Blockchaintechnologie als wondermiddel voor hedendaagse politionele informatie-inefficiënties?

Raf Oostvogels[a] **& Pia Struyf**[b]

[a] Masterstudent, Vakgroep Criminologie, Vrije Universiteit Brussel
[b] Mandaatassistent en doctoraal onderzoeker, Onderzoeksgroep Crime & Society (CRiS), Vakgroep Criminologie, Vrije Universiteit Brussel (corresp.: pia.struyf@vub.be)

Wil de politie een antwoord bieden op de maatschappelijke uitdagingen die de criminaliteit hen in de huidige op informatie gebaseerde maatschappij geeft, zal ze moeten blijven innoveren en focussen op haar informatiehuishouding. Die informatie wordt momenteel niet altijd adequaat gevat, verwerkt, beheerd, en/of uitgewisseld. In deze bijdrage wordt nagegaan of en waar blockchaintechnologie (Nederlands: gedistribueerde databasetechnologie), een technologie die gebruikt kan worden om gegevens vast te leggen en uit te wisselen, een meerwaarde kan bieden in de interne informatiestromen van de politie.

1. Inleiding

De vierde industriële revolutie zet de wereld schrap voor intelligente en autonome systemen die worden aangedreven door data en *machine learning*. De snelheid waarmee technologische ontwikkelingen en innovaties zich het laatste decennium hebben voltrokken is dan ook van ongeziene aard. Deze voortschrijdende digitaliserende trend maakt dat burgers en het maatschappelijk leven moeite hebben om zich te organiseren, laat staan om steeds bij te blijven. Maar ook overheden kunnen hierin niet onverschillig blijven, waarbij ze bij wijze van *minimum minimorum* de ontwikkelingen dienen op te volgen.

Naast de criminaliteit – als *first adopters* van technologie – moet ook de politie in staat zijn om op nieuwe technologieën een adequaat antwoord te bieden. Tevens zou zij deze technologieën – indien relevant – dienen te implementeren in de eigen werking. Echter blijkt uit onderzoek van Europol (2017) dat de politie vaak niet in staat is om steeds in te spelen op de laatste technologische ontwikkelingen binnen de *hightech crime*. Nochtans wordt de nood aan een geschikt antwoord vanuit politionele hoek steeds prangender, want de mate waarin de *hightech crime* jaarlijks toeneemt is volgens Europol zorgwekkend (Europol, 2017). Zoals Janssens et al. (2017) in hun studie concluderen, is de politieorganisatie tot op heden vaak niet bij machte om een onderzoek te voeren naar criminaliteit gepleegd met Bitcoins en/of blockchaintechnologie. Zelfs voor de gespecialiseerde IT-units is het geen kinderspel, doordat ze in de eerste plaats vaak niet op de hoogte zijn van de desbetreffende werking.

Doordat er zich binnen het Belgisch geïntegreerd politiebestel aanhoudende problemen stellen op vlak van informatievatting, -beheer, -uitwisseling en -verwerking, is er een dringende nood aan wetenschappelijk onderzoek naar de hedendaagse mogelijkheden hieromtrent (Maesschalck et al., 2015). Dat de politie alleszins de oogkleppen niet algeheel sluit voor alles wat met innoverende technologie te maken heeft, is zeker hoopgevend te noemen. Zo benadrukt het actuele Nationale Veiligheidsplan (2019: 24) dat: "*Internet, innovatie en nieuwe technologieën zijn niet alleen een bedreiging maar ook een opportuniteit voor de criminaliteitsbestrijding*".

"*Technologie is een middel, informatie is de core. Bedrijven moeten leren om sneller informatie te verwerken, sneller informatie tot inzicht te brengen. Information is the new oil*" (De Smet, 2012: 3). Het lijkt dan ook van primordiaal belang dat alles daaromtrent op de best mogelijke manier wordt verzameld en verwerkt. In dit verband is technologie de *enabler* om tot correcte informatie te komen. En dat is net waar het politieschoentje onder andere wringt. De mate van informatieversnippering door toedoen van het gebruik van allerlei verschillende informatiekanalen, maakt dat er in de praktijk niet altijd volgens de meest efficiënte manier wordt gewerkt (Bové, 2020).

Het probleem van de gebrekkige informatiedoorstroom werd nogmaals bevestigd door de parlementaire begeleidingscommissie van de zaak Chovanec. De toenmalige commissaris-generaal Catherine De Bolle en de directeur-generaal bestuurlijke politie (waaronder de luchtvaartpolitie valt) André Desenfants, werden nooit correct ingelicht over hetgeen zich had afgespeeld in de cel op de luchthaven van Charleroi (Eeckhaut, 2020). Ook in de nasleep van de terroristische aanslagen op de luchthaven van Brussel-Zaventem op 22 maart 2016 werd een onderzoekscommissie opgericht. In de aanbevelingen van haar onderzoeksrapport staat te lezen dat: "*Relevante informatie moet vlot doorstromen van het ene beleidsniveau naar het andere, van de ene overheidsdienst naar de andere. Die vlotte informatiedoorstroming moet er ook zijn tussen de internationale tegenhangers van onze diensten en de Belgische diensten*" (Kamer van Volksvertegenwoordigers, 2016: 38). Ten slotte wordt in datzelfde rapport door de burgemeesters gesteld dat de informatiedoorstroom tussen de bestuurlijke en gerechtelijke overheden in het kader van terrorisme en radicalisering onvoldoende is. Het bestuurlijk optreden door lokale politie en lokale overheden is cruciaal in het kader van preventie en opvolging van terrorisme en radicalisering. Het rapport stelt dat dit dan ook geprofessionaliseerd en versterkt moet worden. De bestuurlijke en gerechtelijke overheden moeten daarnaast onderling beter samenwerken, evenals tussen de federale en lokale overheden enerzijds en politie anderzijds (Kamer van Volksvertegenwoordigers, 2016).

De karakteristieken van blockchain garanderen informatie die authentiek, transparant en fraudebestendig is. Blockchain is in staat om een aantal problemen te kunnen oplossen waarmee de politie wordt geconfronteerd, zoals de interoperabiliteit[1] van systemen, het verhelpen van informatiebottlenecks en het delen van gegevens tussen verschillende korpsen en andere delen van het strafrechtsysteem (Trendall, 2017). Het Vlaams Parlement wees in 2018 al op het feit dat blockchaintechnologie uitermate geschikt is om toegepast te worden binnen de overheid gezien de efficiënte werking en met het oog op het terugdringen van bureaucratie (Schiltz et al., 2018). Echter is er nog lang niet voldoende onderzoek gevoerd naar blockchainimplementaties in politionele context.

De problematiek bij de Belgische geïntegreerde politie wordt op vlak van informatiestromen ook deels in stand gehouden door het naast elkaar bestaan van twee verschillende systemen. Enerzijds is er informatie die intern gebruikt wordt zoals bijvoorbeeld interne korpsnota's en vertrouwelijke dossiers, anderzijds is er informatie die extern mag gebruikt worden zoals zonale veiligheidsplannen en persberichten. Dit vormt tevens een bijkomend obstakel voor een geïntegreerde informatiehuishouding en -uitwisseling (Maesschalck et al., 2015). Bovendien biedt de federale politie tot nog toe te weinig ICT-steun aan de lokale korpsen, met als resultaat dat de lokale korpsen vaak op zichzelf aangewezen zijn en hierdoor

1 "*Interoperabiliteit is het vermogen van organisaties (en hun personen, processen en systemen) om effectief en efficiënt samen te werken door het delen van informatie*" (van Gennip, 2019: 64).

eigen systemen ontwikkelen die een negatieve impact hebben op de officiële informatiestromen (Maesschalck et al., 2015).

2. Blockchain: drie basisprincipes

Kortweg levert blockchain een nieuwe manier van gegevensopslag en -uitwisseling (Berns, 2019). Om het op een meer bevattelijke manier te illustreren, maken we de vergelijking met een woordenketting. De regels van het spel zijn eenvoudig: "*Ik ben politieagent en mijn job omvat*" is de basis, hierna brengt iedere speler om beurten een relevant woord aan dat begint met de laatste letter van het woord van de vorige speler, en bovendien mogen er geen woorden herhaald worden. De controle op correctheid wordt door de participanten zelf uitgevoerd en niet door één centraal controlerend toezichtsorgaan. Het spel resulteert dan in een lange ketting van woorden die op onomkeerbare manier aan elkaar verbonden zijn (Vingerhoets, 2018).

Een politie-gerelateerde illustratie hiervan zou kunnen zijn: "*Ik ben politieagent en mijn job omvat*": Community policing – **g**eweldsdelic**t** – **t**ase**r** – **r**ecidiv**e** – **e**xterne oriëntering – **g**erechtelijk onderzoe**k** – **k**lantgericht – ...

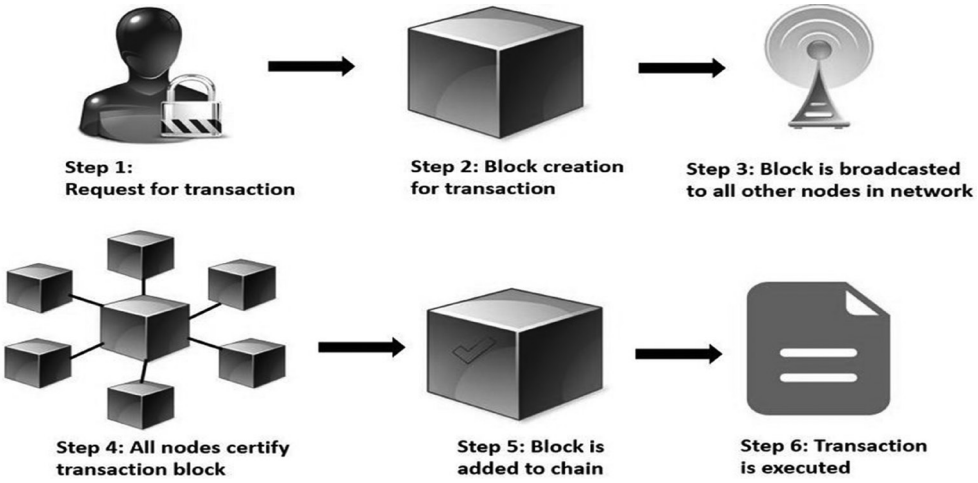
Natuurlijk is de technologie iets complexer dan bovenstaand voorbeeld. Om de nodige theoretische diepgang en de quasi ongebreidelde reikwijdte van de technologie te illustreren, kan men kortweg stellen dat blockchain gekenmerkt wordt door drie basisprincipes.

Ten eerste is het een ketting van gegevensblokken die zich sequentieel opbouwt in de loop van de tijd en die niet eenzijdig aangepast kan worden. De eerste en meest bekende uitwerking van blockchaintechnologie – als onderdeel van *distributed ledger technology* (DLT) – is de digitale munteenheid Bitcoin. In de whitepaper van het Bitcoinprotocol verwijst Satoshi Nakamoto (het pseudoniem van de onbekende uitvinder van Bitcoin) niet naar de term 'blockchain', maar wel naar '*blocks are chained*' (Nakamoto, 2008). Eén blok wordt gecreëerd door een verzameling van transacties die op éénzelfde moment plaatsvinden. Vervolgens wordt het volgende blok van transacties gecreëerd met hierbij een verwijzing of link naar het vorige blok. Op die manier ontstaat er een ketting van blokken dewelke informatie of waarden dragen (Bessems & Bril, 2017).

Ten tweede wordt frauderen of hacken nagenoeg onmogelijk gezien elke transactie bevestigd moet worden door het hele netwerk (Allessie et al., 2019; Schiltz et al., 2018). Bovendien bevat ieder blok een eigen unieke cryptografische digitale vingerafdruk, *hash* genaamd, welke de authenticiteit van het blok garandeert. Deze *hash* wordt gegenereerd door middel van de inzet van wiskundige cryptografie welke mede voor de veiligheid van het netwerk zorgt (Berns, 2019).

Ten derde wordt deze keten gedistribueerd ten aanzien van alle deelnemende partijen. Deze decentralisering houdt ook in dat er geen nood meer is aan één centrale partij die alle rechten heeft, waardoor er dus niet langer een *single point of failure* is (Piscini et al., 2017). Alle participanten die de nodige toegang hebben tot het netwerk kunnen bijdragen aan het aanvullen, veranderen of verbeteren van de informatie. Op die manier kan men een eigen netwerk creëren binnen de organisatie waarbij de verschillende pc's (*nodes*) informatie en waarden met elkaar kunnen uitwisselen, zoals bijvoorbeeld processen-verbaal toevoegen aan een bepaald dossier. In de praktijk zou dit voor de politie betekenen dat ze een individuele blockchain kunnen creëren voor elke dienst binnen een politiezone, zoals bijvoorbeeld beleid, wijkwer-

king en ICT. Zo beschikt ieder personeelslid van de betrokken dienst steeds over de meest recente en transparante informatie (Tapscott & Tapscott, 2018) en zijn er geen 'rondslingerende of gedateerde kopietjes' die de algemene informatiedoorstroom belemmeren.



Figuur 1. Werking van blockchaintechnologie (Nadeem et al., 2019).

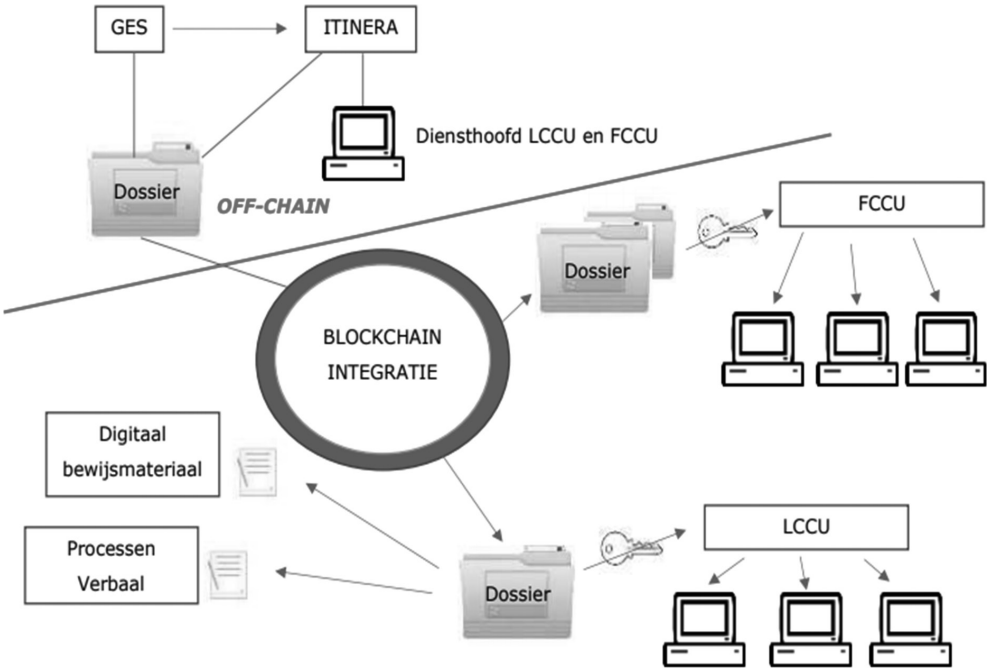
3. Implementaties van blockchaintechnologie voor interne politionele informatiestromen

Deze bijdrage bepleit in geen geval dat blockchain een wondermiddel is voor élk informatiegestuurd bedrijfsproces. In bepaalde gevallen kunnen de bestaande systemen een beter alternatief blijken, na de nodige evaluaties. Beslissingen over de effectieve implementatie moeten dus weloverwogen zijn en onderworpen worden aan een grondige analyse alvorens te worden geïmplementeerd. De uiteindelijke implementatie van blockchaintechnologie zal op een gebruiksvriendelijke manier in de vorm van een applicatie beschikbaar gesteld worden aan de eindgebruiker. Uit de selectie van onderstaande initiatieven is er tot op heden slechts één effectief in de praktijk gebracht, namelijk het voorbeeld van de bodycams. De tot nu toe magere implementatie van blockchaintechnologie is in grote mate toe te schrijven aan het ontbrekende wettelijke kader (Maesschalck et al., 2015). Daarnaast beschrijven Iansiti & Lakhani (2017) blockchaintechnologie als een *foundational technology*, die enkele decennia nodig zal hebben om tot zijn volle potentieel te komen.

3.1 Data-exploitatie

Onder andere bewijsmateriaal, vaststellingen tijdens interventies en processen-verbaal kunnen op de blockchain geplaatst worden, zodoende kunnen de gespecialiseerde diensten verder werken op basis van deze informatie. De gespecialiseerde diensten kunnen toetreden tot de blockchain en zo toegang krijgen tot de informatie die voor hen noodzakelijk is, wat gebeurt via *dApps* (Vrolix, 2019). *dApps* zijn gedecentraliseerde applicaties die ontstaan door twee of meer *smart contracts*[2] aan elkaar te koppelen (Schellekens et al., 2019) en toegankelijk zijn via een versleutelingscode.

2 *"A set of promises, specified in digital form, including protocols within which the parties perform on these promises"* (Szabo, 1996: para. 5).



Figuur 2. Data-exploitatie tussen de gespecialiseerde diensten (Vrolix, 2019).

Neem het voorbeeld uit Figuur 2 waarbij een lokale computer crime unit (LCCU) een ontdekking doet van dubieuze financiële transacties. Na een opsporing van de financiële stromen ontdekt ze dat de criminele handelingen die gesteld worden de grenzen van haar territorium overschrijdt. Bijgevolg doet ze een beroep op de Federale Computer Crime Unit (FCCU). Indien je tewerkgesteld bent bij de LCCU of de FCCU, krijg je een toegangscode om de informatie in de blockchain te raadplegen, aan te vullen en te wijzigen. Deze constellatie zorgt voor een efficiënte en veilige manier van informatie-uitwisseling waarbij enkel de geautoriseerde partijen van de LCCU en de FCCU – gestipuleerd door het *smart contract* – kennis krijgen van de gedeelde informatie.

3.2 Gegevensopslag

De data, die in de cryptografische blokken van de blockchain wordt opgeslagen, is omwille van de blockchain-karakteristieken fraudebestendig (Whittle, 2018). Indien men niet in de mogelijkheid is om het volledige bestand – door bijvoorbeeld bestandsgrootte – op te slaan in de blockchain, kan men wel steeds het *hash* in de chain opslaan, wat verwijst naar het document dat *off-chain* (in een traditionele gecentraliseerde databank of in een Cloud programma) werd opgeslagen (Whittle, 2018). Documenten, zoals juridische dossiers, nemen vaak veel meer ruimte in beslag in vergelijking tot financiële transacties, waarvoor blockchains tot op heden voornamelijk zijn bedoeld. *Hashes* daarentegen nemen een veel kleiner deel van de bestandgrootte in beslag, zijn fraudebestendig en zijn daarom in dit geval een efficiëntere optie (Whittle, 2018). Wanneer er aanpassingen worden doorgevoerd in het *off-chain* databestand, zal er een nieuw blok en nieuw *hash* aan de blockchain worden toegevoegd. De twee *hashes* zijn dus verschillend van elkaar, ondanks ze wel naar hetzelfde document verwijzen.

In een recent artikel in De Tijd (2020) opperde de Belgische Staatveiligheid nog voor een beter beveiligd communicatienetwerk. "*Voor de toekomst vraagt de Staatsveiligheid dat de nodige aandacht wordt besteed aan het ontwikkelen van een adequaat beveiligd netwerk, waarmee de veiligheids- en inlichtingendiensten versleutelde berichten kunnen uitwisselen*" (Bové, 2020: para. 4). Met dit citaat zet Staatsveiligheid de toon en lijkt ze (onbewust?) te wijzen in de richting van blockchain waarbij opslag en beveiliging via encrypties wordt verzekerd.

3.3 Bodycams

Uit Amerikaans onderzoek bleek dat hackers in staat waren om beelden die opgenomen werden met bodycams te verwijderen en/of te editen (Alexandre, 2019; Murdock, 2018). Deze bevindingen ondermijnen het fundamentele doel van bodycams, namelijk transparantie, verantwoording en legitimiteit (Doyle, 2013). Temeer omdat bodycam-beeldmateriaal tegenwoordig frequent wordt gebruikt als bewijs in rechtszaken, moet het gegeven van transparantie en authenticiteit worden behandeld als één van de hoogste intrinsieke pilaren van een democratische rechtsstaat.

Als reactie op deze bevindingen onderzocht het Amerikaans bedrijf *Axon Enterprise Inc.* de mogelijkheid om blockchaintechnologie te integreren in de bodycams van de politie, om zodoende de integriteit van de opnames te garanderen (Ledger Insights, 2019; Alexandre, 2019). In het Amerikaans-Canadees project *Body 3* wordt de toegang tot het beeldmateriaal voor het afspelen, downloaden of bewerken beperkt en zorgt blockchain ervoor dat het beeldmateriaal in *real time* wordt opgeslagen (Ledger Insights, 2019). De beelden die op de blockchain zijn opgeslagen, bevatten drie unieke componenten: (1) een vertrouwde tijdstempel, (2) cameradetails en (3) de identificatie van de persoon die de camera draagt. Deze drie elementen worden samengevoegd in een *hash* welke de authentieke beelden als het ware ondertekent (Ledger Insights, 2019). Tot op heden maken reeds veertien Canadese regio's in Quebec gebruik van deze Axon bodycams (Siegmeth, 2020). Internationaal onderzoek van Khan et al. (2020) wees uit dat bovenstaand proces van opslag tevens mogelijk is voor beeldmateriaal van CCTV-camera's. In België is er tot op heden nog geen sprake van zulke implementaties.

3.4 Kruispuntbanken

Anno 2021 zendt de politie allerlei informatie naar de Arrondissementele Informatiekruispunten (AIK), dewelke deze informatie voor de politie opslaat. Ter illustratie nemen we Kruispuntbank Voertuigen die vervangen zou kunnen worden door een blockchain (Vrolix, 2019). Tot de Kruispuntbank Voertuigen zijn zeven diensten aangesloten, waarvan slechts twee effectief gegevens aanleveren, zijnde *Renta* en *Informex*. De overige vijf diensten zijn bij de werking betrokken als intermediaire partner. Daarnaast zijn er vijftien diensten die in de praktijk instaan voor het inzamelen en bijhouden van de gegevens (waaronder bv. keuringscentra en de politie). Al deze diensten hebben uiteraard onbeperkt toegang tot de gegevens die zij zelf aanleveren. Voor toegang tot de gegevens die de andere partners aanbrengen, is de toestemming nodig van deze betreffende partner en is een machtiging nodig van het Sectoraal Comité voor de Federale Overheid. Zij zijn bevoegd voor de bescherming van de privacy. Sommige van deze vijftien diensten stellen hun eigen databank open, zodat de Kruispuntbank Voertuigen een link kan leggen naar de gevraagde gegevens (Govaert, 2013). In dergelijke constellatie een blockchain implementeren, maakt dat alleen bevoegde partijen inzage in het originele dossier zouden hebben en steeds beschikken over exact

dezelfde informatie, wat noodzakelijk is voor een vlot en efficiënt informatieverloop. Wie bevoegd is zal bepaald worden door middel van een *smart contract*, hetwelk de informatiestroom tussen de verschillende partijen automatiseert en beveiligt (Vrolix, 2019).

Als men bijvoorbeeld het chassisnummer van een voertuig bij eerste registratie linkt aan de eigenaar van het voertuig, kan er bij controle van de politie geen valse of dubieuze informatie door de bestuurder gegeven worden. Een andere optie is de nummerplaat te koppelen aan de eigenaar en deze vervolgens te registreren in de blockchain. In beide gevallen kan de koppeling niet gemanipuleerd worden en is het bewijs authentiek. Wanneer de eigenaar door omstandigheden een nieuwe nummerplaat aanvraagt of een nieuw voertuig koopt, zal de blockchain een nieuwe registratie creëren waarin het de nieuwe nummerplaat of het voertuig koppelt aan de persoon. Deze recentste koppeling is dan de enige geldige.

3.5 Identiteitscontroles

Ook de vaak uitgevoerde taak van een identiteitscontrole kan van een blokchainimplementatie gebruikmaken. Het aanmaken van de identiteit in een blockchain gebeurt door een identiteitsmiddel (bv. een vingerafdruk) te koppelen aan een burger. Door deze authentieke koppeling (vingerafdruk en naam van de persoon) op te nemen in een blockchain kan deze nadien niet meer gemuteerd of gekoppeld worden aan een andere naam (Bessems & Bril, 2017). Dit zou het probleem met valse identiteitsbewijzen of het niet dragen van een identiteitsbewijs (bv. mensen die illegaal op het grondgebied verblijven) verhelpen. Wanneer deze futuristisch klinkende mogelijkheid in de praktijk wordt geïmplementeerd, zal de persoon die wordt gecontroleerd door de politie niet in staat zijn om een valse identiteit op te geven. Wel dient opgemerkt te worden dat een effectieve implementatie nog niet voor morgen zal zijn. Gezien een voorstel tot digitale vingerafdruk op de huidige identiteitskaart eind 2019 al op heel wat controverse stuitte (Lodewijks, 2018), wordt vermoed dat een blockchainkoppeling door middel van een vingerafdruk tevens de wind van voor zal krijgen.

3.6 Track and trace

Enkele bestaande en reeds functionerende projectconcepten met betrekking tot blockchaintechnologie hebben te maken met het traceren van bijvoorbeeld goederen (Tapscott & Tapscott, 2018). Een voorbeeld hiervan is het initiatief van *Everledger* dat gebruik maakt van blockchain bij het traceren van de oorsprong van diamanten om de handel in bloeddiamanten tegen te gaan (Bessems & Bril, 2017). Ook de Antwerpse en Rotterdamse havens doen onderzoek naar de toepassingsmogelijkheden van blockchaintechnologie voor het traceren van bijvoorbeeld containers (Bessems & Bril, 2017). In dit verband zette *Dockflow*, een Antwerpse *start-up* in maritieme logistiek, al grote stappen. Tot slot verwees ook de federale politie in haar directieverslag van 16 april 2018 naar de toepassing van een volledig geautomatiseerd volgsysteem gebaseerd op blockchaintechnologie, dewelke het mogelijk zou maken om het traject van elke container, in het kader van drugssmokkel, nauwgezet in kaart te kunnen brengen (Federale Politie, 2019). Binnen het maritieme goederentransport zijn er wereldwijd al talloze samenwerkingen omtrent blockchain en containertracking, binnen de Belgische politie is dit nog niet operationeel.

Ook het *track and trace*-proces van bewijsmateriaal in juridische procedures (*chain of custody*) kan verbeterd worden door het implementeren van blockchaintechnologie (De Hoon, 2018). De hedendaagse manier van werken wat betreft bewijsmateriaal betrekt vele procespartijen. Elke administratieve handeling die gesteld wordt houdt een risico in, welke ten

gepaste tijde opgeworpen kan worden als een procedurefout. De drie reeds beschreven karakteristieken van blockchain maken dat het bewijsmateriaal authentiek, onveranderbaar en steeds up-to-date is, wat meer processuele garanties biedt voor alle partijen (Maldonado, 2018).

4. Opportuniteiten

Bitcoin, blockchain en aanverwanten worden binnen politionele context vaak benaderd als bedreigingen omdat Bitcoin – toch binnen de politie – voornamelijk wordt gelinkt aan frauduleuze (witwas)praktijken (Elliptic, 2019). Denk maar aan de beginjaren van Bitcoin toen bleek dat de ganse wereld in de mogelijkheid was om op *the dark web*-website *The Silk Road* allerlei drugs en verdovende middelen te kopen. Door te surfen via de anonieme internetbrowser *Tor*, en vervolgens af te rekenen in Bitcoin (Devoe, 2018), konden de gebruikers volledig anoniem en ontraceerbaar blijven doorheen het ganse proces. Zodoende was het voor de speurders zeer moeilijk om te achterhalen wie de middelen aankocht en zelfs wie de beheerder van de website was (Martin, 2013). Uiteraard mag dit er niet toe leiden dat de opportuniteiten van de onderliggende technologie niet worden geëxploreerd, want blockchain is veel meer dan Bitcoin. Volgens het Nederlandse Ministerie van Justitie en Veiligheid (2018) is blockchaintechnologie zelfs interessant voor politie omwille van de veilige en transparante informatie enerzijds en het gegeven van gedistribueerde informatie anderzijds.

Een andere opportuniteit is het gegeven van *real time smart data*: sneller en meer gerichte data vanuit een gedeelde werkelijkheid, welke niet veranderbaar is en bovendien onder supervisie staat van alle *nodes* die tot het netwerk behoren (Bessems & Bril, 2017). Hierdoor wordt frauderen en hacken nagenoeg onmogelijk. Ten slotte stelt blockchaintechnologie de politie en andere veiligheidsdiensten in staat om op een veilige manier informatie met elkaar te delen. Hierdoor wordt de informatiekloof tussen de verschillende veiligheidsactoren verkleind en wordt er mogelijks een antwoord geboden op de aanbevelingen zoals deze staan gestipuleerd in de onderzoeksrapporten naar aanleiding van de aanslagen van 22 maart 2016 en de parlementaire begeleidingscommissie van de zaak Chovanec.

5. Valkuilen

De politie zal pas een technologie implementeren indien er een specifiek wetgevend kader daartoe is gecreëerd (Schiltz et al., 2018). Gezien persoonsgegevens een Europese bevoegdheid is, is het wachten op een duidelijke Europese visie hieromtrent. In geval van blockchain zal het voor de Europese wetgever geen sinecure zijn om wetgeving te ontwikkelen die de persoonsgegevens van de Europese burgers op afdoende wijze kan beschermen, zonder dat de exploratie naar innovatie wordt beknot. Bijgevolg is het een evenwichtsoefening en een juridisch puzzelwerk om beide (soms) contradictorische uitgangspunten met elkaar te versmelten tot een juridisch correcte en legitieme mix waarbij het één het ander niet mag uitsluiten.

Zeker omdat de blockchaintechnologie een technologie is die ook op de publieke sector een grote impact zal hebben, is het aanlokkelijk om de regelgevende molen te activeren en te bekijken hoe het basisprincipe van gedistribueerdheid en automatische gegevensopslag juridisch past binnen het centraal uitgangspunt van de Europese GDPR-wetgeving. Tegelijkertijd is het vanuit de overheid verstandig om een nieuwsgierige houding aan te nemen en bewustzijn te creëren ten aanzien van technologische innovaties (Schiltz et al., 2018; BELTUG, 2017). Zo stelde het Grieks Europarlementslid Eva Kaili in een resolutie dat "*ruimden-*

kende, vooruitstrevende en innovatievriendelijke regelgeving" inzake DLT en blockchain aan de orde is (Schiltz et al., 2018). Ook onze Vlaamse overheid stelt in haar conceptnota dat er een antwoord moet komen op de vraag welke impact de technologie op de bestaande ICT-systemen van de overheid zal hebben (Schiltz et al., 2018).

Het is alleszins duidelijk dat de GDPR-wetgeving niet werd ontworpen met gedecentraliseerde platformen en DLT in het achterhoofd van de Europese wetgever. Men zou kunnen besluiten dat de wetgeving op sommige punten al verouderd was, alvorens de GDPR effectief werd geïmplementeerd. De gedecentraliseerde, gedistribueerde en permanente eigenschap van blockchaintechnologie zorgt, gezien het recht op vergetelheid, voor de meeste problemen (Simal, 2018).

Een mogelijkheid waarbij DLT en blockchaintechnologie toch door de wetgevende instanties ontwikkeld – en door de overheden geratificeerd – zou kunnen worden, is indien de wetgever *lex specialis* zou ontwikkelen omtrent blockchain en DLT als aanvulling op de GDPR. Zodoende ontstaat er geen discussie omtrent de legaliteit van blockchain (cf. *lex specialis derogat legi generali*) (Simal, 2018). Kortom sluit de huidige situatie niet uit dat er in de toekomst geen nieuwe blockchainvormen ontwikkeld zullen worden die wel conform de uitgangspunten van de GDPR-wetgeving zijn (Simal, 2018). Zonder enige twijfel zijn er nog meerdere bekommernissen aan blockchain in overheidscontext verbonden die zeer diepgeworteld zitten in juridische en technische aangelegenheden. Toekomstig onderzoek zal dit moeten uitwijzen.

Naast de juridische valkuil rijzen er ook vragen omtrent de opslagcapaciteit. Deze zal aanzienlijk groter moeten zijn gezien alle transacties op alle *nodes* worden opgeslagen. Daarnaast wordt het vinden van consensus omtrent transacties in sommige gevallen duurder dan de huidige hiërarchisch-gestructureerde informatiestructuur. In geval van het Bitcoinnetwerk kunnen de elektriciteitskosten voor het verifiëren van de transacties al snel oplopen (Berbers et al., 2018). Wel dient hierbij opgemerkt te worden dat er in de loop der jaren veel zuinigere blockchains zijn ontworpen. In dit verband wordt Bitcoin wel eens beschouwd als de fossiele brandstof onder de blockchains (De Greef, 2017). Vervolgens zal men de bestaande systemen, welke een totaal tegenovergestelde architectuur hebben, moeten vervangen. Dit zal niet doorgevoerd kunnen worden door het louter inbrengen van een nieuwe functionaliteit, alleen nieuwbouw kan dit bewerkstelligen (Bessems & Bril, 2017). Tevens stelt men zich de vraag wie er verantwoordelijk is voor fouten in een gedecentraliseerde structuur. De moeilijkheid hierbij is dat blockchain het resultaat is van interactie tussen talrijke spelers: de ontwikkelaars van software, de gebruikers, de hardware, etc. Dit brengt een gedeelde verantwoordelijkheid met zich mee. Net zoals in het geval van artificiële intelligentie dringen nieuwe ethische beoordelingsprogramma's voor het toewijzen van de verantwoordelijke(n) zich op (Berbers et al., 2018). Ten slotte kan uiteraard ook de politieke en organisatorische wilskracht niet ontbreken om een blockchain te implementeren. Dit vraagt moedig leiderschap, maar zeker ook doorgedreven wetenschappelijk onderzoek..

6. Conclusie

Wie er nog aan twijfelt dat internet, artificiële intelligentie, blockchain en consoorten onze samenleving niet ingrijpend veranderen is mogelijk in slaap gevallen. Maar, hoe hard er ook in deze bijdrage wordt gehamerd op de voordelen die deze fundamenteel nieuwe manier van organiseren en *managing* kan hebben, mogen we niet blind zijn voor de repercussies en perikelen die blockchaintechnologie tevens met zich meebrengt. Zowel op vlak van wetge-

ving, opslagcapaciteiten, kostenplaatje, politieke moed tot implementatie en verantwoordelijkheden is het blockchainbeeld nog troebel. En ook op andere vlakken, welke buiten het bestek van deze bijdragen vallen, zullen complexe vraagstukken en onvoorziene gevolgen zich ongetwijfeld aanbieden. Toekomstig onderzoek moet dit allereerst duidelijk in kaart brengen, want expertise rond de toepassing van blockchaintechnologie binnen de politieorganisatie dient immers opgebouwd te worden.

Het integreren van blockchaintechnologie werkt toe naar de politievisie die tegen 2025 idealiter ingewilligd zou moeten zijn, namelijk een meer netwerkend politiemodel dat technologische uitdagingen aangaat om een belangrijke speler te blijven op de informatiemarkt (Maesschalck et al., 2015). Met de komst van innovatieve technologieën zoals blockchain, zullen beleidsmakers, wetgevers en academici, in nauw overleg met technische experten in de nabije toekomst moeten samenkomen en nadenken over nieuwe, doordachte en toekomstbestendige wetgevende kaders. De vraag is of de geesten al voldoende gerijpt zijn om over te gaan tot een effectieve toepassing.

Referenties

Alexandre, A. (2019). *US Police Devices Firm Explores Blockchain to Fight Deepfake Videos*. Cointelegraph.

Allessie, D., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government: An assessment of pioneering implementations in public services.* Europese Commissie.

Belgian Association of Digital Technology Leaders. (2019). *Blockchain en de overheid.* BELTUG.

Belgische Kamer van Volksvertegenwoordigers. (2016). *Onderzoekscommissie terroristische aanslagen 22 maart 2016: Beknopt overzicht van de werkzaamheden en aanbevelingen.*

Berbers, Y., Bonte, L., De Man, H., Eynikel, J., Heene, A., Van Overschee, W., & Verstraeten, P. (2018). *Verantwoordelijk omgaan met digitalisering: een oproep naar overheden en bedrijfsleven, waartoe ook de burger toe kan/moet bijdragen* (Vol. 61). Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten.

Berns, S. (2019). *Blockchain: Een praktische handleiding voor overheden*. VNG Realisatie.

Bessems, P., & Bril, W. (2017). *Blockchain Organiseren voor Managers: Management als innovatie opnieuw uitgevonden* (1ste ed.). Mijnmangementboek.

Bové, L. (3 maart 2020). *Staatsveiligheid vraagt beter beveiligd communicatienetwerk*. De Tijd. https://www.tijd.be/politiekeconomie/belgie/algemeen/staatsveiligheid-vraagt-beter-beveiligdcommunicatienetwerk/10211987.html

Bové, L. (8 februari 2020). *Toezichthouder luidt alarmbel over uitwisseling info bij politie*. De Tijd. https://www.tijd.be/politiekeconomie/belgie/algemeen/toezichthouder-luidt-alarmbel-over-uitwisseling-infobij-politie/10206587.html

Eeckhaut, M. (2020). *In de gangen werden grapjes gemaakt over die Hitlergroet*. De Standaard. https://www.standaard.be/cnt/dmf20201214_98114169?&articlehash=03CF01865B39F0B9AB2EAC7ACFFCFA5E2CA8E17DD08E5D762235CEA77AEF55A33D665EF5D279D3258E5A85872478DF2AFB3A597B211533036D142C13B4A277A9

Maldonado, J. (2018). *Chain of Custody for Evidence Using Blockchain Technology. https://www.natlawreview.com/article/chain-custody-evidence-using-blockchain-technology*

Maesschalck, J., Bruggeman, W., Loyens, K., & Van Ryckeghem, D. (2015). De ontwikkeling van 'een visie voor de politie in 2025': Het gebruik van strategische scenario's als techniek voor visieontwikkeling. *Vlaams Tijdschrift voor Overheidsmanagement, 2*, 11-24.

De Greef, J. (2017). *"Bitcoin draait vooral op stroom uit steenkoolverbranding in China"*. VRT. *https://www.vrt.be/vrtnws/nl/2017/12/16/-bitcoin-draait-vooral-op-stroom-uit-steenkool-verbranding-in-chi/*

De Hoon, W. (2018). *De grote zwakte van blockchain: 'Er blijven mensen nodig, en die kunnen fouten maken'.* https://www.bloovi.be/artikels/innoveren/2018/we-moeten-de-illusie-doorprikken-dat-de-blockchain-een-soort-database-is-om-informatie-mee-te-delen

De Smet, S. (2012). *De nieuwe politie* (1ste ed.). Lannoo Campus.

Devoe, R. (2018). *Decentralized Darknet Markets Could Lead to Unstoppable Silk Road Clones.* Blockonomi. https://blockonomi.com/decentralized-darknet-markets/

Doyle, A. (2003). *Arresting Images: Crime and Policing in Front of the Television Camera*. University of Toronto Press.

Elliptic. (2019). *Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act.* Elliptic. https://www.elliptic.co/our-thinking/bitcoin-money-laundering

Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA).* Europol. https://www.europol.europa.eu/activities-services/mainreports/internet-organisedcrime-threat-assessment-iocta-2017

Federale Politie. (2019). *Nationaal Veiligheidsplan 2016-2019*. https://www.politie.be/5998/sites/5998/files/downloads/NVP2016-2019.pdf

Federale Politie. (2019). *Veilig, snel en mobiel politiewerken is een feit.* https://www.politie.be/5998/nl/nieuws/veilig-snel-en-mobielpolitiewerken-is-een-feit

Govaert, C. (2013). *Kruispuntbank Voertuigen gaat in september van start.* Polinfo. https://polinfo.kluwer.be/NewsView.aspx?id=VS300147092&contentdomains=POLINFO&lang=nl

Janssens, J., Soetaert, S., & De Vos, A. (2017). Beslag en beheer van cryptovaluta: de Bitcoin. *Panopticon*, *38*(1), 41-47. http://hdl.handle.net/1854/LU8515715.

Joosten, P. (2020). Blockchain. Definitie, werking, kansen & 6 voorbeelden! https://www.peterjoosten.net/blockchain/

Khan, P., Byun, Y.-C., & Park, N. (2020). A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. *Electronics*, *9*(3), 484. http://dx.doi.org/10.3390/electronics9030484

Ledger Insights. (2019). *Axon explores blockchain for police body-cam footage integrity.* Ledger Insights. https://www.ledgerinsights.com/axonexplores-blockchain-for-police-body-cam-footage-integrity/

Lodewijks, B. (2018). *Toch vingerafdrukken op Belgische ID-kaart vanaf april 2019*. https://techpulse.be/nieuws/228433/toch-vingerafdrukken-op-belgische-id-kaart-vanaf-april-2019/

Martin, J. (2013). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice*, *14*(3), 351-367. doi:10.1177/1748895813505234.

Ministerie van Justitie en Veiligheid. (2018). *De staat van innovatie bij justitie en veiligheid.*

Murdock, J. (2018). *Footage From Police Body Cameras Can Be Altered by Hackers, Researcher Says.* Newsweek. https://www.newsweek.com/footage-police-body-cameras-can-be-alteredhackers-researcher-says-1070088

Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. (2019). Securing Cognitive Radio Vehicular Ad Hoc Network with Fog Node based Distributed Blockchain Cloud Architecture. *International Journal of Advanced Computer Science and Applications, 10*. doi:10.14569/IJACSA.2019.0100138

Oostvogels, R. (2019). *Exploratie van blockchain als innovatieve informatietechnologie in politionele context: "Hoe kan blockchaintechnologie geïmplementeerd worden in de interne informatiestromen van de politie?"* [Onuitg. bachelorproef]. Vrije Universiteit Brussel.

Piscini, E., Dalton, D., & Kehoe, L. (2017). *Blockchain & Cyber Security. Let's Discuss.* Deloitte.

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/ LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Satoshi, N. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Schiltz, W., Vanwesenbeeck, D., De Meulemeester, M., De Ro, J., Taelman, M., & De Clerq, M. (2018). *Conceptnota voor nieuwe regelgeving betreffende blockchaintechnologie*. Vlaams Parlement.

Siegmeth, S. (2020). *Kativik Regional Police Force to Deploy Axon Body Cameras Backed by Axon Evidence In All 14 Communities of Nunavik Region*. Newswire.

Simal, J. (2018). *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR* [Gepubliceerde masterproef]. KU Leuven.

Tapscott, D., & Tapscott, A. (2018). *Blockchainrevolutie: De technologie achter de bitcoin zal de wereld voor altijd veranderen*. Xander Uitgevers BV.

Trendall, S. (2017). *Police need to consider the implications of blockchain technology, says Police Foundation think tank*. https://www.holyrood.com/news/view,police-need-to-consider-the-implications-of-blockchain-technology-says-police-foundation-think-tank_13654.htm

van Gennip L. (2019). Interoperabiliteit. In F. Kreier & I. Verberk-Jonkers (Eds.), *De dokter en digitalisering*. Bohn Stafleu van Loghum. doi: 10.1007/978-90-368-2161-2-9

Vingerhoets, K. (2018). Ontketen de blokken! In E. De Munck (Ed.), *Blockchain in de juridische wereld: Enkele toepassingen* (pp. 19-30). Larcier.

Vrolix, T. (2019). *Innovatie in de opsporing: blockchain onder de loep* [Gepubliceerde masterproef]. Universiteit Gent.

Whittle, B. (2018). *Storing Documents on the Blockchain: Why, How, and Where*. Coincentral. https://coincentral.com/storing-documents-on-the-blockchain-why-how-and-where/