchain.info, "Bitcoin Charts", https://blockchain.info/charts/n-transactions; Ethereum.org, "Data and network stats", https://ethstats.net; Visa, "Power Your Retail Business beyond the Point of Sale", https://usa.visa.com/run-your-business/small-business-tools/retail.html; M. TRILLO, "Stress Test Prepares VisaNet for the Most Wonderful Time of the Year", oktober 2013, http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/ index.html

[203] K. CROMAN, C. DECKER, I. EYAL, A. E. GENCER, A. JUELS, A. KOSBA, A. MILLER, P. SAXENA, E. SHI, E. G. SIRER, D. SONG en R. WATTENHOFER, "On Scaling Decentralized Blockchains", *Financial Cryptography Workshops* 2016, p.1

[204] Blockchain.info, "Total Transaction Fees", https://blockchain.info/nl/charts/transaction-fees; Ethereum.org, "Data and network stats", https://ethstats.net/ (noteer dat op de Ethereumblockchain een transactie 'gas' kost: de vergoeding die dient te worden betaald voor een transactie is de vereiste hoeveel gas vermenigvuldigd met de gasprijs).

[205] J. EBERHARDT en S. TAI "On or Off the Blockchain? Insights on Off-Chaining Computation and Data", *Springer International Publishing, Lecture Notes in Computer Science* 2017, *LNCS-10465*, p.2

locaties waar de persoonsgegevens worden verwerkt. Het is natuurlijk belangrijk dat deze andere locaties voldoende waarborgen bieden op vlak van gegevensbescherming.

Zowel voor de Bitcoinblockchain als voor de Ethereumblockchain werd een oplossing uitgewerkt voor het schaalbaarheidsprobleem waarbij gebruik wordt gemaakt van off-chain opslag. Voor Bitcoin werd Lightning Network ontwikkeld, bij Ethereum gaat Raiden zorgen voor een betere schaalbaarheid.

Lightning Network, dat zich momenteel nog in een testfase bevindt, stelt in zijn *white paper* het volgende voor: *"A decentralized system […] where transactions are sent over a network of micropayment channels […] whose transfer of value occurs off-blockchain."*[206] Het is een systeem van smart contracts dat bovenop Bitcoin wordt ontwikkeld en dat partijen toelaat om ogenblikkelijk betalingen te versturen en te ontvangen met een lage transactievergoeding, door deze buiten de Bitcoinblockchain te laten plaatsvinden. Raiden werkt op ongeveer dezelfde manier als Lightning Network en wordt omschreven als "*an off-chain scaling solution for performing ERC20-compliant token transfers on the Ethereum blockchain. It is Ethereum's version of Bitcoin's Lightning Network, enabling near-instant, low-fee, scalable, and privacy-preserving payments."*[207] Het is zo dat, aangezien Ethereum nog andere transactiemogelijkheden biedt dan louter het verzenden en ontvangen van betalingen, Raiden ook andere transacties dan louter financiële transacties mogelijk maakt.

Beide systemen werken als volgt: twee partijen openen een transactiekanaal om transacties tussen hen beiden te kunnen laten plaatsvinden buiten de blockchain om. Elke transactie kan worden voorgesteld als een *IOU letter*[208], waarin bijvoorbeeld, in het geval van Lightning Network, staat dat Alice 4 Bitcoin verschuldigd is aan Bob. Elke IOU letter kan op elk moment op de blockchain geplaatst worden, al brengt dat natuurlijk transactievergoedingen en een relatief lange wachttijd met zich mee. Stel dat Alice en Bob samen gaan eten en Alice betaalt 2 Bitcoin voor hen beide, dan is Alice nog maar 3 Bitcoin verschuldigd aan Bob. Bob updatet de IOU letter dan ook op die manier. Stel dat Bob Alice opeens niet meer vertrouwt, dan 'geeft' Bob de IOU letter aan de blockchain en maakt het op deze manier officieel. Er is dus geen nood aan vertrouwen tussen beide partijen in dit systeem aangezien elk van hen de tussentijdse balans op elk moment officieel kan maken.

[206] J. POON en T. DRYJA, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", 14 januari 2016, https://lightning.network/lightning-network-paper.pdf
[207] Raiden Network, "What is the Raiden Network?", https://raiden.network/101.html
[208] Staat voor 'I Owe You'. Zie Wikipedia, "IOU", https://en.wikipedia.org/wiki/IOU

Enkel het openen, het sluiten en de eindbalans na het sluiten van het transactiekanaal, dienen te worden gecommuniceerd op de publieke blockchain. Er is dus geen sprake van de weergave van de volledige transactiegeschiedenis op de blockchain wanneer men gebruik maakt van dergelijke transactiekanalen. Hierdoor zou kunnen worden aangenomen dat het gebruiken van dergelijke transactiekanalen privacyverhogend kan werken.[209]

Dit klinkt veelbelovend. Toch is het belangrijk om waakzaam te blijven: de transactiegeschiedenis zal dan wel grotendeels onzichtbaar zijn op de blockchain, binnen deze transactiekanalen is nog ruimte voor verbetering van de privacystandaarden die worden gehanteerd. Momenteel maken beide netwerken gebruik van een principe dat zeer gelijkend is aan *onion routing,* waarbij transacties doorheen verschillende transactiekanalen worden gestuurd waarbij ondertussen slechts een minimum aan informatie wordt doorgegeven aan de desbetreffende nodes, om op die manier de oorsprong en bestemming van een transactie te verbergen. Onion routing verhoogt de privacy aanzienlijk, maar is niet volledig waterdicht.[210]

Verder bestaat de kans dat de systemen zullen evolueren naar een *hub-and-spoke* model.[211] Dit betekent dat de systemen gecentraliseerd zouden kunnen worden in de plaats van gedecentraliseerd, wat eerst werd vooropgezet.[212] Dit leidt gegarandeerd tot een verlies van privacy aangezien bepaalde nodes zicht zullen kunnen krijgen op de transacties die passeren.[213]

Lightning Network en Raiden zorgen voor een lager aantal verwerkingen van persoonsgegevens op de blockchain omdat een groot deel wordt verplaatst naar deze externe transactiekanalen. Het openen en sluiten van het transactiekanaal evenals de eindbalans, moeten nog steeds worden gecommuniceerd via de blockchain. Het gebruik van Lightning Network of Raiden kan de privacy verhogen, aangezien ze er in alle geval voor zorgen dat er minder transactiegegevens op de publieke blockchain worden opgeslagen. Daar staat tegenover dat de systemen (nog) niet volledig waterdicht functioneren op vlak van bescherming van persoonsgegevens.

---

[209] J. EBERHARDT en S. TAI "On or Off the Blockchain? Insights on Off-Chaining Computation and Data", *Springer International Publishing, Lecture Notes in Computer Science* 2017, *LNCS-10465*, p.7

[210] M. GREEN en I. MIERS, "Bolt: Anonymous Payment Channels for Decentralized Currencies", *ACM SIGSAC Conference on Computer and Communications Security* 2017, p.21

[211] In dit model is er geen sprake van één centraal punt, maar wel van meerdere centrale punten (hubs) die een deel van het verkeer centraliseren. Dit in tegenstelling tot een gedecentraliseerd systeem dat geen centrale punten kent. Zie Wikipedia, "Spoke-hub distribution paradigm", https://en.wikipedia.org/wiki/Spoke%E2%80%93hub_distribution_paradigm

[212] K. CROMAN et al., "On Scaling Decentralized Blockchains", *Financial Cryptography Workshops* 2016, p.14

[213] *Ibid.*

Er worden dus nog steeds persoonsgegevens verwerkt in de blockchain. Dit betekent dat het gebruik van dergelijke transactiekanalen de GDPR niet buiten spel kan zetten. Wanneer men een nieuwe blockchainapplicatie zou ontwikkelen en gebruik zou maken van off-chain transactiekanalen, verwerkt men reeds een groot deel van de persoonsgegevens buiten de blockchain, wat positief is. Vereist is wel dat de gebruikte systemen om deze transacties off-chain te laten plaatsvinden, voldoende privacywaarborgen bieden. De tijd zal leren hoe deze systemen in de toekomst zullen evolueren.

3.4. Besluit

De verschillende aanbevelingen die werden gedaan, kunnen leiden tot een verhoogde bescherming van de privacy en de persoonsgegevens van de betrokkene. De voorbeelden geven een idee van hoe deze aanbevelingen reeds werden geïmplementeerd in andere blockchains. Het is momenteel nog koffiedik kijken of de Artikel 29 Werkgroep of de Europese wetgever deze methodes en technieken in de toekomst in sommige gevallen zal beschouwen als anonimiseringstechnieken of niet, en of de implementatie van dergelijke methoden en technieken kan leiden tot een blockchain die conform de gelden regels is. Het lijdt echter geen twijfel dat de implementatie van dergelijke technieken steeds een stap in de goede richting is.

4. Conclusie

Dat het niet helemaal duidelijk is of blockchaintechnologie verzoenbaar is met de vereisten die worden gesteld door de GDPR, zorgt voor wettelijke onzekerheid. Wat daarentegen wel helemaal duidelijk is, is dat de GDPR niet werd ontworpen met gedecentraliseerde platformen in het achterhoofd. Men zou dus eigenlijk kunnen stellen dat de wetgeving op sommige punten reeds verouderd was alvorens ze effectief werd geïmplementeerd.

Het gedecentraliseerde, gedistribueerde en permanente karakter van blockchaintechnologie zorgen voor de meeste problemen. Het is niet duidelijk of en op welke manier hieraan kan verholpen worden. In theorie is het de ideale oplossing om geen persoonsgegevens te bewaren op de blockchain, maar in de praktijk zal dit niet steeds haalbaar zijn. Het is zo dat er steeds voor elk geval afzonderlijk een beoordeling zal moeten worden gemaakt. Een algemene beoordeling van blockchaintechnologie in zijn geheel, is niet mogelijk. De wijze waarop een blockchain wordt ontworpen en welke additionele methoden en technieken er worden gebruikt om de bescherming van persoonsgegevens te optimaliseren, zullen allesbepalend zijn om te kunnen besluiten tot het al dan niet conform zijn van de blockchain met de GDPR.

Het is ook belangrijk om niet uit het oog te verliezen dat de bescherming van het recht op privacy van de betrokkene en zijn fundamentele rechten en vrijheden enerzijds, moeten worden afgewogen tegen het aanmoedigen van innovatie anderzijds. Op zoek gaan naar goede manieren om technologie en regelgeving met elkaar te verzoenen opdat innovatie niet wordt afgeremd maar de persoonsgegevens van Europese burgers toch afdoende worden beschermd, zal één van de volgende uitdagingen zijn van de Europese wetgever. In dit kader werd recent een resolutie aangenomen die werd ingediend door het Griekse Europarlementslid Eva Kaili, waarin ze oproept tot *"ruimdenkende, vooruitstrevende en innovatievriendelijke regelgeving"* met betrekking tot distributed ledger technologieën en blockchains.[214]

Een beslissing tot onverenigbaarheid van blockchaintechnologie met de GDPR door de Europese wetgever, zou een stap achteruit zijn. Een *lex specialis* omtrent distributed ledger technologieën en blockchaintechnologie die de GDPR aanvult en op sommige punten soepeler interpreteert en waarmee dezelfde objectieven worden nagestreefd, kan er daarentegen toe leiden dat blockchains kunnen worden ontwikkeld zonder dat er twijfel dient te bestaan omtrent de legaliteit ervan.

[214] Voorontwerp van resolutie, "Distributed ledger"-technologieën en blockchains: vertrouwen opbouwen via desintermediatie, 1 maart 2018, PE616.877v01-00

BIBLIOGRAFIE

WETGEVING

Verordening EU 2016/679 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming, 'AVG' of 'GDPR')

ADVIEZEN

Advies 4/2007 van de Artikel 29 Werkgroep over het begrip persoonsgegevens

Advies 05/2014 van de Artikel 29 Werkgroep over anonimiseringstechnieken

ONTWERPRESOLUTIES

Voorontwerp van resolutie, "Distributed ledger"-technologieën en blockchains: vertrouwen opbouwen via desintermediatie, 1 maart 2018, PE616.877v01-00

RECHTSPRAAK

HvJ 13 mei 2014, nr. C131/12, ECLI:EU:C:2014:317, 'Google Spain'

RECHTSLEER

Bijdragen in tijdschriften

BELL, T. W., "Copyrights, Privacy, and the Blockchain", *Ohio Northern University Law Review* 2016, Afl. 2, 439-470

BERBERICH, M. en STEINER, M., "Blockchain technology and the GDPR – How to reconcile privacy and distributed ledgers", *European Data Protection Law Review* 2016, Afl. 3, 422-426

BERKE, A., "How safe are blockchains? It depends", *Harvard Business Review,* 7 maart 2017, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

BRANDMAN, G. en THAMPAPILLAI, S., "Blockchain- Considering the regulatory horizon", *University of Oxford Business Law Blog*, 7 juli 2016, https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/blockchain-%E2%80%93-considering-regulatory-horizon

CLARK, B., "Blockchain and IP law: a match made in crypto heaven?", *WIPO Magazine*, februari 2018, http://www.wipo.int/wipo_magazine/en/2018/01/article_0005.html

CUCCURU, P., "Beyond Bitcoin: An Early Overview on Smart Contracts", *International Journal of Law and Information Technology* 2017, Afl. 3, 179-195

DE JONG, J., MEYER, A. en OWENS, J., "Using Blockchain for Transparant Beneficial Ownership Registers", *International Tax Review* 2017, Afl. 5, 47-50

DE JONGHE, D. en LAAN, V.I., "Blockchain in de realiteit", *Computerrecht* 2017, Afl. 6, 347-354

DE BACKER, A. en DE BOE, V., "Smart contracts in de financiële sector: grote verwachtingen en regulatoire uitdagingen", *Computerrecht* 2017, Afl. 6, 355-363

FINCK, M., "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation & Competition Research Paper,* No. 18-01, 30 november 2017, 31 p.

GABISON, G., "Policy considerations for the blockchain technology public and private applications", *SMU Science and Technology Law Review* 2016, Afl. 3, 327-350

LAAN V.I. en RUTJES A., "Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?", *Computerrecht* 2017, Afl. 6, 364-371

LINNEMAN J., "Juridische aspecten van (toepassingen van) blockchain", *Computerrecht* 2016, Afl. 6, 319-324

LYNSKEY, O., "Regulating 'platform power', *LSE Law, Society and Economy Working Papers,* No. 1/2017, 21 februari 2017, 31 p.

REYES, C. L., "Moving beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal", *Vill. L. Rev*. 2016, Afl. 1, 191-234

SCHURINGA, H., "Enkele civielrechtelijke aspecten van blockchain", *Computerrecht* 2017, Afl. 6, 372-378

SWINEHEART, M. en BAER, M., "Those Things You Have Heard about Bitcoin: Distinguishing Signal from Noise", *Geo. J. Int'l Aff.* 2015, Afl. 3, 144-157

TJONG TJIN TAI T.F.E, "Juridische aspecten van blockchain en smart contracts", *TPR* 2017, Afl. 2, 563-608

VALGAEREN E. en LINNEMAN J., "Blockchain ontketend", *Computerrecht* 2017, Afl. 6, 343-346

VALGAEREN E., "Aan de binnenkant van blockchain – start van datarecht?", *Computerrecht* 2017, Afl. 6, 341-342

VERHELST E.W., "Blockchain aan de ketting van de Algemene Verordeningen Gegevensbescherming?", *Privacy & Informatie* 2017, Afl. 1, 17-23

Boeken

DE FILIPPI, P. en WRIGHT, A., *"Blockchain and the law"*, Cambridge, Harvard University Press, 2018, 300 p.

WETENSCHAPPELIJKE ARTIKELS

Bijdragen in tijdschriften

ABERER, K. en HAUSWIRTH, M., "An Overview of Peer-to-Peer Information Systems", *WDAS* 2002, 171-188

BEN SASSON E., CHIESA, A., GARMAN, C., GREEN, M., MIERS, I., TROMER, E. en VIRZA, M., "Zerocash: Decentralized Anonymous Payments from Bitcoin*", IEEE Symposium on Security and Privacy* 2014, 459-474

BRADBURY, D., "The problem with Bitcoin", *Computer Fraud and Security* 2013, Afl. 11, 5-8

BRUNTON, F. en NISSENBAUM, H., "Political and ethical perspectives on data obfuscation", *Privacy, Due Process and the Computational Turn* 2013, 164-188

CROMAN, K., DECKER, C., EYAL, I., GENCER, A. E., JUELS, A., KOSBA, A., MILLER, A., SAXENA, P., SHI, E., SIRER, E. G., SONG, D. en WATTENHOFER, R., "On Scaling Decentralized Blockchains", *Financial Cryptography Workshops* 2016, 1

DE FILIPPI, P., "The interplay between decentralization and privacy: the case of blockchain technologies", *Journal of Peer Production* 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/

EBERHARDT, J. en TAI, S. "On or Off the Blockchain? Insights on Off-Chaining Computation and Data", *Springer International Publishing, Lecture Notes in Computer Science, LNCS-10465*, 2017, 3-15

HEINES, *K.*, "The Risks and Rewards of Blockchain Technology", *Risk Management* 2016, Afl. 4, 6-7

IANSITI M., en LAKHANI, K. R., "The Truth about Blockchain", *Harvard Business Review* 2017, https://hbr.org/2017/01/the-truth-about-blockchain

KOSBA, A., MILLER, A., SHI, E., WEN, Z., en PAPAMANTHOU, C., 'Hawk: The Blockchain Model of Cryptography and Privacy Preserving Smart Contracts", *IEEE Symposium on Security and Privacy* 2016, 839-858

GREEN, M. en MIERS, I., "Bolt: Anonymous Payment Channels for Decentralized Currencies", *ACM SIGSAC Conference on Computer and Communications Security* 2017, 473-489

KROLL, J.A., DAVEY, I.C. en FELTEN, W., "The economics of Bitcoin mining, or Bitcoin in the presence ad adversaries", *WEIS 2013*

MÖSER, M., "Anonymity of Bitcoin transactions", Münster Bitcoin Conference 2013

NARAYANAN, A. en MÖSER, M., "Obfuscation in Bitcoin: Techniques and Politics", *International Workshop on Obfuscation: Science, Technology, and Theory* 2017

NARAYANAN, A. en SHMATIKOV, V., “Robust Deanonymization of Large Sparse Datasets”, *IEEE Symposium on Security and Privacy* 2008, 111-125

REID, F. en HARRIGAN, M., “An Analysis of Anonimity in the Bitcoin System”, *IEEE International Conference on Privacy, Security, Risk, and Trust* 2011, *and IEEE International Conference on Social Computing* 2011, 1318-1326

ROSS, E. S., “Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues, *Cath. U. J. L. & Tech* 2017, Afl. 2, 353-386

SZABO, N., “Formalizing and Securing Relationships on Public Networks”, *First Monday 1997*, Afl. 9, http://ojphi.org/ojs/index.php/fm/article/view/548/469

ZYSKIND, G., NATHAN, O. en PENTLAND, A., “Decentralizing privacy: using blockchain to protect personal data”, *Security and Privacy Workshops* 2015, 180-184

ZYSKIND, G., NATHAN, O. en PENTLAND, A., “Enigma: Decentralized computation platform with guaranteed privacy”, 2015, *https://enigma.co/enigma_full.pdf*

Boeken

GALLOWAY, A.R., *“Protocol: How control exists after decentralization”*, Cambridge, MIT Press, 2004, 286 p.

NARAYANAN, A., BONNEAU, J., GOLDFEDER, S., MILLER, A., FELTEN, E. W. en FELTEN, E., *“Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”*, Princeton, Princeton University Press, 2016, 336 p.

OVERIGE BOEKEN

DRESCHER, D., “*Blockchain basics: A non-technical introduction in 25 steps*”, New York, Apress, 2017, 255 p.

TAPSCOTT, D. en TAPSCOTT, A., “*Blockchain revolution: how the technology behind bitcoin is changing money, business and the world*”, New York, Portfolio Penguin, 2016, 348 p.

ONLINEBRONNEN

Blogs

BACK, A., “Bitcoins with homomorphic value (validatable but encrypted)”, 1 oktober 2013, https://bitcointalk.org/index.php?topic=305791.0

BALIGA, A., “Understanding Blockchain Consensus Models”, april 2017, https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

BURNISKE, C., “Bitcoin and Ethereum: How smart contracts work”, 29 mei 2016, https://ark-invest.com/research/smart-contracts-work

BUTERIN, V., “Privacy on the blockchain, 15 januari 2016, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain

BUTERIN V., “What Proof of Stake is and why it matters”, 26 augustus 2013, https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463

COX, T. en SOLOMON, A., “Blockchain: is the GDPR out of date already?”, 30 augustus 2017, https://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab917e66207

CZARNECKI, J., “Blockchain and personal data protection regulations explained”, 26 april 2017, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained

JAYACHANDRAN, P., “The difference between public and private blockchain”, 31 mei 2017, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

JOHNSTON, D. B., “More on the law of blockchain”, 11 april 2016, https://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3

MARTIN, L., “Blockchain versus the GDPR”, 29 augustus 2017, https://www.voltage.com/blockchain/blockchain-versus-gdpr/

MAXWELL, G., “CoinJoin: Bitcoin privacy for the real world”, 22 augustus 2013, https://bitcointalk.org/index.php?topic=279249

MEYER, D., “Blockchain is on a collission course with EU privacy law”, 26 maart 2018, https://thenextweb.com/syndication/2018/03/26/blockchain-collision-course-eu-privacy-law/

MUNDIS, J., “What does the GDPR mean for blockchain technologies?”, 28 september 2017, https://www.cbronline.com/news/enterprise-it/gdpr-mean-blockchain-technologies/

PESALE, E., “Blockchain technology may not be the best solution for GDPR compliance”, 18 oktober 2017, https://www.csoonline.com/article/3232386/cyber-attacks-espionage/blockchain-technology-may-not-be-the-best-solution-for-gdpr-compliance

SMOLENSKI, N., “The EU General Data Protection Regulation and the Blockchain”, 1 augustus 2017, https://medium.com/learning-machine-blog/the-eu-general-data-protection-regulation-and-the-blockchain-1f1d20d24951

TENNISON, J., “What is the impact of blockchains on privacy?”, *Open Data Institute*, 12 november 2015, https://theodi.org/blog/impact-of-blockchains-on-privacy

TRILLO, M., “Stress Test Prepares Visa Net for the Most Wonderful Time of the Year”, oktober 2013, http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/ index.html

VAN HUMBEECK, A., “The Blockchain-GDPR Paradox”, 21 november 2017, https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

X., Visa, “Power Your Retail Business beyond the Point of Sale”, https://usa.visa.com/run-your-business/small-business-tools/retail.html

Krantenartikels

AITKEN, R., “IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com”, 14 december 2017, https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#a653e867d9c5

BALAJI, S. “India’s blockchain revolution goes beyond banks into land records and private firms”, 28 december 2017, https://www.forbes.com/sites/sindhujabalaji/2017/12/28/indias-blockchain-revolution-goes-beyond-banks/#2e9ce9aa4123

FUNG, B., “Marc Andreessen: In 20 years, we’ll talk about Bitcoin like we talk about the Internet today”, 21 mei 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/?utm_term=.1252983fa32e

HESSEKIEL, D., “The Future of Social Impact is… Blockchain”, 3 april 218, https://www.forbes.com/sites/davidhessekiel/2018/04/03/the-future-of-social-impact-is-blockchain/#4ca3ddc9c3fd

JOHNSON, S., “Beyond the Bitcoin Bubble”, 16 januari 2018, https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

POPPER, N., “Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitocin”, 15 mei 2015, https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html

TWEAKERS, “Nederlandse DJ Hardwell neemt blockchain in gebruik voor registratierechten”, 17 oktober 2016, https://tweakers.net/nieuws/116839/nederlandse-dj-hardwell-neemt-blockchain-in-gebruik-voor-registratie-rechten.html

VAN HOOF, N., “GDPR en blockchain topprioriteit voor Belgische bedrijven”, 27 september 2017, http://www.smartbiz.be/nieuws/172633/gdpr-en-blockchain-topprioriteit-voor-belgische-bedrijven

VAN STEENKISTE, M., “Antwerpse start-up laat je je online identiteit beheren met blockchain”, 7 augustus 2017, http://datanews.knack.be/ict/start-ups/antwerpse-start-up-laat-je-je-online-identiteit-beheren-met-blockchain/article-normal-885539

WONG, J. I., “Sweden’s blockchain-powered land registry is inching towards reality”, 3 april 2017, https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/

X., N.Y. Times, “Ranking the Top Fintech Companies”, N.Y. Times, 6 april 2016, https://www.nytimes.com/interactive/2016/04/07/business/dealbook/The-Fintech-Power-Grab.html

Technische documentatie

MACKENZIE, A., NOETHER S. en het Monero Core Team: “Improving Obfuscation in the Cryptonote Protocol”, 26 januari 2015, https://lab.getmonero.org/pubs/MRL-0004.pdf

NAKAMOTO, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, https://bitcoin.org/bitcoin.pdf.

NOETHER, S., MACKENZIE, A. en het Monero Core Team: “Ring Confidential Transactions”, februari 2016, https://lab.getmonero.org/pubs/MRL-0005.pdf

POON, J. en DRYJA, T., “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”, 14 januari 2016, https://lightning.network/lightning-network-paper.pdf

X., Blockchain.info, “Bitcoin Charts”, https://blockchain.info/charts/n-transactions

X., Blockchain.info, “Hashrate Distribution”, https://blockchain.info/pools

X., Blockchain.info, “Total Transaction Fees”, https://blockchain.info/nl/charts/transaction-fees

X., Ethereum.org, “Data and network stats”, https://ethstats.net

X., Ethereum Homestead Documentation, “What is Ethereum?”, 2016, http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

X., Ethereum Homestead Documentation “What’s the future of Ethereum?”, http://ethdocs.org/en/latest/frequently-asked-questions/frequently-asked-questions.html

X., Raiden Network, “What is the Raiden Network?”, https://raiden.network/101.html

X., Tor Project, “Tor Overview”, https://www.torproject.org/about/overview.html.en

Overige onlinebronnen

Investopedia.com, “Coinjoin”, https://www.investopedia.com/terms/c/coinjoin.asp

Learncryptography.com, “Bitcoin Mining”, 2017, https://learncryptography.com/cryptocurrency/bitcoin-mining

Learncryptography.com, “Proof of Work System”, 2017, https://learncryptography.com/cryptocurrency/proof-of-work-system

Learncryptography.com, “What are hash functions”, 2017, https://learncryptography.com/hash-functions/what-are-hash-functions

Learncryptography.com, “51% Attack”, 2014, https://learncryptography.com/cryptocurrency/51-attack

Wikipedia, “IOU”, https://en.wikipedia.org/wiki/IOU

Wikipedia, “Spoke-hub distribution paradigm”, https://en.wikipedia.org/wiki/Spoke%E2%80%93hub_distribution_paradigm

Wikipedia, “Zero-knowlegde proof”, https://en.wikipedia.org/wiki/Zero-knowledge_proof