FACULTEIT
RECHT EN CRIMINOLOGIE

INNOVATIE IN DE OPSPORING: BLOCKCHAIN ONDER DE LOEP

Masterproef neergelegd tot het behalen van
de graad van Master in de Criminologische Wetenschappen
door (01511852) Vrolix Thomas

Academiejaar 2018-2019

Promotor:
Prof. dr. Verhage Antoinette

Commissaris:
Slabbekoorn Geert

UNIVERSITEIT
GENT

“Every once in a while, a new technology, an old problem, and a big idea turn into an innovation.”

Dean Kamen

Executive summary

DOEL – Een bijdrage leveren aan de kennisontwikkeling omtrent de inzet en toepassing van de blockchaintechnologie binnen de geïntegreerde politie en de impact ervan op criminaliteit, door de kansen en bedreigingen van blockchain in kaart te brengen.

RELEVANTIE – Blockchaintechnologie wordt beschouwd als een disruptieve technologie die een grote impact zal hebben in tal van sectoren en die zich leent tot tal van toepassingen. Daarnaast omarmen ook criminelen blockchain. Het Nationaal Politioneel Veiligheidsbeeld toont aan dat criminelen vaak 'first adopters' zijn van de nieuwe technologische mogelijkheden. Daarnaast experimenteren vele overheden en ondernemingen met blockchaintechnologie. Het antwoord op de vraag of blockchaintechnologie ook kansen kan bieden voor de geïntegreerde politie, is zeer relevant.

BENADERING – In een eerste stap werd nagegaan wat de barrières en hinderpalen zijn bij het digitaal forensisch onderzoek. De grote opsporingsvraagstukken vandaag de dag liggen immers vooral op het terrein van één van de belangrijkste misdaadproblemen van het huidige tijdsgewricht: high-tech crime. In een volgende stap werd nagegaan wat de basiseigenschappen zijn van blockchaintechnologie. Met deze basiseigenschappen in het achterhoofd werd vervolgens eerst gekeken naar de mogelijkheden die ze bieden binnen de criminele wereld, om te begrijpen waarom politiediensten aandacht moeten hebben voor deze technologie. Daaropvolgend werden de basiseigenschappen van blockchain afgetoetst aan de barrières en hinderpalen bij het digitaal forensisch onderzoek en de (werk)processen binnen de geïntegreerde politie. Op deze manier wordt een integraal beeld gegeven van de potentiële bedreigingen van blockchain, maar ook van de kansen die de technologie te bieden heeft voor publieke opsporingsdiensten waardoor wordt bijgedragen aan de agenda-bepaling en kennisontwikkeling omtrent blockchaintechnologie.

BEVINDINGEN – Sedert het eerste gebruik van blockchain, als technische onderbouw van de Bitcoin munt, is een niet te stoppen verspreiding van deze technologie voor andere toepassingen in gang gezet. Zowel in de criminele als in niet-criminele sfeer. Blockchain is een innovatieve, zeer veilige, onkraakbare database die kan worden gerepliceerd, gedeeld en gesynchroniseerd over alle computers die deelnemen aan het (blockchain)netwerk. De data zijn onveranderdbaar (*immutable*): eens opgeslagen kunnen ze niet worden aangepast, er kan alleen iets worden toegevoegd. Dit biedt transparantie voor alle deelnemers, vermits alle veranderingen en transacties over de tijd zichtbaar zijn. Er is geen centraal beheer of eigenaarschap. Via een mechanisme van consensus tussen (anonieme) deelnemers, worden nieuwe data (transacties) geaccepteerd en toegevoegd aan de blockchain. Het totaal open en niet-centraal gecontroleerde aspect van de (*public*) blockchain, zoals die voor Bitcoin werd ontwikkeld, is niet geschikt voor veel toepassingen. De technologie werd uitgebreid om controle over toegang tot en toevoeging van data voor te behouden aan specifieke deelnemers (private/hybride blockchains). Voor de cybercriminelen is resistentie en versleuteling van blockchainnetwerken erg aanlokkelijk. Binnen de criminele wereld worden zowel toepassingen van publieke (cryptocurrencies zoals Bitcoin en Monero, darknetmarkten) als private (*cryptofoons*, decentrale DNS) blockchains gebruikt. Forensisch onderzoek in dergelijke high-tech criminaliteit vergt, naast traditioneel opsporingswerk, ook een specifieke technische kennis om sporen te onderzoeken. Binnen de eigen politionele werking kan blockchain bijdragen tot de oplossing van een aantal bekende lacunes. Er dienen instrumenten ontwikkeld te worden om problemen waarmee men te maken krijgt, aan te pakken (versnipperde kennis, kennisbeheer, geïntegreerde informatiehuishouding en -uitwisseling, …). Blockchain is niet altijd de beste technische oplossing, maar voor een aantal onderzochte *Use Cases* zijn voordelen te halen. Voornamelijk voor de betere doorstroming tussen diensten (ketenbenadering), informatiedeling (intern en extern) en de bewaking van integriteit van

digitale objecten. Mits een weloverwogen implementatiestrategie kan dit, zonder bestaande systemen en databanken overboord te gooien, waardoor vroegere investeringen beschermd worden.

WIJZERS – Blockchain wordt algemeen beschouwd als spitstechnologie en de druk bij bedrijven en overheden om de boot niet te missen is groot. Het ontwikkelen van applicaties op deze technologie staat nog in het beginstadium en er is weinig veldervaring. De introductie binnen de eigen werking is met de nodige terughoudendheid te benaderen. De kost ten opzichte van traditionele ICT-oplossingen (typisch Kruispuntbanken) moet worden afgewogen. Een beperkte *Proof of Concept* voor een kleine *Use Case* is aan te raden. Het is aan te bevelen om ervaringen van anderen aan te boren. Vele overheidsinstellingen zijn op deze technologie gesprongen. De Nederlandse Justitie heeft bijvoorbeeld al geëxperimenteerd met een blockchain in de strafrechtketen. Het verst staat wellicht Estland met hun "chain-geïntegreerde" X-Road[*], voor data uitwisseling, die reeds vóór de Bitcoin werd geconcipieerd.

[*] e-Estonia. (2018). X-Road not to be confused with blockchain. Retrieved from https://e-estonia.com/why-x-road-is-not-blockchain/

Woord vooraf

Deze masterproef kwam tot stand in het kader van het behalen van het diploma Master in de Criminologische Wetenschappen aan de Universiteit Gent. Het is de plaats die blockchain inneemt op de maatschappelijke, politieke en media-agenda die de interesse voor dit thema in de opleiding criminologische wetenschappen onder meer heeft aangewakkerd en de onderwerpskeuze van dit onderzoek mee heeft beïnvloed. De keuze voor dit onderwerp moet echter ook gesitueerd worden in het schrijven van de bachelorproef[12] en in het verlengde van de stage-ervaringen[13] in de bacheloropleiding criminologische wetenschappen. In het kader van het schrijven van die bachelorproef, kon uit de conclusie worden afgeleid:

> (…) van groot belang om op de hoogte te blijven van de kennisontwikkeling op technologisch gebied en van de wijze waarop deze ontwikkelingen mogelijkheden kunnen bieden voor de overheid en de crimineel. De kansen en bedreigingen dienen zowel op het terrein van de preventie als van de opsporing systematisch in kaart gebracht te worden (Vrolix, 2017).

Via deze weg zou ik ook graag een dankwoord richten aan alle mensen die mij geholpen hebben om mijn masterproef tot een goed einde te brengen. Vooreerst wil ik prof. dr. Antoinette Verhage, mijn promotor, bedanken voor de nuttige contactmomenten, zinvolle richtlijnen, tips en feedback die een grote hulp waren bij het schrijven van deze masterproef en om mij bij te sturen waar nodig. Zij gaf mij de mogelijkheid om een onderwerp dat mij persoonlijk interesseert te vertalen in een masterproef. Daarnaast wil ik graag de stageplaats van vorig jaar, namelijk de Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent, bedanken.

Inhoudsopgave

Lijst van figuren en tabellen

CONCEPTUEEL ONTWERP

1. Projectkader

1.1 Inleiding

In de literatuur worden heel wat definities gegeven met betrekking tot innovatie. De definitie van het woord innovatie is subtiel veranderd sinds de late jaren zestig (Easton, 2015). Mulgan & Albury (2003) definiëren innovatie als *"new ideas that work"* en om preciezer te zijn *"successful innovation is the creation and implementation of new processes, products, services and methods of delivery which result in significant improvements in outcomes efficiency, effectiveness or quality"* (Mulgan & Albury, 2003).

Innovatie is de implementatie van een nieuw of sterk verbeterd product, een proces, een nieuwe marketing- of organisatiemethode in de bedrijfsvoering, binnen de organisatie op de werkvloer of externe relaties (Dalle, 2015). Innovatie wordt gekenmerkt door verschillende dimensies, waaronder de mate van nieuwigheid, de aard van de innovatie (product- en procesinnovatie), de effecten van radicale en incrementele innovatie en de bron van innovatie (technologisch – niet-technologisch) (Dalle, 2015). Wereldwijd wordt aangenomen dat innovatie de noodzakelijke voorwaarde is om op lange termijn existentiële uitdagingen het hoofd te kunnen blijven bieden (Dalle, 2015). Aanvullend hierop zijn de volgende redenen eveneens een motivatie om in te zetten op innovatie: voldoen aan nieuwe maatschappelijke verwachtingen ten aanzien van de politie- en veiligheidsdiensten, het verhogen van de legitimiteit en versterken van het imago, en ten slotte om als volwaardige (veiligheids)partners mee te spelen op het (inter)nationale vlak (Dalle, 2015). Als werkdefinitie werd door enkele directie brevethouders van de geïntegreerde politie een werkdefinitie voorgesteld waar wij ons perfect in kunnen vinden: *"Innovatie is het stimuleren van mensen om nieuwe ideeën om te zetten in meerwaarde."* (Dalle, 2015).

De inhoud van dit concept weerspiegelt de huidige maatschappelijke druk op publieke en private organisaties over de hele wereld om succesvol te zijn in het omgaan met maatschappelijke transformaties (Easton, 2015). Deze maatschappelijke transformaties zijn nauw verbonden met een voortschrijdende technologisering (FOD Justitie, 2016). Het mag dan ook niet verwonderen dat heel wat criminologen en waarnemers argumenteren dat we in de (begin)fase zitten van een nieuwe technologische revolutie die ook de organisatie en werking van politiediensten drastisch aan het wijzigen is/zal wijzigen (De Pauw & Vermeersch, 2015).

De grote opsporingsvraagstukken vandaag de dag liggen vooral op het terrein van één van de belangrijkste misdaadproblemen van het huidige tijdsgewricht: 'high-tech crime'[1] (Kleemans, de Poot, & Verhage, 2014). Nieuwe complexe vormen van criminaliteit zoals high-tech crime[2] hebben gevraagd om aanpassingen en vernieuwingen in de opsporing (Terpstra, Ponsaers, de Poot, Bockstaele, & Gunther Moor, 2013). Technologische innovaties zorgen er immers voor dat nieuwe technologieën de concrete uitvoering van de verschillende fases van een als misdrijf omschreven feit continu wijzigen (FOD Justitie, 2016). Daartegenover staat dat de innovatieve technologische ontwikkelingen, al dan niet via het internet, binnen de wettelijke normen ook ongekende mogelijkheden bieden op het stuk van opsporing en vervolging (FOD Justitie, 2016). Als er rekening gehouden wordt met de snelheid waarmee technologie de laatste decennia het politiewerk heeft beïnvloed, moet *technology-led policing*[3] worden beschouwd als een belangrijke innovatie in de opsporing (Easton, 2015). Het is duidelijk dat innovatief

[1] Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA)* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

[2] High-tech crime als overkoepelend containerbegrip verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT. Tegenover de term cybercrime biedt high-tech crime een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen vandaag de dag. Nieuwe criminaliteitsvormen die kunnen ontstaan door innovaties van ICT (en niet alleen het internet) worden door dit containerbegrip afgedekt (van der Hulst & Neve, 2008).

[3] Technologie heeft altijd een belangrijke rol gespeeld bij de taakuitvoering van de politie. Die rol is de laatste jaren niet alleen uitgebreid maar ook vernieuwd (De Pauw, Ponsaers, van der Vijver, Bruggeman, & Deelman, 2011).

denken, het investeren in nieuwe werkmethodes en/of nieuwe technologieën een absolute must, zelfs een overlevingsstrategie is geworden[4] (Dalle, 2015).

Blockchain is vandaag de dag een actueel thema. Het is momenteel (anno 2018-2019) één van de meest veelbelovende technologieën (Key, 2018). De berichtgeving over dit onderwerp spreekt van een baanbrekende technologie die de komende decennia alle maatschappelijke sectoren van de samenleving drastisch zal veranderen. Ook criminelen omarmen blockchain (Europol, 2017b). Wat betekent deze technologie dan voor publieke opsporingsdiensten? De verwachting is dat blockchain onder meer op de technologische, financiële en dienstverleningssector (dus ook de overheidssector en veiligheidssector) een grote impact zal hebben (Schiltz et al., 2018). De Europese Unie laat zich in het blockchainverhaal alvast niet onbetuigd. In februari van 2017 al publiceerde het Europees Parlement een diepteanalyse over *'Hoe blockchain ons leven kan veranderen'*[5]. Terecht stelt het rapport dat Europa moet anticiperen op de mogelijke impact van blockchain in de samenleving (Pomp & Verhaert, 2018). Mede door deze omstandigheden besloot ook het 'Centre for Policing and Security' (CPS vzw)[6] een studievoormiddag[7] te wijden aan dit thema (Centre for Policing and Security, 2018a).

[4] Deze stelling wordt eveneens gedeeld door Steven De Smet, hoofdcommissaris van de Gentse politie en adviseur communicatie, veiligheid en strategie bij de Oost-Vlaamse provinciegouverneur: "In mijn ogen staan we voor een van de meest belangrijke evoluties in de wereld van het politiewezen mee te maken, waarin technologie plots een hoofdrol gaat spelen." (De Smet, 2012).

[5] Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives. In-depth analysis*. Retrieved from Panel for the Future of Science and Technology (STOA): http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[6] Het CPS streeft het doel na samen met de hele veiligheidssector gemeenschappelijk bij te dragen aan het oplossen van maatschappelijke vraagstukken en problemen in de ruime veiligheidssfeer (Centre for Policing and Security, 2018b).

[7] 20 september 2018: CPS-studievoormiddag: 'Innovatie in de opsporing: kansen en bedreigingen van Blockchain', Digityser Brussel (http://www.politiestudies.be/vrij.cfm?Id=412).

Criminologisch onderzoek naar innovatieve technologische ontwikkelingen, en in het bijzonder de blockchaintechnologie, is dus om verschillende redenen uitermate relevant. Want blockchain is niet alleen die ene nieuwe technologie achter Bitcoin maar ook de inspiratie voor vele verwante technologieën, een andere manier van organiseren en zelfs denken (Kaptijn, Bergman, & Gort, 2016). Dit zal een grote impact hebben op organisaties en de samenleving (Kaptijn et al., 2016).

1.2 Probleemstelling

Binnen de geïntegreerde politie bestaat er tot nog toe niet zoiets als een technologiebeleid, noch staan er specifieke actoren in voor de 'research and development' in verband met IT-toepassingen (Bruggeman, 2014). Dat blijkt ook uit het onderzoek van De Pauw en Vermeersch (2015) over politie, surveillance en technologie in 2025, waarin zo goed als alle respondenten aangeven dat er momenteel een gebrek is aan onder andere beleid en visie omtrent de inzet van technologie bij de politie (De Pauw & Vermeersch, 2015). Het gevolg is dat opsporings- en handhavingsdiensten niet altijd over duidelijke, aansprekende voorbeelden beschikken over het gebruik van technologie in de handhaving, opsporing of vervolging[8] (Custers & Vergouw, 2016). Waardoor de kennis over wat werkt op het gebied van technologie voor de handhaving, opsporing en vervolging beperkt is (Custers & Vergouw, 2016) en het optimaal uitvoeren van forensisch onderzoek (opsporing) in een geïnformatiseerde omgeving onder druk komt te staan (Comité P, 2018a). Achterstanden bij het uitvoeren van dergelijke opdrachten, illustreren deze vaststelling (Comité P, 2018a).

[8] Zie tabel 2 van bijlage 4.

Uit het toezichtsonderzoek (21/06/2018)[9] van het Vast Comité P[10] komt naar voren dat de voornaamste bedreigingen die de werking van de geïntegreerde politie hypothekeren bij het uitvoeren van onder meer het forensisch onderzoek in een geïnformatiseerde omgeving, inderdaad verband houden met een ontbrekende geïntegreerde visie en strategie en het kennisbeheer[11] in het kader van de achterstand ten opzichte van de technologische realiteit (Comité P, 2018a). Dit vertaalt zich in het ontbreken van eenvormige performante systemen en een reëel geïntegreerde informatiehuishouding en -uitwisseling, zoals verderop nog duidelijk zal worden.

Gezien de hoge verwachtingen van technologisch gedreven veranderingen en ontwikkelingen binnen politiewerk en het feit dat blockchaintechnologie wordt beschouwd als een revolutionaire digitale innovatie met een ongezien potentieel (Barclay, Preece, & Theodorakopoulos, 2017); is het verrassend dat er weinig tot geen (empirisch) wetenschappelijk onderzoek is gedaan naar de toepassing van dergelijke technologische ontwikkelingen binnen politieorganisaties en de impact ervan op zowel de organisatie als op criminaliteit (Grapperhaus, Akerboom, & Kuijs, 2018). Want zoals in de inleiding werd vermeld, omarmen ook criminelen blockchain. Het Nationaal Politioneel Veiligheidsbeeld toont aan dat criminelen vaak 'first adopters' zijn van de nieuwe technologische mogelijkheden

[9] Comité P. (2018). *De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving*. Kamer van Volksvertegenwoordiger Retrieved from https://comitep.be/document/onderzoeksrapporten/2018-06-21%20Forensisch%20onderzoek.pdf

[10] Het Vast Comité van Toezicht op de politiediensten, kortweg Comité P, werd opgericht in 1991 vanuit de behoefte van het federale parlement om te beschikken over een extern controleorgaan op de politie. Door de vele toezichtsonderzoeken en onderzoeken naar klachten die de Dienst Enquêtes van het Comité P verricht, heeft het Comité P een beeld van de actuele werking van de politie. Dit beeld, aangevuld met informatie uit talrijke andere bronnen, stelt het Comité P in staat om een observatoriumfunctie van de politiewerking uit te oefenen ten behoeve van het federale parlement (Comité P, 2018b).

[11] Kennisbeheer wordt meer en meer, terecht, gezien als een strategische managementtool binnen bedrijven en organisaties. Door het efficiënt en effectief beheren en gebruiken van kennis en ervaringen kan ingespeeld worden op tools en technieken, processen, (bedrijfs)risico's, … (Vanacker, 2018).

(FOD Justitie, 2016). Onderzoek is nodig om deze kennis te vergroten waarbij de masterproef tegemoet wil komen aan deze lacune.

Kortom, dit onderzoek richt zich op het verkennen van de verschillende mogelijkheden voor de integratie van blockchain in de (werk)processen van de geïntegreerde politie. Hierbij wordt onderzocht welke kansen er zijn die de blockchaintechnologie kan bieden (voor de opsporing van high-tech crime), maar ook welke bedreigingen er zijn die deze nieuwe technologie met zich meebrengt. Door het analyseren van de huidige barrières en noden bij het forensisch onderzoek in een geïnformatiseerde omgeving binnen de geïntegreerde politie en het verwerven van kennis over blockchaintechnologie, wordt onderzocht hoe deze (werk)processen baat kunnen hebben bij het gebruik van deze technologie. De onderzoeksresultaten dragen bij aan de kennisontwikkeling van de mogelijkheden voor een (brede) implementatie van blockchain binnen de geïntegreerde politie door middel van een onderbouwd onderzoeksdocument. Het biedt een overzicht van de verschillende mogelijkheden voor het gebruik van blockchain. Het vergroot het bewustzijn van de impact die deze technologie met zich mee kan brengen. Dit onderzoek levert argumenten voor de mogelijkheden om blockchaintechnologie te implementeren in de (opsporings)processen van de geïntegreerde politie en kan fungeren als een trigger voor verder onderzoek naar dit onderwerp.

2. Conceptueel ontwerp

2.1 Doelstelling

Aangezien blockchain een recent fenomeen is en er nog maar beperkt (wetenschappelijk) onderzoek voor handen is, wordt in deze masterproef de gelegenheid aangegrepen deze technologie van naderbij te bekijken. Uit de probleemstelling (cfr. 1.2) kan de lezer ook afleiden dat er tot op heden geen (wetenschappelijk) onderzoek naar de (potentiële) mogelijkheden en bedreigingen van blockchain voor onze opsporingsdiensten bestaat; en dat bedreigingen die de werking van de geïntegreerde politie hypothekeren bij het uitvoeren van onder meer forensisch onderzoek in een geïnformatiseerde omgeving, verband houden met het kennisbeheer. Niettegenstaande dat uit de (niet-gepubliceerde) bachelorproef overigens blijkt dat het voor wetshandhavingsdiensten van groot belang is om op de hoogte te blijven van de kennisontwikkeling op technologisch gebied en van de wijze waarop deze ontwikkelingen mogelijkheden kunnen bieden voor de overheid en de crimineel. Het is immers contradictorisch dat high-tech crime als één van de belangrijkste misdaadproblemen van het huidige tijdsgewricht wordt beschouwd, terwijl er maar beperkte aandacht geschonken wordt aan de impact van de blockchaintechnologie die de komende decennia alle maatschappelijke sectoren van de samenleving radicaal kan veranderen.

De primaire doelstelling van dit onderzoek luidt dan ook als volgt: *Een bijdrage leveren aan de kennisontwikkeling omtrent de inzet en toepassing van de (veelbelovende) blockchaintechnologie (ICT-innovatie) binnen de geïntegreerde politie en de impact ervan op criminaliteit, door de kansen en bedreigingen van blockchain (voor de opsporing van high-tech crime) in kaart te brengen.*

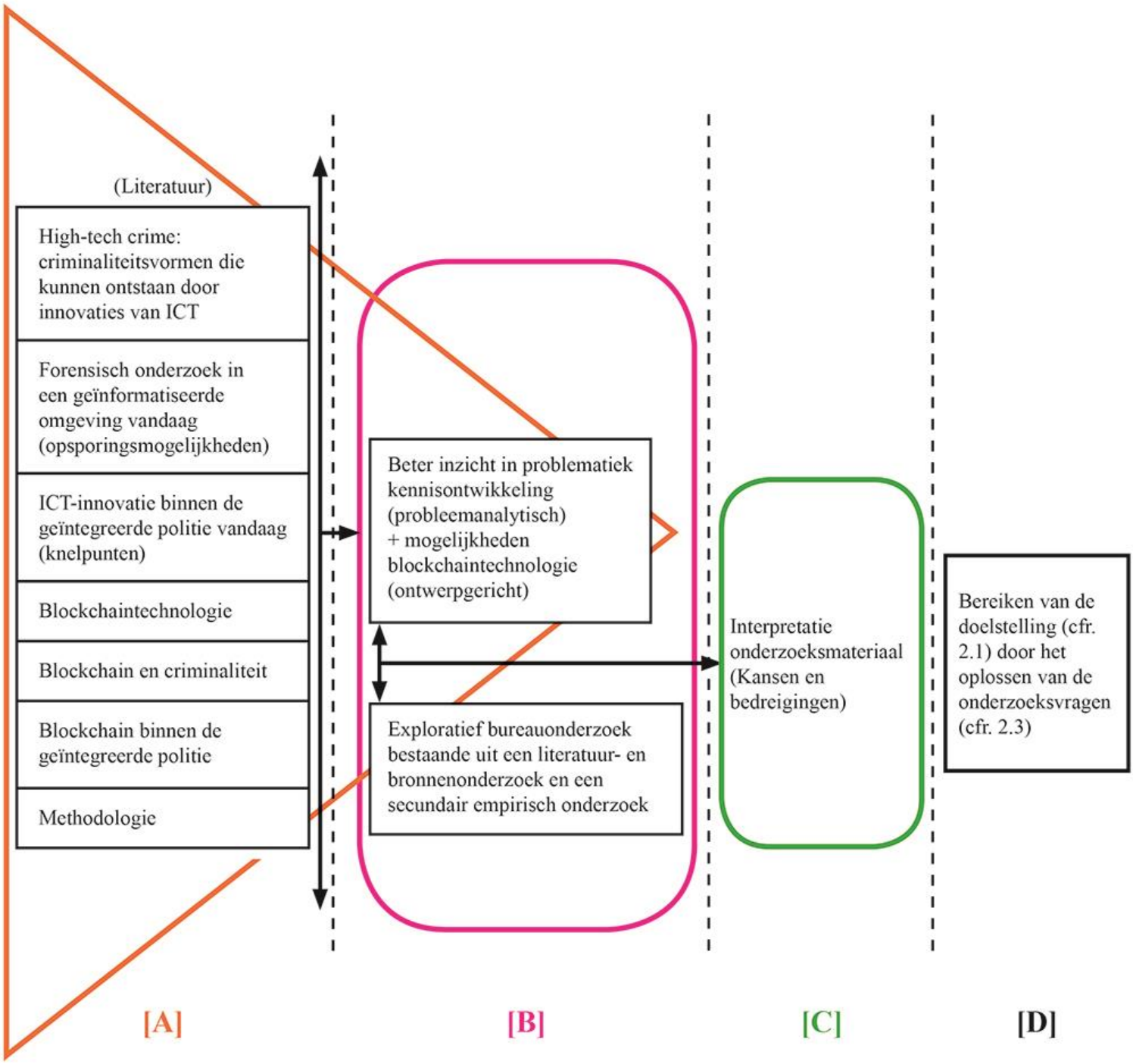
2.2 Onderzoeksmodel

2.2.1 Onderzoeksoptiek

Uit de probleemstelling kan geconcludeerd worden dat de masterproef vooral de vorm aanneemt van een praktijkgericht onderzoek omdat er vertrokken wordt vanuit een praktijksituatie, namelijk het problematische karakter van het gebrek aan kennisontwikkeling van de wijze waarop (blockchain)technologie mogelijkheden (kan) bieden voor de crimineel, met de bedoeling deze problematische situatie onder de aandacht te brengen (agenda-setting). Er zal met andere woorden een probleemanalytisch onderzoek worden gevoerd waarbij het de bedoeling is de aandacht te vestigen op dit probleem door de bedreigingen van blockchain in kaart te brengen en ervoor te zorgen dat dit zichtbaar en bespreekbaar wordt.

Daarnaast zal de masterproef ook de kansen van de blockchaintechnologie trachten te achterhalen waardoor er niet uitsluitend sprake is van een probleemanalytisch onderzoek, maar tevens ook van een ontwerpgericht onderzoek: op die manier worden namelijk voorstellen tot verbetering van de (werk)processen van de geïntegreerde politie en het gebruik van blockchaintechnologie (voor de opsporing van high-tech crime) gedaan.

2.2.2 Schematisering van het onderzoeksmodel[*]



[*] Hardyns, W. (2018). *Onderzoeksontwerp in de criminologie*: Universiteit Gent, pg. 80.

2.3 Vraagstelling

Centraal in deze bijdrage staan de volgende onderzoeksvragen die de masterproef vormgeven:

Onderzoeksvraag 1	Wat is de huidige situatie op het vlak van barrières en noden voor de opsporing (van high-tech crime) binnen de geïntegreerde politie? – *Wat zijn de knelpunten bij de opsporing (van high-tech crime)?* – *Wat zijn de noden bij de opsporing (van high-tech crime)?*
Onderzoeksvraag 2	Wat houdt blockchain precies in? – *Waarom, wanneer en hoe is blockchain ontstaan?* – *Op welke manier werkt de blockchaintechnologie?* – *Wat betekent blockchain vandaag? Waarom is daar zoveel over te doen?*
Onderzoeksvraag 3	Waarom omarmen criminelen blockchain? – *Wat zijn de voordelen en/of opportuniteiten van blockchain voor de crimineel?* – *Wat zijn de toepassingsmogelijkheden van blockchain binnen het criminele milieu?*
Onderzoeksvraag 4	Wat zijn de (potentiële) 'Use Cases' van blockchain binnen de geïntegreerde politie (voor de opsporing van high-tech crime)? – *Wat zijn de toepassingsmogelijkheden van blockchain binnen de geïntegreerde politie?* – *Wat zijn de barrières voor, en de haalbaarheid van, blockchaintoepassingen voor de geïntegreerde politie?*

Dit zijn beschrijvende en verkennende vragen, om te gaan verklaren moet eerst hier een (wetenschappelijk) kritisch antwoord op geformuleerd worden. Pas dan kan het worden ingebed in een groter kader dat toepasbaar is voor de probleemstelling.

2.4 Gevolgde structuur

Deze masterproef is opgedeeld in twee grote delen die telkens werden onderverdeeld in hoofdstukken. Op het einde van elk hoofdstuk wordt in de conclusie een helder antwoord geformuleerd op een van de desbetreffende hoger geëxpliciteerde onderzoeksvragen.

Het eerste deel van de masterproef wordt gewijd aan een overzicht van de huidige situatie omtrent de opsporing van high-tech crime (digitaal forensisch onderzoek) binnen de geïntegreerde politie. In het *eerste hoofdstuk* van dit deel wordt dieper ingegaan op de barrières en hinderpalen (anno 2018-2019) bij het digitaal forensisch onderzoek binnen de geïntegreerde politie, welke problemen ze hierbij ervaren. Hieruit volgen de noden van het forensisch onderzoek in een geïnformatiseerde omgeving, welke instrumenten politiediensten nodig hebben om de (opsporings)processen te verbeteren. Zodat later een terugkoppeling in het licht van blockchain kan plaatsvinden.

Het tweede deel van de masterproef behandelt de blockchaintechnologie. In een *eerste hoofdstuk* wordt bijgedragen aan de beeldvorming rond blockchain. Het is de bedoeling de lezer op een globale, duidelijke manier kennis te laten maken met de blockchaintechnologie en te duiden waarom daar (vandaag) zoveel rond te doen is. Aan de hand van het *tweede hoofdstuk* wordt de lezer op de hoogte gebracht over de rol die de blockchaintechnologie kan spelen in verschillende criminele feiten om te begrijpen waarom politiediensten aandacht moeten hebben voor deze (veelbelovende) technologie. Tot slot worden in het *derde hoofdstuk* de potentiële '*Use Cases*' van blockchain binnen de geïntegreerde politie uitgelicht in het kader van de barrières en hinderpalen bij de geïntegreerde politie die zorgen dat het optimaal uitvoeren van forensisch onderzoek in een geïnformatiseerde omgeving (digitaal forensisch onderzoek) onder druk komt te staan. Op deze manier wordt een integraal beeld gegeven van de kansen die de

technologie te bieden heeft voor publieke opsporingsdiensten en wordt ook bijgedragen aan de agenda-setting om de blockchaintechnologie verder onder de aandacht te brengen.

2.5 Begripsbepaling[*]

Specifieke begrippen die in de masterproef een centrale rol krijgen toebedeeld, zullen ten gepaste tijde een concrete invulling krijgen. Daarnaast kan ook de trefwoordenlijst achteraan deze masterproef, geraadpleegd worden voor een begripsomschrijving.

[*] Trefwoordenlijst (zie achteraan deze masterproef).

ONDERZOEKSTECHNISCH ONTWERP

3. Methodologie

3.1 Onderzoeksstrategie

3.1.1 Algemeen: design van het onderzoek

Om de centrale vragen, die deze masterproef vooropstelt, te kunnen beantwoorden, is het noodzakelijk een onderzoek op het getouw te zetten. Voordat het onderzoek begint is het nodig om een methodologisch kader uit te bouwen dat als plan dient om het hele proces vorm te geven. Dit onderdeel en bij uitbreiding de hele masterproef wordt ontwikkeld op basis van een iteratief-parallelle visie. Het onderzoek wordt dus gezien als een proces waarvan diverse aspecten gelijktijdig worden gerealiseerd en waarbij continu teruggekeken wordt naar eerdere bevindingen en beslissingen, die indien nodig worden afgestemd (Hardyns, 2018).

In deze masterproef worden de gegevens verzameld aan de hand van een verkennend literatuuronderzoek aangevuld met resultaten (afkomstig van empirische gegevens) die werden verzameld tijdens de stageperiode bij de Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent – Plukteam (academiejaar 2017-2018). Het onderwerp leent zich uitstekend voor een exploratief onderzoek. Decorte en Zaitch (2016) omschrijven het exploratief onderzoek als volgt:

> Het doel van een exploratief onderzoek is te komen tot inzichten op een domein waar tot nu toe weinig over geweten is. (…) De verantwoording van een verkennend onderzoek gaat in essentie over het ontdekken van nieuwe domeinen. Het kan ook zijn dat de onderzoeker een domein waar al wel heel veel over geweten is gebruikt om een nieuwe onderzoeksdoelgroep te bestuderen. Los van de doelgroep waarvoor dit

> belangrijk kan zijn, wordt het belang van dit soort onderzoek gekenmerkt door het feit dat er weinig is geweten over het onderwerp en dat er een zekere noodzaak is om meer te weten (Decorte & Zaitch, 2016).

Het exploratief onderzoek dient beschouwd te worden als een verkenning van een nagenoeg onbetreden terrein. Dit is ook hier het geval. Er is immers (in België) nog niet onderzocht hoe blockchain de (werk)processen binnen de (geïntegreerde) politie kan beïnvloeden. Er zal dan ook getracht worden om uit de resultaten van dit onderzoek nieuwe kennis te vergaren, die aanleiding kunnen geven tot verder onderzoek. Voorliggende studie wil met andere woorden een bijdrage leveren aan de kennisontwikkeling.

Om de onderzoeksvragen te kunnen beantwoorden wordt de focus gelegd op een literatuur- en bronnenonderzoek. Het gaat hierbij om een exploratief onderzoek o.b.v. een bureauonderzoek als onderzoeksstrategie, waarbij tot doel gesteld wordt de bestaande kennislacunes op te vullen.

3.1.2 Keuze voor de onderzoeksstrategie

Bij het uitvoeren van een onderzoek dienen er diverse keuzes te worden gemaakt. Er dient gekozen te worden voor een bepaalde onderzoeksstrategie: ‘een geheel van met elkaar samenhangende beslissingen over de wijze waarop je het onderzoek gaat uitvoeren’ (Hardyns, 2018).

In deze masterproef zal de onderzoeksstrategie “bureauonderzoek” worden toegepast. Gezien het fenomeen dat behandeld wordt in dit onderzoek (de blockchaintechnologie), en de complexiteit ervan, zal het onderzoek eerder focussen op breedte, dan op diepgang. De logische

onderzoeksstrategie (die voortkomt uit de doel-, vraagstelling en onderzoeksobject) is dan ook het bureauonderzoek.

Een bureauonderzoek is een onderzoeksstrategie waarbij de onderzoeker gebruik maakt van door anderen geproduceerd materiaal, dan wel waar hij of zij probeert via reflectie en het raadplegen van literatuur tot nieuwe inzichten te komen (Hardyns, 2018). Dit betekent dat er bij bureauonderzoek niet het veld in wordt gegaan om door middel van eigen zintuiglijke waarneming data te verzamelen. Er kunnen twee varianten van het bureauonderzoek onderscheiden worden, namelijk literatuuronderzoek en secundair onderzoek (Hardyns, 2018). In dit werkstuk zal, in een eerste luik, de focus op het literatuuronderzoek gelegd worden. Hierbij wordt ook gebruik gemaakt van empirisch materiaal dat werd verzameld tijdens de stageperiode. Deze manier van onderzoeken wordt gebruikt om de stand van zaken op een bepaald terrein of thema (in dit geval barrières en noden binnen de geïntegreerde politie bij de opsporing van high-tech crime) in kaart te brengen. In een tweede luik zal het literatuur- en bronnenonderzoek worden aangewend voor een technologieverkenning en een analyse van een aantal (bestaande) blockchain-initiatieven.

Voor deze keuze zijn een aantal redenen te noemen. Op de eerste plaats is een dergelijke strategie aantrekkelijk indien er materiaal voorhanden is dat past bij de doel- en vraagstelling (Hardyns, 2018). Op basis van de (niet-gepubliceerde) bachelorproef[12] en na een kort vooronderzoek, is gebleken dat het benodigde onderzoeksmateriaal kan worden gevonden uit onder meer de (internationale) (vak)literatuur. De keuze voor deze onderzoeksstrategie moet echter ook gesitueerd worden in het schrijven van de bachelorproef en in het verlengde van de

[12] Vrolix, T. (2017). *Technologie & Innovatie: De keerzijde van de medaille. Onderzoek naar de illegale (internet)handel*. Faculteit Recht en Criminologie. Universiteit Gent.

stage-ervaringen[13] in de bacheloropleiding criminologische wetenschappen en het daaraan gekoppeld uitwerken van de stageopdracht. In het kader van het maken van die stageopdracht werd interne literatuur[14] geraadpleegd. Bijgevolg zijn er voldoende kennis- en databronnen voorhanden die passen bij de doel- en vraagstelling van dit onderzoek.

Kortom, dataverzameling over het onderzoeksobject op basis van eigen zintuigelijke waarnemingen is hier niet noodzakelijk om de doel- en vraagstelling van het onderzoek te kunnen bereiken. Immers, één alles dominerende stelregel die voor elke onderzoeksstrategie geldt, is namelijk dat bij de uitvoering van een onderzoek systematisch wordt toegewerkt naar een antwoord op de vragen in de vraagstelling (Hardyns, 2018). Dit is dan ook de belangrijkste voorwaarde voor een geslaagd onderzoek (Hardyns, 2018).

Net als alle onderzoeksstrategieën heeft het bureauonderzoek een aantal voor- en nadelen. Het belangrijkste voordeel is dat de onderzoeker met behulp van deze onderzoeksstrategie snel over een groot aantal gegevens kan beschikken (Hardyns, 2018). Gezien de beperkte tijd (één academiejaar) die voor deze masterproef beschikbaar is, is dit een belangrijk voordeel. Een ander voordeel van deze strategie ligt in de betrouwbaarheid van het verzamelde materiaal. Tijdschriften en/of boeken met een goede reputatie streven ernaar alleen de beste, belangrijkste en meest actuele artikelen en/of materiaal te publiceren, en hanteren dus een strenge toetsing. Een nadeel van het bureauonderzoek is dat het materiaal waarvan gebruik wordt gemaakt door de onderzoeker, in principe voor andere doeleinden is verzameld. De onderzoeker moet daarom

[13] Stageplaats: Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent – Plukteam. Stageopdracht 2017-2018 – "Inbeslagname van virtueel crimineel vermogen (e-currency). Een (praktische) handleiding voor politieambtenaren": De stageopdracht omvatte het schrijven van een handleiding om virtuele currencies (bijv. Bitcoin) in beslag te nemen in het kader van een (vermogens)onderzoek. De blockchaintechnologie is ontstaan als de technologie achter het elektronische betaalmiddel Bitcoin.

[14] Processen-verbaal, gerechtelijke dossiers, documenten (gevoelige informatie en vertrouwelijke documenten) die tijdens de stage konden ingekeken en bestudeerd worden.

zijn onderzoeksontwerp vaak aanpassen aan de aard en omvang van het beschikbare materiaal (Hardyns, 2018). Dit nadeel impliceert dat de onderzoeker bijna onvermijdelijk een eenzijdige blik op het onderzoeksmateriaal krijgt. In deze masterproef wordt getracht dit probleem op te lossen door gebruik te maken van materiaal van verschillende auteurs. De resultaten van dit onderzoek zullen enkel exploratief gebruikt moeten worden.

3.1.3 (Methodologische) beperkingen

Een beperking van deze studie is dat de blockchaintechnologie relatief nieuw en nog steeds volop in ontwikkeling is waardoor concrete toepassingen zich meestal in een vroeg stadium bevinden (d.w.z. de meeste zijn voorgestelde concepten en systemen die nog moeten worden geïmplementeerd). Bovendien heeft de keuze voor het bureauonderzoek als gevolg dat de onderzoeksresultaten enkel gebaseerd zijn op doorgenomen (vak)literatuur, interne literatuur[14], secundaire data en resultaten van eerder verricht onderzoek.

Hieronder volgt een overzicht van de methode van dataverzameling en het onderzoeksmateriaal waarop een beroep werd gedaan om een antwoord te formuleren op de verschillende onderzoeksvragen.

3.2 Methode van dataverzameling en data-analyse*

Het internetgebruik is sinds lang aan een opmars bezig. Vandaag pluggen we moeiteloos en zonder merkbare vertraging op het internet in via tablets, gsm's en andere elektronische hulpmiddelen (Decorte & Zaitch, 2016). Volgens Decorte en Zaitch (2016) heeft het sociale

* De discretieplicht en alle gangbare normen voor de ethisch correcte behandeling van onder meer de interne literatuur worden gerespecteerd. Hierbij wordt rekening gehouden met 'onderzoeksintegriteit' (zie www.ugent.be/integriteit). De student blijft per slot van rekening gebonden door de discretieplicht en aan de beroepscode van de stageplaats (Pauwels, 2018).

leven zich hierdoor voor een deel naar de onlinewereld verplaatst en kan het vaak niet meer los van mekaar gezien worden (Decorte & Zaitch, 2016). Het internet verdringt vandaag immers meer en meer de klassieke communicatiemiddelen. Birnhaum (2004)[15] stelt vast dat deze toename van het internetgebruik hand in hand gaat met de groei van dito research. Barchard en Williams (2008)[16] voorspellen dat deze onderzoeksvorm in de toekomst nog zal toenemen (Decorte & Zaitch, 2016).

Het mag dan ook niet verbazen dat wetenschappers zich steeds meer op onlineonderzoek toeleggen (Decorte & Zaitch, 2016). 'Telemetrics', het verzamelen van gegevens over een afstand, biedt wetenschappers enkele belangrijke voordelen. Zo genieten ze hetzelfde gebruiksgemak (snelle en constante toegang) als de gebruikers van het web. Bovendien kunnen klassieke onderzoeksmethoden vaak eveneens in een onlinesetting, toegepast worden (Decorte & Zaitch, 2016). Zo is documentanalyse eveneens mogelijk via het internet. Vele boeken, tijdschriften, rapporten en magazines zijn in quasi oorspronkelijke vorm online te vinden. In dit geval kunnen de principes van traditionele documentanalyse vrijwel geheel op deze onlinevariant geprojecteerd worden (Decorte & Zaitch, 2016).

Zoals eerder aangehaald zullen de benodigde gegevens om een antwoord te zoeken op de onderzoeksvragen verzameld worden aan de hand van een literatuur- en bronnenonderzoek aangevuld met de resultaten uit de interne stageopdracht. De combinatie van beide moet

[15] Birnbaum, M. H. (2004). Human research and data collection via the internet. *Annual Review of Psychology, 55*(1), 803-832. Retrieved from https://www.annualreviews.org/doi/abs/10.1146/annurev.psych.55.090902.141601. doi:10.1146/annurev.psych.55.090902.141601

[16] Barchard, K. A., & Williams, J. (2008). Practical advice for conducting ethical online experiments and questionnaires for United States psychologists. *Behavior Research Methods, 40*(4), 1111-1128. Retrieved from https://doi.org/10.3758/BRM.40.4.1111. doi:10.3758/brm.40.4.1111

toelaten integraal inzicht te krijgen in de materie en een onderbouwde conclusie af te werken die, in een terugkoppeling naar de onderzoeksoptiek, peremptorisch de doelstelling nastreeft.

Het literatuuronderzoek is een diepgaand onderzoek en daarom is de sneeuwbalmethode uitgevoerd. Hierbij is via gevonden literatuur nieuwe bruikbare informatie gevonden. Middels valide bronnen wordt met deze methode efficiënt bruikbare extra informatie achterhaald. Wetenschappelijke (vak)literatuur is gezocht in handboeken, academische tijdschriftartikelen en wetenschappelijke onderzoeken enzovoort. Door gebruik te maken van de databases[17]: BJu Tijdschriften, Google Scholar, IEEE Xplore, Jurisquare, MEDLINE/PubMed, Maklu-Online, ProQuest, ResearchGate, ScienceDirect, Scopus, Springer Link, Taylor & Francis Online, UniCat, Universiteitsbibliotheek Gent (lib.ugent.be), Web of Science en WorldCat, zijn relevante artikelen naar boven gekomen. In deze databanken is gezocht naar literatuur aan de hand van (een combinatie van) volgende trefwoorden[18]:

(*"blockchain of custody", "an overview of blockchain technologies", "bitcoin", "blockchain", "blockchain and law", "blockchain belgië", "blockchain criminal actions", "blockchain europe", "blockchain governance", "blockchain impact on society", "blockchain innovation", "blockchain investigation", "blockchain opportunities", "blockchain revolution", "blockchain technology", "blockchaintechnologie", "comité p", "computer crime units", "consortium blockchain", "criminal investigations blockchain", "cryptocurrency", "cybercrime 2019", "dark web", "decentralization", "decentralized darknetmarkets", "digital currencies", "disruptive technology", "distributed ledger technology", "ethereum", "forensic investigation", "gdpr", "high-tech crime", "innovatieve technologische ontwikkelingen", "kadernota integrale veiligheid", "law enforcement*

[17] De beschikbare databases als UGent student.
[18] Om de transparantie van het onderzoek te verhogen (niet-exhaustieve lijst).

blockchain", "law enforcement directive", "nationaal veiligheidsplan", "nieuwe technologieën", "opsporing in de criminologie", "opsporingsmogelijkheden high-tech crime", "opsporingsvraagstukken", "policing the future", "politionele onderzoekstechnieken", "challenges and opportunities in blockchain", "smart contracts", "supply chain", "systematic literature review of the use of blockchain", "technological innovations", "technology-led policing", "toekomst politie", "toekomstvisie politie", "use cases blockchain").

Sommige relevante gepubliceerde tijdschriftartikelen en/of boeken zijn gevonden in de Universiteitsbibliotheek Gent en/of bibliotheek De Krook (Gent). Deze tijdschriften en/of boeken zijn niet allemaal digitaal toegankelijk, daarom zijn bepaalde uitgaven handmatig doorzocht op relevant materiaal. Met name 'Panopticon'[19] is ook zeer belangrijk geweest bij de totstandkoming van de masterproef. Tevens zijn de voetnoten van reeds gevonden wetenschappelijke artikelen gebruikt om andere artikelen te vergaren. De literatuur werd naderhand opgezocht en inhoudelijk bekeken of het artikel bruikbaar was.

3.3 Onderzoeksmateriaal

Doorgaans verdient het aanbeveling om bij de uitvoering van een onderzoek meerdere bronnen aan te boren. In dit verband spreken we van bronnentriangulatie (Hardyns, 2018). Een reden hiervoor is dat de diverse bronnen, gezien vanuit de doel- en vraagstelling, elk hun eigen mogelijkheden en onmogelijkheden, sterke en zwakke punten kunnen hebben (Hardyns, 2018).

[19] Panopticon werd in 1980 opgericht als "Tijdschrift voor Strafrecht, Criminologie en Forensisch welzijnswerk". Voor het eerst wordt een forum gecreëerd waarin alle informatie over wat er zich in en rond de strafrechtsbedeling, de criminologie en het forensisch welzijnswerk afspeelt, systematische en deskundig aan bod komt (Maklu-Online, 2019).

3.3.1 Literatuur

De literatuur wordt gebruikt om de stand van zaken op te maken in een bepaald onderzoeksgebied. Een grondige kennis van het onderwerp is nodig alvorens het onderzoek van start kan gaan. Zowel wetenschappelijke als niet-wetenschappelijke (grijze) literatuur maken hier deel van uit.

De literatuur biedt de basis (conceptueel model) die nodig is om op een efficiënte manier onderzoeksmateriaal te verzamelen. Dit omdat de literatuur onontbeerlijk is voor het definiëren en operationaliseren van de kernbegrippen uit de doel - en vraagstelling van het onderzoek (Hardyns, 2018). Op die manier kunnen achteraf ook makkelijk de eigen bevindingen (reflectie) gekoppeld worden aan de bestaande informatie. Het is evenwel niet aangewezen om het gebruik van een literatuuronderzoek te beperken enkel om het conceptueel kader uit te werken (Deckx & Cools, 2012). Er zijn altijd ruimere paradigma's waarin de onderzoeksstrategie past. Het kan voor verruiming zorgen door het eigen onderzoek aansluiting te geven in een bredere onderzoekstraditie (Decorte & Zaitch, 2016). Bovendien is de literatuur in deze masterproef gelijk aan het literatuuronderzoek als variant van de gekozen onderzoeksstrategie (cfr. 3.1). De relevante literatuur werd gezocht via de beschikbare databases[17] als UGent student. De meest gebruikte tijdschriften en/of (hand)boeken werden geraadpleegd in een van de vele bibliotheken van de Universiteit Gent en/of bibliotheek De Krook, met als voornaamste de Faculteitsbibliotheek Recht en Criminologie. Opzoekingen werden gedaan via 'lib.ugent.be' (https://lib.ugent.be/), de database van de Universiteitsbibliotheek Gent. De gebruikte wetenschappelijke artikels en/of boeken zijn nagenoeg allemaal op elektronische manier geraadpleegd.

Het grootste voordeel van literatuur is dat er inzicht verkregen kan worden in de complexe werking van blockchain. Daarnaast is het ook een snelle manier om kennis te vergaren aangezien er beroep wordt gedaan op bestaande informatie en inzichten (Jesson, Matheson, & M. Lacey, 2011). Een mogelijk nadeel aan de keuze voor literatuur is het feit dat voor bepaalde onderwerpen literatuur niet altijd even uitgebreid aanwezig is. Om hieraan tegemoet te komen werd ervoor gekozen bepaalde informatie aan te vullen met secundaire data[20].

3.3.2 Interne stageopdracht (websurvey*)

Naast literatuur zijn ook personen (lees: politieambtenaren) zelf onontbeerlijk omdat een deel van de masterproef handelt over de barrières en noden bij de opsporing van high-tech crime binnen de geïntegreerde politie. Bijgevolg is inzicht belangrijk in de (basis)kennis van politieambtenaren omtrent bepaalde thema's die verband houden met het onderwerp van deze masterproef. Als aanvulling op de wetenschappelijke literatuur hieromtrent wordt in deze masterproef gebruik gemaakt van de resultaten verkregen uit eerder verricht onderzoek (secundaire data[!]). De resultaten zijn afkomstig uit de interne stageopdracht. De data werden verzameld in het verlengde van de stage-ervaringen[13] (Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent – Plukteam) in de bacheloropleiding criminologische wetenschappen, als onderdeel van de desbetreffende interne stageopdracht. Het voordeel is dat je als student-stagiair bij de federale politie toegang hebt tot moeilijk bereikbare respondenten en/of groepen. Het contacteren van respondenten en het vervolgens verkrijgen van hun medewerking, zijn namelijk twee aparte zaken (Mariën & Courtois, 2012). Door het effectief deelnemen in de

[20] Empirische gegevens die door andere onderzoekers (of door jezelf) in een eerder onderzoek bijeen zijn gebracht (Hardyns, 2018).

[*] Resultaten afkomstig uit interne stageopdracht (academiejaar 2017-2018): Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent.

[!] Dit houdt in dat de student geen data management plan dient voor te leggen (er worden in dit onderzoek namelijk geen empirische data verzameld). Een informed consent voor het gebruik van de resultaten is echter wel noodzakelijk (interne stageopdracht) (cfr. 3.3.2.3).

dagdagelijkse activiteiten wordt vertrouwen gecreëerd waardoor het effectief verkrijgen van actieve medewerking kan worden bekomen (Mariën & Courtois, 2012).

De empirische gegevens werden verzameld aan de hand van een gestandaardiseerde vragenlijst afgenomen via het internet (websurvey), onder de vorm van een quiz. De digitale quiz werd georganiseerd over de hele FGP Oost-Vlaanderen (Dendermonde, Gent, Oudenaarde). Het onderwerp van deze masterproef sluit (grotendeels) aan bij de materie van de interne stageopdracht waardoor de resultaten ook kunnen gebruikt worden ter ondersteuning van de literatuur in deze masterproef.

3.3.2.1 Quiz

Aan de hand van een korte digitale quiz, georganiseerd tijdens de stageperiode (academiejaar 2017-2018) in samenwerking met de *Innovation Group "Dark Web en E-Currency"* binnen de FGP OVL, werd getracht een beter beeld te krijgen over de stand van kennis betreffende de thema's *dark web*[21] en *e-currency*[22] bij politieambtenaren. De (hyper)link naar de quiz (websurvey) werd via e-mail doorgestuurd naar alle afdelingen (secties) en kon via het interne netwerk van de FGP OVL worden geopend en ingevuld. Er werd gewerkt met een 'incentive' (een beloning of geschenkje om mensen te stimuleren aan het onderzoek mee te doen) waarbij de "groep" die de meeste punten behaalde op de quiz, een beloning kreeg voor de (hele) sectie.

[21] Het dark web kan gezien worden als een vorm van 'high-tech crime'. High-tech crime als overkoepelend containerbegrip verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT (van der Hulst & Neve, 2008). Mede door de ontwikkeling van nieuwe internettechnologieën zijn onder andere illegale onlinemarkten de laatste tien jaar sterk in opmars. Sommige leveranciers zijn actief op het dark web, die ondersteund worden door technologieën en anonimiseringsdiensten die de identiteit van kopers en verkopers geheim houden (Europees Waarnemingscentrum voor drugs en drugsverslaving, 2017). Het is het deel van het internet dat het meest bekend is voor illegale activiteiten, vanwege de anonimiteit die het biedt aan gebruikers (European Monitoring Centre for Drugs and Drug Addiction, 2016).

[22] Virtuele munten ("e-currency") zoals Bitcoin worden ondersteund door blockchaintechnologie. In haar *Internet Organised Crime Threat Assessment (IOCTA)* van 2017 stelt Europol dat e-currency het betaalmiddel blijven voor cybercriminelen (Europol, 2017b).

Het gebruik van 'incentives' of geschenkjes kan de responsgraad drastisch verhogen (Pauwels, 2015). Bij een ex aequo op de quiz was de groep waarvan alle leden het eerste hadden gereageerd, de winnaar.

Deze manier van enquêteren werd toen gekozen opdat alle verschillende afdelingen van de FGP OVL konden worden bevraagd op een 'aantrekkelijke' manier en in een zo kort mogelijk tijdsbestek. De lay-out van een vragenlijst vormt immers het sluitstuk: een vragenlijst die slordig en chaotisch is opgesteld laat een slechte indruk na en kan leiden tot een hogere non-respons en item non-respons (Pauwels, 2015). Onder lay-out verstaat men de grafische lay-out, maar ook de presentatie van de vragen en antwoorden (in dit geval onder de vorm van een digitale quiz) (Pauwels, 2015). Zo kon de bereidheid en de bereikbaarheid van de respondenten (politieambtenaren) om deel te nemen worden vergroot.

De websurvey bestond uit 15 gesloten vragen met voorgestructureerde en vaste antwoordcategorieën[23]. De respondenten dienden het antwoord dat het best bij hen paste aan te kruisen. Men spreekt van *multiple choice* vragen of meerkeuzevragen (Pauwels, 2015). De vragen werden afgestemd op het taalgebruik en de cognitieve kennis van de doelgroep. De (hyper)link naar de websurvey werd via e-mail verstuurd naar 253 medewerkers (politieambtenaren). In totaal hadden 107 medewerkers, verspreid over 19 verschillende afdelingen[24] van de FGP OVL, deelgenomen aan de websurvey. De verkregen data werden (anoniem) verwerkt met het statistisch verwerkingspakket SPSS. De websurvey die werd gebruikt voor de respondenten binnen het politiewezen is terug te vinden in bijlage 1.

[23] De digitale quiz bestond uit 15 vragen waarbij de maximale score per vraag 1 punt is. Het maximaal aantal te behalen punten = 15 en 1 punt = 6,66% van de totaal te behalen punten.
[24] DRUGS DE, DRUGS GE, EIGENDOMMEN GE, EIGENDOMMEN OU / FINCRIM OU, FINCRIM DE, FINCRIM GE, GEWELD DE, GEWELD GE, LIB / SCI, LTWP DE, LTWP OU, MENSENHANDEL, MENSENSMOKKEL, MILIEU & BIJZONDERE ZAKEN, OMA, OPS / REM, PLUK, RCCU, TERRO. (DE = DENDERMONDE, GE = GENT, OU = OUDENAARDE) – Zie bijlage 3: Organigram FGP OVL.

3.3.2.2 Verwerking

Voorafgaand aan het gebruik van de resultaten van de interne stageopdracht werd via e-mail toestemming gevraagd aan de (huidige) stagebegeleider op de stageplaats, om deze te mogen (her)gebruiken voor dit onderzoek. De stageopdracht was immers een interne opdracht enkel bedoeld voor de stageplaats en dus niet geschikt voor publicatie. De student blijft per slot van rekening gebonden door de discretieplicht en aan de beroepscode van de stageplaats (Pauwels, 2018). Bij de rapportering in dit onderzoek worden geen namen van personen vermeld. Zoals eerder beschreven wordt er enkel gebruik gemaakt van de resultaten, statistische gegevens zoals figuren en tabellen, als visuele toelichting ter verduidelijking. Het presenteren van resultaten in de vorm van figuren is vaak zeer verhelderend (Pauwels, 2015). In figuren kunnen gegevens zó worden gepresenteerd dat de onderlinge relaties tussen gegevens, of de dynamiek van gegevens in één oogopslag zichtbaar worden (Pauwels, 2015).

3.3.2.3 Ethische principes: informed consent

Via de schriftelijke communicatie (e-mail) geeft de (huidige) stagebegeleider van de stageplaats de toestemming om de resultaten van de websurvey (uit de interne stageopdracht) op anonieme wijze te bewaren en te rapporteren. In bijlage 2 kan de desbetreffende schriftelijke communicatie hieromtrent worden teruggevonden.

3.3.3 Documenten

Voor dit onderzoek werden ook veel documenten geraadpleegd. Er werden reeds enkele documenten gepubliceerd die de blockchaintechnologie onder de aandacht brachten. Van documenten bestaat een grote diversiteit zoals onderzoeksverslagen, jaarverslagen van

organisaties, rapporten en whitepapers[25]. Hierin worden onder andere (bestaande) blockchain-initiatieven beschreven die nuttige informatie opleveren voor het beantwoorden van de doel- en vraagstelling. In de meeste onderzoeken kunnen documenten van allerlei aard belangrijke aanvullende gegevens opleveren (Hardyns, 2018).

3.3.4 Media

Een vierde informatiebron in deze masterproef is de media, en in het bijzonder het internet. Met media zijn bedoeld overbrengers van informatie die bestemd is voor een breder publiek (Hardyns, 2018). Verreweg de belangrijkste databron van deze soort is het internet. Via allerlei (wetenschappelijke) zoeksystemen op het internet is tegenwoordig op de meest uiteenlopende gebieden een immense stroom van gegevens beschikbaar (Hardyns, 2018). Er zijn verschillende zoeksystemen voorhanden waardoor op een zeer snelle en goedkope manier via het internet naar informatie en gegevens kan worden gezocht. Via het internet kan wetenschappelijke literatuur worden opgezocht maar tevens ook niet-wetenschappelijke bronnen zoals filmpjes, fora, websites, … Er is met andere woorden een hoge informatiedichtheid (Hardyns, 2018). Wat wel in rekening moet worden gebracht, is de mate van validiteit. Een kritisch en selectief gebruik is geboden (Hardyns, 2018). Om hieraan tegemoet te komen werd steeds geprobeerd wetenschappelijke ondersteuning te vinden voor de informatie die verkregen werd uit niet-wetenschappelijke bronnen. Verder geven media in de meeste gevallen informatie over situaties en processen in de empirische werkelijkheid (Hardyns, 2018).

[25] Een witboek of whitepaper is een document dat beschrijft hoe overheidsbeleid, een technologie, en/of product een specifiek probleem oplost. Witboeken worden gebruikt om de lezer van objectieve relevante informatie te voorzien die wordt gebruikt voor het nemen van een beslissing. Witboeken, wanneer deze objectief geschreven zijn, worden vaak beschouwd als een betrouwbare bron van informatie (Wikipedia, 2018).

DEEL I: OPSPORING VAN HIGH-TECH (CYBER)CRIME

1.1 De Belgische politie vandaag: barrières en hinderpalen

1.1.1 Inleiding

De manier waarop de politie functioneert lijkt over de jaren heen weinig te veranderen. De politie surveilleert, reageert op (meldingen van) incidenten en spoort verdachten van misdrijven op. De politie deed dat enkele decennia terug, en zij doet dat nog steeds (van der Vijver & Gunther Moor, 2014). Wie echter iets dieper graaft ziet echter dat er wel degelijk sprake is van veranderingen, op tal van terreinen (van der Vijver & Gunther Moor, 2014).

De veranderingen die men bij de politie kan waarnemen, hangen onder meer samen met veranderingen in de criminaliteit (nieuwe vormen van misdaad, veranderingen in de patronen van misdaad, verschuivende prioriteiten in de maatschappelijke onveiligheid) en ook meer in het algemeen veranderingen in de verwachtingen van de samenleving (van der Vijver & Gunther Moor, 2014). Ook op het gebied van de taken die de politie uitvoert is het nodige veranderd (Koops, 2016). Ondanks een aanzienlijke mate van continuïteit in het functioneren van de politie over de jaren heen, hebben maatschappelijke ontwikkelingen ervoor gezorgd dat de politie zich voortdurend heeft aangepast (van der Vijver & Gunther Moor, 2014). Als het gaat om (veranderingen in de) taken die de politie uitvoert speelt digitalisering een belangrijke rol (Koops, 2016). Die heeft de afgelopen jaren een enorme stempel gedrukt en zal dat, naar verwachting, in de toekomst blijven doen (Ekblom, 2017).

Onderzoeken vergen een steeds gedifferentieerdere en meer specifieke kennis. Sociale kennis en sociale vaardigheden waren altijd sterke punten van de politie, maar steeds vaker komt technologische kennis om de hoek kijken (van der Vijver & Gunther Moor, 2014). De technische vernieuwingen kwamen niet alleen politie en justitie ten goede, maar ook de

criminele wereld bleek ermee gebaat (Conings, 2017). De politie zal steeds meer kennis nodig hebben over vormen van criminaliteit waar gecomputeriseerde informatiesystemen een belangrijke rol spelen (van der Vijver & Gunther Moor, 2014). Cybercriminaliteit wordt immers beschouwd als één van de belangrijkste misdaadproblemen van het huidige tijdsgewricht (Kleemans et al., 2014). De Kadernota Integrale Veiligheid (KIV) 2016-2019[26] weerhoudt terecht "cybercrime en cybersecurity" als één van de 10 prioritaire clusters inzake veiligheid (FOD Justitie, 2016). Dankzij technologische mogelijkheden en netwerken ontstaan nieuwe vormen van criminaliteit en dus ook nieuwe c.q. andere vormen van opsporen (Kop & Klerks, 2017). Het spreekt voor zich dat dit ook veranderingen met zich meebracht voor de digitale recherche (Eeckhaut, De Ruyver, & Vermeulen, 2016). Meer en meer maken zowel politie- als andere diensten gebruik van nieuwe technologieën die op de markt komen[27] (Dalle, 2015). De inzet van informatietechnologie als opsporingsinstrument is, zoals we het kunnen en zullen opmerken, complex. Enerzijds wordt het opsporings- en vervolgingsproces van criminaliteit vereenvoudigd, anderzijds wordt het ook bemoeilijkt (Van Eyken, Vermeulen, & Depauw, 2018). De politie kan zich moeilijk permitteren achter de feiten aan te lopen. Als de samenleving – en daarmee de onveiligheid en criminaliteit van die samenleving – zich verplaatst naar het digitale tijdperk, dan moet de politie dáár ook aanwezig zijn (de Vries & Smilda, 2014). Alles wijst erop dat de (Belgische) digitale recherche een steeds grotere verantwoordelijkheid zal moeten gaan opnemen. Want voor politiediensten is het van belang om steeds up-to-date te blijven over welke technologische ontwikkelingen er op de markt zijn, de voordelen en beperkingen daarvan en welke normen er gelden (Boddez, 2019).

[26] FOD Justitie. (2016). *Kadernota integrale veiligheid 2016-2019*. Retrieved from https://justitie.belgium.be/nl/nieuws/andere_berichten_29

[27] Technologiegebieden voor de politie zijn onder meer: digitale beeldvorming; digitale beveiligingstechnieken; biometrie; chemische technologie; ICT; 'big data'-beheer en -analyse; cloud computing; display-technologie; elektronica; informatietechnologie; innovatieve materiaaltoepassingen; sensoren; nanotechnologie; netwerktechnologie; neurotechnologie; real audio en real video; internet of things (IOT); RFID (radio frequency identification devices) spraaktechnologie; wapentechnologie (Dalle, 2015).

1.1.2 Forensisch onderzoek in een geïnformatiseerde omgeving

1.1.2.1 Begripsafbakening

Het is haast niet mogelijk om cybercrime als één apart crimineel verschijnsel te onderscheiden, omdat veel vormen van criminaliteit tegenwoordig in meer of mindere mate met ICT verweven zijn (Bernaards, Monsma, & Zinn, 2012). De verschijningsvormen zijn zeer divers, evenals de mate waarin het gebruik van ICT een rol speelt. Nationaal en internationaal bestaan verschillen in definities van gebruikte terminologie (Bernaards et al., 2012). Dit maakt het noodzakelijk om te bepalen wat binnen de context van dit onderzoek met de term 'high-tech crime' wordt bedoeld. In deze masterproef wordt gebruik gemaakt van het uitgangspunt van VAN DER HULST en NEVE voor een begripsbepaling van een specifieke categorie van cybercrime: high-tech crime. In hun onderzoek bespreken van der Hulst en Neve (2008) 'High-tech crime' als overkoepelend containerbegrip dat verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT. Tegenover de term cybercrime biedt high-tech crime een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen vandaag de dag. Nieuwe criminaliteitsvormen die kunnen ontstaan door innovaties van ICT (en niet alleen het internet) worden door dit containerbegrip afgedekt (van der Hulst & Neve, 2008).

1.1.2.2 Digitale sporen

Het forensisch onderzoek in een geïnformatiseerde omgeving (digitaal forensisch onderzoek of forensisch ICT- onderzoek) betreft steeds een onderdeel van een opsporings- of gerechtelijk onderzoek (Comité P, 2018a). Met behulp van deze politionele onderzoekstechniek hebben politiediensten de afgelopen jaren technologisch slimme criminelen kunnen in rekenen (Diţu, 2017). Forensisch onderzoek of forensische wetenschap is sporenonderzoek dat gedaan wordt

ten behoeve van het strafrechtelijk onderzoek (N.O. Sadiku, Shadare, & M. Musa, 2017). Het helpt bij het opsporen van daders of de oorzaken van (mogelijke) misdrijven op basis van wetenschappelijk bewijsvoering (Wikipedia, 2017). Aangezien het meeste bewijsmateriaal tegenwoordig in digitale vorm wordt geleverd, werd digitaal forensisch onderzoek geïntroduceerd (Diţu, 2017). Computers spelen een steeds belangrijkere rol in alle aspecten van het menselijk leven, met inbegrip van betrokkenheid bij criminele handelingen (N.O. Sadiku et al., 2017). Criminaliteit laat dan ook vaak een elektronisch spoor achter (Garfinkel, 2013). Het verzamelen van deze forensische gegevens en digitaal bewijsmateriaal is met name van groot belang bij de aanpak van high-tech crime (Prayudi & Sn, 2015). Het levert niet alleen relevante informatie en bewijzen voor lopend onderzoek, maar draagt ook bij tot een beter begrip van de gebruikte criminele instrumenten/technologieën en methoden, waardoor waardevolle kennis wordt gegenereerd (Europol, 2017a).

Het bestrijden van high-tech crime en het verlenen van steun in de vorm van forensisch onderzoek in een geïnformatiseerde omgeving (digitaal forensisch onderzoek) waren en zijn bij de geïntegreerde politie opdrachten voor de computer crime units (CCU's) van de federale gerechtelijke politie (Comité P, 2018a). Naast de bestrijding van high-tech criminaliteit hebben de computer crime units van de federale politie (RCCU's en FCCU) ook als opdracht om steun te verlenen in het kader van de bestrijding van traditionele vormen van criminaliteit. Deze steun betreft dan onder meer bijstand bij huiszoekingen in geïnformatiseerde omgevingen, het kopiëren van digitale data, de forensische analyse van ICT-systemen en van geïnformatiseerde gegevensdragers of de bijstand bij technische verhoren (Comité P, 2018a). Uiteraard staat de bestrijding van high-tech crime niet los van het forensisch onderzoek in een geïnformatiseerde omgeving (Comité P, 2018a).

De organisatie en de werking van de CCU's[28] op federaal en regionaal vlak moeten garant staan voor enerzijds een efficiënte en tijdige bijstand aan politiediensten in het kader van gerechtelijke dossiers om alle relevante informatie in ICT-omgevingen op te sporen, te vrijwaren en in leesbare vorm ter beschikking te stellen van de rechercheurs (Politie, 2019). Anderzijds moet zij garant staan voor een doeltreffende bestrijding van alle vormen van ICT-criminaliteit door specialisatie, preventie, proactieve en reactieve interventies, waardoor de negatieve impact van deze criminaliteitsvorm op het maatschappelijke leven zo klein mogelijk wordt gehouden (Politie, 2019).

1.1.3 Barrières en hinderpalen bij het digitaal forensisch onderzoek

Het optimaal uitvoeren van steun in de vorm van forensisch onderzoek in een geïnformatiseerde omgeving staat evenwel vandaag de dag onder druk (Comité P, 2018a). De steun vanuit de federale politie in het ICT-domein is tot nog toe ondermaats geweest (Bruggeman, 2014). Bovendien wordt het strafrechtstelsel gekenmerkt door inefficiëntie (Devroe & Van de Velde, 2005). Terwijl technologie een (r)evolutie heeft teweeggebracht binnen het criminele milieu, blijft het rechtssysteem vaak verbonden met archaïsche praktijken en verouderde IT-systemen, wat resulteert in inefficiënte en steeds verder tekortschietende diensten (The Police Foundation, 2017). Voorts is de Belgische politie een kleine speler met een beperkt budget wat betreft (nieuwe) technologieën (Bruggeman, 2014). Ontwikkeling van eigen technologie zoals in een 'gesloten systeem' (kenmerkend in het 'bureaucratische' politiescenario[29]) is niet meer vol te houden en ook niet aangewezen (Bruggeman, 2014).

[28] Vanhecke, N. (2018). De laatste trekt de modem uit: eliteteam cyberspeurders loopt leeg. *De Standaard*. Retrieved from http://www.standaard.be/cnt/dmf20181101_03897625

[29] Een politie als sterke groep met een grote aandacht voor regels – een combinatie die dikwijls gepaard gaat met een sterke hiërarchie en veralgemeende acceptatie van de regels waardoor er een sterk risico is op een relatief gesloten gemeenschap (Bruggeman, 2014).

De achterstand ten opzichte van de technologische realiteit maakt het uiteraard erg moeilijk voor politie om het fenomeen van de informaticacriminaliteit (high-tech crime) daadwerkelijk en effectief te kunnen indijken (Van Eyken et al., 2018). Het bewaren van de vrede en het handhaven van de wet zijn verantwoordelijkheden die nu op de proef worden gesteld door de veranderende aard en toenemende gesofisticeerdheid van criminaliteit als gevolg van technologische innovaties (Accenture, 2013). Van der Hulst en Neve (2008) constateren dat gezien de steeds voortschrijdende technologische innovaties, ook op het gebied van ICT, het voor de hand ligt dat ook de criminele mogelijkheden in de toekomst verder zullen toenemen. De technologische expertise voor high-tech crime zal ook in het criminele milieu in toenemende mate professionaliseren (van der Hulst & Neve, 2008).

1.1.3.1 Comité P*

Gezien deze ontwikkelingen zoals hierboven beschreven besliste het Vast Comité P om een toezichtsonderzoek[30] te starten met als probleemstelling: *"Is de geïntegreerde politie optimaal georganiseerd en functioneel om voldoende resultaten te boeken in het kader van het forensisch onderzoek in een geïnformatiseerde omgeving?"* (Comité P, 2018a). Door de vele toezichtsonderzoeken en onderzoeken naar klachten die de Dienst Enquêtes van het Comité P verricht, heeft het Comité P een beeld van de actuele werking van de politie (Comité P, 2018b). In het kader van het toezichtsonderzoek van het Vast Comité P werd aan de federale politie

* De politie kent diverse controleorganen waarbij het Comité P de meest prominente rol opneemt voor wat de externe controle betreft (Bruggeman, 2014). Het Vast Comité van Toezicht op de politiediensten, kortweg Comité P, werd opgericht in 1991 vanuit de behoefte van het federale parlement om te beschikken over een extern controleorgaan op de politie (Comité P, 2018b). In de praktijk heeft de controledienst zich over het algemeen beziggehouden met de controle op conformiteit met wetten en regels ('wettelijke verantwoording'). De vraag of de politie steeds conform en binnen haar wettelijke bevoegdheden ageert is met andere woorden steeds de eerste focus geweest. Toch hebben ook hier evoluties plaatsgevonden. De controledienst is zich tevens gaan toeleggen op audits en studies die dieper ingaan op een goede politiezorg en dienstverlening in een meer algemene zin (Bruggeman, 2014).

[30] Comité P. (2018). *De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving*. Kamer van Volksvertegenwoordiger Retrieved from https://comitep.be/document/onderzoeksrapporten/2018-06-21%20Forensisch%20onderzoek.pdf

gevraagd een schriftelijke zelfevaluatie te maken. Uit het uitgebreide antwoord van de federale politie komen een aantal barrières en hinderpalen naar voor die de organisatie en/of de werking van het forensisch onderzoek in een geïnformatiseerde omgeving bedreigen (Comité P, 2018a).

1.1.3.1.1 Kennisbeheer

Kennisbeheer wordt meer en meer, terecht, gezien als een essentiële strategische managementtool binnen bedrijven en organisaties. Door het efficiënt en effectief beheren en gebruiken van kennis en ervaringen kan ingespeeld worden op tools en technieken, processen, (bedrijfs)risico's, … (Vanacker, 2018). Door de federale politie wordt echter opgemerkt dat er momenteel geen instrument beschikbaar is dat de uitwisseling van goede praktijken, kennis en ervaringen toelaat tussen de R/FCCU's onderling, evenals met de andere partners, de lokale politiezones en de parketten, wat nochtans noodzakelijk is bij een materie die voortdurend in ontwikkeling is (Comité P, 2018a). Aangezien de personele en materiële middelen bij de F/RCCU's beperkt zijn is een dergelijk instrument dringend nodig (Comité P, 2018a).

1.1.3.1.2 Dossierbeheersysteem

Door de federale gerechtelijke politie wordt het dossierbeheersysteem GES[31] gebruikt dat de opvolging van opsporings- of gerechtelijke onderzoeken mogelijk maakt. Het dossierbeheersysteem GES is gekoppeld aan het managementsysteem ITINERA[32] dat een overzicht geeft van alle lopende dossiers binnen de eenheid (zowel van toepassing op de FGP's

[31] Het systeem "GES" (*gestion dossier*) laat toe een digitaal dossier aan te leggen waarin informatie wordt gestructureerd in een vast canvas. Bovendien kan het diensthoofd het dossier digitaal mee opvolgen met behulp van de geïntegreerde werkfiche. Deze tool is beschikbaar voor zowel de federale als voor de lokale politie (Craps, 2017).

[32] Dit werkinstrument leent zich tot een actieve en diepgaande opvolging vanuit coördinatie en leiding. Volgens het principe van de éénmalige vatting worden een aantal gegevens vanuit GES overgenomen in ITINERA. Door een verdere aanvulling van de werkfiche door het diensthoofd in ITINERA, gekoppeld aan de geautomatiseerde flux van de status op niveau parket en de gepresteerde uren per dossier heeft de recherchemanager een goed zicht op de stand van zaken in de lopende dossiers (Craps, 2017).

als op de centrale operationele diensten) (Comité P, 2018a). Uit het onderzoek van het Comité P komt naar voor dat momenteel bij de federale gerechtelijke politie het dossierbeheersysteem GES evenwel niet toepasselijk is op het forensisch onderzoek in een geïnformatiseerde omgeving als onderdeel van een onderzoek (Comité P, 2018a). Om toch aan info- en recherchemanagement[33] te kunnen doen, inbegrepen de "intake procedure" die moet bepalen welke zaken prioritair zijn voor de CCU ten einde efficiënt om te kunnen gaan met de vele aanvragen, heeft elke eenheid zijn eigen methode om deze gegevens bij te houden (Comité P, 2018a). Dit gaat van het gebruik van een Microsoft Excel of Access tabel, tot de programmatie van een eigen ontwikkeld softwareprogramma[34] (Comité P, 2018a). Dit betekent dat bij de federale gerechtelijke politie de onderscheiden eenheden zelf bepalen op welke manier de CCU-werking wordt opgevolgd; er bijgevolg geen eenvormigheid is en het ook quasi onmogelijk is om aan vergelijkingen te doen tussen de eenheden, of om een centraal overzicht te hebben (Comité P, 2018a). Het Comité P beveelt dan ook aan dat in het kader van de geïntegreerde CCU-werking er ook op zeer korte termijn een eenvormig en dynamisch dossierbeheersysteem wordt ingevoerd.

De ontwikkeling van een dergelijk dossierbeheersysteem kan een belangrijke bijdrage leveren aan de ontwikkeling van een geïntegreerde werking, in eerste instantie omdat op die manier de behoeften op een eenvormige wijze zouden kunnen geobjectiveerd worden, waarna in toepassing van een gevalideerd model van taakverdeling, in functie van beschikbare middelen en capaciteit en in functie van de gestelde prioriteiten, de meest geschikte onderzoeker/onderzoekende dienst kan aangeduid worden (Comité P, 2018a).

[33] Recherchemanagement (ReM): de wisselwerking tussen het (zo ideaal mogelijk) afstemmen van de recherchecapaciteit op de beleidsprioriteiten.
[34] Antwoord van de federale politie d.d. 20.3.2017, 10. KISS: beheerprogramma ontwikkeld bij de FGP Turnhout – Keep It Short & Simple: https://www.nieuwsblad.be/cnt/dmf20130712_00657005

1.1.3.1.3 Data exploitatie

Bijkomend wordt door de werkgroep 'Samenwerking tussen de federale en de lokale politie in kader van forensische analyse in IT'[35] verder voorgesteld om een centraal systeem te voorzien waarop de tactische onderzoeker, zowel van de federale gerechtelijke politie als van de lokale recherche, data verder kan exploiteren die na extractie van het forensisch benaderde ICT-materiaal ter beschikking zijn gesteld (Comité P, 2018a). Daaraan zou een systeem kunnen gekoppeld worden voor de digitale neerlegging van de data op de griffies (Comité P, 2018a).

1.1.3.2 Memorandum 2019-2023 VCLP*

1.1.3.2.1 Informatiehuishouding

Al jaren kampt de geïntegreerde politie met problemen op het vlak van de informatievatting, het informatiebeheer en de uitwisseling van informatie (Bruggeman, 2014). De vraag is bovendien hoe informatie beter kan gedeeld worden (Bruggeman, 2014). Vandaag veroorzaakt de optimalisatie van de federale politie duidelijk ook een ontevredenheid bij de lokale politie

[35] In het najaar van 2016 werd de werkgroep 'Samenwerking tussen de federale en de lokale politie in kader van forensische analyse in IT' (ook werkgroep LCCU-RCCU-FCCU genoemd) opgericht nadat vanuit de FGP Oost-Vlaanderen bij directeur DJSOC en bij het diensthoofd van de FCCU een tweevoudige problematiek was aangekaart: (1) vanuit verschillende politiezones uit Vlaanderen werd aan de FCCU of de FGP Oost-Vlaanderen de vraag gericht om een deel van het forensisch onderzoek in de digitale wereld zelf te kunnen doen en daarbij ondersteund te worden in de aankoop van materiaal en de nodige opleidingen door de federale politie; of de vraag om verder ondersteund te worden in initiatieven die in de politiezones reeds genomen waren en dit teneinde deze taken correct te kunnen uitvoeren. (2) Anderzijds was er de vaststelling bij de RCCU's dat er heel wat achterstand was en is in de forensische analyse. Door de directeur-generaal van de federale gerechtelijke politie werd beslist dat deze problematieken in hun geheel dienden bekeken te worden en dat de FGP Oost-Vlaanderen daartoe een werkgroep zou oprichten om een aantal voorstellen uit te werken (Comité P, 2018a).

* De Vaste Commissie van de Lokale Politie (VCLP) werd opgericht bij artikel 91 van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Zij is voornamelijk samengesteld uit korpschefs van de lokale politie en is belast met het onderzoeken van of het geven van adviezen over alle problemen met betrekking tot de lokale politie op verzoek of op eigen initiatief (BeSafe, 2019). Het memorandum vormt de routeplanning voor en door de lokale politie, voor de komende vier jaar. In dit document bundelt de VCLP haar aanbevelingen aan de politieke besluitvormers voor de volgende legislatuur. De aanbevelingen van het Memorandum 2019-2023 zijn het resultaat van een tweedaags seminarie dat de VCLP in mei 2018 organiseerde voor alle korpschefs van de Lokale Politie (Vaste Commissie van de Lokale Politie (VCLP), 2019).

(Vaste Commissie van de Lokale Politie, 2019). De dienstverlening/steunopdracht van de federale politie kent klaarblijkelijk een aantal risico's en hinderpalen die de organisatie en/of de werking bedreigen (cfr. 1.1.3.1). Steeds meer lokale politiediensten worden geconfronteerd met cybercriminaliteit, zonder dat zij daarvoor de expertise van een FCCU of een RCCU in huis hebben (Comité P, 2018a).

Het samen bestaan van twee verschillende systemen vormt een obstakel voor een reëel geïntegreerde informatiehuishouding en -uitwisseling (Bruggeman, 2014). Het gevolg van de verouderde infrastructuur en de gebrekkige steun is dat lokale politiediensten steeds meer op zichzelf zijn aangewezen en dus zelf initiatieven moeten ontwikkelen die een ernstige financiële en/of capacitaire impact hebben (bijvoorbeeld de oprichting van een *Local Computer Crime Unit* (LCCU), etc.) (Vaste Commissie van de Lokale Politie, 2019). Zelfs diensten binnen de federale politie gaan individualistischer handelen en steeds meer eigen systemen ontwikkelen met een negatieve impact op de samenhang tot gevolg (Bruggeman, 2014).

De stijgende vraag naar nieuwe dienstverlening en handhaving in het veiligheidsdomein werken dit soort experimenten nog verder in de hand (Bruggeman, 2014). Deze evolutie heeft met andere woorden niet enkel budgettaire gevolgen, maar eveneens een grote impact op de kwaliteit van de lokale dienstverlening (Vaste Commissie van de Lokale Politie, 2019).

1.1.3.2.2 Centraal contactpunt

Wat de politionele diensten betreft, is er tot slot ook nood aan een centraal contactpunt om melding te maken van cyberaanvallen. Vaak verlopen dergelijke klachten via lokale politiediensten die niet over de vereiste expertise beschikken om hiermee om te gaan (Verbond van Belgische Ondernemingen, 2018). Cybercriminaliteit is grenzeloos, de huidige

gefragmenteerde structuur binnen de opsporingsdiensten is bijgevolg een zwak punt (Verbond van Belgische Ondernemingen, 2018).

1.1.3.3 Resultaten websurvey voor respondenten binnen het politiewezen (FGP OVL)*

De technologische ontwikkelingen en de toenemende complexiteit van de forensische onderzoeken vragen medewerkers met hogere en meer gespecialiseerde kennisniveaus (Comité P, 2018a).

Enerzijds blijkt uit het onderzoek van Janssens, Soetaert en De Vos (2017) dat heel wat politiemensen binnen bepaalde afdelingen van de (federale) politie niet in staat zijn om Bitcoin-onderzoek[36] te voeren omdat zij hier de kennis niet over hebben[37] (Janssens, Soetaert, & De Vos, 2017). De materie is zo complex dat onderzoekers uit andere teams vaak niet op de hoogte zijn van de werking van Bitcoins – dat wordt ondersteund door blockchaintechnologie – en bovendien ook niet weten hoe dit onderzocht dient te worden (Janssens et al., 2017). Bitcoins worden voornamelijk via het internet verstuurd waardoor al snel de link wordt gelegd met computers en bijgevolg het RCCU gecontacteerd wordt wat een (verdere) overbelasting van deze dienst tot gevolg heeft (Janssens et al., 2017).

Anderzijds kunnen we uit de resultaten van de websurvey (cfr. 3.3.2) vaststellen dat er wel enige (basis)kennis aanwezig is bij politieambtenaren van de FGP OVL betreffende dergelijke thema's als *'dark web'* en *'e-currency'*, maar dat deze kennis vooral versnipperd is over de

* Resultaten afkomstig uit interne stageopdracht (academiejaar 2017-2018): Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent (cfr. 3.3.2).

[36] Bitcoin maakt gebruik van de blockchaintechnologie, dit wordt verderop toegelicht.

[37] Dit betekent dat de ontvanger inhoudelijk begrip moet hebben van het onderwerp. Het betreft voornamelijk kennis omtrent het breder spectrum (bv. de mogelijkheden van de blockchaintechnologie, manieren waarop Bitcoins bewaard kunnen worden, aan -en verkoopproces, backupmethoden, multisignature wallets, shapeshift, forks, … etc.).

verschillende diensten heen. Dit bevestigd de nood aan een reëel geïntegreerde informatiehuishouding en -uitwisseling om de expertise omtrent high-tech crime, en bijgevolg de opsporing ervan, te vergroten.

Uit de resultaten kunnen we ook afleiden dat 42,3% van de respondenten (n=107) de vragen van de websurvey geldig beantwoordden. Er zijn 146 missing values. Er is dus sprake van 57,7% (n=146) item-nonrespons. De meest voorkomende score bedraagt 15 punten. De overgrote meerderheid (31,8% of 34 respondenten) van de respondenten die de websurvey wel hebben ingevuld (n=107) hebben dus de maximum score behaald en alle vragen correct beantwoord. De gemiddelde waarde bedraagt 12,96. Dit betekent dat de respondenten gemiddeld een 12,96 scoren op de quiz en aldus 'geslaagd' zijn (score > 9). 3,74% of 4 respondenten zijn 'niet geslaagd' voor de quiz (score < 10).

Bij het beantwoorden van de vragen was 'slechts' 31,8% of 34 respondenten zeker van zijn antwoord en derhalve (goed) op de hoogte van de materie ('*dark web*' en '*e-currency*'). 59,8% (n=64) had daarnaast aangegeven een combinatie te hebben gebruikt van het gokken en het hanteren van een hulplijn bij het beantwoorden van de vragen. Tot slot kan worden meegegeven dat 7,5% (n=8) van de respondenten op alle vragen gegokt hebben.

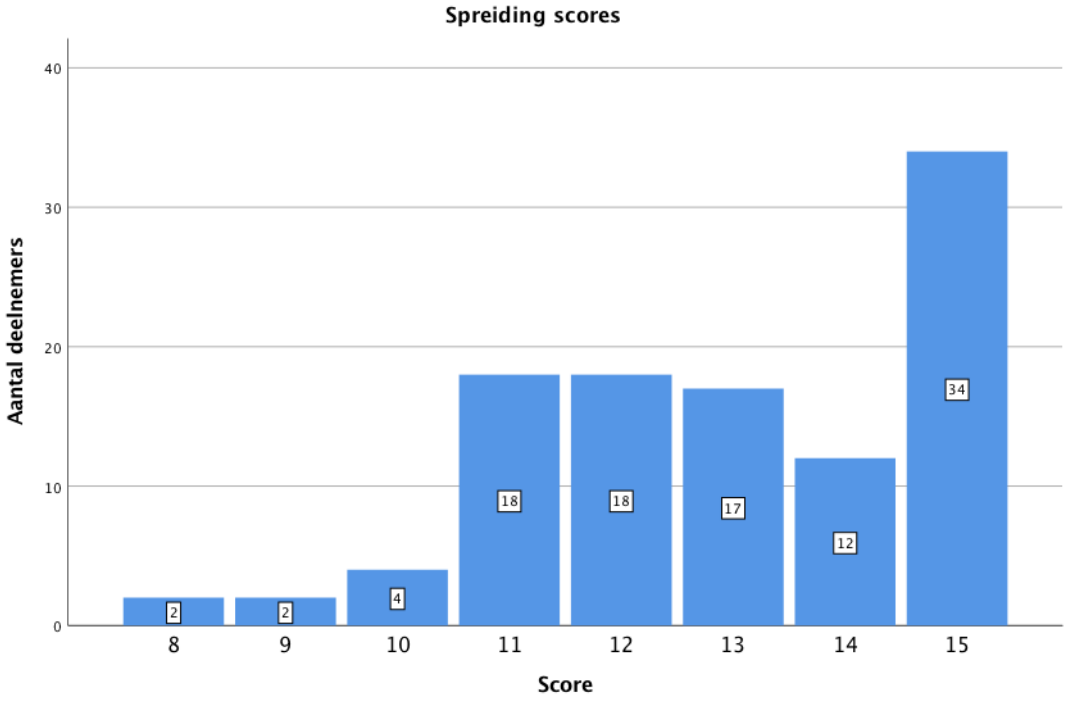
Statistics

score

N	Valid	107
	Missing	146
Mean		12.96
Median		13.00
Mode		15

score

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	8	2	.8	1.9	1.9
	9	2	.8	1.9	3.7
	10	4	1.6	3.7	7.5
	11	18	7.1	16.8	24.3
	12	18	7.1	16.8	41.1
	13	17	6.7	15.9	57.0
	14	12	4.7	11.2	68.2
	15	34	13.4	31.8	100.0
	Total	107	42.3	100.0	
Missing	System	146	57.7		
Total		253	100.0		



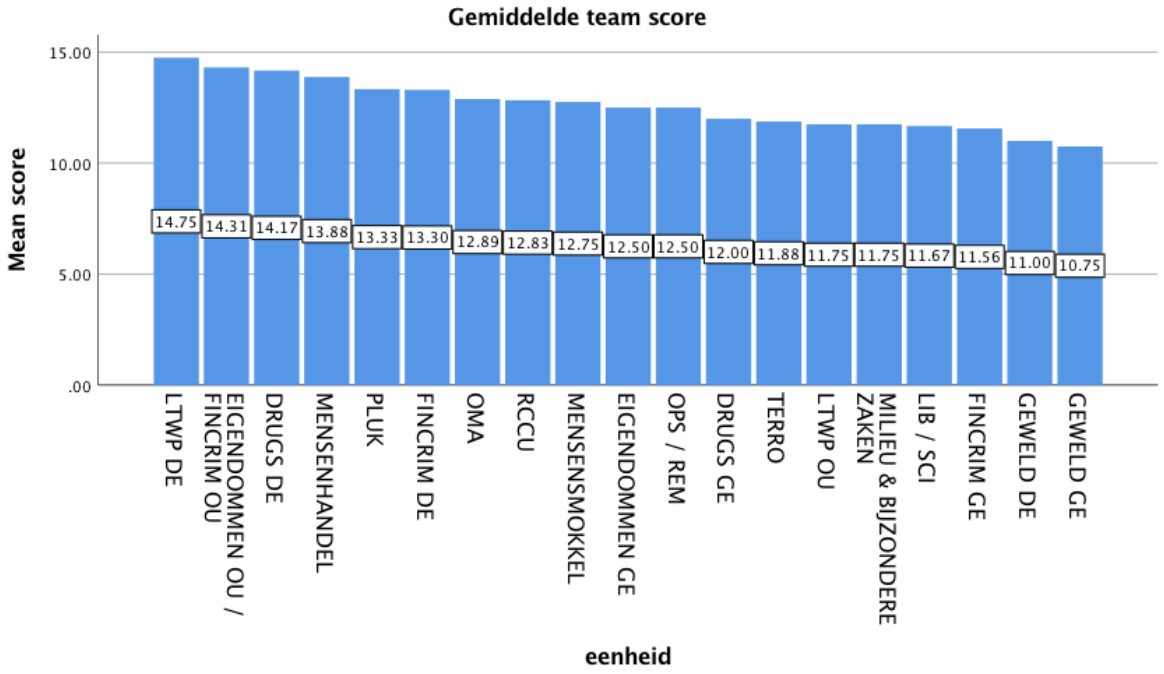
Figuur 1.1: spreiding scores

Case Processing Summary

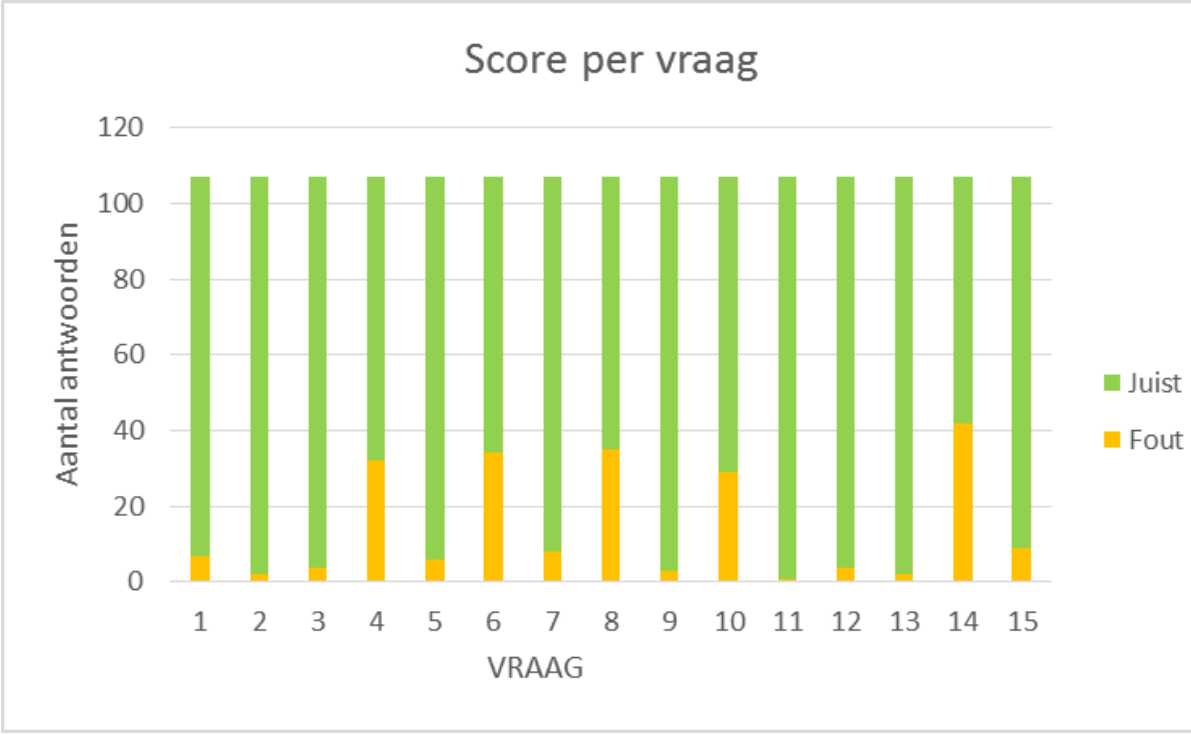
	Cases					
	Included		Excluded		Total	
	N	Percent	N	Percent	N	Percent
score * eenheid	107	42.3%	146	57.7%	253	100.0%

Gemiddelde team score

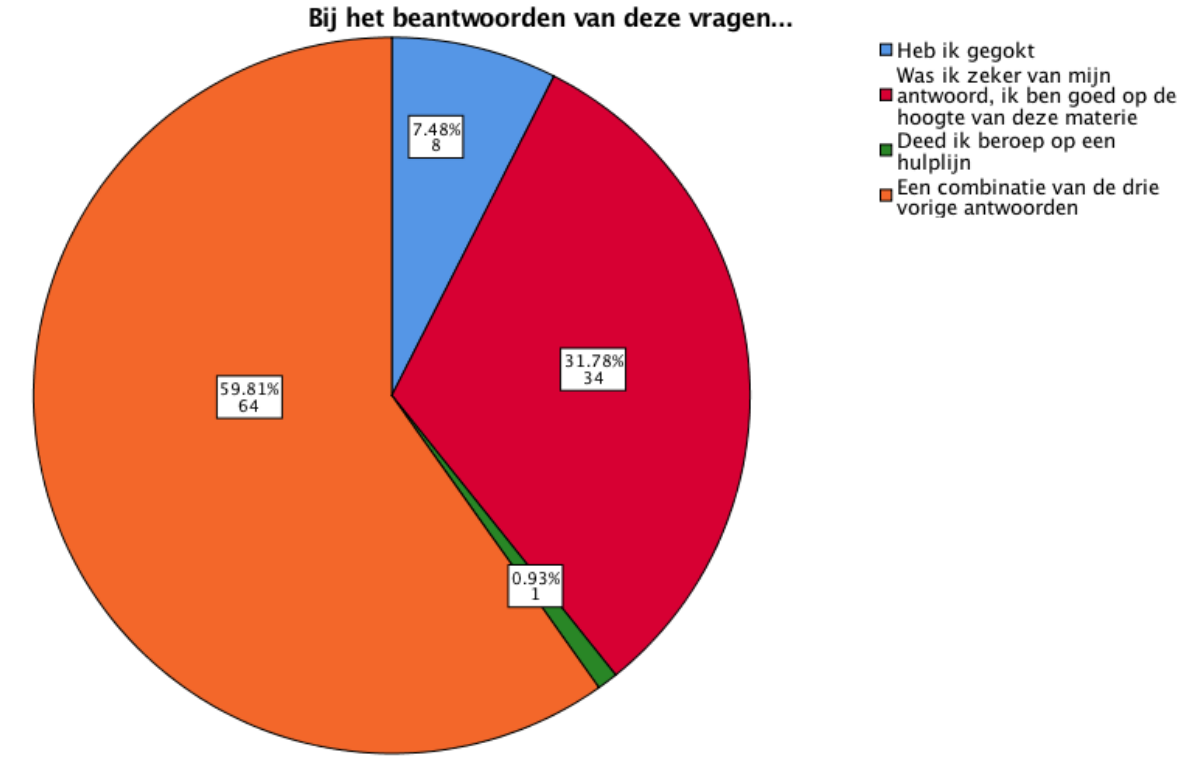
score		
eenheid	Mean	N
DRUGS DE	14.17	12
DRUGS GE	12.00	1
EIGENDOMMEN GE	12.50	2
EIGENDOMMEN OU / FINCRIM OU	14.31	13
FINCRIM DE	13.30	10
FINCRIM GE	11.56	9
GEWELD DE	11.00	1
GEWELD GE	10.75	4
LIB / SCI	11.67	3
LTWP DE	14.75	4
LTWP OU	11.75	4
MENSENHANDEL	13.88	8
MENSENSMOKKEL	12.75	4
MILIEU & BIJZONDERE ZAKEN	11.75	4
OMA	12.89	9
OPS / REM	12.50	2
PLUK	13.33	3
RCCU	12.83	6
TERRO	11.88	8
Total	12.96	107



Figuur 1.2: gemiddelde team score



Figuur 1.3: score per vraag



Statistics

Bij het beantwoorden van deze vragen...

N	Valid	107
	Missing	146

Figuur 1.4: algemene kennis

1.1.4 Conclusie

Voor een deel van het politiewerk is en blijft de klassieke opsporing waarschijnlijk voldoende, maar op nieuwe vormen van criminaliteit die complexer en omvangrijker zijn heeft de opsporing tot op heden onvoldoende antwoord om toekomstbestendig te zijn. De steun vanuit de federale politie in het ICT-domein is tot nog toe ondermaats geweest. We konden uit het eerste deel van dit onderzoek vaststellen dat er binnen de geïntegreerde politie barrières en hinderpalen zijn waardoor het optimaal uitvoeren van forensisch onderzoek in een geïnformatiseerde omgeving (digitaal forensisch onderzoek) onder druk komt te staan. Bijgevolg dienen er bepaalde instrumenten en/of systemen ontwikkeld te worden ingevolge de problemen (kennisbeheer, geïntegreerde informatiehuishouding en -uitwisseling, …) waarmee men geconfronteerd wordt aan te pakken.

Aangezien de Belgische politie slechts een kleine speler is met een beperkt budget wat betreft (nieuwe) technologieën, lijkt de ontwikkeling van eigen instrumenten en/of technologieën niet aangewezen. Uit de probleemstelling van dit onderzoek blijkt alvast dat er binnen de geïntegreerde politie geen specifieke actoren in staan voor de 'research & development' in verband met IT-toepassingen waardoor de kennis over wat precies werkt beperkt is. Bovenvermelde redenen geven duidelijk aan dat het gebruik van nieuwe technologieën dient opgenomen te worden in een globale innovatiestrategie binnen het veiligheidsbeleid in het algemeen en binnen de politieorganisatie in het bijzonder. In het volgende deel wordt daarom dieper ingegaan op de eigenschappen en (technische) aspecten van blockchaintechnologie. De blockchaintechnologie wordt beschouwd als een revolutionaire digitale innovatie met een ongezien potentieel. De blockchaintechnologie onder de loep nemen in het kader van de hierboven vermelde problemen bij het digitaal forensisch onderzoek, lijkt des te meer aangewezen.

DEEL II: BLOCKCHAIN

2.1 Een introductie tot blockchaintechnologie

2.1.1 Inleiding

Er is een stijgende vraag naar nieuwe dienstverlening en handhaving in het veiligheidsdomein (Bruggeman, 2014). De politie ziet zich hierin geconfronteerd met groeiende mogelijkheden en realisaties op het vlak van technologisering en innovatie (Bruggeman, 2014). In veel landen proberen opsporings- en handhavingsdiensten voortdurend hun prestaties te verbeteren. Om efficiënter en effectiever te werken wordt gekeken naar de mogelijkheden die nieuwe technologieën bieden om het werk van opsporings- en handhavingsdiensten te optimaliseren (Custers & Vergouw, 2016).

Volgens Byrne en Marx (2011) kunnen innovaties in '*criminal justice technology*' worden onderverdeeld in twee grote categorieën: harde technologie (hardware of materialen) en zachte technologie (computersoftware, informatiesystemen). Innovaties op het gebied van harde technologie omvatten nieuwe materialen, apparaten en apparatuur die kunnen worden gebruikt om criminaliteit te plegen of om criminaliteit te voorkomen en te beheersen (Byrne & Marx, 2011). Zachte technologieën daarentegen omvatten het strategische gebruik van informatie om criminaliteit te voorkomen en om de prestaties van de politie te verbeteren. Tot de zachte technologische innovaties behoren nieuwe softwareprogramma's, classificatiesystemen, technieken voor criminaliteitsanalyse en technieken voor gegevensdeling en systeemintegratie (Byrne & Marx, 2011).

Uit onderzoek van Custers en Vergouw (2016) over technologie voor opsporing en handhaving is alvast gebleken dat het gebruik van bekende technologieën, met name het gebruik van

databanken, het meest wijdverspreid zijn onder opsporings- en handhavingsdiensten[38] (Custers & Vergouw, 2016).

Niettemin blijkt uit de barrières en hinderpalen bij het digitaal forensisch onderzoek in België, zoals hierboven besproken (cfr. 1.1.3), dat er nood is aan eenvormige performante systemen en een reëel geïntegreerde informatiehuishouding en -uitwisseling (zachte technologieën). Mede vanwege het ontbreken van voldoende capaciteit, knowhow en financiële middelen moet ons land niet de pretentie hebben voor elk criminaliteitsprobleem zelf de technologische oplossing te willen ontwikkelen (Winsemius, 2005). Zich als politie begeven op de technologiemarkt lijkt des te meer aangewezen (Bruggeman, 2014). Zoals we in het eerste hoofdstuk van dit deel zullen zien, kan blockchaintechnologie onder meer de manier waarop wetshandhavingsdiensten informatie opslaan en uitwisselen, ingrijpend veranderen. Blockchain bevindt zich in de categorie van zachte technologieën, het is een gedistribueerde databasetechnologie. Wat dit precies inhoudt wordt verderop omstandig toegelicht.

Om in het Belgische democratische bestel, een goede politiezorg te verzekeren moet de politie een permanente focus houden op efficiëntie en blijven zoeken naar mogelijkheden om de werking te verbeteren (Bruggeman, 2014). Het betekent ook dat de politie zich moet blijven in vraag stellen en bereid moet zijn om werkprocessen te herzien (Bruggeman, 2014). Voor de politie betekent dit dat technologie en innovatie steeds belangrijker zullen worden voor haar slagkracht en impact, wil zij zich aan de goede 'zijde' van de kenniskloof bevinden (Bruggeman, 2014).

[38] Zie tabel 1 van bijlage 4.

2.1.2 Blockchain (r)evolutie

Volgens een toonaangevend artikel in het Harvard Business Review[39] zal de impact van blockchain op de samenleving enorm zijn (Schiltz et al., 2018). Een decennium geleden werd blockchain geïntroduceerd binnen de financiële sector (d.w.z. de technologie die ten grondslag ligt aan Bitcoin[40]), en sindsdien onderzoeken zowel onderzoekers als praktijkmensen manieren om de technologie in verschillende sectoren en industrieën te implementeren (Akram & Bross, 2018).

Interessant genoeg speelt Europa een belangrijke rol in deze (r)evolutie en is dit geen exclusief Silicon Valley verhaal. De Europese Unie laat zich in het blockchainverhaal dan ook niet onbetuigd. In februari van 2017 al publiceerde het Europees Parlement een diepteanalyse over *'Hoe blockchain ons leven kan veranderen'*[41]. De EU reageerde met een aantal belangrijke initiatieven om de ontluikende blockchainindustrie te onderzoeken en te ondersteunen (European Commission, 2019). Dit omvat onder meer de lancering van het *European Union Blockchain Observatory & Forum*[42] in februari 2018, de oprichting van het *European Blockchain Partnership (EBP)*[43] in april 2018 en de recente oprichting van de *International*

[39] Iansiti, M., & R. Lakhani, K. (2017). The truth about blockchain. *Harvard Business Review*(January–February), 118–127.

[40] De blockchaintechnologie is een techniek die in potentie eindeloze toepassingen kent. De best gekende is momenteel Bitcoin, een cryptocurrency. Bitcoin is een innovatief betalingsnetwerk en een nieuw soort geld (Gandal & Halaburda, 2014). Het is een manier om, op een betrouwbare wijze, wereldwijde elektronische betalingen te organiseren tussen twee partijen, zonder tussenkomst of mogelijke manipulaties van derden. De betrouwbaarheid van de digitale munt wordt gegarandeerd door een ingenieus cryptografisch systeem (vandaar ook de naam "cryptocurrency").

[41] Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives. In-depth analysis*. Retrieved from Panel for the Future of Science and Technology (STOA): http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[42] Het European Union Blockchain Observatory and Forum heeft tot doel de innovatie van de blockchain en de ontwikkeling van het ecosysteem van de blockchain binnen de EU te versnellen en zo de positie van Europa als wereldleider in deze transformatieve nieuwe technologie te versterken (European Union Blockchain Observatory and Forum, 2019). https://www.eublockchainforum.eu/

[43] Een poging van nationale regeringen in Europa om innovatie in de blockchain te stimuleren en de ontwikkeling van blockchaintoepassingen voor overheids- en openbare diensten te ondersteunen (European Union Blockchain Observatory & Forum, 2018b).

Association for Trusted Blockchain Applications (INATBA)[44] in België op 6 maart 2019, als wereldwijd multi-stakeholder forum voor ontwikkelaars en gebruikers van blockchain (European Union Blockchain Observatory & Forum, 2018b).

Tot op heden heeft de Europese Commissie ongeveer 80 miljoen euro toegekend aan EU-projecten die zich bezighouden met blockchain in verschillende sectoren en heeft zij plannen aangekondigd om de financiering tegen 2020 met maximaal 300 miljoen euro te verhogen, met name via haar EU-onderzoeks- en innovatieprogramma Horizon 2020 (European Union Blockchain Observatory & Forum, 2018b). Maar ook in België is blockchain sterk in opmars[45] (Pomp & Verhaert, 2018). Ondanks dat België nog altijd een beetje de *"new kid on the blockchain"* is, verdiept een aantal Vlaamse bedrijven en overheden zich wel degelijk in de blockchaintechnologie (De Lameillieure, 2018) en is blockchain ook op de politieke agenda beland.

In België is onder meer een transversale werkgroep actief op initiatief en onder aansturing van de federale overheidsdienst Beleid en Ondersteuning (FOD BOSA)/directie generaal Digitale Transformatie (DG DT) (Daems, 2017). Binnen deze werkgroep zijn alle beleidsniveaus vertegenwoordigd, samen met een aantal expertisecentra (Daems, 2017). De objectieven van deze werkgroep zijn dubbel: enerzijds bekijken hoe processen tussen verschillende overheidsniveaus op een creatieve en gecoördineerde wijze geoptimaliseerd kunnen worden om eventuele blockchainoplossingen mogelijk te maken (Daems, 2017). De werkgroep doet dat door in verschillende transversale teams processen dwars door alle niveaus heen, in kaart te brengen en op zoek te gaan naar mogelijke problemen, opportuniteiten tot vereenvoudiging

[44] Website INATBA: https://www.inatba.org/
[45] Lanssens, P. (2018). Nieuw: hogescholen zetten blockchain op menu. *HLN*. Retrieved from https://www.hln.be/regio/kortrijk/nieuw-hogescholen-zetten-blockchain-op-menu~a783ff77/

of schrapping, enzovoort (Daems, 2017). Het tweede objectief is om een technologisch platform aan te bieden waarop iedereen blockchain zaken kan delen om toe te laten elkaars ervaring te delen (Daems, 2017). In 2019 nemen de investeringen in blockchaintechnologie door de overheidssector fors toe (Verbond van Belgische Ondernemingen, 2018): het is voortdurend in ontwikkeling en wordt gekenmerkt door onophoudelijke experimenten en R&D. Nieuwe systemen, toepassingen en implementaties zijn bijna dagelijks in opkomst (B. Walton & Dhillon, 2017). Onze overheidssector kan (moet?) deze revolutie mee trekken[46].

Blockchain blijft echter voor veel mensen nog steeds een onbekend begrip. Sommigen kennen het als de technologie achter Bitcoin, maar blockchain is veel meer dan dat alleen (Schiltz et al., 2018). Deze technologie louter koppelen aan digitale munten, is een achterhaald idee. De concepten en structuren van blockchain zijn uiterst draagbaar en uitbreidbaar naar andere activiteiten (Walport, 2016). Achter de term blockchain zit een technologie waarvan nu nog maar het topje van de ijsberg zichtbaar is en die nog veel meer mogelijkheden biedt dan wat nu bekend is (Schiltz et al., 2018).

Hoewel niet duidelijk is of alle veronderstelde toepassingsmogelijkheden van blockchaintechnologie realiteit zullen worden, heeft het meerwaarde als de overheid maar ook de politie zich verdiept in blockchaintechnologie en de mogelijke gevolgen daarvan (WODC, Lopend).

[46] WODC. (Lopend). Verkennend onderzoek naar de sociale en ethische gevolgen van de Blockchain en hoe de overheid zich hiertoe zou kunnen/moeten verhouden. *Projectnummer: 2815*. Retrieved from https://www.wodc.nl/onderzoeksdatabase/2815-verkennend-onderzoek-naar-de-sociale-en-ethische-gevolgen-van-de-blockchain-en-hoe-de-overheid-zich-hiertoe-zou-kunnenmoeten-verhouden.aspx

2.1.3 Het ontstaan en de kenmerken van blockchaintechnologie

De technologie kent een lange ontstaansgeschiedenis. Het werd ontwikkeld door mensen die bijzonder veel waarde hechtte aan privacy en door middel van sterke cryptografie[47] de maatschappij wilden veranderen (Foryard Academy, 2018).

Tijdens de economische crisis van 2008 daalde het vertrouwen in de bankwereld tot een dieptepunt. Banken vielen om, de huizenmarkt zakt in elkaar en veel mensen kregen te maken met woekerpolissen (BTC Direct, 2019). Dit moet anders, dacht Satoshi Nakamoto (een persoon of groep mensen, dit is niet duidelijk). In 2008 werd door Satoshi Nakamoto een *whitepaper*[25] gelanceerd voor de creatie en verhandeling van een virtuele munt[48] (de Bitcoin[49]). In het baanbrekende werk beschrijft Satoshi Nakamoto de ruggengraat van de blockchaintechnologie. Een compleet nieuwe benadering van data transactie opslag en gegevensuitwisseling.

Om de revolutie in de benadering te illustreren, volgt hierna een voorbeeld van een 'probleem' en een mogelijke oplossing, zoals die kan worden uitgewerkt met een traditionele benadering en daarnaast de blockchain benadering. Aan de hand van dit voorbeeld zullen de typische kenmerken en terminologie van de blockchain worden toegelicht. De uitleg is bedoeld voor een niet ICT-technisch publiek en er is gepoogd om de uitleg helder te houden, en niet te

[47] De hoofdgedachte achter cryptografie is gegevens beveiligen tegen toegang door onbevoegden. Cryptografie is het digitale equivalent van deursloten of bankkluizen, die ook tegengaan dat onbevoegden toegang krijgen tot hun inhoud. Net als bij sloten en sleutels in de fysieke wereld, maakt cryptografie gebruik van sleutels om gegevens te beveiligen (Drescher, 2017). Moderne cryptografie wordt opgedeeld in symmetrische en asymmetrische cryptografie (Wikipedia, 2019c).

[48] Definitie virtuele munt FOD Financiën: "virtuele valuta": een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld.

[49] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

vervallen in een technische beschrijving die weinig bijdraagt aan de doelstelling van deze masterproef.

2.1.3.1 Voorbeeld probleemstelling

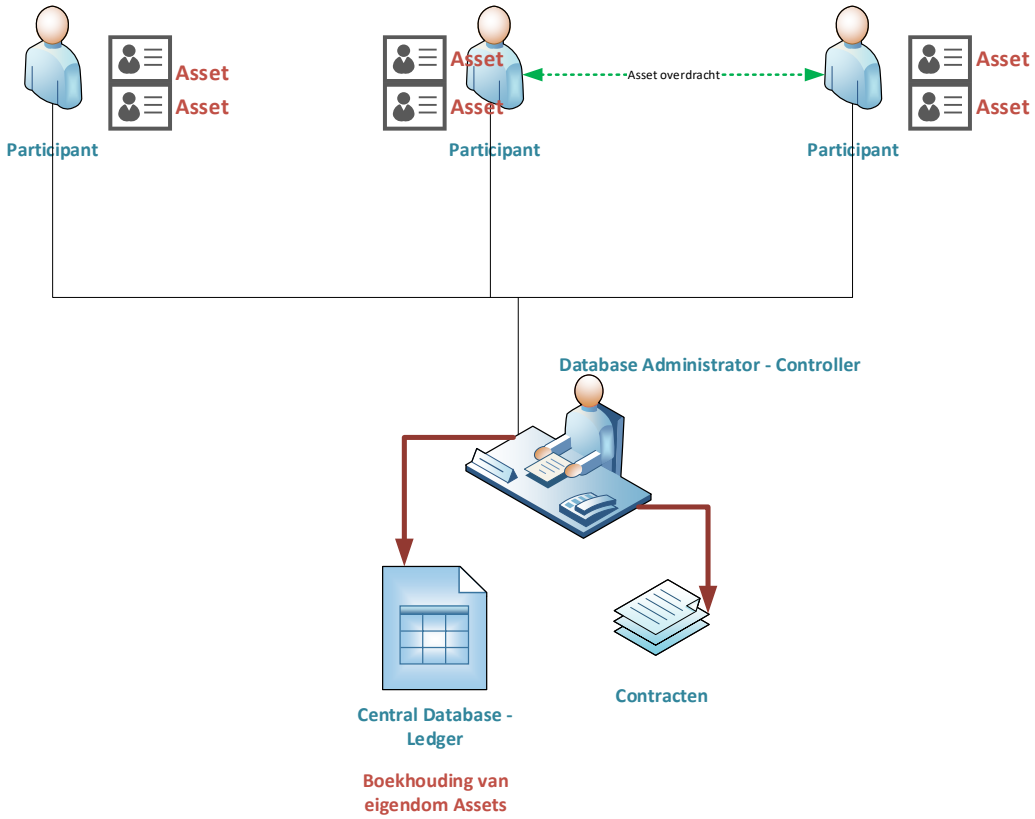
Nemen we een school met 100 leerlingen. Deze leerlingen bezitten Panini Stickers[50] van onze nationale Rode Duivels. Er wordt duchtig geruild, maar al snel ontstaan er klachten over onrechtmatige toe-eigening van andermans stickers of het niet nakomen van beloften, bijvoorbeeld om gekregen stickers niet verder te ruilen met iemand anders. De schooldirectie kan deze discussies niet beslechten, omdat het niet duidelijk is wie de eigenaar is en wat er vrijwillig verhandeld is en wat is afgesproken.

2.1.3.1.1 Traditionele oplossing

Er wordt een derde partij, het schoolsecretariaat, ingeschakeld om toe te zien dat alles correct verloopt. Het secretariaat stelt een database op (Microsoft Excel), waarin voor iedere leerling wordt bijgehouden welke stickers hij of zij bezit. Wanneer iemand wil ruilen of wegschenken treedt het secretariaat op als tussenpersoon – om te garanderen dat beide partijen instemmen – en past de database overeenkomstig aan. Eventuele afspraken tussen leerlingen i.v.m. verder doorverkopen van een sticker, worden door het secretariaat in een apart document bijgehouden en het secretariaat zorgt dat dit nageleefd wordt. Een leerling kan bij het secretariaat aankloppen om na te gaan of zijn gegevens in de database kloppen. Dit is een traditionele boekhouding, waarbij de database (in de praktijk ook wel aangeduid als '**grootboek**' of in het Engels *Ledger*) wordt bijgehouden door een **centrale derde partij** (het secretariaat), die door alle leerlingen wordt vertrouwd, en die ruilen of doorgeven (=**transacties**) van stickers (=**bezit**,

[50] Panini. (2019). Panini België. Retrieved from http://collectibles.paninibelgium.com/home

waarde/*asset, value*) begeleidt, en er voor zorgt dat bijkomende afspraken (=**contracten**) worden nagekomen. Alleen het secretariaat heeft toelating (=***permission***) om de database aan te passen (=**database administrator**).



Figuur 2.1: traditionele oplossing (database)

Waarin schiet deze traditionele benadering tekort?

De leerlingen vinden het niet leuk dat alles door de school wordt gecontroleerd en de school van iedereen alles weet. Het is omslachtig om voor iedere transactie naar het secretariaat te moeten gaan. Bovendien is gebleken dat de Excel soms verkeerd is aangepast, door een vergissing of door een hacker, en het is niet te achterhalen wanneer precies. De bijkomende afspraken worden door het secretariaat niet altijd afgedwongen, omdat het document met alle afspraken moeilijk te volgen is, door de vele, uiteenlopende afspraken.

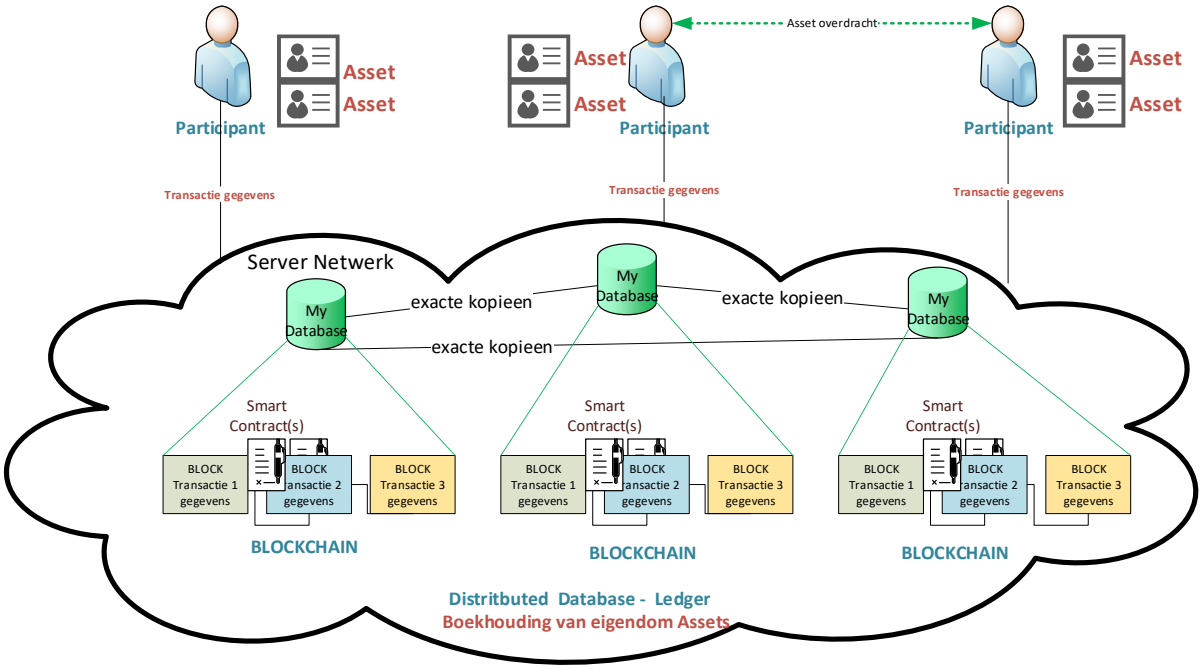
2.1.3.1.2 De blockchain benadering

Het schoolsecretariaat wordt niet meer betrokken (een flinke lastbesparing voor de school). De leerlingen stellen zelf een grootboek (*ledger*) op in een database (blockchain). Iedere leerling heeft een server in een netwerk (internet of intranet school), en op ieders server staat, op ieder moment (=*real time*) een volledige, correcte kopie van de database (=***distributed database***). Iedereen kan op elk moment zien wat er in zijn database staat.

Iedere leerling mag meedoen, zonder dat iemand toestemming moet geven (=***permissionless***), hij of zij moet enkel een server hebben die tot het netwerk behoort. Wanneer een leerling een sticker wil doorgeven, dan stuurt hij een bericht naar alle servers/leerlingen met de gewenste transactie. Alle servers kijken in hun database of de transactie klopt (bezit de gever wel de stickers?) en als een meerderheid (of een substantieel aantal) servers akkoord gaat (=**consensus**) wordt dit geaccepteerd en is de transactie bezegeld en aan de database toegevoegd. De database (blockchain) is gegarandeerd gelijk op alle deelnemende servers.

Om te vermijden dat iets overschreven wordt in de database, wordt iedere nieuwe transactie toegevoegd aan de database en wordt nooit iets bestaands overschreven. Er wordt een transactie (data 'block') toegevoegd aan de ketting (=*block* ***'chain'***). Eens een transactie in de database, verdwijnt ze nooit meer (=***immutable***). In de database kan daardoor iedereen de hele historiek en transacties, van bij het begin, volgen door alle blokken in de ketting te doorlopen (=***transparancy***). Een leerling kan alleen zijn eigen stickers transfereren. Hij moet in het bezit zijn van het unieke passwoord (=***public/private key***) dat bij de sticker hoort, anders zal de database de transactie niet aanvaarden. Als onderdeel van een ruil kunnen beide partijen afspraken maken (=contract), dat automatisch uitgevoerd wordt als aan de contractvoorwaarden is voldaan (=***smart contract***).

Merk op dat de stickers, de *assets*, zich niet in de database (blockchain) bevinden (=***off-chain***). Dit kan ook niet want het zijn fysieke objecten. Enkel de gegevens van de transactie (overdracht van welke stickers van wie naar wie en wanneer) bevindt zich in de *chain*. Indien de asset iets elektronisch zou zijn (zoals bijvoorbeeld een Bitcoin, of een digitale foto), dan kan die ook in een 'block' van de blockchain geplaatst worden.



Figuur 2.2: blockchain benadering

2.1.3.2 Samenvattende omschrijving blockchain

Zoals misschien al duidelijk werd, is blockchain een gedistribueerde **databasetechnologie** die wordt ingezet in een netwerk van deelnemende computers, zogeheten *nodes*. Tussen deze *nodes* vinden elektronische transacties[51] plaats. Nodes zijn hierdoor onontbeerlijk want zij zijn de derde partijen die verantwoordelijk zijn voor het toevoegen van transacties aan de blockchain (Soetaert, Verhage, & De Middeleer, 2017). Blockchain dankt zijn naam aan het feit dat de transacties worden opgeslagen in groepen die bekend staan als blokken. Elke transactie wordt in de vorm van een blok ('block') automatisch geregistreerd in een register (grootboek). Nadat een transactie is verwerkt in een block, en daarmee in het register, kan deze niet worden gewijzigd of ongedaan worden gemaakt. De veelheid[52] aan transacties leidt ertoe dat in het register een (groeiende) ketting ('chain') van transacties – geregistreerd als blocks – ontstaat; zie daar de 'blockchain' (Verhelst, 2017).

De technologie heeft bijgevolg een belangrijke toegevoegde waarde in situaties waar vandaag een centrale autoriteit een transactie of eigendomsoverdracht moet verifiëren. De blockchain maakt in veel situaties de tussenkomst van een intermediair, een centrale instantie of beheerder, overbodig omdat de deelnemers collectief voor het nodige vertrouwen zorgen (Verbond van Belgische Ondernemingen, 2018). Anders gezegd, het doel van de blockchain is om een specifiek niet-functioneel aspect van een gedistribueerd softwaresysteem te waarborgen, en wel: zorgen voor en handhaven van de integriteit van het systeem (Drescher, 2017).

[51] Een transactie is de overdracht van eigendom van de ene naar de andere eigenaar. De feitelijke overdracht steunt op gegevens die de voorgenomen overdracht beschrijven. Deze gegevens bevatten informatie die nodig is om de transactie uit te voeren. Blockchain gebruikt de volgende gegevens om een transactie te beschrijven: een ID van het account dat eigenaarschap gaat overdragen naar een ander account; een ID van het account dat eigenaar gaat worden; de hoeveelheid over te dragen goederen; het tijdstip waarop de transactie wordt gedaan; een vergoeding die aan het systeem wordt betaald voor het uitvoeren van de transactie; een bewijs dat de eigenaar van het account dat zijn eigenaarschap overdraagt, het eens is met die overdracht (Drescher, 2017).
[52] Elk blok van gegevens wordt cryptografisch gekoppeld aan het vorige blok.

In wat volgt wordt kort ingegaan op hoe blockchaintechnologie technisch precies in elkaar zit en wat de belangrijkste aspecten zijn. Een conceptueel begrip van de technische basis van de blockchain is noodzakelijk om specifieke blockchainapplicaties te begrijpen, toepassingen (*Use Cases*) te evalueren of de discussie over de verwachte impact te kunnen volgen (Drescher, 2017). Zonder waardering van de onderliggende concepten is het niet mogelijk de waarde en de potentiële impact van de blockchain in het algemeen te beoordelen of de toegevoegde waarde van specifieke blockchainapplicaties te begrijpen. Een gebrek aan kennis van een nieuwe technologie kan er namelijk toe leiden dat men zich laat meeslepen door de hype (Drescher, 2017).

2.1.4 De (technische) werking van blockchaintechnologie

Het kernprobleem dat door de blockchain moet worden opgelost, is het bewerkstelligen en behouden van integriteit in een puur gedistribueerd peer-to-peersysteem[53] dat bestaat uit een onbekend aantal deelnemers (knooppunten of *nodes* genoemd) met onbekende betrouwbaarheid. Blockchaintechnologie zorgt ervoor dat er vertrouwen wordt gecreëerd door middel van slimme codering. Op abstracte wijze kan een blockchain worden omschreven als een gedecentraliseerde en gedistribueerde database[54] van gegevens die permanent worden opgeslagen en moeilijk tot niet kunnen worden gewijzigd, waarbij het geheel wordt beveiligd

[53] Peer-to-peernetwerken zijn een special soort gedistribueerde systemen. Ze bestaan uit afzonderlijke computers (ook wel knooppunten genoemd), die hun resources (verwerkingskracht, opslagcapaciteit, data- of netwerkbandbreedte) direct ter beschikking stellen aan alle andere leden in het netwerk, zonder tussenkomst van enig centraal coördinatiepunt. De knooppunten in het netwerk zijn elkaars gelijke voor wat betreft hun rechten en rollen in het systeem. Bovendien zijn ze allemaal zowel leverancier als consument van resources. Peer-to-peersystemen kennen interessante toepassingen, zoals het delen van bestanden, contentdistributie en privacybescherming. De meeste van deze toepassingen gaan daarbij uit van een eenvoudig maar krachtig idee, namelijk de computers van de gebruikers omvormen tot knooppunten die het hele gedistribueerde systeem vormen. Het resultaat is dat hoe meer gebruikers of klanten gebruikmaken van de software, hoe groter en krachtiger het systeem wordt (Drescher, 2017).

[54] De twee belangrijkste architecturale benaderingen voor het organiseren van softwaresystemen zijn de gecentraliseerde en de gedistribueerde aanpak. In gecentraliseerde softwaresystemen zijn de componenten verbonden met en gegroepeerd rond één centrale component. Daarentegen vormen de componenten van gedistribueerde systemen een netwerk van verbonden componenten zonder enig centraal element voor coördinatie of controle (Drescher, 2017).

door asymmetrische encryptie[55] en gehandhaafd door een consensusmechanisme (Simal, Valcke, & Schroers, 2018).

De database is gedistribueerd[56], wat betekent dat iedere deelnemer aan het netwerk een identiek exemplaar van het register (grootboek) heeft, die voortdurend wordt bijgewerkt als nieuwe geldige blokken worden toegevoegd (European Union Blockchain Observatory & Forum, 2018a). De database wordt niet bewaard op één centrale server maar op alle computers van de deelnemers waardoor elke deelnemer een kopie van de blockchain bewaart op zijn (persoonlijke) computer. Dat maakt het netwerk robuuster dan een centrale database (Smits, 2018). Die laatste kan namelijk veel makkelijker gehackt worden (Smits, 2018). Belangrijk om te onthouden is dat elke computer altijd de laatste, meest up-to-date kopie van die database heeft. De database is ook gedecentraliseerd, wat betekent dat er niet één centraal beheer is maar dat elke deelnemer eigen beslissingen neemt die achteraf door het systeem zelf worden gevalideerd (Simal et al., 2018). Dit wil zeggen dat er niet één instantie (of bedrijf) eigenaar is (van blockchain) maar dat niemand exclusief eigenaar is (Akram & Bross, 2018). En om deze reden is het een open netwerk waaraan iedereen die dat wil kan deelnemen (Bolt, 2018a).

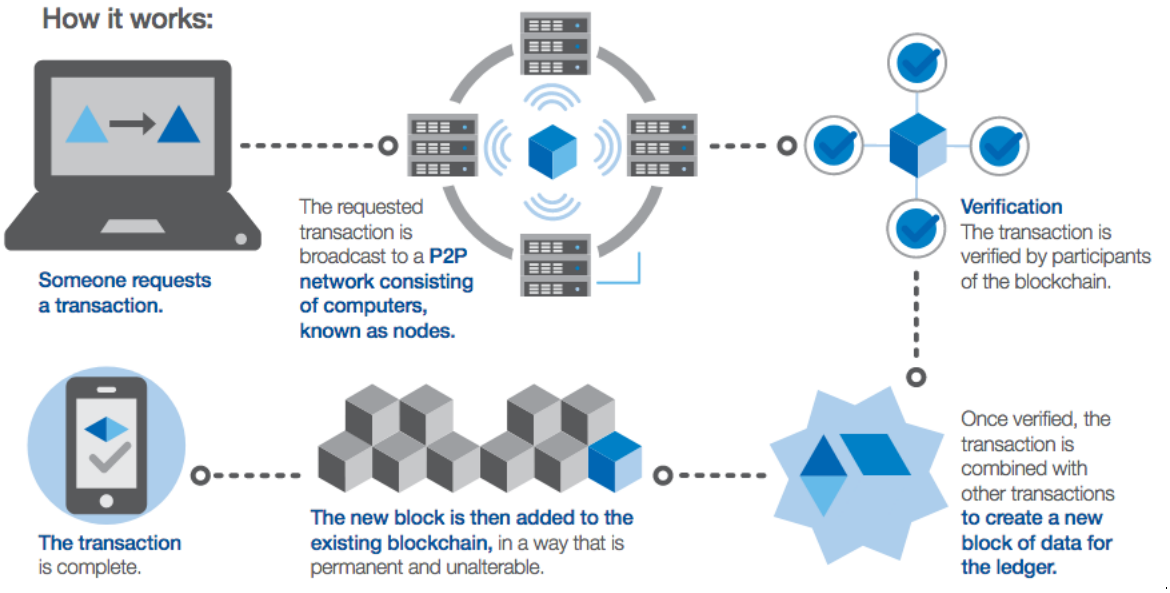
Het permanente en zo goed als onwijzigbare karakter van de gegevens in de blockchain wordt verkregen via *cryptografische hashfuncties*[57]. Een consensusmechanisme, tot slot, is een

[55] De (transactie)gegevens in de blockchain zijn transparant en daardoor voor alle deelnemers zichtbaar. Vandaar dat er gebruik wordt gemaakt van zogeheten 'privacy-preserving technologies'. Zo'n technologie die in één adem wordt genoemd met blockchain is asymmetrische encryptie. 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 (Simal et al., 2018). Het gebruik van asymmetrische encryptie binnen de blockchain geeft daarmee een bepaalde mate van zekerheid over de identiteit van de verzender alsmede over de integriteit en authenticiteit van het bericht. Asymmetrische encryptie wordt tevens gebruikt om een tijdstempel ('time stamp') op een elektronisch bericht te plaatsen (Verhelst, 2017).

[56] Als er één enkele component is, bijvoorbeeld een uitschakelknop die het hele systeem kan stoppen, is het systeem niet gedistribueerd (Drescher, 2017).

[57] Cryptografische hashfuncties genereren digitale vingerafdrukken voor elk soort gegevens. Cryptografische hashfuncties hebben de volgende eigenschappen: ze genereren op snelle wijze hashwaarden voor allerlei soorten gegevens; ze zijn deterministisch (verschillen in de hashwaarden van gegevens worden uitsluitend veroorzaakt

mechanisme dat de integriteit van de blockchain bewaart doordat de deelnemers aan de blockchain consensus bereiken over de nieuw toegevoegde gegevens (Simal et al., 2018). De aaneenkoppeling van een nieuw 'block' met gegevens aan het vorige blok, vindt plaats wanneer alle deelnemers aan het netwerk akkoord gaan met de authenticiteit van het nieuwe blok en dit blok willen aanvaarden[58] (Simal et al., 2018). Omdat er een gebrek is aan een centrale autoriteit worden de (publieke) blockchains beveiligd door middel van cryptografische verificatie in de vorm van 'Proof-of-Work'[59] (het consensusmechanisme) (Ducas & Wilner, 2017). Zo wordt het blok als het ware verzegeld (Smits, 2018).



Figuur 3: blockchain transactie (bron: World Economic Forum)*

door verschillen in de invoergegevens); ze zijn pseudowillekeurig (de hashwaarde van gewijzigde gegevens moet altijd een verrassing zijn, het moet niet mogelijk zijn de hashwaarde te voorspellen op basis van de invoergegevens); het zijn eenrichtingsfuncties (het is onmogelijk om de originele invoergegevens te herstellen op basis van de hashwaarde); ze zijn 'botsingbestendig' (de kans op een identieke hashwaarde voor verschillende gegevens is heel klein). Verschillende invoer moet dus leiden tot verschillende uitvoer. Botsingbestendigheid is verplicht voor hashwaarden om bruikbaar te zijn als digitale vingerafdruk (Drescher, 2017).

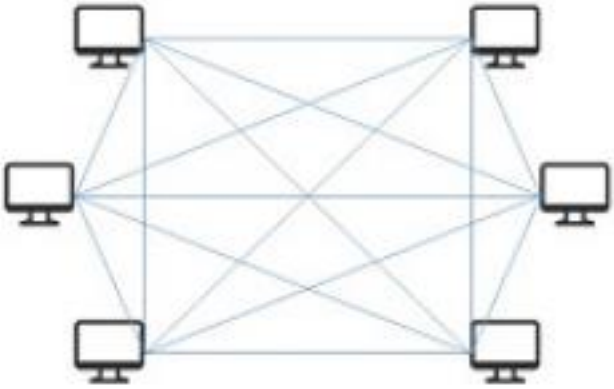
[58] De informatie die in een blockchaindatabase wordt toegevoegd moet dus worden goedgekeurd door de participanten in het netwerk (Soetaert et al., 2017).

[59] Trefwoordenlijst (zie achteraan deze masterproef).

* World Economic Forum. (2018). *Building block(chain)s for a better planet*. Retrieved from https://www.weforum.org/reports/building-block-chain-for-a-better-planet

2.1.4.1 Publieke en Private blockchains

De werking van blockchain zoals deze hierboven werd beschreven, is de werking hoe deze oorspronkelijk werd bedacht door S. Nakamoto, namelijk een permissieloze, of in het Engels *permissionless*, blockchain: een open en publiek toegankelijke blockchain waar geen voorafgaande toestemming vereist is en waarin iedereen kan participeren (Simal et al., 2018). Deze blockchain is *open source*[60], wat betekent dat alle gebruikers of knooppunten lees- en schrijftoegang hebben. Iedereen kan een gebruiker of knooppunt (node) worden en kan transacties verifiëren en nieuwe blokken maken en toevoegen aan de blockchain-gegevensstructuur (Drescher, 2017).



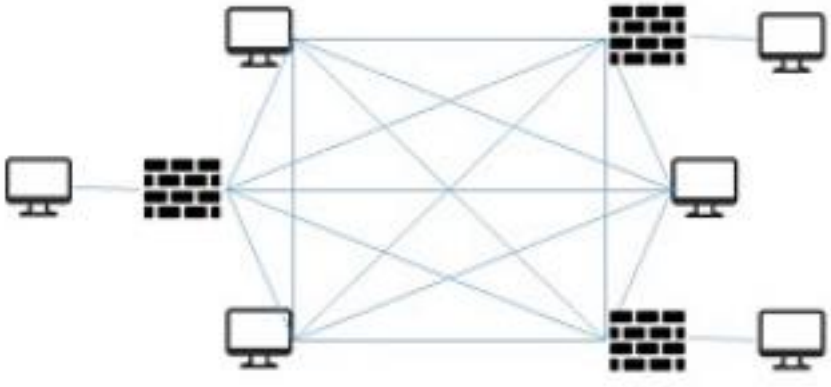
Figuur 4.1: publieke blockchain (bron[*]*)*

Elke beperking met betrekking tot lees- en schrijftoegang tot de blockchain-gegevensstructuur levert een van de 'alternatieve versies' op (Girasa, 2018). Een variant op de publieke (permissieloze) blockchain is een blockchain die zich op een privaat netwerk bevindt, zoals

[60] Open source of open bron beschrijft de praktijk die in productie en ontwikkeling vrije toegang geeft tot de bronmaterialen (de source) van het eindproduct. Hierbij komen eindproducten en de daar aan ten grondslag liggende basismaterialen (bijvoorbeeld ontwerpen, beschrijvende documentatie en dergelijke), vrij ter beschikking voor het publieke domein (Wikipedia, 2019d).

[*] Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659. Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf. doi:10.6633/IJNS.201709.19(5).01(Lin & Liao, 2017)

een intranet. Het verschil tussen beide heeft betrekking op wie deel kan uitmaken van het netwerk: een private of consortium blockchain is afgeschermd met toegangscontrole en werkt onder een specifieke organisatie waardoor een deelnemer moet uitgenodigd en goedgekeurd worden (Cai et al., 2018). 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 het in stand houden van de blockchain (Simal et al., 2018). De permissie-gebonden blockchains beperken hierdoor leestoegang en het recht om nieuwe transacties te creëren tot een vooraf geselecteerde groep gebruikers of knooppunten die via een instapprocedure als betrouwbaar zijn aangemerkt (J. Bambara et al., 2018). Alleen de groep knooppunten die schrijftoegang heeft, mag transacties verifiëren en deelnemen aan de gedistribueerde consensusprocedure (Drescher, 2017).



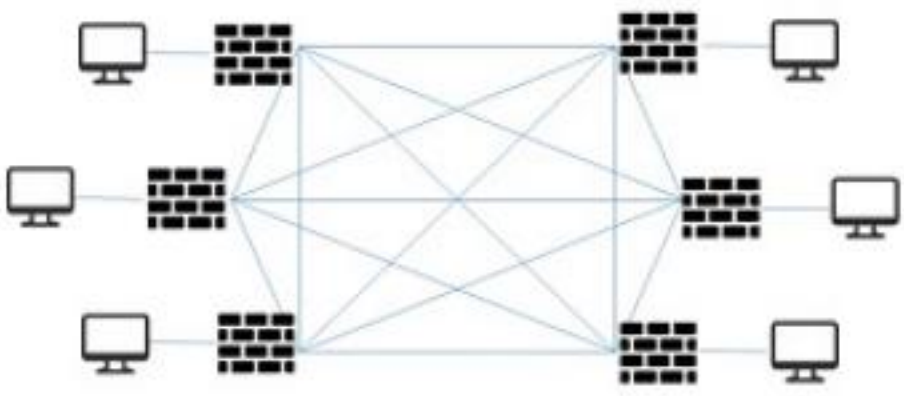
Figuur 4.2: consortium blockchain (bron[*])

Private blockchains hebben de strengste deelnamecontrole. Alle lees-, transactie- en recht van deelname aan het consensus proces (*mining*rechten) worden strikt gecontroleerd binnen één enkele organisatie door de netwerkeigenaar. Ter vergelijking: consortiumblockchains verschillen subtiel van private blockchains waarbij in plaats van een organisatie die de

[*] Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659. Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf. doi:10.6633/IJNS.201709.19(5).01

volledige controle over de blockchain heeft, de consortiumblockchain een blockchain is waarbij het consensusproces wordt gecontroleerd door een vooraf geselecteerde reeks knooppunten; zo moeten bijvoorbeeld ten minste 10 van de 15 organisaties in dit consortium een 'block' ondertekenen en goedkeuren om geldig te zijn (Cai et al., 2018).

Bij publieke blockchains (*trustless*, *permissionless*) is het mechanisme om tot consesus te komen een complex protocol ('Proof-of-Work' - PoW). Dit protocol – het oplossen van een crypto raadsel – vraagt zeer veel rekenkracht. Bij private of consortium blockchaintoepassingen, wordt de validatie meestal toevertrouwd aan specifieke participanten (=*validators*), beperkt in aantal, met de nodige autoriteit ('Proof-of-Authority').



Figuur 4.3: private blockchain (bron[*])

Openbare / publieke blockchains	Privé- / Consortium-blockchains
Voor iedereen toegankelijk.	Schrijfrechten worden gecentraliseerd bij één organisatie of consortium.
Iedereen kan transacties verzenden.	Leesrechten kunnen openbaar of beperkt zijn.

[*] Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659. Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf. doi:10.6633/IJNS.201709.19(5).01

Iedereen ziet transacties opgenomen als deze geldig zijn.	Inclusief databasebeheer, auditing, etc.
Iedereen kan deelnemen aan het consensusproces.	Consortium van geselecteerde knooppunten neemt deel aan consensusproces.
Volledig gedecentraliseerd.	

Leestoegang en aanmaak van transacties		
Schrijftoegang	**Iedereen**	**Beperkt**
Iedereen	Publiek & permissieloos	Privé & permissieloos
Beperkt	Publiek & permissiegebonden	Privé & permissiegebonden

Tabellen: vier versies van de blockchain als resultaat van de combinatie van lees-en schrijfbeperkingen

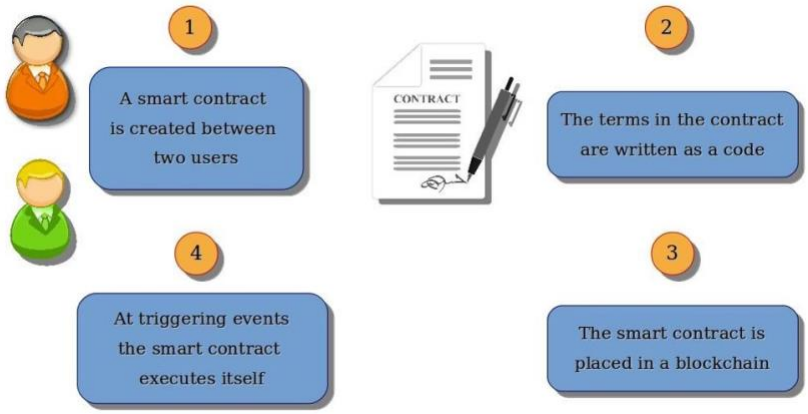
Het opleggen van beperkingen aan lees- en schrijftoegang kan conflicten veroorzaken met de definitie van het peer-to-peersysteem, de gedistribueerde aard ervan en het doel van de blockchain. De blockchain is echter ook nuttig voor het handhaven van integriteit, zelfs in het meest beperkende geval van een permissie-gebonden private blockchain.

2.1.4.2 Smart contracts en decentrale applicaties (dApps)

Naast het vastleggen van informatie en gegevens kan de blockchain worden gebruikt om contractuele afspraken te verifiëren of af te dwingen met behulp van zogenaamde ‘smart contracts’ (slimme contracten) (Ducas & Wilner, 2017). In tegenstelling tot eenvoudige transactiegegevens, zijn slimme contracten veel flexibeler met betrekking tot de objecten, subjecten, handelingen en voorwaarden om de gewenste overdracht van eigendom te beschrijven. Vanuit technisch oogpunt zijn slimme contracten zelfstandige

computerprogramma's die zijn geschreven in een voor de blockchain ontwikkelde programmeertaal (Drescher, 2017). Om slimme contracten te ondersteunen, is de blockchaintechnologie uitgebreid met de mogelijkheid om programmacode uit te voeren.

Doordat de blockchain programmacode kan uitvoeren, heeft dit geleid tot mogelijkheden voor applicatieontwikkeling in plaats van alleen maar het bijhouden van transactiegegevens (Drescher, 2017). Het woord 'contract' kan verwarrend zijn in deze context. Dit suggereert een juridische afspraak, terwijl een smart contract dat zeer zeker niet is (De Breed & Partners, 2019). Een smart contract is een geprogrammeerd contract waarvan de afspraken in computercode staan vastgelegd op de blockchain en die in staat is om beslissingen te nemen wanneer aan bepaalde voorwaarden is voldaan (Kolvart, Poola, & Rull, 2016). Voor een breed scala aan potentiële toepassingen kunnen op blockchain-gebaseerde slimme contracten een aantal voordelen bieden: snelheid en real-time updates, nauwkeurigheid, minder uitvoeringsrisico, minder tussenpersonen, lagere kosten, nieuwe bedrijfs- of operationele modellen (Mohanta, Panda, & Jena, 2018). Als gevolg hiervan is het slimme contract de belangrijkste, meest veelbelovende ontwikkeling van de blockchain in de afgelopen jaren (Ackermann & Meier, 2018).



Figuur 5: smart contract (bron[*])

[*] Driesen, Y. (2018). Van 'blockchain of custody' tot 'criminal smart contracts'. Criminelen én politie omarmen blockchain: Centre for Policing and Security.

Smart contracts zijn een hulpmiddel om softwareapplicaties meteen op de blockchain te kunnen installeren – en niet op een centrale server – die overeenkomsten en engagementen bevatten die decentraal door de gedistribueerde knooppunten automatisch worden uitgevoerd wanneer de voorwaarden vervuld zijn (Cai et al., 2018). Ze maken bijgevolg zogenaamde gedecentraliseerde applicaties (dApps) mogelijk (J. Bambara et al., 2018). In tegenstelling tot normale (web)applicaties, gebruiken dApps de blockchain om transacties te verzenden en gegevens op te halen (Getso & Johari, 2017).

Wanneer we bijvoorbeeld communiceren met een App zoals Facebook op onze smartphone, zal de App communiceren met gecentraliseerde servers en diensten. Een dApp daarentegen kan er qua gebruikersinterface precies hetzelfde uitzien, maar de back-end[61] diensten worden vervangen door slimme contracten die op het gedecentraliseerde blockchainnetwerk draaien (J. Bambara et al., 2018).

Op decentrale applicaties (dApps) kunnen er oneindig veel deelnemers betrokken worden, uit allerlei verschillende marktsegmenten (Darren, 2019). Om het verschil tussen dApps en smart contracts goed te kunnen begrijpen zou je een decentrale applicatie eigenlijk moeten zien, als een "blockchain-toegankelijke website" en de smart contracts als het element dat zorgt voor de "verbinding" met de blockchain (Darren, 2019). Een gewone website-applicatie maakt gebruik van HTML, CSS en javascript om een webpagina te creëren. Met behulp van een API[62] worden er gegevens van een database verkregen (Darren, 2019). Als je naar een sociale netwerk site

[61] Een backend (van het Engelse back end) is een programma of deel van een programma dat onzichtbaar is voor de gebruiker. De interactie met gebruikers verloopt niet rechtstreeks met de backend maar via de grafische gebruikersinterface oftewel frontend van het programma (Wikipedia, 2019b).

[62] Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel. Een API definieert de toegang tot de functionaliteit die er achter schuil gaat. De buitenwereld kent geen details van de functionaliteit of implementatie, maar kan dankzij de API die functionaliteit wel gebruiken (Wikipedia, 2019a).

zoals Facebook gaat, dan zal de pagina een API aanwenden voor je persoonlijke informatie en deze vervolgens op de pagina tonen (Darren, 2019). Dit is hoe een traditionele website of applicatie werkt. Een decentrale applicatie lijkt in een aantal opzichten heel erg op een traditionele website-applicatie. Het grote verschil bij dApps is echter dat in plaats van dat de API een verbinding maakt met een database, hier een smart contract een verbinding maakt met de blockchain (Darren, 2019). In tegenstelling tot traditionele applicaties, waar de back-end code op "centrale" servers draait, hebben decentrale applicaties de back-end code draaien op een gedecentraliseerd peer-to-peer netwerk (Darren, 2019).

Om een App aan te merken als een dApp moet de applicatie aan een aantal maatstaven voldoen: In de eerste plaats moet de applicatie volledig open source zijn: vanwege het vertrouwde karakter van de blockchain moeten dApps hun codes open source maken, zodat audits van derden mogelijk worden (Cai et al., 2018). De toepassing moet autonoom kunnen functioneren zonder de bemoeienis van een entiteit, die de meerderheid van de identificatie-eenheden (tokens) controleert. De applicatie kan zijn protocol wellicht aanpassen aan veranderende marktomstandigheden en andere ontwikkelingen, maar het is echter alleen "de consensus", dus de overeenstemming binnen het netwerk, die bepaalt of die aanpassing ook daadwerkelijk mag worden doorgevoerd (Darren, 2019). DApps worden uitgevoerd onder een "open source licentie", waardoor decentrale applicaties altijd open staan voor innovaties (Darren, 2019).

Een andere belangrijke factor die een App tot een decentrale applicatie maakt, is het gegeven dat alle data en registraties cryptografisch beveiligd en opgeslagen moeten zijn, in een gedecentraliseerde blockchain (Darren, 2019). Alleen dan is er geen sprake meer van een *"central point of failure"*: een volledig gedecentraliseerd systeem zou geen centraal storingspunt moeten hebben, aangezien alle onderdelen van de applicaties in de blockchain

worden gehost en uitgevoerd (Cai et al., 2018). Daarnaast moet een decentrale applicatie cryptocurrencies genereren en gebruiken om te kunnen worden aangemerkt als een dApp (Cai et al., 2018). Dit is noodzakelijk om toegang te krijgen tot de decentrale applicatie en het belonen van de *miners*, als zij eenmaal hun belangrijke werk hebben gedaan (Darren, 2019). De *miners* worden namelijk beloond met de desbetreffende digitale betalingseenheid (Darren, 2019). De *miners* doen hun algoritmische berekeningen, creëren blokken in de vorm van Proof-of-Work en ontvangen hun vergoeding[63] (Darren, 2019).

Momenteel worden er dagelijks nieuwe dApps ontwikkeld (Blockchain uitgelegd, 2019b). Er bestaan verschillende blockchains waarop gemakkelijk smart contracts (en dApps) gebouwd kunnen worden. Ethereum[64] is hiervan de meest bekende. Het is een decentraal platform waar programmeurs relatief eenvoudig een smart contract kunnen programmeren (Derek, 2018).

Als je naar de 'State of the DApps' website (www.stateofthedapps.com) navigeert, zie je dat er momenteel meer dan 2.000 voorbeelden van dApps op basis van Ethereum in verschillende stadia van ontwikkeling zijn.

2.1.5 Blockchain heeft ook nadelen

(1) Grootte: vermits een blockchain voortdurend groeit (er verdwijnen nooit blokken), kan dit aanleiding geven tot een omvangrijke blockchain, die bovendien via het netwerk op iedere *node* gekopieerd moeten worden.

[63] Trefwoordenlijst: Proof-of-Work (PoW) (zie achteraan deze masterproef).
[64] Ethereum.org. (2019). Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world. Retrieved from https://www.ethereum.org/

(2) Ondervragingen: de data in de *chain* zijn geëncrypteerd en ongestructureerd (transactie blokken). Dit maakt dat, het doorzoeken van de data, speciale technieken vereist, die nog in volle ontwikkeling zijn (bijvoorbeeld Graph[65]). Traditionele, relationele databanken zijn hiervoor veel beter geschikt.

(3) Persoonlijke data: het opslaan van persoonsgegevens[66] op de blockchain, kan juridische problemen stellen. Dankzij de technologie kunnen bij activiteiten zoals de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen meer dan ooit tevoren persoonsgegevens worden verwerkt (Europees Parlement en de Raad van de Europese Unie, 2016). Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming en de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming[67] of "AVG" genoemd) is van toepassing op elke verwerking[68] van persoonsgegevens in de lidstaten, zowel in de publieke als in de particuliere sector. Die richtlijn is echter niet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking (Europees Parlement en de Raad van de Europese Unie, 2016). De nieuwe Richtlijn (EU) 2016/680 (richtlijn "politie justitie")[69] vormt daarom een aanvulling op de AVG. De

[65] Graph. (2019). The Graph. Scalable queries for a decentralized future: The Graph is a decentralized protocol for indexing and querying blockchain data. Retrieved from https://thegraph.com/

[66] 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 identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon; (Europees Parlement en de Raad van de Europese Unie, 2016).

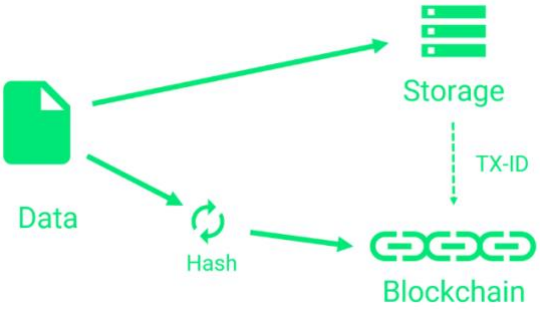
[67] https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:32016R0679

[68] Verwerking: 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, bekendmaking door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens; (Europees Parlement en de Raad van de Europese Unie, 2016).

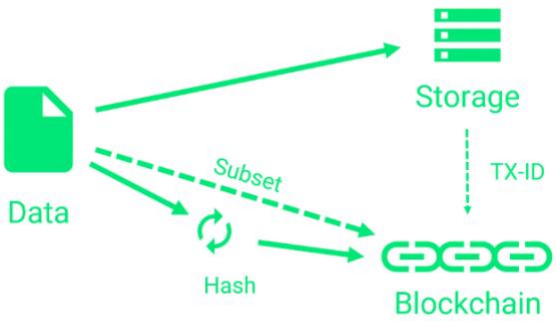
[69] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016L0680&from=EN

eigenschappen en technische aspecten van blockchain kunnen echter in strijd zijn met de AVG en de richtlijn “politie justitie”. Deze werden immers niet ontworpen met gedecentraliseerde platformen, zoals blockchain, in het achterhoofd (Simal et al., 2018). Volgens Artikel 5 van de richtlijn “politie justitie” bijvoorbeeld, moeten lidstaten erin voorzien dat passende termijnen worden vastgelegd voor het wissen van persoonsgegevens (Europees Parlement en de Raad van de Europese Unie, 2016). De manipulatiebestendigheid van de blockchain maakt het echter moeilijk, zo niet onmogelijk, om de gegevens te corrigeren, te bewerken en/of te vernietigen (Hofman, Lemieux, Joo, & Batista, 2019).

Een mogelijk alternatief, om deze nadelen op te vangen, is om enkel een *hash* (vingerafdruk) van de data op te nemen in de *chain* en de eigenlijke, ruwe data in een relationele database, buiten de blockchain (*off-chain*) op te slaan. De hash in de blockchain dient dan eigenlijk om de integriteit van de data in de relationele databank te bewaken. Indien data in de databank gewijzigd worden, dan verandert de hash en moet dit aan de blockchain bekend gemaakt worden door een blok met de nieuwe (aangepaste) hash toe te voegen. De hash in de blockchain kan gebruikt worden om de data, of slechts een subset van de data op de blockchain, in de relationele databank te checken.



Figuur 6.1: off-chain opslag van data



Figuur 6.2: off-chain opslag van een subset van de data

2.1.6 Waarom is blockchain zo revolutionair?

De blockchain is een puur gedistribueerde peer-to-peer gegevensopslag (gedistribueerde ledger database): dit maakt efficiënte en effectieve gegevensdeling tussen (veel) betrokken partijen mogelijk. Iedere deelnemer beschikt over zijn eigen database kopie, die steeds de actueelste gegevens bevat. Bij een systeem met centrale database is een complexe communicatie-infrastructuur nodig om gegevens vanuit de centrale database te verdelen naar de geïnteresseerde partijen, die de ontvangen informatie dan weer opslaan in een eigen database. Met het risico van verschillen. De beheerder van het centrale systeem moet ook toegang voorzien voor alle partijen om gegevens in de centrale databank te raadplegen en/of aan te passen. Dit leidt tot hoge kosten.

Blockchain heeft ook geen '*single point of failure*': het is "in principe" niet mogelijk om in de blockchain opgeslagen informatie te manipuleren of op welke manier dan ook zomaar te veranderen (bijvoorbeeld één database *crasht* of wordt beschadigd door een hacker). Dat komt omdat er binnen het netwerk meerdere kopieën worden opgeslagen (die gepaard gaan met het complexe consensus-mechanisme). Blockchain is tevens onveranderbaar (*immutable*): gegevens in de database kunnen niet veranderd (of verwijderd) worden. Er kunnen enkel datablokken worden toegevoegd (*append-only*). Een blok met data die eenmaal in de blockchain zit, blijft er voor altijd in zitten, onlosmakelijk verbonden met het voorgaande blok in de keten (Meijers, 2016). Daardoor weet iedereen zeker dat alles wat in de blockchain zit correct is en correct blijft (Meijers, 2016). Dit zorgt voor een traceerbaarheid van de aanpassingen (herkomst tracering/*provenance tracking*).

Nieuwe datablokken kunnen alleen worden toegevoegd, wanneer er een consensus is tussen de (geautoriseerde) deelnemers, dat de data correct zijn.

Tot slot wordt de integriteit van de datablokken beschermd door een digitale vingerafdruk (*hash*), waardoor kwaadwillig of ongeautoriseerd aanpassen van data of verwijderen van blokken snel kan worden gedetecteerd, door het regelmatig verifiëren van de correctheid van de hashes (één per blok en alle blokken aan mekaar verbonden). Via cryptografie kan data selectief worden afgeschermd en enkel toegankelijk worden gemaakt voor deelnemers met de vereiste *credentials* (*keys*).

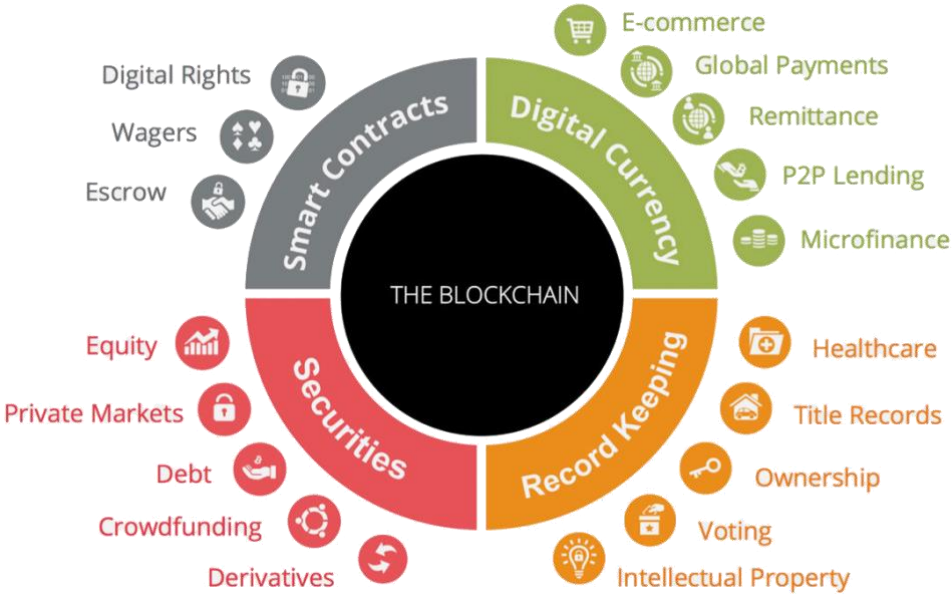
Deze eigenschappen van de blockchain (onveranderbaar; append-only; geordend; met tijdstempel; veilig – identificatie, authenticatie en autorisatie; uiteindelijk consistent) hangen niet af van de specifieke gegevens die erin worden opgeslagen.

2.1.7 Blockchain toepassingen

Vanuit een vereenvoudigd oogpunt kunnen we de blockchain zien als een speciaal soort doos voor het opslaan van digitale voorwerpen. De blockchain heeft geen weet van de gegevens die hij opslaat (Drescher, 2017). Op basis van de eigenschappen van de blockchain en zijn aard van generieke gegevensopslag voor allerlei gegevens kunnen we de volgende algemene toepassingen bedenken: bewijs van bestaan; bewijs van niet-bestaan; bewijs van tijd; bewijs van ordening; bewijs van identiteit; bewijs van auteurschap; bewijs van eigenaarschap (Drescher, 2017).

Bovendien beperkt de combinatie van blockchaintechnologie en asymmetrische encryptie de noodzaak van vertrouwde intermediairs (tussenpersonen). Het is een technologie die gebruikt kan worden om processen in een groot aantal contexten te decentraliseren en te automatiseren. De potentiële toepassingen (*Use Cases*) voor blockchain zijn enorm.

In onderstaande figuur worden enkele van de mogelijke toepassingen van blockchain weergegeven, waarbij een onderverdeling wordt gemaakt in ‘smart contracts’, ‘digital currency’, ‘record keeping’ en ‘securities’ (Verhelst, 2017).



Figuur 7: mogelijke toepassingen met blockchain (bron: BTCS Inc., www.btcs.com)

Volgens het World Economic Forum[70] zijn we, na het tijdperk van het internet van informatie, nu getuige van het opkomen van het tijdperk van het internet van waarde. Het is in dat klimaat dat blockchaintechnologie businessmodellen, de economie en de samenleving grondig kan veranderen (Schiltz et al., 2018).

[70] Het World Economic Forum is een jaarlijkse bijeenkomst van de CEO's van de grootste bedrijven ter wereld, internationale politici (presidenten, ministers-presidenten en anderen), intellectuelen, academici en technologievernieuwers, waardoor het een invloedrijk platform is (World Economic Forum, 2019).

2.1.8 Conclusie

Blockchain vormt sinds 2008 de basis voor de Bitcoin. Dat was de start. Nu begint het pas echt interessant te worden. Toch is er ook scepticisme. Dat is terecht. Bedenkingen rond de technologie helpen het algemeen niveau én het discours errond naar boven te tillen. Inmiddels zijn er tal van blockchain-initiatieven op het internet actief. Een daarvan is de Ethereum-blockchain. Ethereum is interessant omdat het toelaat om *smart contracts* en decentrale applicaties (dApps) te programmeren. Iedereen moet intussen wel begrijpen dat blockchain veel meer is dan Bitcoin. Het is een grondleggende technologie met het potentieel om nieuwe fundamenten te bouwen, in het bijzonder op het vlak van samenwerking en data-uitwisseling. Blockchaintechnologie kan zo onder meer de manier waarop wetshandhavingsdiensten informatie opslaan en uitwisselen, ingrijpend veranderen.

Blockchain is een gedistribueerde databasetechnologie (een innovatief type veilige database) die kan worden gerepliceerd, gedeeld en gesynchroniseerd over alle computers die deelnemen aan het (blockchain)netwerk en waarbij er geen centraal beheer (nodig) is. Het is veiliger dan andere manieren om informatie op te slaan en te delen (vooral omdat voor een verstoring meerdere — in plaats van één — faalpunten binnen het netwerk nodig zouden zijn), daarnaast biedt het, ondanks lagere kosten, ook veel meer mogelijkheden voor personalisatie van diensten. De slimme codering achter blockchain laat partijen toe betrouwbare transacties uit te voeren waarvan de authenticiteit wordt vastgesteld door massale samenwerking tussen verschillende deelnemende computers (knooppunten) aan het netwerk die worden gedreven door een collectief eigenbelang, niet door tussenpersonen, en dat is nieuw. De rode draad in dit verhaal is dat de tussenkomst van een derde instantie wordt uitgeschakeld. Desintermediatie door deze systemen kan hele industrieën op de schop nemen.

Een blockchain verkrijgt zijn permanente karakter via cryptografische hashfuncties, de wiskundige berekeningen die blockchain gebruikt, en maakt gebruik van asymmetrische encryptie. Hieruit kunnen we afleiden dat: een blockchain gedecentraliseerd en gedistribueerd, permanent en versleuteld is.

De parallellen tussen nieuwe maatschappelijke tendensen als peer-to-peer samenwerkingen, gedecentraliseerd vertrouwen, … enerzijds en *distributed ledger technology* anderzijds zijn te belangrijk om blockchain als een hype weg te zetten. Zoals elke technologie is blockchain een instrument, geen doel op zich. Daarom moeten de experimenten worden voortgezet. Het kan mogelijke oplossingen bieden voor de ontwikkeling van een geïntegreerde informatiehuishouding en -uitwisseling zoals besproken in Deel I, over de barrières en hinderpalen bij het digitaal forensisch onderzoek.

Hoe dan ook moeten toepassingen van dergelijke technologische ontwikkelingen ook onderzocht worden in het kader van de impact die ze hebben op criminaliteit. Technologie biedt niet alleen politie en justitie kansen voor een betere uitoefening van hun taken, ze biedt ook criminelen meer gelegenheden en mogelijkheden tot het plegen van criminaliteit.

In het volgende hoofdstuk wordt dieper ingegaan op de rol van blockchaintechnologie en de impact ervan op criminaliteit (lees: bedreigingen van blockchain). Dit om te begrijpen waarom de overheid en politiediensten aandacht moeten hebben voor deze veelbelovende technologie. Want ook criminelen omarmen blockchain.

2.2 Blockchaintechnologie en criminaliteit (bedreigingen)

2.2.1 Inleiding

Uit de toekomstvisie voor de Belgische politie van Bruggeman (2014) kunnen we afleiden dat de technologisering – waarbij we slechts op middellange termijn de effecten ervaren van de vandaag ontwikkelde technieken – waarneembaar is in tal van maatschappelijke domeinen waaronder het veiligheidsdomein (Bruggeman, 2014). Maar zoals bij bijna alle nieuwe innovatieve technologieën kan ook blockchaintechnologie gebruikt worden voor schadelijke en illegale doeleinden (Girasa, 2018).

Uit onderzoek is gebleken dat zodra technologie voor het publiek beschikbaar komt, criminelen behoren tot de '*first adopters*'[71] (Bruggeman, 2014). Het ontstaan van geheel nieuwe verschijningsvormen van high-tech crime is daarbij niet uitgesloten (van der Hulst & Neve, 2008). Want ook criminelen omarmen blockchain (Europol, 2017b).

2.2.2 Criminal smart contracts en dApps: De donkere kant van de gedecentraliseerde wereld

Op basis van de verschillende eigenschappen van blockchain zoals reeds vermeld (cfr. 2.1) en zijn aard van generieke gegevensopslag voor allerlei gegevens, komen we tot enkele vaststellingen over de impact van de blockchaintechnologie op criminaliteit.

[71] Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars: The future of terror, crime, and militancy.* Santa Monica, CA: RAND Corporation.

2.2.2.1 Gedecentraliseerde en geëncrypteerde communicatie

Het is bij politie en Openbaar Ministerie al langer bekend dat criminelen op uitgebreide schaal gebruik maken van de mogelijkheid om vertrouwelijk met elkaar te communiceren. Criminelen zijn steeds op zoek naar betrouwbare, veilige communicatie (Europol, 2018). Dat doen zij onder andere met behulp van beveiligde chatapps die versleuteling (end-to-end encryptie[72]) aanbieden, de zogenaamde '*secure & encrypted messaging apps*'[73], en andere (vaak buitenlandse) aanbieders van encryptie en privacy tools (Europol, 2018). Encryptie wordt dan gebruikt om de identiteit van communicaties te verbergen (Diţu, 2017). Dit houdt in dat alleen de verzender en de ontvanger het bericht kunnen lezen. Omdat alleen de ontvanger over de juiste sleutel beschikt om het bericht weer leesbaar te maken, is de ontvanger beschermd als het bericht onderweg wordt onderschept (Jacobsen, 2017). Communicatie tussen verdachten (van georganiseerde misdaad) is hierdoor voor opsporingsdiensten niet of nauwelijks zichtbaar, omdat het veel traditionele opsporingstechnieken, zoals de telefoontap, ineffectief maakt (Europol, 2017b). In het advies met betrekking tot de Kadernota Integrale Veiligheid 2016-2019 wijst het College van procureurs-generaal op de moeilijkheden die de politiediensten ondervinden inzake lokalisatie en onderscheppen van communicatie ten gevolge de niet te stuiten technologische evoluties (College van procureurs-generaal, 2016).

Een voorbeeld hiervan zijn de versleutelde telefoons, ook wel '*cryptofoons*' genoemd, die gebruikt worden in het criminele milieu. Dit zijn telefoons waarbij de communicatie tussen twee toestellen beveiligd is met een unieke encryptie (versleuteling). Het dataverkeer verloopt

[72] Zorgt ervoor dat alleen jij en het contact waarmee je communiceert de berichten kunnen lezen. Niemand anders kan de berichten lezen. Zelfs de beheerder van de software kan dat niet. Je berichten zijn beveiligd met een slot en alleen de verzender en de ontvanger hebben de sleutel om het slot te openen en het bericht te lezen.
[73] Smartphone apps die gebruik maken van end-to-end encryptie, een hele sterke vorm van versleuteling. Bij end-to-end encryptie wordt een bericht op een speciale manier versleuteld waardoor alleen de ontvanger het kan inzien. Op de webpagina: Secure Messaging Apps (www.securemessagingapps.com); kun je zien welke apps versleuteling aanbieden, waar de servers staan en hoe het betreffende bedrijf denkt over privacy.

via eigen servers, waardoor de communicatie verder afgeschermd wordt voor de autoriteiten (Politie.nl, 2018). De telefoons zien eruit als een normale telefoon maar de meeste reguliere functies zijn onklaar gemaakt. Je kunt er dan ook alleen maar berichten en afbeeldingen mee verzenden en ontvangen. Ook kun je alleen communiceren met iemand met hetzelfde toestel. De toestellen zijn enorm prijzig gemiddeld zo'n € 1.500,- per toestel. Op het toestel zit tevens een paniekknop waarmee in één keer alle gegevens kunnen worden gewist.

Desondanks kent elke modus operandi zwakke plekken en elke technologie brengt ook kansen voor politie en justitie met zich mee (WODC, 2018). Vorig jaar (2018) heeft de Nederlandse politie een doorbraak bereikt in het onderscheppen en ontsleutelen van versleutelde communicatie tussen criminelen[74]. Experts van de politie in Oost-Nederland zijn er in geslaagd om toegang te krijgen tot de communicatie van bovenvermelde cryptofoons, die gebruik maken van de applicatie IronChat[75], en deze te ontsleutelen. De server waarover de versleutelde communicatie plaatsvond, werd ontdekt nadat de politie in Oost-Nederland een leverancier van de cryptofoons op het spoor kwam. Op de door justitie in beslag genomen server stonden niet alleen de versleutelde berichten van criminelen, maar ook de cryptografische sleutels om ze te kunnen lezen; merk op dat het encryptieprotocol zelf niet werd gekraakt (Huijbregts, 2018). Omdat de politie toegang tot de server had waar de encryptiesleutels op stonden, kon er live meegekeken worden met de berichten die werden verstuurd vanaf de cryptofoons. Volgens de politie ging het om 258.000 berichten van meer dan honderd mensen en ging de communicatie vrijwel uitsluitend over criminele zaken (Politie.nl, 2018).

[74] Politie.nl. (2018). Doorbraak in onderscheppen cryptocommunicatie [Press release]. Retrieved from https://www.politie.nl/nieuws/2018/november/6/02-doorbraak-in-onderscheppen-cryptocommunicatie.html

[75] Online is een handleiding uit 2015 te vinden van het gebruik van de chatdienst (https://docplayer.nl/20054801-Hybrid-alle-rechten-voorbehouden-blackbox-security-2015.html). Daarin beweert het bedrijf: *"Met IronChat kunt u er zeker van zijn dat uw communicatie privé is en blijft!"*. In de telefoon was ook een 'paniekknop' ingebouwd waarmee de inhoud van de telefoon snel kon worden gewist (van Lonkhuyzen, 2018).

De zaak lijkt op die van Ennetcom (2016)[76]. Ennetcom was een aanbieder van versleutelde communicatie die volgens het Openbaar Ministerie (OM) veelvuldig werd gebruikt door criminelen. In het opsporingsonderzoek kon een kopie worden gemaakt van de server waarop diensten van Ennetcom draaiden (WODC, 2018). Miljoenen versleutelde berichten (3,6 miljoen PGP-berichten)[77] konden worden ontcijferd, waarmee politie en justitie een ware goudmijn leken te hebben aangeboord[78] (Politie.nl, 2017b).

Op basis van de hierboven beschreven politionele interventies kan blockchaintechnologie een oplossing bieden voor de crimineel. Blockchaintechnologie is gedecentraliseerd: de *nodes* zijn niet verbonden met één centrale server maar zijn daarentegen allemaal onderling verbonden. Doordat geen gebruik wordt gemaakt van centrale servers, is de communicatie en data beveiligd tegen datalekken en inbeslagnames. Computernetwerken en applicaties als IronChat maken gebruik van gecentraliseerde oplossingen voor de ondersteuning van communicatiekanalen met versleuteld verkeer (J. Bambara et al., 2018). Blockchain voorkomt dergelijke *'single points of failure'*: decentralisatie van (transactie)data verkleint het risico dat informatie wordt veranderd, verloren gaat of wordt gestolen (Blockchain uitgelegd, 2019a).

Anders gezegd, blockchaintechnologie kan worden gebruikt om de veiligheid en betrouwbaarheid in gedistribueerde netwerken te verbeteren (Casino, Dasaklis, & Patsakis,

[76] Politie.nl. (2017). Versleutelde berichten: schat aan criminele informatie [Press release]. Retrieved from https://www.politie.nl/nieuws/2017/maart/9/11-versleutelde-berichten.html

[77] Pretty Good Privacy (meestal afgekort tot PGP) is een specifieke encryptiesoftware die de inhoud van de berichten afschermd. Het is een van de veel gebruikte vercijferingsmethodes op internet die ook gebruik maakt van een public en een private key. PGP combineert traditionele encryptie met asymmetrische cryptografie om berichten onleesbaar te maken. Een PGP-key bestaat uit drie onderdelen: een publieke sleutel, een privésleutel en een wachtwoord. De publieke sleutel mag met iedereen worden gedeeld: deze wordt gebruikt om berichten of bestanden te verzenden. De privésleutel moet de eigenaar geheimhouden, want deze maakt het, in combinatie met het wachtwoord, mogelijk om berichten te ontsleutelen. Door deze encryptie zijn berichten niet te ontcijferen door overheden en de politie.

[78] Landelijk Parket. (2019). Onderzoek PGP-servers levert meer dan miljoen nieuwe berichten op [Press release]. Retrieved from https://www.om.nl/actueel/nieuwsberichten/@105040/onderzoek-pgp/

2019). Enkele voorbeelden hiervan zijn: Rival Messenger (www.rivalmessenger.com), Bitmessage (https://bitmessage.org/)[79], e-Chat (https://echat.io/), SENSE Chat (www.sense.chat) en Crypviser (https://crypviser.network/#benefits). In 2017 werd ‘s Werelds eerste blockchain cryptocommunicator, BitVault®[80], voorgesteld. Dit is een crypto-focused smartphone (cryptofoon) die gebruik maakt van veilige geëncrypteerde berichtgeving via een private blockchain. Ook HTC’s nieuwste smartphone (HTC Exodus 1)[81] is een blockchain-gebaseerde smartphone waarop onder andere gedecentraliseerde applicaties kunnen worden gedraaid.

2.2.2.2 Gedecentraliseerde (darknet)markten

Die resistentie van blockchainnetwerken zorgt ervoor dat de technologie erg aanlokkelijk is voor online zwarte markten (Cludts, 2019). ICT-toepassingen hebben op verschillende terreinen tot vernieuwing van criminele werkwijzen geleid (WODC, 2018). Zo zijn er dankzij het internet nieuwe mogelijkheden ontstaan om vraag en aanbod op criminele markten bij elkaar te brengen (WODC, 2018). De verkoop van drugs en andere illegale producten en diensten is zo verschoven naar wat bekend is geworden als "darknetmarkten” of cryptomarkten, een min of meer afgeschermd deel van het internet dat niet toegankelijk is via standaardwebbrowsers (European Monitoring Centre for Drugs and Drug Addiction, 2016). Ze

[79] Warren, J. (2012). Whitepaper – Bitmessage: A peer-to-peer message authentication and delivery system. Retrieved from https://bitmessage.org/bitmessage.pdf
[80] Swiss Bank In Your Pocket. (2017). BitVault – World’s first blockchain cryptocommunicator. Retrieved from https://swissbankinyourpocket.com/product/bitvault/
[81] HTC Corporation. (2019). Exodus 1. The native web 3.0 blockchain phone. Retrieved from https://www.htcexodus.com/eu/

bevinden zich in het dark web[82] en zijn enkel toegankelijk via Tor[83] (Martin, 2014a). Een cryptomarkt kan worden gedefinieerd als een onlineforum waar goederen en diensten worden uitgewisseld tussen partijen die digitale encryptie gebruiken om hun identiteit te verbergen (Martin, 2014b).

Cryptomarkten, de online criminele markten van de 'tweede generatie', betekenen een stap voorwaarts in criminele innovatie. Visueel zien ze er net zo uit als elke andere legitieme online marktplaats (eBay, bijvoorbeeld): ze brengen een scala van verkopers samen op een locatie, ieder met een lijst van producten te koop, en stellen klanten in staat om te vergelijken en winkelen. Ze bieden dezelfde mogelijkheden om te netwerken en zakelijke transacties uit te voeren als de eerste generatie criminele markten, maar dan in een veel 'veiligere' omgeving. Cryptomarkten vonden niet per se enige technologie uit, maar brachten vier beveiligingsmaatregelen samen die nooit eerder samen werden gebruikt. Om te beginnen vereisen cryptomarkten dat gebruikers hun betalingen doen in cryptocurrencies zoals Bitcoin. Transacties in virtuele valuta's zijn buitengewoon moeilijk te traceren en het gebruik ervan omvat geen controle door regelgevende instanties, bijvoorbeeld met betrekking tot de antiwitwaswetgeving[84]. Ten tweede, vereisen cryptomarkten dat hun gebruikers een anonimiseringsdienst gebruiken zoals Tor, om hun identiteit te verbergen wanneer ze

[82] Het dark web houdt een anoniem en besloten deel van het internet in (Bossuyt, 2017). Deze term mag niet verward worden met het deep web, die alle onbereikbare inhoud omvat voor zoekmachines. De meeste van deze pagina's zijn onschuldig, zoals databases van bedrijven die je enkel na authenticatie kan opvragen. Het deep web is een koepelterm waar het dark web slechts een klein deel van uitmaakt (Bossuyt, 2017). Websites op het dark web liggen meestal versleuteld achter het Tor-netwerk en kan je niet bereiken met een normale browser (Dițu, 2017). Het dark web is ook niet opgenomen in zoekmachines zoals Google of Yahoo. Het is het deel van het internet dat het meest bekend is voor illegale activiteiten, vanwege de anonimiteit die het biedt aan gebruikers (European Monitoring Centre for Drugs and Drug Addiction, 2016). Zo houden de meeste verkooptransacties op darknetmarkten verband met drugs (Europees Waarnemingscentrum voor drugs en drugsverslaving, 2017).

[83] Tor is de afkorting van The Onion Router, een speciaal netwerk dat gebruikers anonimiseert.

[84] De antiwitwaswetgeving van 18 januari 2010 legt verschillende verplichtingen op aan de tussenpersonen, zoals het identificeren van cliënten, het controleren van hun identiteit, bijzondere waakzaamheid vóór en na het afsluiten van een overeenkomst, en het actief samenwerken met de Cel voor Financiële Informatieverwerking (CFI). Wanneer de tussenpersoon weet of vermoedt dat een uit te voeren verrichting verband houdt met het witwassen van geld of de financiering van terrorisme, moet hij de CFI hierover onmiddellijk verwittigen (Autoriteit voor Financiële diensten en Markten (FSMA), 2019).

verbinding maken met de server. Cryptomarkten maken ook gebruik van deze diensten om hun IP-adressen[85] te verbergen, waardoor het voor wetshandhavingsinstanties moeilijker wordt om beslag te leggen op hun servers (European Monitoring Centre for Drugs and Drug Addiction, 2016). Dit betekent ook dat speurders moeilijker in staat zullen zijn de identiteit te achterhalen van wie de goederen koopt of verkoopt, of waarnaar illegale goederen worden verzonden (Martin, 2014a). Het gebruik van encryptietechnologie onderscheidt cryptomarkten van andere soorten Online Illegale Markten (OIM), bijvoorbeeld sites die afhankelijk zijn van spam-marketing om illegale goederen en diensten te verkopen vanaf centrale locaties (Martin, 2014a).

Het basisontwerp voor het opzetten van zo'n cryptomarkt is echter nog steeds één enkele (centrale) computer/server ergens op het internet. Het stelt de éne (centrale) machine/server open voor een verscheidenheid aan politionele onderzoekstechnieken door wetshandhavingsdiensten, om het internetverkeer en de gebruikersactiviteiten te de-anonimiseren en de hele illegale handelsoperatie bloot te leggen[86] (European Monitoring Centre for Drugs and Drug Addiction, 2016). Een voorbeeld hiervan zien we in het politieoptreden tegen *Hansa*[87]. *Hansa* was een ondergrondse marktplaats, waarop kopers en verkopers van drugs elkaar troffen. In 2017 hield de Nederlandse politie niet alleen de beheerders van deze marktplaats aan, maar nam ook de servers in beslag waardoor de politie het beheer van de marktplaats in handen kreeg (WODC, 2018). Bovendien hielden politie en OM de marktplaats voor een bepaalde periode operationeel. Zo zijn grote aantallen transacties

[85] IP-adres (Internet Protocol adres). Een uniek identificerend nummer van met internet verbonden apparaten. Het IP-adres is, simpel gezegd, het huisadres van de computer.
[86] Europol. (2019). Double blow to dark web marketplaces [Press release]. Retrieved from https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces
[87] Politie.nl. (2017). Ondergrondse Hansa Market overgenomen en neergehaald [Press release]. Retrieved from https://www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html

én kopers en verkopers in beeld gekomen (WODC, 2018). De criminele gemeenschap op dark markets was bekend met het risico van een 'gewone' sluiting van een marktplaats zoals Silk Road[88]. De criminelen waren echter onbekend met het risico van een overname en wisten niet welke gegevens de politie van hen had weten te bemachtigen. De Hansa-overname heeft daarmee het vertrouwen van de gemeenschap in de onderliggende faciliterende principes van darknetmarkten meer geschaad dan andere interventies (Verburgh et al., 2018). Het effect van deze actie liet zich duidelijk voelen[89]. Verkopers en kopers en ook beheerders van online criminele marktplaatsen wanen zich vaak ongrijpbaar voor politie en justitie. Door het uitvoeren van strafrechtelijke onderzoeken en strafvervolging van deze criminelen wordt duidelijk dat het dark web helemaal niet zo anoniem is als de gebruikers mogelijk denken (Politie.nl, 2017a).

Naarmate wetshandhavingsinstanties beter worden in het sluiten van criminele marktplaatsen door succesvolle interventies[90], ontstaan er nieuwe en mogelijks zelfs nog veerkrachtigere modellen voor dergelijke criminele marktplaatsen[91] (Europol, 2018). De markten verplaatsen zich naar gedecentraliseerde netwerken en vormen zo gedecentraliseerde (darknet)markten[92] (Holland, Amado, & Marriott, 2018). Uit deze behoefte werd onder meer OpenBazaar

[88] De allereerste grote mondiale politieoperatie betreft Operatie Marco Polo, die in 2013 leidde tot sluiting van het befaamde Silk Road 1.0 en arrestatie van de administrator Ross Ulbricht. Operatie Onymous was de tweede mondiale operatie, deze leidde in 2014 tot de sluiting van meerdere sites op het dark web. Silk Road 2.0 was één van deze sites. De meest recente en laatste mondiale operatie betreft die van Operatie Bayonet in 2017. Deze operatie leidde tot de sluiting van de twee grootste markplaatsen van dat moment, namelijk Alphabay en Hansa market (Verburgh, Smits, & van Wegberg, 2018).

[89] Europol. (2017). Massive blow to criminal Dark Web activities after globally coordinated operation [Press release]. Retrieved from https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[90] Europol. (2019). Global law enforcement action against vendors and buyers on the dark web [Press release]. Retrieved from https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web

[91] Devoe, R. (2018). Decentralized darknet markets could lead to unstoppable silk road clones. Retrieved from https://blockonomi.com/decentralized-darknet-markets/

[92] Cludts, D. (2019). Een gedecentraliseerd dark web: hoe de zwarte markt zich wapent met blockchain. Retrieved from https://www.techzine.be/blogs/35330/een-gedecentraliseerd-dark-web-hoe-de-zwarte-markt-zich-wapent-met-blockchain.html

ontwikkeld, een volkomen gedecentraliseerde online (zwarte) markt zonder specifieke eigenaar (Raval, 2016).

Met het succes van de blockchaintechnologie begint zo een nieuwe generatie zwarte markten[93] te verschijnen (European Monitoring Centre for Drugs and Drug Addiction, 2016). De belangrijkste kandidaat voor identificatie als een zwarte markt van de volgende generatie is OpenBazaar[94]. OpenBazaar werkt door de transacties van de e-commerce software te distribueren over alle deelnemers van de markt. De markt zelf is niet gebaseerd op één instantie van de e-commerce software, die draait op één enkele centrale computer/server ergens op het internet, maar op de software die draait op alle computers die deelnemen aan de markt. Dit wordt gerealiseerd met behulp van de basisprincipes van de blockchaintechnologie (European Monitoring Centre for Drugs and Drug Addiction, 2016).

OpenBazaar past deze blockchain logica toe op alle transacties op de markt. Daarom, wanneer iemand de OpenBazaar software op zijn computer draait, wordt het onmiddellijk onderdeel van de markt zelf. Dit creëert het potentieel voor een volledig gedistribueerde en gedecentraliseerde marktplaats verspreid over duizenden computers over de hele wereld. Elke computer verwerkt slechts een deel van de markt, eerder dan dat alles op één enkele computer of server wordt behandeld. Het decentrale karakter zorgt ervoor dat de gegevens nooit kunnen worden verwijderd door bijvoorbeeld wetshandhavingsinstanties of hackers (DeepDotWeb, 2017). Anonimiseringsdiensten zoals Tor en de implementatie van privacy-focused cryptocurrencies

[93] Een zwarte markt is de handel in goederen of diensten die illegaal zijn of verdeeld worden via illegale kanalen. Enkele voorbeelden van een zwarte markt zijn: het verkopen van gestolen goederen, drugs of wapens (Celestini, Me, & Mignone, 2016).

[94] OpenBazaar is een andere manier van online zakendoen. Het is een peer-to-peer applicatie op basis van blockchaintechnologie die geen tussenpersonen nodig heeft, wat betekent dat er geen kosten zijn en geen beperkingen. OpenBazaar verbindt mensen rechtstreeks via blockchain. Gegevens worden verspreid over het netwerk in plaats van opgeslagen in een centrale database. Niemand heeft controle over OpenBazaar. Elke gebruiker draagt evenveel bij aan het netwerk en heeft de controle over zijn eigen privégegevens (www.openbazaar.org).

("privacy coins") [95] zoals Monero (XMR)[96], kunnen worden gebruikt met dit model om de identiteit en privacy van gebruikers verder te beschermen (European Monitoring Centre for Drugs and Drug Addiction, 2016). OpenBazaar is zeker niet de enigste kandidaat voor identificatie als een (zwarte) markt van de volgende generatie. Andere platformen zijn volop in de ontwikkelingsfase[97].

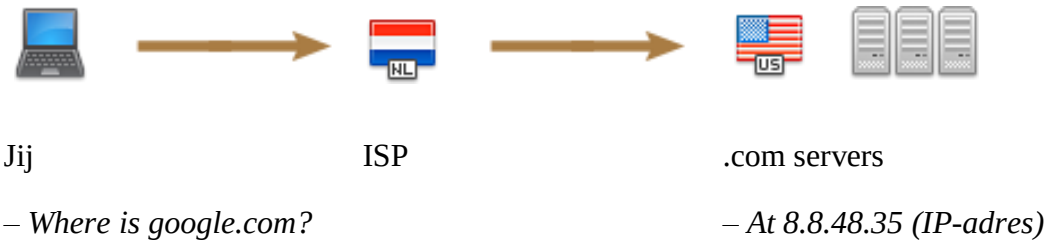
Toch hoeft een marktplaats niet eens een eigen blockchainnetwerk op te zetten om zijn diensten aan te bieden. Dat kan bijvoorbeeld ook via een legitiem publiek platform, zoals Ethereum, zonder dat de deelnemers van het netwerk enig benul hebben dat er illegale handel op wordt gedreven (Cludts, 2019). De combinatie van anonimiteit, decentralisatie kan het in de toekomst een stuk lastiger maken voor politiediensten om hardhandig op te treden tegen illegale online marktplaatsen (Cludts, 2019).

2.2.2.3 Gedecentraliseerde DNS

Ook het gebruik van blockchain Domain Name System (DNS) groeit gestaag onder (cyber)criminelen (Holland et al., 2018). Het Domain Name System is een fundamenteel onderdeel van het internet. DNS is in essentie het internettelefoonboek. Iedere op internet aangesloten computer heeft ten minste één IP-adres. Dit IP-adres maakt het mogelijk om andere computers te adresseren en dus te bereiken. DNS is het technische systeem dat namen koppelt aan deze IP-adressen en zo elke computer op het internet bereikbaar maakt onder een voor mensen begrijpelijke naam (GOVCERT.NL, 2008). Het hart van het Domain Name System

[95] Altcoins die zich vooral op (nog) meer anonimiteit toespitsen. Altcoin is een afkorting van "Bitcoin Alternative". In dit opzicht beschrijft de term altcoin elke afzonderlijke cryptocurrency die geen Bitcoin is.
[96] Reddit. (2018). OpenBazaar is looking for Monero integration. Retrieved from https://www.reddit.com/r/Monero/comments/9jx1ne/openbazaar_is_looking_for_monero_integration/
[97] DeepDotWeb. (2017). Behind-the-scenes: a darknet market on the ethereum blockchain. Retrieved from https://www.deepdotweb.com/2017/07/08/behind-scenes-darknet-market-ethereum-blockchain/

wordt gevormd door name-servers: de computers met de programmatuur die domeinnamen omzet naar IP-adressen. Vaak is dit een server van een *internet service provider (ISP)*, de partij die de internetverbinding verzorgt, bijvoorbeeld Telenet of Belgacom (Ippo, 2017). Wanneer we een website in een adresbalk typen, vraagt de computer automatisch aan een DNS om een IP-adres. Als we bijvoorbeeld zoeken naar google[.]com, zoekt de computer in een DNS-server naar het overeenkomende IP-adres. Het laatste deel van het domein (zoals .com, .be, .nl, .org) staat bekend als een *Top Level Domain (TLD)* en wordt beheerd door een centrale autoriteit zoals ICANN[98]. ICANN beheert eigenlijk zelf geen domeinnamen. Daarvoor doet het dan weer een beroep op TLD-operators of registrars, zoals DNS Belgium. Registrars kunnen het beste vergeleken worden met een telefooncentrale: zij schakelen binnenkomende oproepen voor een domeinnaam door naar de juiste *name servers* (DNS Belgium, 2018).



Figuur 8: 'standaard' DNS (bron: https://blockchain-dns.info/)

Blockchain DNS werkt anders, want dat is een gedecentraliseerde DNS. Blockchain-TLD's (zoals .bazar, .bit, .coin, .emc, .eth, .lib en .neo)[99] worden namelijk niet beheerd door een

[98] ICANN (Internet Corporation for Assigned Names and Numbers) is een onafhankelijke non-profit niet-gouvernementele organisatie die met behulp van een 'multistakeholder'-model beleid maakt en die een aantal internet-gerelateerde beslissingen neemt over het technisch beheer van het internet, zoals het toekennen en specifiëren van topleveldomeinen, toewijzen van domeinnamen en de distributie van IP-nummers. Zij is de internationale autoriteit op het gebied van domeinnaambeheer (DNS Belgium, 2018).

[99] Voorbeelden zijn:
- Namecoin Dot-Bit: (https://bit.namecoin.org/);
- EmerDNS: (https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction);
- Ethereum Name Service: (https://ens.domains/);
- Neo Name Service: (https://neons.name/index_En.html).

centrale autoriteit[100]. Dit is ook gelijk het grootste verschil tussen een 'standaard' DNS en blockchain DNS. Bij een gewone DNS kan een overheid *internet service providers* verplichten om bepaalde domeinnamen niet meer naar het bijbehorende IP-adres door te sturen (offline halen) (Amado, 2018). Bij blockchain DNS moet een meerderheid van de gebruikers hiervoor toestemming geven (consensus). De belangrijkste voordelen van een gedecentraliseerde DNS-aanpak zijn veiligheid, censuurbestendigheid en privacy (Casino et al., 2019).

Inmiddels wordt deze technologie ook ingezet door criminelen. Criminele sites zoals Joker's Stash (http://jstassh.bazar/)[101], een populaire Automated Vending Cart (AVC)-site[102] die wordt gebruikt om gestolen creditcardgegevens te kopen, gebruiken blockchain 'hosting'. Gebruikers die toegang willen krijgen tot de .bazar-versie van de site, moeten een blockchain DNS-browserextensie of add-on installeren (Holland et al., 2018). Joker's Stash is niet de eerste die experimenteerde met gedecentraliseerde DNS. Ook andere sites die worden gebruikt om gestolen gegevens te verhandelen, experimenteren met peer-to-peer DNS-technologie om criminele activiteiten te verbergen (Holland et al., 2018).

Een gevolg is dat onder meer WHOIS-databases niet meer kunnen worden geraadpleegd door wetshandhavingsinstanties. WHOIS-databases zijn bijzonder waardevol om internetcriminelen te strikken (van Loon, 2018). Kwaadwillenden kunnen — al dan niet per ongeluk — echte of herleidbare informatie in hun DNS-registraties gebruiken. Mensen maken fouten, zelfs

[100] PeerName. (2019). Blockchain-based domain names. Retrieved from https://peername.com/

[101] Cimpanu, C. (2019). Credit card details worth nearly $3.5 million put up for sale on hacking forum. *ZDNet*. Retrieved from https://www.zdnet.com/article/credit-card-details-worth-nearly-3-5-million-put-up-for-sale-on-hacking-forum/

[102] Hoewel het heel goed mogelijk is dat cybercriminelen gestolen creditcardgegevens zelf voor frauduleuze doeleinden gebruiken, komt het vaker voor dat ze de verkregen informatie aan een distributeur verkopen. Automated Vending Carts (AVC's) zijn webwinkels die een cruciale rol spelen bij de verkoop van gestolen creditcardgegevens. Ze kopen grote partijen creditcardgegevens in en verkopen die mondjesmaat aan iedereen die creditcardfraude wil plegen. AVC's in de Verenigde Staten zijn met afstand het populairst (FinanceInnovation, 2018).

cybercriminelen (van Loon, 2018). De internationale internetorganisatie publiceert informatie over registratie van domeinnamen. Met het WHOIS-protocol wordt de informatie achter een domein publiekelijk inzichtelijk gemaakt (Löwik, 2018). Gebruikers kunnen zo inzage krijgen in de persoon of organisatie achter een website, inclusief contact- en registratiegegevens (Löwik, 2018). Hierdoor zijn naamregistreerders, maar ook beheerders en eigenaren van internetsites te traceren. Dit geldt ook voor domeinnamen die dienstdoen voor malafide doeleinden. WHOIS-gegevens zijn dus bijzonder waardevol om criminelen zelf op te sporen (van Loon, 2018).

Aangezien blockchaindomeinen geen centrale autoriteit hebben en registraties unieke gecodeerde *hashes* bevatten in plaats van de naam en het adres van een individu, is het voor wetshandhavingsinstanties bijzonder moeilijk om internetcriminelen te identificeren en deze websites te verwijderen[103] (Holland et al., 2018).

2.2.3 Cryptocurrencies

De blockchaintechnologie is een techniek die in potentie eindeloze toepassingen kent. De best gekende is momenteel Bitcoin, een cryptocurrency. Het is een innovatief betalingsnetwerk en een nieuw soort geld (Gandal & Halaburda, 2014). Het is een manier om, op een betrouwbare manier, wereldwijde elektronische betalingen te organiseren tussen twee partijen, zonder tussenkomst of mogelijke manipulaties van derden.

Deze munteenheid wordt online en digitaal gebruikt, vaak als een alternatief geldsysteem. Bitcoin is op dit moment de best gekende digitale munteenheid maar daarnaast worden constant

[103] Computer Business Review. (2018). Rise in malicious infrastructure hosted on blockchain identified. Retrieved from https://www.cbronline.com/news/malicious-infrastructure-blockchain

nieuwe virtuele munten (ook "altcoin"[104] genoemd) ontwikkeld op basis van het protocol van Satoshi Nakamoto[105] zoals Monero, Ethereum, Zcash en noem maar op[106]. Vrijwel alle gedecentraliseerde valuta zijn min of meer afgeleid van Bitcoin (Cointelegraph, 2018). De betrouwbaarheid van de digitale munt wordt gegarandeerd door een ingenieus cryptografisch systeem (vandaar ook de naam "cryptocurrency").

Aangezien Bitcoin wordt beschouwd als geld heeft het waarde (Bolt, 2018b). Tegenwoordig wordt de prijs bepaald door de waarde die handelaren toekennen aan Bitcoins, door middel van vraag en aanbod op wisselmarkten (cryptocurrency exchanges)[107] en het vertrouwen dat er in de munteenheid bestaat (Bolt, 2018b). Om waarde te verkrijgen steunt Bitcoin op de principes van schaarsheid[108] en cryptografie.

Uit het onderzoek van Janssens, Soetaert en De Vos (2017) blijkt dat ten gevolge van de groeiende populariteit en waarde van cryptocurrencies, ook de interesse bij criminelen groeide om deze te stelen en te gebruiken. In het bijzonder ook het gedecentraliseerd karakter van de virtuele munt dat gebruikers grotere anonimiteit bezorgt door een combinatie van cryptografie met een peer-to-peer architectuur, maakte dat het anonieme Bitcoin-betaalnetwerk een toevluchtsoord werd voor witwassers, hackers, drugdealers en andere criminelen (Janssens et

[104] Altcoin is een afkorting van "Bitcoin Alternative". In dit opzicht beschrijft de term altcoin elke afzonderlijke cryptocurrency die geen Bitcoin is.
[105] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
[106] Een recent overzicht van alle virtuele valuta is te vinden op https://coinmarketcap.com/all/views/all/.
[107] Een cryptocurrency exchange is een website die kan vergeleken worden met een wisselkantoor waarbij 'echt' geld (fiatgeld) kan omgezet worden naar Bitcoins, en omgekeerd. Wanneer je via een exchanger geld omzet naar Bitcoins zal daar een kleine transactiekost aan verbonden worden. Het is onder meer door deze transactiekosten dat exchangers inkomsten verwerven.
[108] Er is geen centrale organisatie achter Bitcoin. De uitgifte (creatie) van nieuwe Bitcoins gebeurt via het mining-proces. Ook het minen gebeurt niet door een centrale organisatie, maar door groepen van miners die specifieke mining-software gebruiken. Er is een gelimiteerde omvang Bitcoins die op geregelde (vastgelegde) tijdstippen — via het mining-proces — wordt vermeerderd. Het Bitcoin-netwerk is zo ingesteld dat er per jaar nooit meer dan een vastgestelde hoeveelheid Bitcoins kan worden aangemaakt. Er kan dus niet zomaar geld worden bijgedrukt, wat maakt dat de geldhoeveelheid niet aan artificiële (kunstmatige) inflatie gevoelig is. Bovendien worden 'slechts' maximaal 21 miljoen Bitcoins in omloop gebracht (Vitse, 2016).

al., 2017). Het is tevens de enige munt die op de meeste darknetmarkten wordt geaccepteerd (Europol, 2017b).

Omdat er (momenteel) nog geen centrale registratiedienst is, betekent dit dat er geen mechanisme[109] is om een Bitcoin-adres[110] aan een echte persoon te koppelen. In de strijd tegen terrorisme en witwaspraktijken werden de Europese Richtlijnen in verband met witwassen (*Anti-money Laundering* – AML)[111] in Juni 2018 daartoe uitgebreid. Het centrale register met gegevens van bankrekeninghouders (CAP bij de Nationale Bank van België), dat de identificatie bevat van natuurlijke of rechtspersonen die houder zijn van of zeggenschap hebben over betaalrekeningen en bankrekeningen die worden aangehouden door een kredietinstelling in België, wordt met de AML5 richtlijn ook verplicht voor cryptocurrencies. De entiteiten die aan de richtlijn zijn onderworpen (en dus gegevens ter beschikking dienen te stellen) zijn: (1) aanbieders die zich bezighouden met diensten voor het wisselen tussen virtuele valuta en fiat valuta (cryptocurrency exchanges) en (2) aanbieders van bewaarportemonnees[112]. Er komt dus ook een registratieplicht voor aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta en aanbieders van bewaarportemonnees.

[109] Er is geen centrale controle of ingebouwd Customer Due Diligence: ook wel bekend als het 'know your customer (KYC)'- of 'ken uw klant'-beginsel. Wie is uw cliënt? Kan de cliënt een bedreiging vormen? Een goed CDD-beleid biedt een instelling meer dan alleen een integere bedrijfsvoering. Het kan ook twee specifieke integriteitsrisico's bestrijden: financiering van terrorisme en witwassen. Met de antiwitwaswetgeving van 18 januari 2010 zijn bepaalde ondernemingen verplicht om vooraf specifieke acties te ondernemen alvorens een klantenrelatie aan te gegaan. Het gaat onder andere om banken, verzekeringsmaatschappijen, wisselinstellingen, etc. De ondernemingen dienen in eerste instantie vooraf een klantenonderzoek te doen via een identiteitsidentificatie én – verificatie. Vervolgens moeten zij de zakelijke transactie onder de loupe nemen. En tot slot dienen ze de identiteit na te gaan van de begunstigde. Met andere woorden: voor wiens rekening wordt deze transactie uitgevoerd?

[110] Het sturen en ontvangen van cryptobetalingen wordt geregeld door beveiligingssleutels. De private key is nodig om geld te versturen en de public key (Bitcoin-adres) om geld te ontvangen. Met andere woorden, betalingen worden verstuurd naar een Bitcoin-adres (net zoals een bankrekeningnummer) en ondertekend met de private sleutel (een handtekening) (Vrolix, 2017).

[111] Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, (2018).

[112] "aanbieder van een bewaarportemonnee": een entiteit die diensten aanbiedt om namens haar cliënten cryptografische privésleutels te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen.

Helaas voor de wetshandhavingsdiensten is er internationaal een grote vraag naar een anoniem muntsysteem om zowel legale als illegale transacties te vergemakkelijken (Diţu, 2017). In haar *Internet Organised Crime Threat Assessment (IOCTA)* van 2017 stelt Europol dat de Bitcoin het betaalmiddel blijft voor (cyber)criminelen[113] (Europol, 2017b).

Bovendien blijkt dat heel wat politiemensen binnen bepaalde afdelingen van de federale politie niet in staat zijn om Bitcoin-onderzoek te voeren omdat zij hier de kennis niet over hebben (Soetaert et al., 2017). De materie is zo complex dat onderzoekers uit andere teams vaak niet op de hoogte zijn van de werking van Bitcoins en bovendien ook niet weten hoe dit onderzocht dient te worden. Dit zorgt ervoor dat er mogelijks heel wat Bitcoins, die bijvoorbeeld bij huiszoekingen aanwezig zijn, niet worden opgemerkt (Soetaert et al., 2017).

Ten slotte is er vandaag de dag nog steeds een gebrek aan duidelijke wettelijke definiëring omtrent cryptocurrencies (Ducas & Wilner, 2017). Virtueel geld heeft wettelijk gezien geen waarde. Het wordt slechts aanvaard als betaalmiddel binnen een bepaalde (virtuele) gemeenschap. Het verschil tussen elektronisch en virtueel geld heeft juridisch gezien grote gevolgen. Elektronisch geld wordt immers gereguleerd en mag enkel uitgegeven worden door daartoe vergunde financiële instellingen, terwijl virtueel geld niet gereguleerd is en de uitgevers ervan dan ook niet gezien kunnen worden als financiële instellingen (Vitse, 2016). Volgens de Europese Centrale Bank (ECB) zijn Bitcoins virtueel geld en vallen ze dus niet onder de Europese 'Elektronisch geld' -richtlijn (2009/110/EG).

[113] Di Salvo, M. (2019). Bitcoin use on darknet markets doubled in 2018. Retrieved from https://news.bitcoin.com/report-bitcoin-use-on-darknet-markets-doubled-in-2018/

Cryptocurrencies zijn revolutionair. Helaas is de wetgevende macht dit niet. Noch de nationale, noch de Europese, noch de internationale wetgever durven zich tot nog toe te wagen aan het creëren van een wetgevend kader (Jubel, 2017). De wisselkantoren (cryptocurrency exchangers) kunnen misschien wel gereguleerd worden, aangezien zij betrokken zijn bij het omruilen van cryptocurrencies naar fiatgeld en omgekeerd. Nochtans kopen of verkopen de wisselkantoren zelf geen cryptocurrencies. Zij maken het alleen mogelijk om cryptocurrencies te kopen van en te verkopen aan andere gebruikers (Vitse, 2016).

2.2.3.1 Privacy-focused cryptocurrencies

Aan de andere kant verkiezen criminelen ook vaker cryptomunten die minder 'traceerbaar'[114] zijn en transacties doelgericht verborgen houden, zoals Monero[115] (McGuire, 2018). Omdat speurders vaker gebruik maken van gespecialiseerde software om mensen die in Bitcoin verhandelen, te identificeren (Europol, 2016). Private bedrijven zoals Chainalysis, die nauw samenwerken met wetshandhavingsinstanties[116], slagen er steeds meer in om de Bitcoin te linken met criminele activiteiten zoals witwassen.

Anoniem of niet, het feit dat criminelen op een bepaald moment 'echt' fiatgeld moeten overmaken naar crypto-valuta en crypto-valuta terug naar fiatgeld betekent dat met de juiste

[114] Bitcoin maakt gebruik van een openbaar grootboek. Normaal gesproken heeft iedere bank een apart grootboek. In dit grootboek worden alle rekeninghouders, saldi en transacties geregistreerd. Die grootboeken moeten onderling met elkaar communiceren. Daarbij moeten banken elkaar vertrouwen en zijn veel complexe IT-systemen nodig. Bij Bitcoin heeft iedereen hetzelfde gemeenschappelijke grootboek en kan iedereen een kopie van datzelfde grootboek hebben. Dit grootboek is de basis van Bitcoin (=de blockchain). Alle transacties van over de hele wereld staan in het grootboek en het is volledig openbaar. Via bijvoorbeeld een site als https://blockexplorer.com/ kun je alle transacties bekijken. Het is bijgevolg mogelijk om transacties van publieke sleutel naar publieke sleutel te volgen. De enige informatie die een Bitcoin-gebruiker identificeert is met andere woorden een Bitcoin-adres (Tamminga, 2014).

[115] Monero (XMR) is een open source cryptocurrency die werd gecreëerd in april 2014 en gericht is op privacy en decentralisatie (privacy-focused cryptocurrencies). Monero gebruikt onder meer "ring signatures" en "stealth adresses" als privacyverhogende maatregelen (The Monero Project, 2018).

[116] Europol. (2016). Europol and Chainalysis reinforce their cooperation in the fight against cybercrime. Retrieved from https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime

software voor transactiecontrole, de wetshandhavingsautoriteiten het financiële gedrag van criminelen kunnen de-anonimiseren. Door zich te concentreren op de blockchain transacties die 'zichtbaar' zijn en door bij te houden waar het geld naartoe gaat (het 'volgen van het geld': *follow the money*[117]) als het van een cryptocurrency exchange komt, kunnen ze potentieel abnormale en verdachte financiële stromen ontdekken en die informatie gebruiken om bredere onderzoeken naar mogelijke daders te helpen richten (The Police Foundation, 2018).

Dit maakt alternatieven ("altcoins") aantrekkelijker. Bepaalde altcoins (bijvoorbeeld Monero) bieden een nog grotere anonimiteit dan Bitcoin. De handel in Bitcoins maakt gebruik van de Bitcoin-blockchain, waardoor dus van alle transacties – het exacte tijdstip en bedrag –, zender én ontvanger 'gekend' zijn (KV, 2018). Dat is allesbehalve geruststellend voor criminelen.

Monero (XMR) is niet te traceren. Zowel het verzenden en ontvangen van adressen als de verwerkte bedragen zijn standaard versluierd. Transacties op de Monero-blockchain kunnen niet worden gekoppeld aan een bepaalde gebruiker of identiteit uit de echte wereld. Monero is een van de vele op privacy gerichte munten (privacy-focused cryptocurrencies) (Mahmoud, Lescisin, & AlTaei, 2019). Als Bitcoin als *http* voor geld is, is Monero de *https* variant daarvan (The Monero Project, 2018).

[117] Een uitdrukking die weergeeft dat gebeurtenissen vaak te verklaren zijn door de geldstromen, het geldspoor te volgen en te kijken welke partijen ervan profiteren c.q. betalingen hebben verricht.

2.2.4 Conclusie

De blockchaintechnologie biedt tal van nieuwe criminele mogelijkheden. In dit hoofdstuk werden enkele van de belangrijkste bedreigingen van blockchain aangehaald. Een daarvan is gedecentraliseerde en geëncrypteerde communicatie waardoor het onderscheppen en ontsleutelen van versleutelde communicatie tussen criminelen, door de inbeslagname van servers waarlangs versleutelde communicatie verloopt, bemoeilijkt wordt.

Daarnaast maakt blockchain het mogelijk om volledig gedistribueerde en gedecentraliseerde cryptomarkten te ontwikkelen die het moeilijker maken om dergelijke markten van het internet te weren. Het is een taak voor criminologen om verder onderzoek te doen naar cryptomarkten en licht te werpen op de nieuwe varianten hiervan. Verder kunnen criminelen gebruik maken van een zogenaamde blockchain DNS waardoor het voor wetshandhavingsinstanties moeilijker wordt om (malafide) websites te verwijderen van het internet.

Tot slot blijkt ook het gebruik van cryptocurrencies een zorgwekkend fenomeen te zijn. Meer bepaald de privacy-focused cryptocurrencies ("privacy coins") die minder traceerbaar zijn en transacties doelgericht verborgen houden.

2.3 Blockchain: Use Cases binnen de geïntegreerde politie (kansen)

2.3.1 Inleiding

De jaarlijkse toename van innovatieve vormen van high-tech crime is zorgwekkend (Europol, 2018). Erger nog is het feit dat misdaadorganisaties al wel (grootschalig) gebruikmaken van technologieën als blockchain (cfr. 2.2) en daarmee een voorsprong hebben op de politie en opsporingsdiensten (Europol, 2017b). Want ook voor hen kan blockchain een oplossing bieden. Enerzijds transparante en veilige informatie – blockchain geeft geen ruimte voor manipulatie en vervalsing – en anderzijds gedistribueerde informatie zijn de twee elementen die blockchaintechnologie zo interessant maken (Ministerie van Justitie en Veiligheid, 2018).

Blockchain maakt gebruik van encryptie en *hashing* om onveranderlijke records op te slaan en veel van de bestaande cyberbeveiligingsoplossingen maken ook gebruik van zeer vergelijkbare technologie. Het merendeel van de bestaande beveiligingsmaatregelen is echter afhankelijk van één vertrouwde autoriteit om informatie te verifiëren of gecodeerde gegevens op te slaan. Dit maakt het systeem vatbaar voor cyberaanvallen; veel hackers kunnen hun inspanningen richten op één enkel doelwit om cyberaanvallen te plegen (Taylor, Dargahi, Dehghantanha, Parizi, & Choo, 2019). Zeker één keer per week krijgt een federale overheidsdienst in België een doelgerichte cyberaanval te verduren (Bové, 2018). De beveiliging laat dus nog te wensen over. Geen enkele technologie is 100% veilig, maar tot nu toe is nog niemand er in geslaagd de encryptie van de blockchain te compromitteren (R. Butcher, Cohn, & J.W. Rennock, 2018). Met de aanstaande verspreiding van *Quantum Computing* verhoogt het risico dat *digital signatures* toch gekraakt kunnen worden (K. Fedorov, O. Kiktenko, & I. Lvovsky, 2018).

Hoewel de blockchaintechnologie duidelijk nog in de kinderschoenen staat, zou het gebruik ervan binnen wetshandhavingsinstanties aanzienlijke voordelen kunnen opleveren (The Police Foundation, 2017). In dit hoofdstuk wordt gekeken of de aspecten van blockchaintechnologie mogelijkheden kunnen bieden binnen de geïntegreerde politie om de eerder besproken barrières en hinderpalen bij het digitaal forensisch onderzoek (cfr. 1.1.3) en de (werk)processen ervan te verbeteren.

2.3.2 Toepassingsmogelijkheden van blockchain binnen de geïntegreerde politie

Een van de meest gehoorde kritieken op het gebied van de blockchain is dat een groot aantal blockchaintoepassingen al kunnen worden geïmplementeerd met behulp van bestaande technologieën, zoals (goed beveiligde) gecentraliseerde databases (Gatteschi, Lamberti, Demartini, Pranteda, & Santamaria, 2018). **Beslissingen over de implementatie van blockchaintoepassingen moeten dus zorgvuldig worden overwogen** en geanalyseerd voordat ze worden geïmplementeerd (J. Bambara et al., 2018).

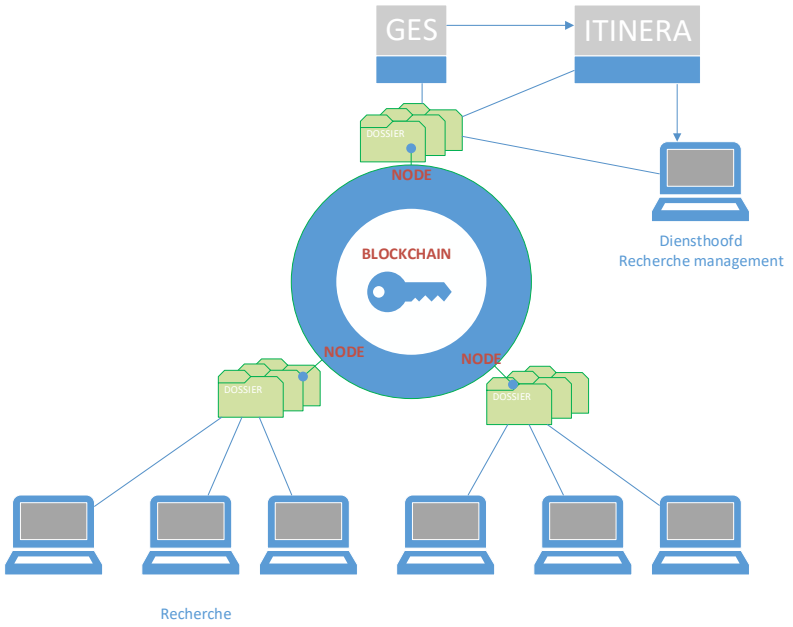
2.3.2.1 Kennisbeheer

Het Comité P wijst op de dringende noodzaak aan een instrument voor het delen van kennis, goede praktijken en ervaringen (Comité P, 2018a). Kan blockchain hier een oplossing bieden? Neen. Een traditionele benadering met een centraal systeem waar documenten kunnen geraadpleegd en opgeslagen worden, is hiervoor beter geschikt. Documenten delen in de blockchain loopt al snel tegen de eerder beschreven nadelen. De blockchain wordt enorm groot en het zoeken naar informatie binnen de *Chain* is een uitdaging (en dat is toch een kritische voorwaarde wanneer men kennis of ervaringen wil delen). Voor deze *Use Case* is geen nood aan het bijhouden van iedere verandering en er is ook geen transactie van een *asset* die moet

worden bewaakt. Het *'single point of failure*' speelt weinig rol. Gebruikelijke *backups* van documenten en database zijn ruim voldoende. Afscherming en toegang van documenten heeft geen vereisten die huidige systemen niet zouden bieden. Men kan hier eerder opteren voor het uitrollen van een *e-learning* platform, een *Learning Management System* (LMS). Er zijn vele, gratis, open source oplossingen beschikbaar die snel en tegen lage kost kunnen worden geïnstalleerd. Men kan op een gestructureerde manier trainingen (kennis/ervaring) aanbieden en, indien gewenst, leerpaden, testen, online trainingen et cetera organiseren. Bij de Politie Opleiding Oost-Vlaanderen (PAULO) maakt men reeds gebruik van dergelijk elektronisch leerplatform, met name Chamilo[118], gehost bij Arteveldehogeschool[119].

2.3.2.2 Dossierbeheersysteem

Het Comité P beveelt aan dat er in het kader van de geïntegreerde CCU-werking op zeer korte termijn een eenvormig en dynamisch dossierbeheersysteem wordt ingevoerd. Een blockchain oplossing kan hier een meerwaarde bieden.



Figuur 9: eenvormig en dynamisch dossierbeheersysteem

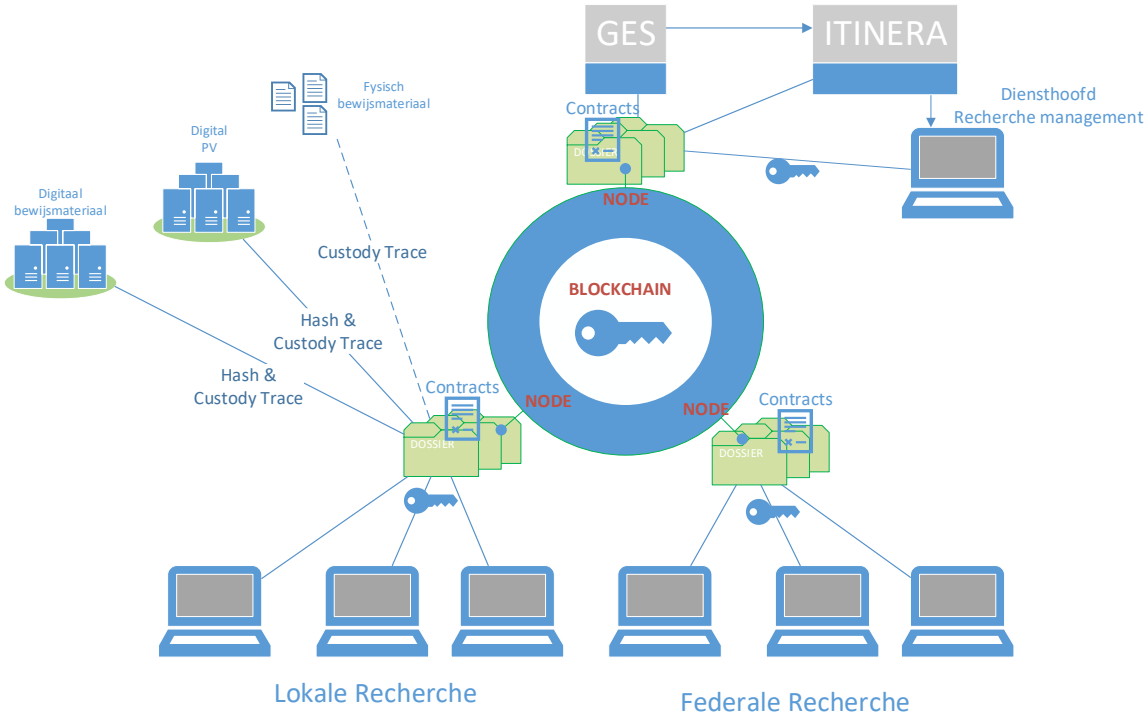
[118] Chamilo. (2019). Simplify e-learning with Chamilo LMS. Retrieved from https://chamilo.org/en/
[119] PAULO-Politieopleiding. (2019). Leerplatform PAULO-Politieopleiding. Retrieved from https://opac.hogent.be/

Dossiers worden aangemaakt in een blockchain. Het blockchain dossier is de unieke verzameling van alle dossierstukken. Het bevat gegevens, maar kan ook verwijzen naar data die in huidige GES of ITINERA zijn opgeslagen. Er dient tijdens het ontwerp bepaald te worden in hoeverre data uit GES/ITINERA verplaatst worden naar de blockchain. Verplaatsen betekent dat de blockchain, de beheerder (=bron van waarheid) wordt van die data. Indien GES/ITINERA dezelfde data nodig hebben, dan kopiëren ze die van de blockchain in hun eigen database. Managementbeslissingen (bijvoorbeeld prioriteitsstelling) komen in de blockchain, zodat ze onmiddellijk voor iedereen zichtbaar worden. Analyses moeten uitwijzen waar data best thuishoren: in de blockchain of in GES/ITINERA (=off-chain, met een verwijzing vanuit de blockchain naar die data). Het dossier is dynamisch en alle wijzigingen worden als transacties opgeslagen in de blockchain. De hele geschiedenis van het dossier is transparant. Vanuit management oogpunt is het verloop en de progressie van een dossier gemakkelijk op te volgen.

2.3.2.3 Data exploitatie

Er is nood aan een centraal systeem waarop de tactische onderzoeker, zowel van de federale gerechtelijke politie als van de lokale recherche, data verder kan exploiteren die na extractie van het forensisch benaderde ICT-materiaal ter beschikking zijn gesteld. Daaraan zou een systeem kunnen gekoppeld worden voor de digitale neerlegging van de data op de griffies (Comité P, 2018a).

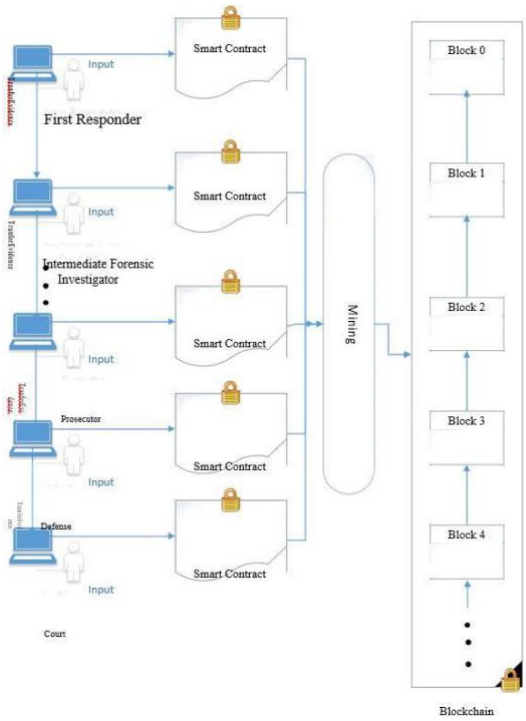
Om dit te verwezenlijken kan verder gebouwd worden op de hierboven beschreven oplossing voor het dossierbeheersysteem.



Figuur 10.1: data exploitatie

Alle betrokken recherche eenheden kunnen aansluiten op de blockchain en zo toegang krijgen tot het bewijsmateriaal van een dossier, via dApps. In de huidige digitale wereld, met een snelle toename van cybercriminaliteit, neemt het belang van digitaal bewijsmateriaal toe. Digitaal bewijsmateriaal speelt een belangrijke rol in de opsporing van high-tech crime, omdat het wordt gebruikt om personen in verband te brengen met criminele activiteiten (Lone & Mir, 2017). Het meeste digitaal bewijsmateriaal zal niet in de blockchain zelf worden opgeslagen, maar in andere off-chain (bestaande) systemen. Op de blockchain worden *hashes* (digitale vingerafdrukken) van de off-chain digitale data opgenomen. Via dApps kan gelinkte data uit bronsystemen worden opgehaald en gecheckt tegenover de in de blockchain opgeslagen hash (*checksum*), om de authenticiteit en integriteit van het elektronisch materiaal te verifiëren. Het is duidelijk dat de blockchaintechnologie kan worden gebruikt om de integriteit van bestanden te bewaken, wat een van de belangrijkste taken van informatiebeveiliging is (Zikratov, Kuzmin, Akimenko, Niculichev, & Yalansky, 2017).

De blockchain is van nature zeer geschikt voor het ondersteunen van het "proces van bewijsvoering". ‘Chain of custody’ kan worden gedefinieerd als een proces dat wordt gebruikt voor het bijhouden en documenteren van de chronologische geschiedenis van de omgang met bewijsmateriaal (Lone & Mir, 2017). De registratie van bewijsmateriaal, de persoon die verantwoordelijk is geweest voor het materiaal en de handelingen die met het materiaal zijn uitgevoerd, zijn van essentieel belang om de integriteit van het materiaal te kunnen aantonen (Forensicon, 2019). Het kan zowel om fysisch als digitaal bewijsmateriaal gaan. Elke eigendomsoverdracht wordt beschreven door transactiegegevens die duidelijk aangeven welke eigenaar het eigenaarschap van welk item overhandigt aan wie op welk moment. De hele geschiedenis van transactiegegevens die in een grootboek zijn opgeslagen, wordt een controlespoor (audit trail) dat weergeeft hoe iedereen aan zijn of haar bezit gekomen is (Drescher, 2017). Smart contracts kunnen het correcte verloop van de procedures mee helpen ondersteunen.



Figuur 10.2: Forensic-chain, een Ethereum-gebaseerde blockchain voor digitaal bewijsmateriaal (Bron[*])

[*] Lone, A. H., & Mir, R. N. (2017). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Scientific and Practical Cyber Security Journal*. Retrieved from https://journal.scsa.ge/papers/forensic-chain-ethereum-blockchain-based-digital-forensics-chain-of-custody/.

Smart contracts kunnen ondersteunen om het dossier door de keten te leiden. Bijvoorbeeld, wanneer alle vastgelegde voorwaarden voor neerlegging bij de griffie zijn vervuld, kan het dossier 'zichtbaar' gemaakt worden voor de griffie. Of, indien de griffie zich niet op de blockchain zou bevinden, een automatische neerlegging via een ander raakvlak met de griffie. Het is eenduidig welke stukken zich in het dossier bevinden. De bewijsstukken in het dossier zijn door de hash in de blockchain indirect beveiligd tegen manipulaties. De bron databases blijven een 'centraal, single point' en kwetsbaar voor hacking, maar de blockchain zal data manipulaties snel detecteren, waarna de nodige herstelmaatregelen in gang kunnen worden gezet. Dit is geen overbodige luxe. Volgens een artikel in De Tijd krijgt een federale overheidsdienst zeker één keer per week een doelgerichte cyberaanval te verduren[120]. Vermits in cybercrime bewijsstukken dikwijls digitaal zijn en onderzoeksinformatie digitaal worden opgeslagen, is het niet denkbeeldig dat beschuldigden zullen pogen om gegevens (al dan niet subtiel) aan te passen om zo de rechtsgang te beïnvloeden. Zeker bij de steeds verdere digitalisering, waarbij fysieke documenten worden vervangen door digitale dossiers, is het cruciaal dat integriteit wordt bewaakt. In Nederland is reeds geëxperimenteerd met bovenbeschreven scenario, voor een eenvoudige strafrechtketen[121]. Het concept dat is opgesteld, lijkt na de eerste sessie zeker haalbaar en kan een toevoeging leveren op het huidige systeem. Er zijn mogelijkheden, mits alle ketenpartners (politie, justitie, OM, rechtbank, advocaten) bereid zijn hun systemen (afgeschermd) te koppelen aan de blockchain (Ministerie van Justitie en Veiligheid, 2018).

[120] Bové, L. (2018). Elke week cyberaanval op federale overheidsdienst. *De Tijd*. Retrieved from https://www.tijd.be/politiek-economie/belgie/federaal/elke-week-cyberaanval-op-federale-overheidsdienst/10043950.html

[121] Guardtime. (2018). Dutch government deploys guardtime's KSI blockchain for integrity assurance. Retrieved from https://guardtime.com/blog/dutch-government-deploys-guardtime-s-ksi-blockchain-for-integrity-assurance

Het Chinese ministerie van Openbare Veiligheid heeft een blockchainsysteem ontwikkeld dat erop gericht is om de bewijzen die tijdens politieonderzoeken zijn verzameld, veiliger op te slaan. Volgens gegevens vrijgegeven door het Chinese Bureau voor de Intellectuele Eigendom, heeft de afdeling Onderzoek van het ministerie een octrooiaanvraag ingediend in november 2017 voor een blockchain-gebaseerd systeem dat gegevens die in de *cloud* worden toegevoegd opslaat en tijdstempelt in een poging om een meer transparante en fraudebestendige depositie procedure te bieden (Zhao, 2018).

2.3.2.4 Informatiehuishouding

Het bestaan van verschillende systemen die worden beheerd door verschillende diensten, dikwijls historisch gegroeid, kan een obstakel vormen voor een geïntegreerde informatiehuishouding en -uitwisseling. Voor deze problematiek kan de blockchain een oplossing zijn voor integratie. Zoals aan het begin van dit hoofdstuk beschreven, kunnen de meeste *Use Cases* voor blockchain ook worden opgelost met bestaande technologieën. Een veel gehanteerde oplossing is de creatie van Kruispuntbanken. Alle informatie, komend uit verschillende diensten/databanken wordt doorgeven naar een 'centrale' databank, waar alle betrokkenen toegang toe krijgen. Dit is technisch niet altijd eenvoudig[122]. Deze masterproef is geen ICT werk, we gaan niet in detail, maar mogelijke problemen zijn:

– integratie en communicatie tussen databanken kan complex zijn[123]. Soms is er zelfs geen directe digitale communicatie tussen bron- en kruispuntbank en

[122] Duizenden foutieve adressen in Kruispuntbank sinds gemeentefusies: “We roepen bedrijven op om eigen gegevens te controleren”. (2019). *Het Laatste Nieuws*. Retrieved from https://www.hln.be/nieuws/binnenland/duizenden-foutieve-adressen-in-kruispuntbank-sinds-gemeentefusies-we-roepen-bedrijven-op-om-eigen-gegevens-te-controleren~a486d743/

[123] Schadeclaim dreigt voor falende Kruispuntbank. (2003). *De Morgen*. Retrieved from https://www.demorgen.be/nieuws/schadeclaim-dreigt-voor-falende-kruispuntbank~b7ef9a16/

"Het opzet ging gepaard met een gigantische operatie van informatietechnologie, waarbij verschillende databanken op elkaar afgestemd moesten worden, met elkaar moesten kunnen communiceren en ook nog gemakkelijk toegankelijk moesten zijn."

voorloopt dit via andere raakvlakken (lijsten ter beschikking stellen aan derden die de gegevens inbrengen, manueel invoeren in Kruispuntbank, ...).

- data worden soms gekopieerd. De bronsystemen blijven de 'bron van waarheid' en Kruispuntbank werkt met een kopie. Wanneer gegevens niet goed doorstromen (om technische of andere redenen), dan zijn gegevens in de Kruispuntbank niet actueel.

Een blockchainoplossing zou deze problemen kunnen ondervangen.

- De blockchain kan gebruikt worden om gegevens tussen bestaande databanken op een eenvoudige en zekere manier – via een Node – te delen, mogelijks onder voorwaarden die via smart contracts worden afgedwongen. Geen onderlinge connecties tussen systemen.
- De blockchain wordt door de deelnemers gebruikt als enige, correcte bron voor data. Ofwel zitten de gegevens in de blockchain, of er is een referentie naar het bronsysteem en de blockchain bevat de hash/vingerafdruk van de data, om hun echtheid ('waarheid') te controleren.

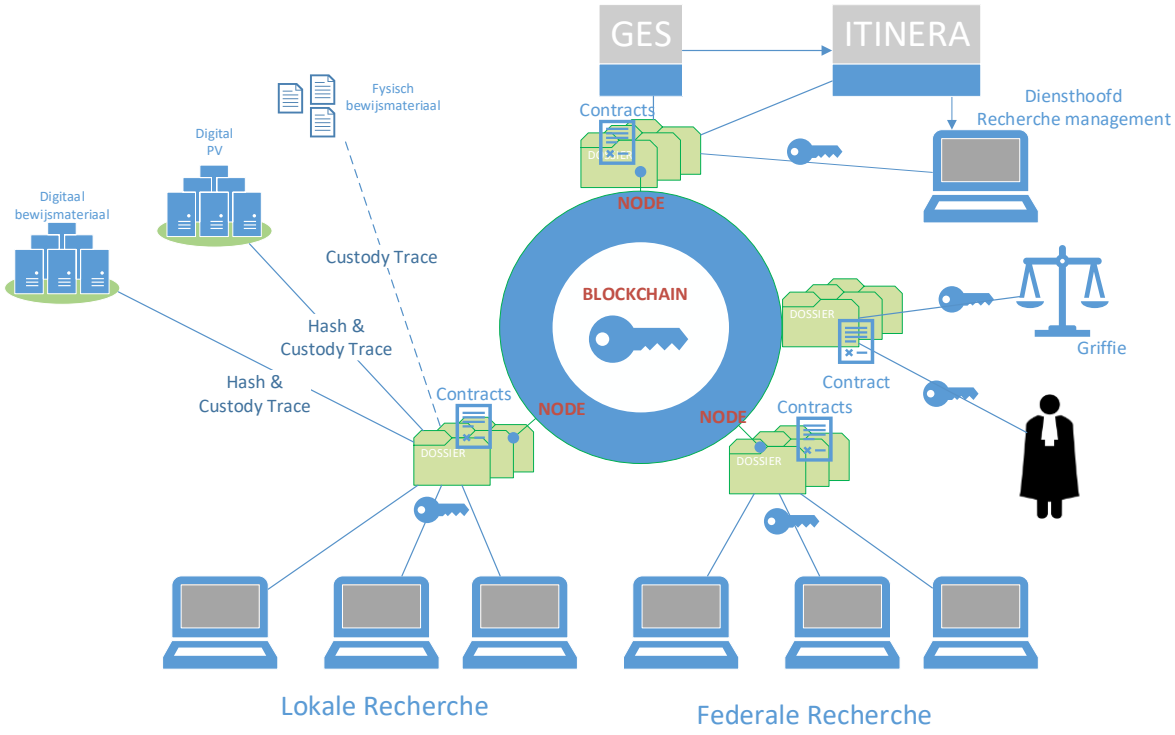
Door middel van een privaat-publieke (hybride) blockchain kunnen ook belanghebbenden buiten de overheid participeren. Via *private keys* en cryptografie kan informatie worden afgeschermd voor bepaalde partijen. Niet alle deelnemers kunnen informatie toevoegen (deelname in blockchain consensus, Proof-of-Authority). Nemen we het voorbeeld van de bestaande Kruispuntbank voor voertuigen[124]: er zijn zeven 'diensten die behoren tot het netwerk', waarvan er maar twee die ook effectief gegevens aanleveren: Renta en Informex. De anderen zijn bij de werking betrokken als intermediaire partner. Er zijn een 15-tal diensten die

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

in de praktijk zullen instaan voor het inzamelen en bijhouden van de gegevens. Al deze diensten hebben onbeperkt toegang tot de gegevens die zij zelf aanleveren. Voor een recht op toegang tot andere gegevens, is de toestemming nodig van de andere gegevensleverancier, en is een machtiging nodig van het Sectoraal Comité voor de Federale Overheid[125], dat bevoegd is voor de bescherming van de privacy. Sommige diensten stellen hun eigen databank open, zodat de Kruispuntbank een link kan leggen naar de gevraagde gegevens. Anderen – zoals de politie – zenden een selectie van hun gegevens door naar de beheersdienst, die de informatie voor hen bijhoudt. De Kruispuntbank voertuigen zou perfect vervangen kunnen worden door een blockchain.

Een blockchain faciliteert ook informatiedeling bij processen met een ketenbenadering. Door alle belanghebbenden bij de keten, bijvoorbeeld van een gerechtelijk onderzoek, aan te sluiten op de blockchain en zo toegang te geven tot alle gegevens van een dossier. Via een hybride blockchain kunnen met name advocaten en burgers, direct inzage krijgen in gegevens die op hun zaak betrekking hebben (transparantie). Alle betrokkenen hebben inzage in het originele dossier, geen onvolledige kopieën die bilateraal worden uitgewisseld. Alle partijen beschikken steeds over exact dezelfde informatie, wat noodzakelijk is voor een vlot en efficiënt proces. Vandaag is dit een gekend probleem, met heel wat wachttijden tot gevolg. Tenslotte automatiseren & beveiligen smart contracts de documentenstroom tussen de verschillende partijen, zodat bepaalde toegangsregels kunnen worden afgedwongen en nieuwe informatie zonder vertraging en op een veilige manier met de betrokken partijen wordt gedeeld (T-Mining, 2018).

[125] Het Sectoraal comité voor de Federale Overheid is binnen de Gegevensbeschermingsautoriteit opgericht bij de Wet van 8 december 1992. Deze wet beschermt de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Het Comité ziet toe op de elektronische mededeling van persoonsgegevens binnen de Federale Overheid (Gegevensbeschermingsautoriteit, 2019).



Figuur 11: informatiehuishouding

2.3.2.5 Alternatief voor centrale registers

Een blockchain kan ook gebruikt worden om de 'middleman' te vermijden. Als voorbeeld, het CAP[126] register dat wordt bijgehouden door de Nationale Bank van België, met informatie over alle in België geopende bankrekeningen (binnenkort – vanwege Europese AML5 Richtlijn – uitgebreid naar crypto-rekeningen) en ook buitenlandse rekeningen van natuurlijke personen. Initieel geconcipieerd als een louter fiscaal databestand, dat enkel toegankelijk was ten behoeve van de controlediensten inzake de inkomstenbelastingen. Nadien werd de machtiging om de informatie op te vragen, uitgebreid naar onder andere: het gerechtelijk apparaat; de Cel voor Financiële Informatieverwerking (CFI) in het kader van dossiers inzake het witwassen van geld, de financiering van terrorisme en de zware criminaliteit; notarissen; … De instellingen die gehouden zijn om de gegevens aan het CAP mee te delen zijn de bank-, wissel-, krediet-

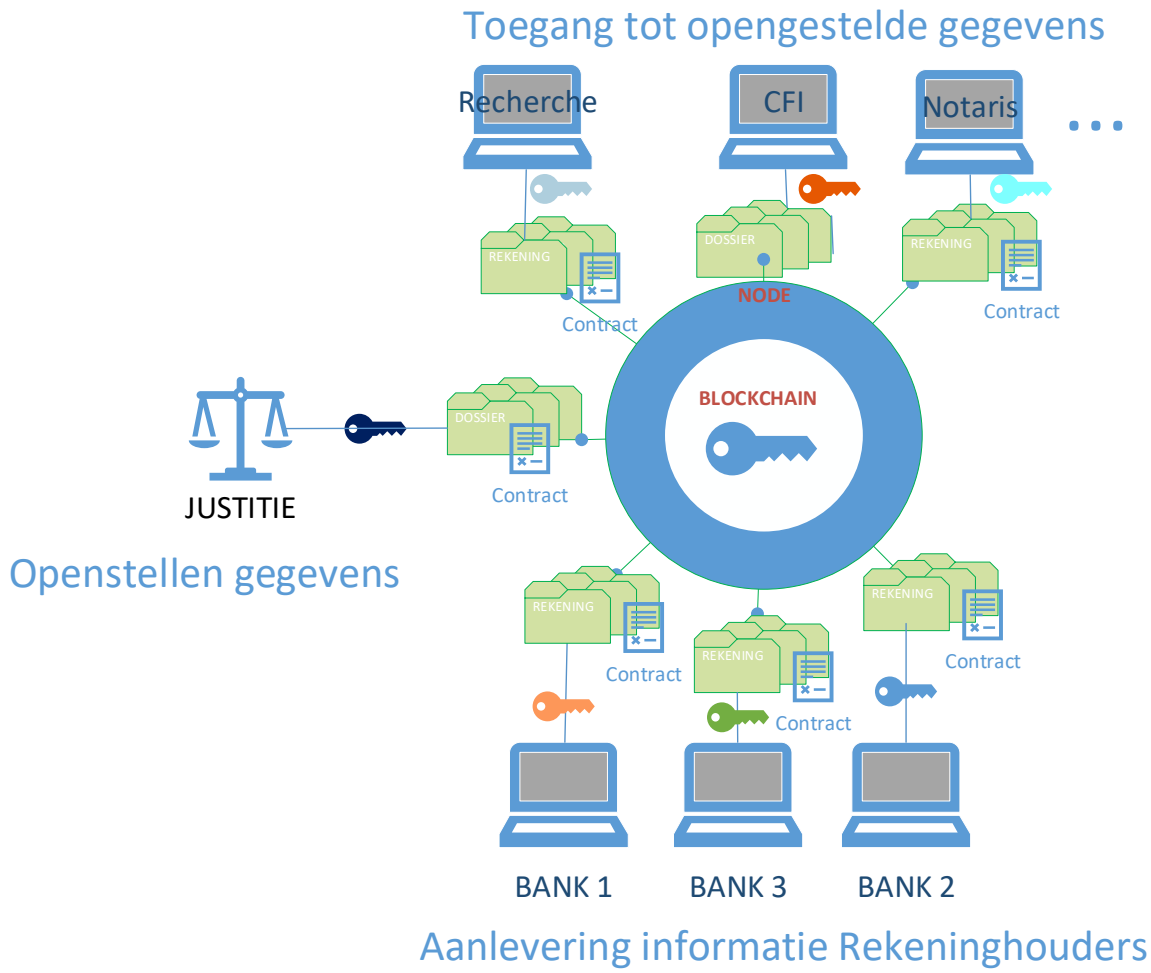
[126] Nationale Bank van België. (2019). Centraal aanspreekpunt (CAP). Retrieved from https://www.nbb.be/nl/kredietcentrales/centraal-aanspreekpunt

en spaarinstellingen gevestigd in België. Eén keer per jaar, ten laatste op 31 maart, delen de declaranten de identificatiegegevens van hun cliënten mee, alsook de nummers van hun bankrekeningen en de soorten contracten lopende tijdens het vorige jaar. De gegevens worden gedurende acht jaar bewaard (Nationale Bank van België, 2019).

Via blockchain zou dit register op een aantal manieren kunnen verbeterd worden:

- Het wegnemen van de 'middle man'. Door de vorming van een blockchain, met alle declaranten (banken, aanbieders cryptowallets, ...), CFI, Gerecht, notarissen, ... kan de Nationale Bank als verzamelpunt en beheerder van het register weggenomen worden.
- Veel betere performantie en snelheid. Nieuwe gegevens (bijvoorbeeld opening bankrekening door natuurlijke persoon) worden onmiddellijk bekend bij de CFI en het Gerecht. De huidige jaarlijkse aanpassing van het register, met gegevens van het voorbije jaar is voor doeleinden van onderzoek naar zware criminaliteit ontoereikend.
- Justitie, als deelnemer in de blockchain, kan toelatingen voor de recherche (om bankgegevens van iemand te raadplegen) rechtstreeks in de blockchain toevoegen en/of wegnemen.
- Traceerbaarheid van aanpassingen en raadplegingen. In de blockchain is zichtbaar wie toegang heeft gekregen tot de gegevens (transactie in de *chain*) en wanneer gegevens werden opgevraagd (smart contract). Het is duidelijk wanneer data door de bank werden toegevoegd of aangepast.

Het vereiste verwijderen van gegevens na 8 jaar stelt mogelijks een probleem (zie hogervermelde discussie in verband met persoonlijke data in een blockchain).



Figuur 12: alternatief voor centrale registers

2.3.3 Conclusie

De blockchain heeft waardevolle kenmerken, maar is niet per definitie de beste oplossing voor ieder probleem van informatiebeheer of vereenvoudiging van werkprocessen. Voor veel toepassingen werken reeds gekende technologieën beter. Het gebruik van zuiver publieke blockchains, waarbij iedere deelnemer gegevens kan toevoegen, en nieuwe data door consesus tussen niet vertrouwde partijen worden gevalideerd, is niet bruikbaar voor *Use Cases* binnen de geïntegreerde politie. Private- of hybride blockchains, waarbij enkel de daartoe geautoriseerde deelnemers de controle over de data behouden zijn wel van toepassing. De blockchain wordt dan vooral gebruikt voor efficiënte gegevensdeling, tussen vertrouwde en niet vertrouwde partijen, met garantie dat iedere partij dezelfde gegevens krijgt en nieuwe data snel doorstromen, en met de nodige afscherming. Blockchain is gericht op het opslaan van transacties (een historische neerslag van activiteiten, bijvoorbeeld het documenteren van de '*Chain of Custody*' van bewijsstukken), maar niet geschikt voor het gestructureerd opslaan van gegevens en het leggen van relaties tussen deze gegevens (=een relationele database). Werkprocessen waarbij data door verschillende partijen worden aangeleverd en door een centrale partij opgeslagen, kunnen door blockchain vereenvoudigd worden (alternatieven voor Kruispuntbanken). Het bewaren van digitale bewijsstukken in de blockchain is niet aangewezen, vanwege de omvang van de (te distribueren) database en het feit dat data nooit verwijderd kunnen worden. De blockchain kan wel gebruikt worden om de integriteit van *off-chain* opgeslagen digitale bewijsstukken te bewaken en manipulaties snel te ontdekken (door *hashes* van de bewijsstukken in de *chain* op te nemen en regelmatig te vergelijken met de bron data). De recherche dient bij onderzoeken ook gegevens te raadplegen die beheerd worden door externe partijen/overheidsinstellingen. Daar kan het interessant zijn om te streven naar een gemeenschappelijke blockchain, om efficiënter data uit te wisselen.

BESLUIT

Sedert het eerste gebruik van blockchain, als technische onderbouw van de Bitcoin munt, is een niet te stoppen verspreiding van deze technologie voor andere toepassingen in gang gezet. Zowel in de criminele als in niet-criminele sfeer. De politiediensten worden met beide aspecten geconfronteerd. Enerzijds het gebruik van blockchaintoepassingen door criminelen (eerst cryptomunten zoals Bitcoin, maar ondertussen ook andere), en anderzijds de vraag om het invoeren van blockchaintoepassingen voor efficiëntere werking en internationale gegevensuitwisseling.

Blockchain is vanuit ICT perspectief een moeilijke, wiskundige materie. Het gaat om cryptografie, data versleuteling, hashing, et cetera. Om opsporing te verrichten naar high-tech crime die van deze technologie gebruik maakt is, naast klassieke opsporing, ook zeer gespecialiseerde technische kennis nodig. De middelen om hierin expertise op te bouwen zijn voor de Belgische diensten beperkt. Het is daarom aangewezen om de beschikbare kennis optimaal in te zetten, door een goede organisatie en kennisdeling, en daarnaast te streven naar internationale samenwerking.

Voor het gebruik van blockchain, ter verbetering van interne werking en informatiedeling (nationaal en internationaal), is een ander – meer beschikbaar – niveau van technische kennis vereist. Er zijn talrijke open source implementaties van blockchain voorhanden, die kunnen worden aangewend om applicaties op te bouwen. Ook hier kan het nuttig zijn om internationale samenwerking te zoeken. Kijken we naar Estland[127], een voorloper in internet technologie en e-samenleving, waarmee Finland samenwerking zoekt.

[127] e-Estonia. (2019). e-Estonia: Security and safety. Retrieved from https://e-estonia.com/solutions/security-and-safety/

Blockchain wordt algemeen beschouwd als spitstechnologie en de druk bij bedrijven en overheden om de boot niet te missen is groot. Europa speelt hierin een rol met het *European Union Blockchain Observatory and Forum*, dat als doelstelling heeft om blockchain innovatie te versnellen en een blockchain ecosystem in de EU te ontwikkelen, om zo Europa's positie als wereldleider in deze technologie te verankeren. Blockchain is echter geen zaligmakend systeem dat alle, reeds lang bekende en gerapporteerde noden voor betere (nationale) samenwerking en informatie-uitwisseling tussen verschillende diensten, kan oplossen. Soms is blockchain zelfs niet de juiste oplossing.

Desalniettemin biedt de blockchain grote mogelijkheden voor efficiëntieverbetering en vlottere afwikkeling van de hele strafrechtketen. Mits een weloverwogen implementatie strategie kan dit, zonder bestaande systemen en databanken overboord te gooien, waardoor vroegere investeringen beschermd worden. De blockchain dient dan voornamelijk voor de betere doorstroming tussen diensten, informatiedeling en de bewaking van integriteit van digitale objecten.

Gezien de technologie nog volop evolueert en echte toepassingen van blockchain eerder experimenteel zijn, is het aangewezen om te starten met kleinere proefprojecten[*], om zodoende ervaring op te bouwen.

[*] Deze studie heeft geen analyse gemaakt van ICT ontwikkelingskosten en nodige budgetten.

Bibliografie

Wetenschappelijke literatuur

Ackermann, J., & Meier, M. (2018). Blockchain 3.0 - The next generation of blockchain systems. Retrieved from https://www.researchgate.net/publication/327672110_Blockchain_30_-_The_next_generation_of_blockchain_systems.

Akram, A., & Bross, P. (2018). *Trust, privacy and transparency with block-chain technology in logistics*. Paper presented at the Mediterranean Conference on Information Systems (MCIS), Cofu, Greece. https://www.researchgate.net/publication/329070204_TRUST_PRIVACY_AND_TRANSPARENCY_WITH_BLOCK-CHAIN_TECHNOLOGY_IN_LOGISTICS

B. Walton, J., & Dhillon, G. (2017). *Understanding digital crime, trust, and control in blockchain technologies*. Paper presented at the Americas Conference on Information Systems. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/36/

Barclay, I., Preece, A., & Theodorakopoulos, G. (2017). *Innovative applications of blockchain technology in crime and security.* Cardiff University, Retrieved from https://www.researchgate.net/publication/327915599_Innovative_Applications_of_Blockchain_Technology_in_Crime_and_Security

Bruggeman, W. (2014). *Een politie in verbinding. Een visie voor de politie in 2025*. Retrieved from Leuven Institute of Criminology (LINC): https://lirias.kuleuven.be/bitstream/123456789/523179/1/visiepolitie.pdf

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Cahiers Politiestudies, 3*(20), 17-40. Retrieved from http://www.ncjrs.gov/App/publications/abstract.aspx?ID=260054.

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE Access, 6*, 53019-53033. Retrieved from https://ieeexplore.ieee.org/document/8466786. doi:10.1109/ACCESS.2018.2870644

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55-81. Retrieved from http://www.sciencedirect.com/science/article/pii/S0736585318306324. doi:https://doi.org/10.1016/j.tele.2018.11.006

Celestini, A., Me, G., & Mignone, M. (2016). *Tor marketplaces exploratory data analysis: The drugs case*, Cham.

Comité P. (2018a). *De geïntegreerde politie en het forensisch onderzoek in een geïnformatiseerde omgeving*. Kamer van Volksvertegenwoordiger Retrieved from https://comitep.be/document/onderzoeksrapporten/2018-06-21%20Forensisch%20onderzoek.pdf

Conings, C. (2017). Hoofdstuk I. De zoeking. In *Klassiek en digitaal speuren naar strafrechtelijk bewijs* (pp. 9). Jurisquare: Intersentia.

Custers, B., & Vergouw, B. (2016). Technologie voor opsporing en handhaving. Kansen, ervaringen en knelpunten. In WODC (Ed.), *Nieuwe technologieën in opsporing en veiligheidszorg* (Vol. 3, pp. 48-67). Den Haag: Boom juridisch.

Dalle, J.-L. (2015). Nieuwe technologieën en policing: perfect huwelijk of geboren lat-relatie? In P. Ponsaers, W. Bruggeman, M. Easton, & A. Lemaitre (Eds.), *De toekomstpolitie. Triggers voor een voldragen debat (Reeks Veiligheidsstudies, nr. 10)* (pp. 165-186). Antwerpen, Apeldoorn: Maklu.

De Pauw, E., Ponsaers, P., van der Vijver, K., Bruggeman, W., & Deelman, P. (2011). Technology-led policing. *Cahiers Politiestudies, 3*(20). Retrieved from https://lib.ugent.be/catalog/rug01:001665663

De Pauw, E., & Vermeersch, H. (2015). Politie, surveillance en technologie in 2025. Wie legt de kaarten? In P. Ponsaers, W. Bruggeman, M. Easton, & A. Lemaitre (Eds.), *De toekomstpolitie. Triggers voor een voldragen debat (Reeks Veiligheidsstudies, nr. 10)* (pp. 165-186). Antwerpen, Apeldoorn: Maklu.

de Vries, A., & Smilda, F. (2014). *Social media: het nieuwe DNA. Een revolutie in opsporing*. Amsterdam: Reed Business Education.

Decorte, T., & Zaitch, D. (2016). *Kwalitatieve methoden en technieken in de criminologie*. Leuven: Acco.

Devroe, E., & Van de Velde, L. (2005). *Onderzoek Justitie doorgelicht*. Department of Penal law and criminology: Academia Press.

Dițu, B. V. (2017). New crime landscapes and new technologies for community policing. In P. S. Bayerl, R. Karlović, B. Akhgar, & G. Markarian (Eds.), *Community policing - A European perspective: Strategies, best practices and guidelines* (pp. 159-166). Cham: Springer International Publishing.

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal, 72*(4), 538-562. Retrieved from https://journals.sagepub.com/doi/10.1177/0020702017741909. doi:http://dx.doi.org/10.1177/0020702017741909

Easton, M. (2015). Het managen van innovatie door een netwerkende publieke politie. De triple-helix als vehikel. In P. Ponsaers, W. Bruggeman, M. Easton, & A. Lemaitre (Eds.), *De toekomstpolitie. Triggers voor een voldragen debat (Reeks Veiligheidsstudies, nr. 10)* (pp. 151-164). Antwerpen, Apeldoorn: Maklu.

Ekblom, P. (2017). Technology, opportunity, crime and crime prevention: current and evolutionary perspectives. In B. LeClerc & E. U. Savona (Eds.), *Crime Prevention in the 21st Century: Insightful Approaches for Crime Prevention Initiatives* (pp. 319-343). Cham: Springer International Publishing.

European Monitoring Centre for Drugs and Drug Addiction. (2016). The internet and drug markets. (21). Retrieved from http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf doi:10.2810/324608

European Union Blockchain Observatory & Forum. (2018a). *Blockchain for government and public services*. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf?width=1024&height=800&iframe=true

European Union Blockchain Observatory & Forum. (2018b). *Blockchain innovation in Europe*. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true

Europees Waarnemingscentrum voor drugs en drugsverslaving. (2017). *Europees drugsrapport 2017: Trends en ontwikkelingen*. Retrieved from Bureau voor publicaties van de Europese Unie, Luxemburg: http://www.emcdda.europa.eu/system/files/publications/4541/TDAT17001NLN.pdf

Europol. (2017a). *Europol review 2016 - 2017*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/europol-review-2016-2017

Europol. (2017b). *Internet Organised Crime Threat Assessment (IOCTA)* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA)* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

FOD Justitie. (2016). *Kadernota integrale veiligheid 2016-2019*. Retrieved from https://justitie.belgium.be/nl/nieuws/andere_berichten_29

Gandal, N., & Halaburda, H. (2014). Competition in the cryptocurrency market *Bank of Canada Working Paper 2014-33*. Retrieved from https://www.bankofcanada.ca/wp-content/uploads/2014/08/wp2014-33.pdf

Garfinkel, S. L. (2013). Digital forensics. *American Scientist, 101*(5), 370-377. Retrieved from https://search.proquest.com/docview/1435386577?accountid=11077.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaria, V. (2018). To blockchain or not to blockchain: That is the question. *IT Professional, 20*(2), 62-74.

Retrieved from https://www.researchgate.net/publication/324551383_To_Blockchain_or_Not_to_Blockchain_That_Is_the_Question. doi:10.1109/MITP.2018.021921652

Getso, M. M. A., & Johari, Z. (2017). The blockchain revolution and higher eucation. *International Journal of Information System and Engineering, 5*(1), 57-65. Retrieved from https://www.researchgate.net/publication/323716952_THE_BLOCKCHAIN_REVOLUTION_AND_HIGHER_EUCATION. doi:10.24924/ijise/2017.04/v5.iss1/57.65

Girasa, R. (2018). *Regulation of cryptocurrencies and blockchain technologies. National and international perspectives*: Palgrave Macmillan, Cham.

Grapperhaus, F., Akerboom, E., & Kuijs, L. (2018). *Kennis voor de politie van morgen. Een conferentie over onderzoek bij, naar en voor de politie*. In Politieacademie (Ed.). Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/94490.PDF

Hardyns, W. (2018). *Onderzoeksontwerp in de criminologie*: Universiteit Gent.

Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). "The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance. *29*(1/2), 240-257. Retrieved from https://www.emeraldinsight.com/doi/abs/10.1108/RMJ-12-2018-0045. doi:doi:10.1108/RMJ-12-2018-0045

J. Bambara, J., R. Allen, P., Iyer, K., Madsen, R., Lederer, S., & Wuehler, M. (2018). *Blockchain: A practical guide to developing business, law, and technology solutions*: McGraw-Hill Education.

Jacobsen, K. M. (2017). Game of phones, data isn't coming: Modern mobile operating system encryption and its chilling effect on law enforcement. *George Washington Law Review, 85*(2), 566-612. Retrieved from http://heinonline.org/HOL/P?h=hein.journals/gwlr85&i=594.

Janssens, J., Soetaert, S., & De Vos, A. (2017). Beslag en beheer van cryptovaluta: de Bitcoin. *Panopticon, 38*(1), 41-47. Retrieved from http://hdl.handle.net/1854/LU-8515715.

Jesson, J., Matheson, L., & M. Lacey, F. (2011). *Doing your literature review: traditional and systematic techniques*. Los Angeles, California ; London: SAGE.

K. Fedorov, A., O. Kiktenko, E., & I. Lvovsky, A. (2018). Quantum computers put blockchain security at risk. *Nature*, 465-467. Retrieved from https://www.nature.com/articles/d41586-018-07449-z?utm_source=briefing-dy&utm_medium=email&utm_campaign=briefing&utm_content=20181119#ref-CR1. doi:doi: 10.1038/d41586-018-07449-z

Kleemans, E., de Poot, C., & Verhage, A. (2014). Criminologie en opsporing. *Tijdschrift voor Criminologie, 56*(4). Retrieved from https://www.bjutijdschriften.nl/tijdschrift/tijdschriftcriminologie/2014/4/TvC_0165-182X_2014_056_004_001. doi:10.5553/TvC/0165182X2014056004001

Kolvart, M., Poola, M., & Rull, A. (2016). Smart contracts. In TanelKerikmäe & AddiRull (Eds.), *The future of law and eTechnologies* (pp. 133-147): Springer, Cham.

Koops, B.-J. (2016). Megatrends and grand challenges of cybercrime and cyberterrorism policy and research. In B. Akhgar & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (pp. 3-15). Cham: Springer International Publishing.

Kop, N., & Klerks, P. (2017). Aanzetten tot verbetering van de opsporing. 'Handelen naar Waarheid' een jaar later. In WODC (Ed.), *Justitiële verkenningen* (Vol. 4, pp. 26-36). Den Haag: Boom juridisch.

Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659. Retrieved from http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf. doi:10.6633/IJNS.201709.19(5).01

Lone, A. H., & Mir, R. N. (2017). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Scientific and Practical Cyber Security Journal*. Retrieved from https://journal.scsa.ge/papers/forensic-chain-ethereum-blockchain-based-digital-forensics-chain-of-custody/.

Mahmoud, Q. H., Lescisin, M., & AlTaei, M. (2019). Research challenges and opportunities in blockchain and cryptocurrencies. *Internet Technology Letters, 2*(2), e93. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.93. doi:10.1002/itl2.93

Mariën, I., & Courtois, C. (2012). *Kwantitatief onderzoek en kwetsbare groepen: Naar het representatief insluiten van verborgen of moeilijk bereikbare groepen*. Paper presented at the Etmaal van de Communicatiewetenschap, Leuven, Belgium. http://hdl.handle.net/1854/LU-2062643

Martin, J. (2014a). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. London: Palgrave Macmillan UK.

Martin, J. (2014b). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367. Retrieved from http://crj.sagepub.com/content/14/3/351.abstract. doi:10.1177/1748895813505234

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). *An overview of smart contract and use cases in blockchain technology.* Paper presented at the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

Mulgan, G., & Albury, D. (2003). *Innovation in the public sector*. Retrieved from http://www.sba.oakland.edu/faculty/mathieson/mis524/resources/readings/innovation/innovation_in_the_public_sector.pdf

N.O. Sadiku, M., Shadare, A., & M. Musa, S. (2017). Digital chain of custody. *International Journals of Advanced Research in Computer Science and Software Engineering, 7*(7). Retrieved from http://www.ijarcsse.com/index.php/ijarcsse/article/view/109. doi:10.23956/ijarcsse.v7i7.109

Pauwels, L. (2015). *Kwantitatieve criminologie. Basishandboek kwantitatieve methoden van criminologisch onderzoek*. Gent: Academia Press.

Prayudi, Y., & Sn, A. (2015). Digital chain of custody: state of the art. *International Journal of Computer Applications, 114*(5). Retrieved from https://www.researchgate.net/publication/273694917_Digital_Chain_of_Custody_State_of_The_Art. doi:10.5120/19971-1856

R. Butcher, J., Cohn, A., & J.W. Rennock, M. (2018). Blockchain technology & regulatory investigations. *Practical Law The Journal*(February/March), 34-44. Retrieved from https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf.

Tamminga, J. (2014). Bitcoin – wat is het, hoe werkt het? *Tijdschrift voor de Politie, 76*(3), 23-27. Retrieved from https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/89524.pdf.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2019). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*. Retrieved from http://www.sciencedirect.com/science/article/pii/S2352864818301536. doi:https://doi.org/10.1016/j.dcan.2019.01.005

Terpstra, J., Ponsaers, P., de Poot, C. J., Bockstaele, M., & Gunther Moor, L. (2013). Vernieuwing in de opsporing: een terreinverkenning. *Cahiers Politiestudies*, *3*(28), 7-20. Retrieved from http://hdl.handle.net/1854/LU-4291942.

van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders: een literatuurinventarisatie* (264). Retrieved from Den Haag: https://www.wodc.nl/binaries/ob264_volledige%20tekst_tcm28-69413.pdf

van der Vijver, K., & Gunther Moor, L. (2014). Welke toekomst heeft de politie? In E. Devroe, W. Hardyns, K. van der Vijver, & A. van Dijk (Eds.), *De toekomst van de politie* (Vol. 4, pp. 103-118). Antwerpen, Apeldoorn: Maklu.

Vaste Commissie van de Lokale Politie. (2019). *Memorandum 2019-2023*. Retrieved from http://www.lokalepolitie.be/5806/nl/downloads/file/Memorandum+NL.pdf

Verburgh, T., Smits, E., & van Wegberg, R. (2018). Uit de schaduw. Perspectieven voor wetenschappelijk onderzoek naar dark markets. In *De digitalisering van georganiseerde misdaad* (Vol. 44, pp. 68-82). Den Haag: Boom juridisch.

Verhelst, E. W. (2017). Blockchain aan de ketting van de Algemene verordening gegevensbescherming? *Privacy & Informatie (P&I)*(1), 17-23. Retrieved from https://www.uitgeverijparis.nl/scripts/read_article_pdf?editie=199502&id=1001310070.

Walport, M. (2016). *Distributed ledger technology: beyond block chain*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Winsemius, P. (2005). *Technologie en misdaad: Kansen en bedreigingen van technologie bij de beheersing van criminaliteit.* Retrieved from https://www.recht.nl/doc/kst27834-39.pdf

WODC. (2018). Inleiding. In *De digitalisering van georganiseerde misdaad* (Vol. 44). Den Haag: Boom juridisch.

WODC. (Lopend). Verkennend onderzoek naar de sociale en ethische gevolgen van de Blockchain en hoe de overheid zich hiertoe zou kunnen/moeten verhouden. *Projectnummer: 2815*. Retrieved from https://www.wodc.nl/onderzoeksdatabase/2815-verkennend-onderzoek-naar-de-sociale-en-ethische-gevolgen-van-de-blockchain-en-hoe-de-overheid-zich-hiertoe-zou-kunnenmoeten-verhouden.aspx.

Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017). *Ensuring data integrity using blockchain technology.* Paper presented at the 2017 20th Conference of Open Innovations Association (FRUCT).

Grijze literatuur

Accenture. (2013). Preparing police services for the future: six steps toward transformation. Retrieved from https://www.accenture.com/cz-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_7/Accenture-Preparing-Police-Services-Future.pdf

Bernaards, F., Monsma, E., & Zinn, P. (2012). *High Tech Crime. Criminaliteitsbeeldanalyse 2012*. Retrieved from Woerden: https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2012/cba-hightechcrime.pdf

College van procureurs-generaal. (2016). *Jaarverslag 2016*. Retrieved from https://www.om-mp.be/sites/default/files/u1/jaarverslag_2016_nl.pdf

Daems, R. (2017). *Schriftelijke vraag nr. 6-1596*. Senaat Retrieved from https://www.senate.be/www/?MIval=/Vragen/SchriftelijkeVraag&LEG=6&NR=1596&LANG=nl

De Smet, S. (2012). *De nieuwe politie*: LannooCampus.

Deckx, S., & Cools, M. (2012). *Het wetenschappelijk belang van de casestudie in het kader van inlichtingenstudies. Een onderzoek naar "Opération Satanique" en "Operatie Mongool"*. (Unpublished master's thesis), Universiteit Gent, Retrieved from https://lib.ugent.be/catalog/rug01:001891806

Drescher, D. (2017). *Blockchain basics, a non-technical introduction in 25 steps*: Apress.

Eeckhaut, T., De Ruyver, B., & Vermeulen, G. (2016). *Cybercrime: een casuïstische benadering*. (Unpublished master's thesis), Universiteit Gent, Retrieved from https://lib.ugent.be/fulltxt/RUG01/002/304/233/RUG01-002304233_2016_0001_AC.pdf

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (2016).

GOVCERT.NL. (2008). *DNS-misbruik van herkenning tot preventie*. Retrieved from https://www.ncsc.nl/actueel/whitepapers/dns-misbruik-van-herkenning-tot-preventie.html

Holland, R., Amado, R., & Marriott, M. (2018). *Seize and desist? The state of cybercrime in the post-AlphaBay and Hansa Age*. Retrieved from https://info.digitalshadows.com/rs/457-XEY-671/images/SeizeandDesist.pdf

Kaptijn, B., Bergman, P., & Gort, S. (2016). Whitepaper blockchain. Retrieved from https://www.ictu.nl/sites/default/files/documents/ICTU_Whitepaper_Blockchain.pdf

McGuire, M. (2018). *Into the web of profit. An in-depth study of cybercrime, criminals and money*. Retrieved from https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Ministerie van Justitie en Veiligheid. (2018). De staat van innovatie bij justitie en veiligheid, 40-41. Retrieved from https://www.innoveermeemetjenv.nl/documenten/publicaties/2018/01/08/magazine-de-staat-van-innovatie-bij-justitie-en-veiligheid

Pauwels, L. (2018). *De masterproef binnen de opleiding Criminologische Wetenschappen*. Universiteit Gent.

Pomp, M., & Verhaert, R. (2018). *Blockchain in de praktijk. Meer dan vijftig use cases in Nederland en België*. Brugge: Vanden Broele.

Raval, S. (2016). *Decentralized applications: Harnessing Bitcoin's blockchain technology*: O'Reilly Media.

Schiltz, W.-F., Vanwesenbeeck, D., De Meulemeester, M., De Ro, J., Taelman, M., & De Clercq, M. (2018). *Conceptnota voor nieuwe regelgeving betreffende*

blockchaintechnologie. Brussel: Vlaams Parlement Retrieved from http://docs.vlaamsparlement.be/pfile?id=1390090

Simal, J., Valcke, P., & Schroers, J. (2018). *Blockchain en privacy: een onderzoek naar de verzoenbaarheid van blockchaintechnologie met de GDPR.* (Unpublished master's thesis), KU Leuven, De Vlaamse ScriptieBank. Retrieved from https://www.scriptiebank.be/sites/default/files/thesis/2018-09/SIMAL_J_masterproef_privacy_en_blockchain.pdf

Smits, G. (2018). *Blockchain is wtf (waarschijnlijk toch fundamenteel)*: Die Keure.

Soetaert, S., Verhage, A., & De Middeleer, F. (2017). *Bitcoins en criminaliteit, een onvermijdelijk verband? Onderzoek naar de uitdagingen bij de aanpak van criminaliteit gepleegd met bitcoins.* (Unpublished master's thesis), Universiteit Gent, Retrieved from https://lib.ugent.be/catalog/rug01:002349307

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*: Penguin.

The Police Foundation. (2017). *Reforming justice for the digital age*. Retrieved from http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/pf_cgi_digital_justice.pdf

Van Eyken, L., Vermeulen, G., & Depauw, S. (2018). *Offline vs. online infiltratie: evaluatie van de bijzondere onderzoeksmethode van infiltratie in de informaticacriminaliteit in België.* (Unpublished master's thesis), Universiteit Gent, Retrieved from https://lib.ugent.be/fulltxt/RUG01/002/479/280/RUG01-002479280_2018_0001_AC.pdf

Verbond van Belgische Ondernemingen. (2018). Digitale agenda 2.0. Retrieved from http://www.vbo-feb.be/globalassets/publicaties/digitale-agenda-2.0/digitale-agenda-2.0-final-nl.pdf

Vitse, K., Adviseur DJF/CDGEFID. (2016). *Bitcoin: "What it is and how it works"*.

Vrolix, T. (2017). *Technologie & Innovatie: De keerzijde van de medaille. Onderzoek naar de illegale (internet)handel*. Faculteit Recht en Criminologie. Universiteit Gent.

Websites

Amado, R. (2018). Blockchain DNS niet alleen een wapen tegen, maar ook van cybercriminelen. Retrieved from http://www.beveiligingswereld.nl/Achtergrondartikelen/106/6655-blockchain_dns_niet_alleen_een_wapen_tegen,_maar_ook_van_cybercriminelen_

Autoriteit voor Financiële diensten en Markten (FSMA). (2019). Welke verplichtingen legt de antiwitwaswetgeving op aan tussenpersonen? Retrieved from https://mcc-

info.fsma.be/nl/welke-verplichtingen-legt-de-antiwitwaswetgeving-op-aan-tussenpersonen)

BeSafe. (2019). Vaste Commissie van de Lokale Politie. Retrieved from https://www.besafe.be/nl/veiligheidsthemas/politieorganisatie-financiering/organisatie-en-werking/vaste-commissie-van-de

Blockchain uitgelegd. (2019a). Wat is decentralisatie? Retrieved from https://www.uitlegblockchain.nl/decentralisatie/

Blockchain uitgelegd. (2019b). Wat zijn dapps? Retrieved from https://www.uitlegblockchain.nl/dapps/

Boddez, A. (2019). Nieuwe technologische ontwikkelingen bij de politie. Retrieved from https://www.politeia.be/nl/artikels/158424-nieuwe+technologische+ontwikkelingen+bij+de+politie

Bolt, M. (2018a). Wat is Blockchain? Alles wat u moet weten over gedistribueerd vertrouwen. Retrieved from http://www.watisblockchain.nl/wat_is_blockchain.php.

Bolt, M. (2018b). Wat maakt een Bitcoin waardevol? Retrieved from http://www.watisbitcoin.nl/waarde.php

Bossuyt, T. (2017). Dit moet je weten over het dark web. Retrieved from https://www.techpulse.be/achtergrond/217628/wat-het-dark-web/

Bové, L. (2018). Elke week cyberaanval op federale overheidsdienst. *De Tijd*. Retrieved from https://www.tijd.be/politiek-economie/belgie/federaal/elke-week-cyberaanval-op-federale-overheidsdienst/10043950.html

BTC Direct. (2019). Wat is de geschiedenis van blockchain? Retrieved from https://btcdirect.eu/nl-nl/geschiedenis-blockchain

Centre for Policing and Security. (2018a). CPS-studiedag: 'Innovatie in de opsporing: kansen en bedreigingen van Blockchain'. Retrieved from http://www.politiestudies.be/vrij.cfm?Id=412

Centre for Policing and Security. (2018b). Missie en doelstellingen. Retrieved from http://www.politiestudies.be/index.cfm?Id=85

Cludts, D. (2019). Een gedecentraliseerd dark web: hoe de zwarte markt zich wapent met blockchain. Retrieved from https://www.techzine.be/blogs/35330/een-gedecentraliseerd-dark-web-hoe-de-zwarte-markt-zich-wapent-met-blockchain.html

Cointelegraph. (2018). Altcoin news. Retrieved from https://cointelegraph.com/tags/altcoin

Comité P. (2018b). Over het Comité P. Retrieved from https://comitep.be/over-het-comiteacute-p.html

Craps, L. (2017). Geïntegreerd recherchemanagement. Retrieved from https://www.blueconnect.be/nl/highlight/74029018386531936

Darren, C. (2019). Wat is het verschil tussen decentrale applicaties (dapps) en smart contracts? Retrieved from https://www.uitlegblockchain.nl/verschil-decentrale-applicaties-smart-contracts-dapps/

De Breed & Partners. (2019). Blockchaintechnologie: het heden en de toekomst. Retrieved from https://www.debreed.nl/blog/blockchaintechnologie-heden-toekomst/

De Lameillieure, M. (2018). Blockchain: what's in it for you? Retrieved from https://blog.antwerpmanagementschool.be/nl/blockchain-whats-in-it-for-you

DeepDotWeb. (2017). Behind-the-scenes: a darknet market on the ethereum blockchain. Retrieved from https://www.deepdotweb.com/2017/07/08/behind-scenes-darknet-market-ethereum-blockchain/

Derek. (2018). Smart contracts uitleg – Wat zijn smart contracts? Retrieved from https://allesovercrypto.nl/article/smart-contracts-uitleg

DNS Belgium. (2018). ICANN en registries. Retrieved from https://www.dnsbelgium.be/nl/blog/icann-en-registries

European Commission. (2019). Blockchain technologies. Retrieved from https://ec.europa.eu/digital-single-market/en/blockchain-technologies

European Union Blockchain Observatory and Forum. (2019). EU Blockchain Observatory & Forum. Retrieved from https://www.eublockchainforum.eu/

Europol. (2016). Europol and Chainalysis reinforce their cooperation in the fight against cybercrime. Retrieved from https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime

FinanceInnovation. (2018). Cyberdreigingen in de financiële wereld: creditcardfraude. Retrieved from https://financeinnovation.nl/cyberdreigingen-in-de-financiele-wereld-creditcardfraude/

Forensicon. (2019). Chain of custody and evidence. Retrieved from https://www.forensicon.nl/chain-of-custody-and-evidence/

Foryard Academy. (2018). De geschiedenis van de blockchain. Retrieved from https://foryard.teachable.com/courses/blockchain-bitcoin-1o1/lectures/3786223

Gegevensbeschermingsautoriteit. (2019). Onze adviezen, machtigingen en aanbevelingen. Retrieved from https://www.gegevensbeschermingsautoriteit.be/beslissingen

Huijbregts, J. (2018). Politie keek mee met chatberichten van criminelen door toegang tot server. Retrieved from https://tweakers.net/nieuws/145403/politie-keek-mee-met-chatberichten-van-criminelen-door-toegang-tot-server.html

Ippo. (2017). Wat is DNS? Een korte, krachtige, niet technische uitleg van DNS. Retrieved from https://www.ippo.nl/blog/wat-is-dns/

Jubel. (2017). Bitcoins: de nieuwe IT-coins? Retrieved from https://www.jubel.be/bitcoins-de-nieuwe-it-coins/

Key, M. (2018). De brede invloed en het potentieel van blockchain. Retrieved from https://www.techzine.be/blogs/12537/de-brede-invloed-en-het-potentieel-van-blockchain.html

KV. (2018). Criminelen verliezen interesse in bitcoin. *HLN*. Retrieved from https://www.hln.be/geld/economie/criminelen-verliezen-interesse-in-bitcoin~ac2dacf2/

Löwik, S. (2018). WHOIS in de problemen door GDPR (AVG). Retrieved from https://www.antagonist.nl/blog/2018/04/gdpr-whois/

Maklu-Online. (2019). Panopticon. Oprichting en doelstelling. Retrieved from http://www.maklu-online.eu/nl/crime/panopticon/

Meijers, J. (2016). Blockchain, de hype voorbij. Retrieved from https://www.mt.nl/business/wat-je-moet-weten-over-blockchain/526823

Nationale Bank van België. (2019). Meegedeelde informatie. Retrieved from https://www.nbb.be/nl/kredietcentrales/centraal-aanspreekpunt/meegedeelde-informatie

Politie. (2019). Federal Computer Crime Unit. Retrieved from https://www.politie.be/5998/nl/over-ons/centrale-directies/federal-computer-crime-unit

Politie.nl. (2017a). Ondergrondse Hansa Market overgenomen en neergehaald [Press release]. Retrieved from https://www.politie.nl/nieuws/2017/juli/20/ondergrondse-hansa-market-overgenomen-en-neergehaald.html

Politie.nl. (2017b). Versleutelde berichten: schat aan criminele informatie [Press release]. Retrieved from https://www.politie.nl/nieuws/2017/maart/9/11-versleutelde-berichten.html

Politie.nl. (2018). Doorbraak in onderscheppen cryptocommunicatie [Press release]. Retrieved from https://www.politie.nl/nieuws/2018/november/6/02-doorbraak-in-onderscheppen-cryptocommunicatie.html

Straub, D. (2018). 'Proof of stake' versus 'proof of work': Dit moet je weten over hoe je transacties op de blockchain verifieert. Retrieved from https://www.businessinsider.nl/blockchain-technologie-proof-of-stake/

T-Mining. (2018). Antwerps blockchain pilootproject pioniert met veiligere en efficiëntere oplossing voor documenten [Press release]. Retrieved from

https://static1.squarespace.com/static/5a4c923580bd5e51e5536643/t/5b2782a0aa4a99e2ba580730/1529316001759/FinalPressRelease-T-Mining-150618.pdf

The Monero Project. (2018). Monero - secure, private, untraceable. Retrieved from https://getmonero.org/

The Police Foundation. (2018). Is blockchain good news or bad when it comes to policing and crime? Part 2. Retrieved from http://www.police-foundation.org.uk/2018/09/is-blockchain-good-news-or-bad-when-it-comes-to-policing-and-crime-part-2/

van Lonkhuyzen, L. (2018). Agenten konden stiekem meelezen met bij criminelen populaire cryptophones. Retrieved from https://www.nrc.nl/nieuws/2018/11/06/agenten-kraken-bij-criminelen-populaire-cryptophones-a2754131

van Loon, C. (2018). DNS vecht hard tegen GDPR over behoud WHOIS-database [Press release]. Retrieved from https://www.techzine.be/nieuws/11788/dns-vecht-hard-tegen-gdpr-over-whois-database.html

Vanacker, B. (2018). Kennisbeheer als strategische managementtool. Retrieved from https://www.kwinta.be/nieuws/kennisbeheer-als-strategische-managementtool

Vaste Commissie van de Lokale Politie (VCLP). (2019). VCLP presenteert haar aanbevelingen [Press release]. Retrieved from http://www.lokalepolitie.be/5806/nl/nieuws/21-vclp-presenteert-haar-aanbevelingen

Wikipedia. (2017). Forensisch onderzoek. Retrieved from https://nl.wikipedia.org/wiki/Forensisch_onderzoek

Wikipedia. (2018). Witboek (document). Retrieved from https://nl.wikipedia.org/wiki/Witboek_(document

Wikipedia. (2019a). Application programming interface. Retrieved from https://nl.wikipedia.org/wiki/Application_programming_interface

Wikipedia. (2019b). Backend. Retrieved from https://nl.wikipedia.org/wiki/Backend

Wikipedia. (2019c). Cryptografie. Retrieved from https://nl.wikipedia.org/wiki/Cryptografie

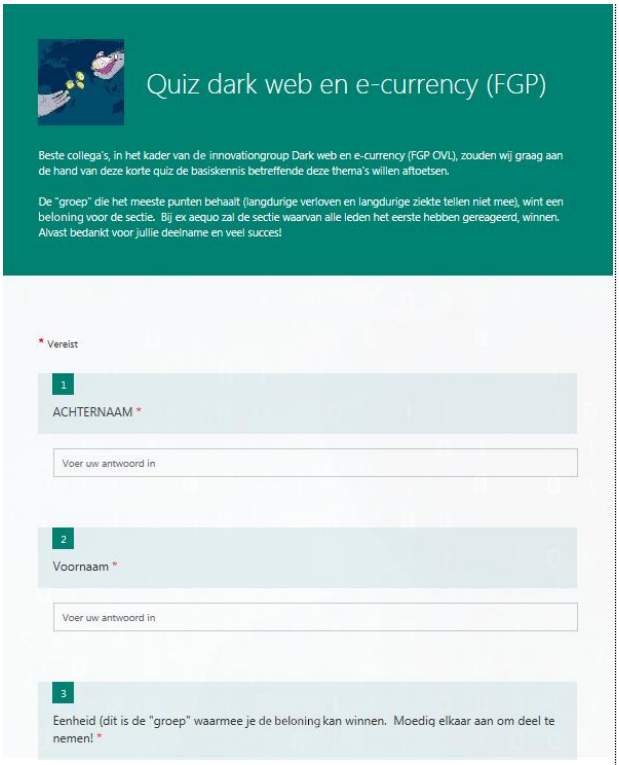
Wikipedia. (2019d). Open source. Retrieved from https://nl.wikipedia.org/wiki/Open_source

World Economic Forum. (2019). Our Mission. Retrieved from https://www.weforum.org/about/world-economic-forum

Zhao, W. (2018). China's security ministry touts blockchain for evidence storage. Retrieved from https://www.coindesk.com/chinas-police-ministry-touts-blockchain-for-secure-evidence-storage

Bijlagen

Bijlage 1: Websurvey voor respondenten binnen het politiewezen (FGP OVL)



Quiz dark web en e-currency (FGP)

Beste collega's, in het kader van de innovationgroup Dark web en e-currency (FGP OVL), zouden wij graag aan de hand van deze korte quiz de basiskennis betreffende deze thema's willen aftoetsen.

De "groep" die het meeste punten behaalt (langdurige verloven en langdurige ziekte tellen niet mee), wint een beloning voor de sectie. Bij ex aequo zal de sectie waarvan alle leden het eerste hebben gereageerd, winnen. Alvast bedankt voor jullie deelname en veel succes!

* Vereist

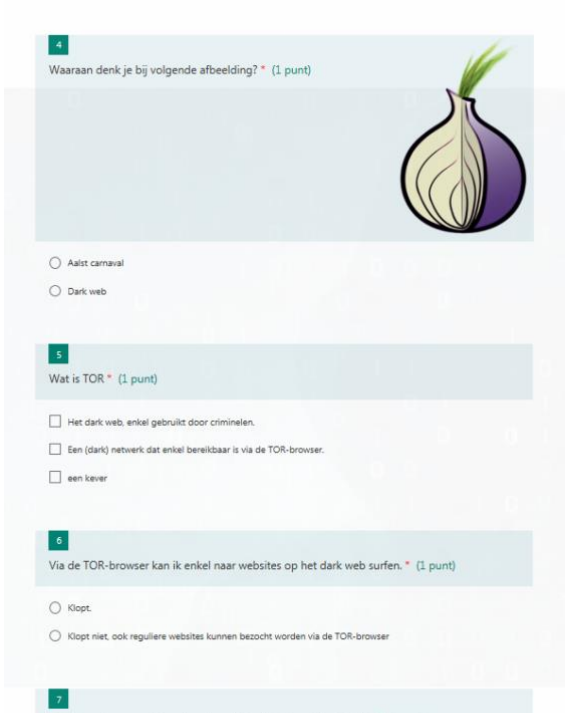
1 ACHTERNAAM *

Voer uw antwoord in

2 Voornaam *

Voer uw antwoord in

3 Eenheid (dit is de "groep" waarmee je de beloning kan winnen. Moedig elkaar aan om deel te nemen! *



4 Waaraan denk je bij volgende afbeelding? * (1 punt)

- Aalst carnaval
- Dark web

5 Wat is TOR * (1 punt)

- Het dark web, enkel gebruikt door criminelen.
- Een (dark) netwerk dat enkel bereikbaar is via de TOR-browser.
- een kever

6 Via de TOR-browser kan ik enkel naar websites op het dark web surfen. * (1 punt)

- Klopt.
- Klopt niet, ook reguliere websites kunnen bezocht worden via de TOR-browser

7 Het internet, www, dark web,... eigenlijk is dat allemaal hetzelfde. * (1 punt)

- Klopt
- Klopt niet

8 Om de weg naar het dark web te vinden heb je toch enige programmeerkennis/ervaring nodig. * (1 punt)

- Klopt.
- Neen, iedereen kan op het dark web.

9 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

- Ja
- Neen

10 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

- Ja
- Neen

11 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

12 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

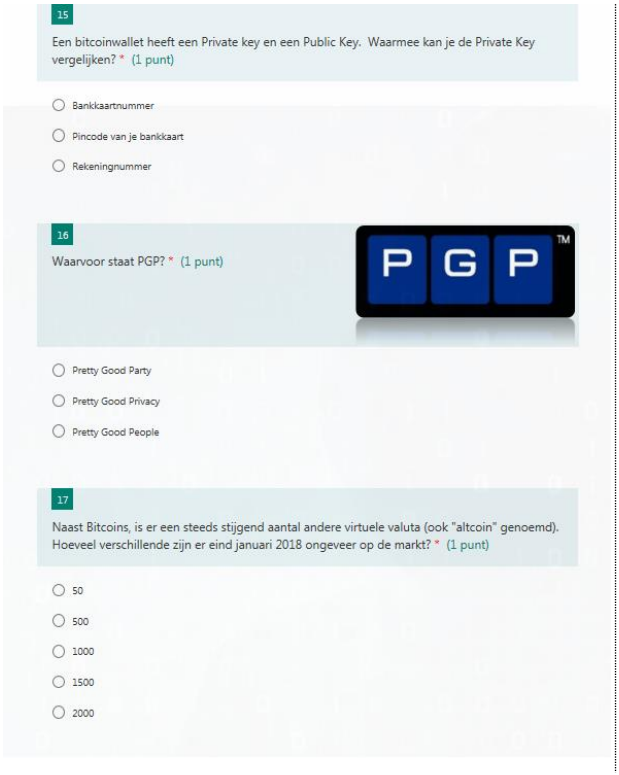
- Ja
- Neen

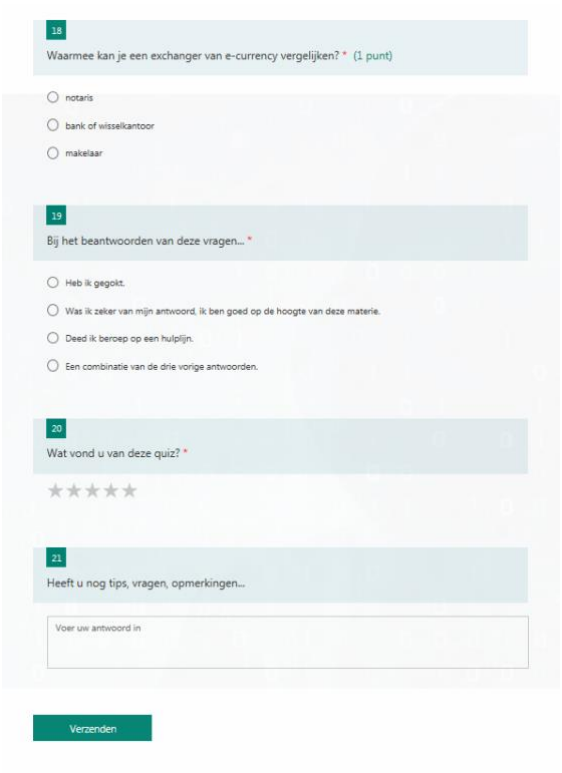
13 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

- Ja
- Neen

14 Komt volgende afbeelding in aanmerking voor het thema dark web of virtuele valuta? * (1 punt)

- Ja
- Neen





Bijlage 2: Informed consent

UGent student (ex-stagiair): gebruik enquête gegevens verzameld tijdens stageperiode bij FGP OVL (2017-2018).

TV Thomas Vrolix
vr 10/05, 12:05
[redacted]@police.belgium.eu

Allen beantwoorden

Verzonden items

gegevens.zip
1 MB

Alle 1 bijlagen (1 MB) weergeven Downloaden Opslaan in OneDrive - UGent

Geachte [redacted],

In het kader van het behalen van het diploma Master in de Criminologische Wetenschappen aan de Universiteit Gent, had ik in mijn masterproef (onderwerp: blockchain) graag nog even kort gebruik gemaakt van enkele gegevens uit mijn stageopdracht ('Inbeslagname van virtueel crimineel vermogen') die ik vorig jaar (academiejaar 2017-2018) bij jullie heb gemaakt in het kader van mijn toenmalige stage.

Het gaat voornamelijk om figuren/tabellen (zie bijlagen) die (volledig anoniem!!!) het resultaat weergeven van de data die werden verzameld aan de hand van een quiz, intern georganiseerd bij jullie (FGP OVL) door de *"Innovation Group "Dark Web en E-Currency"*.

Om er zeker van te zijn dat dit geen enkel probleem vormt i.v.m. de discretieplicht en de beroepscode van de stageplaats, had ik graag nog even uw toelating (als opvolger van [redacted]) gekregen hieromtrent.

Alvast bedankt!

Met vriendelijke groeten,
Thomas Vrolix
Master criminologische wetenschappen UGent.

RE: UGent student (ex-stagiair): gebruik enquête gegevens verzameld tijdens stageperiode bij FGP OVL (2017-2018).

DE [redacted]@police.belgium.eu> Allen beantwoorden

Vandaag, 10:18
Thomas Vrolix

Postvak IN

Beste,

Geen probleem om deze gegevens nogmaals te gebruiken voor je masterproef.

Vriendelijke groeten

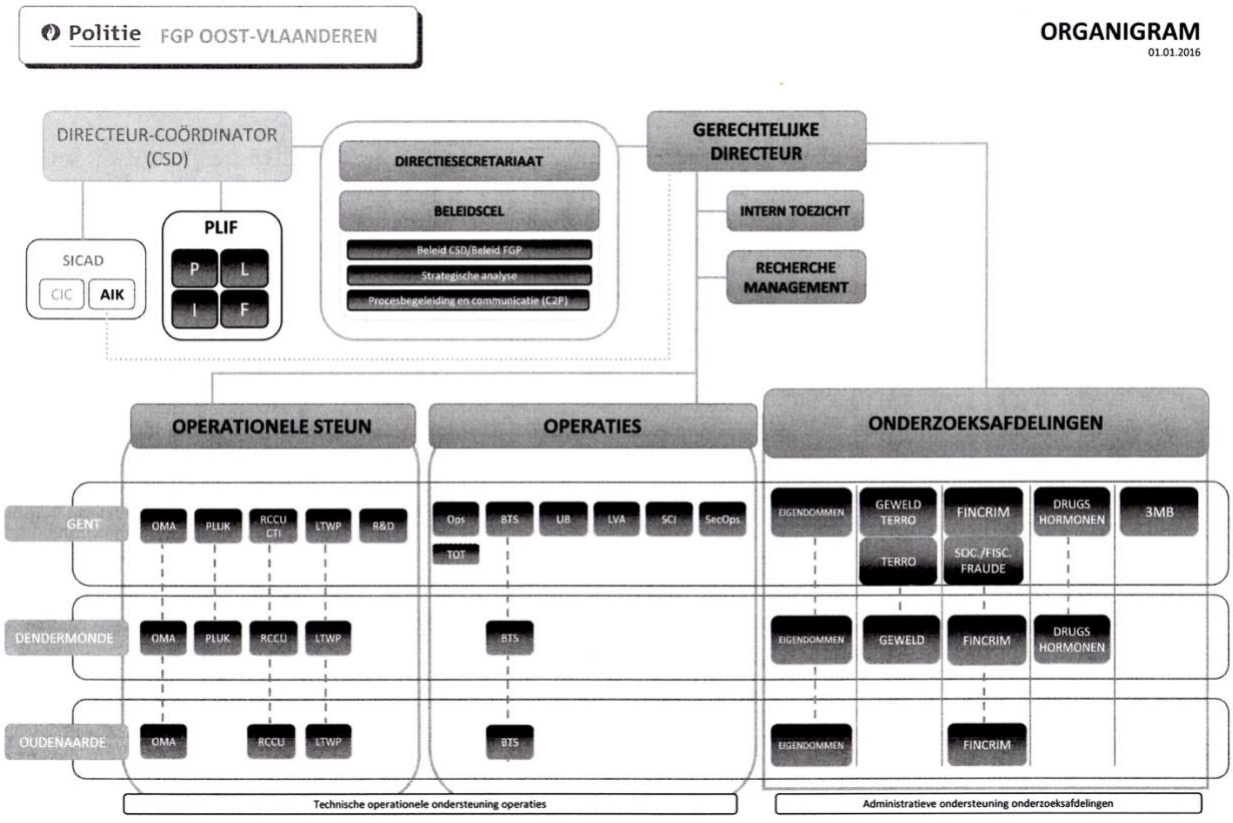
[redacted]
Eerste hoofdcommissaris
Coördinator Beleidscel

Federale gerechtelijke politie
Groendreef 181, B-9000 GENT

Tel: [redacted] *Mob:* [redacted]
Email : [redacted]@police.belgium.eu

Samen sterk tegen criminaliteit

Bijlage 3: Organigram FGP OVL



Bijlage 4: Enquête (N=46) over het gebruik van nieuwe technologieën door politiediensten en rechtshandhavingsinstanties in 11 verschillende landen (EU + Australië)[*]

Tabel 1 – Prevalentie van technologieën onder opsporings- en handhavingsdiensten	
Technologie	Percentage respondenten dat deze technologie gebruikt
Databanken/koppelen van bestanden en databanken	72
Cameratoezicht/CCTV	63
Vingerafdrukken	63
GPS/peilbakens/*tracking systems*	61
Sensing	52
Cryptografie/*data recovery*	50
DNA	50
Biometrie	48
Burgerparticipatienetwerken	48
Aftappen	46
Datamining/geautomatiseerde data-analyses	46
Bodycams	43
Netwerkanalyses	43
Profiling/doelgroepanalyses	41
Sociale media	41
ANPR/geautomatiseerde kentekenherkenning	37
Stemherkenning	37
Leugendetectors	35
RFID	33
Privacy-enhancing technologieën	33
Wapentechnologie	30
Narrowcasting/doelgroepenbenadering via netwerken	26
Drones/onbemande luchtvaartuigen	26
Gezichtsherkenning	24
Anders…	24
Virtual reality	11

[*] Custers, B., & Vergouw, B. (2016). Technologie voor opsporing en handhaving. Kansen, ervaringen en knelpunten. In WODC (Ed.), *Nieuwe technologieën in opsporing en veiligheidszorg* (Vol. 3, pp. 48-67). Den Haag: Boom juridisch.

Tabel 2 – Top 5 van juridische, organisatorische en technologische knelpunten bij politiediensten		
Knelpunt	Type	Percentage
Onvoldoende financiering	Organisatorisch	80
Onvoldoende beschikbaarheid	Technologisch	56
Onvoldoende juridische basis	Juridisch	44
Onvoldoende inzicht in wat er 'te koop' is	Technologisch	36
Onvoldoende inzicht en overzicht	Organisatorisch	29

Bijlage 5: Samenvatting blockchain*

Doel	Hoofdconcept
Beschrijving van eigenaarschap	Geschiedenis van transactiegegevens
Bescherming van eigenaarschap	Digitale handtekening
Opslag van transactiegegevens	Blockchaingegevensstructuur
Grootboeken voorbereiden op distributie	Onveranderbaarheid
Distributie van grootboeken	Informatie doorsturen over netwerken
Nieuwe transacties toevoegen	Blockchainalgoritme
Beslissen welk grootboek overeenstemt met de waarheid	Gedistribueerde consensus

Tabel 1: Overzicht van de taken voor het ontwerpen van een gedistribueerd peer-to-peersysteem voor het beheer van eigenaarschap.

Concept	Doel
Transactiegegevens	Beschrijving van overdracht van eigenaarschap
Transactiegeschiedenis	Bewijs van de huidige staat van eigenaarschap
Cryptografische hashwaarde	Identificeren van unieke gegevens
Asymmetrische cryptografie	Gegevens coderen en decoderen
Digitale handtekening	Instemmen met de inhoud van de transactiegegevens

* Drescher, D. (2017). *Blockchain basics, a non-technical introduction in 25 steps*: Apress.

Veranderingsgevoelige gegevensstructuren	Opslag van gegevens op een manier die elke manipulatie direct doet opvallen
Hashpuzzel	Het opleggen van een rekenkundig dure taak
Blockchaingegevensstructuur	Transactiegegevens op veranderingsgevoelige manier opslaan en hun volgorde handhaven
Onveranderbaarheid	Onmogelijk maken om de geschiedenis van transactiegegevens te wijzigen
Gedistribueerd peer-to-peernetwerk	De transactiegeschiedenis delen onder alle knooppunten in het netwerk
Berichten doorgeven	Ervoor zorgen dat alle knooppunten van het systeem alle informatie krijgen
Blockchainalgoritme	Ervoor zorgen dat alleen geldige transactiegegevens worden toegevoegd aan de blockchaingegevensstructuur
Gedistribueerde consensus	Ervoor zorgen dat alle knooppunten in het systeem dezelfde geschiedenis van transactiegegevens hanteren
Vergoeding	Knooppunten stimuleren tot handhaving van de integriteit

Tabel 2: Technische concepten van de blockchain en hun doel.

Laag	Functionele aspecten	Niet-functionele aspecten
Applicatie	– Vaststelling van eigenaarschap – Overdracht van eigenaarschap	– In hoge mate beschikbaar – Betrouwbaar – Open – Pseudo-anoniem
Implementatie	– Eigenaarschapslogica – Transactiebeveiliging – Transactieverwerkingslogica – Opslaglogica – Consensuslogica – Puur gedistribueerde peer-to-peerarchitectuur	– Veilig – Veerkrachtig – Uiteindelijk consistent – Behoud van integriteit

Tabel 3: Lagen en aspecten van de blockchain

Trefwoordenlijst

Altcoin	Is een afkorting van "Bitcoin Alternative". In dit opzicht beschrijft de term altcoin elke afzonderlijke cryptocurrency die geen Bitcoin is.
Anonimiseringstools- en diensten	Anoniem surfen kan via diensten zoals Tor (The Onion Router). Deze diensten zorgen ervoor dat het IP-adres (Internet Protocol adres) van de gebruiker onherkenbaar blijft. Elke computer die op internet is aangesloten heeft een IP-adres. Dat adres kan tot persoonlijke herkenning leiden. Anonimiseringsdiensten leiden het internetverkeer om via veilige servers. Webmasters en internetaanbieders kunnen hierdoor niet meer zien welke privépersoon, bedrijf of abbonee welke site bezoekt etc.
API (Application Programming Interface)	Een application programming interface (API) is een verzameling definities op basis waarvan een computerprogramma kan communiceren met een ander programma of onderdeel. Een API definieert de toegang tot de functionaliteit die er achter schuil gaat. De buitenwereld kent geen details van de functionaliteit of implementatie, maar kan dankzij de API die functionaliteit wel gebruiken.
Append-only blockchaingegevensstructuur	Het is mogelijk om nieuwe transacties toe te voegen aan de blockchain, maar het is bijna onmogelijk om gegevens te wijzigen die in het verleden zijn toegevoegd.
Asymmetrische encryptie	Een blockchain wordt beveiligd door asymmetrische encryptie. 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. 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.

Beveiligde chatapps (secure & encrypted messaging apps)	Smartphone apps die gebruik maken van end-to-end encryptie, een hele sterke vorm van versleuteling. Bij end-to-end encryptie wordt een bericht op een speciale manier versleuteld waardoor alleen de ontvanger het kan inzien. Op de webpagina: Secure Messaging Apps (https://www.securemessagingapps.com/); kun je zien welke apps versleuteling aanbieden, waar de servers staan en hoe het betreffende bedrijf denkt over privacy.
Bitcoin (BTC)	Bitcoin (afgekort BTC) is een virtuele munteenheid die is opgeslagen op Bitcoin-adressen die in Bitcoin-wallets zitten. Bitcoin is een innovatief betalingsnetwerk en een nieuw soort geld. Het is een technologie om, op een betrouwbare manier, wereldwijde elektronische betalingen te organiseren tussen twee partijen, zonder tussenkomst of mogelijke manipulaties van derden. Bitcoin is open source; het ontwerp is openbaar, niemand is eigenaar of beheerder van Bitcoin en iedereen kan meedoen. Het maakt gebruik van een decentraal peer-to-peer (P2P) netwerk (blockchain).
Bitcoin-adres	Het sturen en ontvangen van cryptobetalingen wordt geregeld door beveiligingssleutels. De private key is nodig om geld te versturen en de public key (Bitcoin-adres) om geld te ontvangen. Met andere woorden, betalingen worden verstuurd naar een Bitcoin-adres (net zoals een bankrekeningnummer) en ondertekend met de private sleutel (een handtekening).
Blockchaintechnologie	Blockchain of Distributed Ledger Technology (DLT) kent een lange ontstaansgeschiedenis. In 2009 is de blockchaintechnologie ontstaan als de technologie achter het elektronische betaalmiddel Bitcoin. 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 (POW). Simpel gezegd gaat het om een database waarvan heel veel mensen een kopie op hun computer hebben staan. Die database is een universeel gezamenlijk grootboek.
CAP	Het Centraal aanspreekpunt (CAP) is een register dat de bankrekeningnummers en soorten contracten bevat die door

	natuurlijke personen en rechtspersonen, al dan niet woonachtig in België, gehouden worden bij financiële instellingen in België.
CCU's FCCU LCCU RCCU's	Computer Crime Units Federal(e) Computer Crime Unit Local Computer Crime Unit Regional(e) Computer Crime Units
Centre for Policing and Security (CPS vzw)	Het CPS streeft het doel na samen met de hele veiligheidssector gemeenschappelijk bij te dragen aan het oplossen van maatschappelijke vraagstukken en problemen in de ruime veiligheidssfeer.
CFI	Cel voor Financiële Informatieverwerking
Comité P	Het Vast Comité van Toezicht op de politiediensten, kortweg Comité P, werd opgericht in 1991 vanuit de behoefte van het federale parlement om te beschikken over een extern controleorgaan op de politie. Door de vele toezichtsonderzoeken en onderzoeken naar klachten die de Dienst Enquêtes van het Comité P verricht, heeft het Comité P een beeld van de actuele werking van de politie. Dit beeld, aangevuld met informatie uit talrijke andere bronnen, stelt het Comité P in staat om een observatoriumfunctie van de politiewerking uit te oefenen ten behoeve van het federale parlement.
Cryptocurrencies	De blockchaintechnologie is een techniek die in potentie eindeloze toepassingen kent. De best gekende is momenteel Bitcoin, een cryptocurrency (e-currency). Deze munteenheid wordt online en digitaal gebruikt, vaak als een alternatief geldsysteem. Bitcoin is op dit moment de best gekende digitale munteenheid. De betrouwbaarheid van de digitale munt wordt gegarandeerd door een ingenieus cryptografisch systeem (vandaar ook de naam "cryptocurrency"). Een recent overzicht van alle virtuele valuta (cryptocurrencies) is te vinden op: https://coinmarketcap.com/all/views/all/.
Cryptocurrency exchange	Een cryptocurrency exchange is een website die kan vergeleken worden met een wisselkantoor waarbij 'echt' geld (fiatgeld) kan omgezet worden naar Bitcoins, en omgekeerd. Wanneer je via een exchanger geld omzet naar Bitcoins zal daar een kleine transactiekost aan verbonden

	worden. Het is onder meer door deze transactiekosten dat exchangers inkomsten verwerven.
Cryptomarkt	Cryptomarkten of darknetmarkten bevinden zich in het dark web en zijn toegankelijk via speciale software (vb. Tor browser). Een cryptomarkt kan worden gedefinieerd als een onlineforum waar goederen en diensten worden uitgewisseld tussen partijen die digitale encryptie gebruiken om hun identiteit te verbergen.
Dark web	Het dark web houdt een anoniem en besloten deel van het internet in. Deze term mag niet verward worden met het deep web, die alle onbereikbare inhoud omvat voor zoekmachines. De meeste van deze pagina's zijn onschuldig, zoals databases van bedrijven die je enkel na authenticatie kan opvragen. Het deep web is een koepelterm waar het dark web slechts een klein deel van uitmaakt. Websites op het dark web liggen meestal versleuteld achter het Tor-netwerk en kan je niet bereiken met een normale browser. Het dark web is ook niet opgenomen in zoekmachines zoals Google of Yahoo. Het is het deel van het internet dat het meest bekend is voor illegale activiteiten, vanwege de anonimiteit die het biedt aan gebruikers.
Deep web	Databanken, medische gegevens, overheidsgegevens, … alles waarvoor een login nodig is om tot de informatie te komen en dus niet geïndexeerd is bij standaard zoekmachines.
Desintermediatie	Vervanging van de tussenpersoon wordt ook wel desintermediatie genoemd. Het wordt gezien als een ernstige bedreiging voor veel ondernemingen en bedrijven die voornamelijk optreden als intermediair tussen verschillende groepen mensen, zoals kopers en verkopers, kredietnemers en kredietverstrekkers, of producenten en consumenten.
Digitaal forensisch onderzoek	Is onderzoek naar digitale sporen en gegevens die op andere wijze niet mogelijk waren om te achterhalen. Iedere persoon laat tegenwoordig digitale sporen achter op de computer, het internet of in een mailbox. Doordat vrijwel iedereen gebruik maakt van digitale technologie spelen digitale sporen vaak een belangrijke rol tijdens een onderzoek om specifieke zaken aan te tonen.

DNS (Domain Name System)	Wanneer iemand een webadres opgeeft aan zijn browser gaat de browser als eerste achterhalen welk IP-adres er bij het betreffende domein hoort. Hiervoor klopt het aan bij een zogenaamde Recursive Name Server (DNS server). Vaak is dit een server van een internet access provider, de partij die de internetverbinding verzorgt, bijvoorbeeld Telenet of Belgacom.
Een bureaucratische politie	Een politie als sterke groep met een grote aandacht voor regels – een combinatie die dikwijls gepaard gaat met een sterke hiërarchie en veralgemeende acceptatie van de regels waardoor er een sterk risico is op een relatief gesloten gemeenschap.
Een netwerkende politie	Een politie als sterke groep maar met minder aandacht voor regels: een combinatie die makkelijker interactie met andere groepen toelaat (een sterke groep die makkelijk met andere groepen interageert).
End-to-end encryptie	Zorgt ervoor dat alleen jij en het contact waarmee je communiceert de berichten kunnen lezen. Niemand anders kan de berichten lezen. Zelfs de beheerder van de software kan dat niet. Je berichten zijn beveiligd met een slot en alleen de verzender en de ontvanger hebben de sleutel om het slot te openen en het bericht te lezen.
FGP	Federale gerechtelijke politie.
FGP OVL	Federale Politie, FGP Oost-Vlaanderen, Afdeling Gent.
Fiatgeld	Fiatgeld is fiduciair geld waarbij de overheid met de centrale bank verantwoordelijk zijn voor monetaire politiek en de geldhoeveelheid die in omloop wordt gebracht. Het ontleent zijn waarde aan het vertrouwen dat er goederen en diensten mee gekocht kunnen worden. Vaak zal aan dit vertrouwen een wettelijke basis ten grondslag liggen, zoals bij een wettig betaalmiddel. Voor de doorsnee gebruiker van Bitcoin, moet je vertrouwen hebben in de wetenschappelijke doorbraken binnen cryptografie en gedistribueerde computertechnologie. Bitcoin beschikt niet over een centrale bank met een geldpers. Het monetaire beleid en de geldhoeveelheid is cryptografisch vastgelegd en wordt automatisch uitgevoerd.
FINCRIM	Financiële criminaliteit

First adopters	Is iemand die een bepaald product of een bepaalde technologie begint te gebruiken voordat de grote massa dat doet.
Gedecentraliseerd	Dit betekent dat er geen derde, controlerende of regulerende partij in het spel is. Die taken worden collectief door het netwerk, de gebruikers, beheerd. Het zijn toepassingen die draaien binnen het blockchainnetwerk.
Gedecentraliseerde en gedistribueerde databases	De twee belangrijkste architecturale benaderingen voor het organiseren van softwaresystemen zijn de gecentraliseerde en de gedistribueerde aanpak. In gecentraliseerde softwaresystemen zijn de componenten verbonden met en gegroepeerd rond één centrale component. Daarentegen vormen de componenten van gedecentraliseerde en gedistribueerde systemen een netwerk van verbonden componenten zonder enig centraal element voor coördinatie of controle. Als er één enkele component is, bijvoorbeeld een uitschakelknop die het hele systeem kan stoppen, is het systeem niet gedistribueerd.
High-tech crime	High-tech crime als overkoepelend containerbegrip verwijst naar een veelheid aan criminele activiteiten waarbij gebruik wordt gemaakt van ICT. Tegenover de term cybercrime biedt high-tech crime een breder en meer dynamisch perspectief dat beter aansluit bij de snelle technologische ontwikkelingen vandaag de dag. Nieuwe criminaliteitsvormen die kunnen ontstaan door innovaties van ICT (en niet alleen het internet) worden door dit containerbegrip afgedekt.
ICANN (Internet Corporation for Assigned Names and Numbers)	Is een onafhankelijke non-profit niet-gouvernementele organisatie die met behulp van een 'multistakeholder'-model beleid maakt en die een aantal internet-gerelateerde beslissingen neemt over het technisch beheer van het internet, zoals het toekennen en specifiëren van topleveldomeinen, toewijzen van domeinnamen en de distributie van IP-nummers. Zij is de internationale autoriteit op het gebied van domeinnaambeheer.
ICT	Informatie- en communicatietechnologie.

IP-adres (Internet Protocol adres)	Een uniek identificerend nummer van met internet verbonden apparaten. Het IP-adres is, simpel gezegd, het huisadres van de computer.
Kennisbeheer	Kennisbeheer wordt meer en meer, terecht, gezien als een strategische managementtool binnen bedrijven en organisaties. Door het efficiënt en effectief beheren en gebruiken van kennis kan ingespeeld worden op tools en technieken, processen, (disruptieve) technologieën, (bedrijfs)risico's, …
LIB / SCI	Lokale informantenbeheerders / Sectie Criminele Informatie
LTWP	Laboratoria voor Technische en Wetenschappelijke Politie
Mining	Een participant op het (blockchain)netwerk die zijn of haar computer laat werken voor het netwerk en zich actief bezighoudt met het koppelen van blokken omdat hij of zij hiervoor een *incentive* (beloning) krijgt. Miners krijgen een beloning voor het inzetten van hun rekenkracht (specifieke mininghardware en -software en elektriciteit) voor het oplossen van de berekening. Door het oplossen van de berekening (Proof-of-Work) wordt een nieuwe 'block' (verschillende transacties vormen samen een block) aan de blockchain toegevoegd. Het is met andere woorden een stimulans voor miners in ruil voor energie die zij hebben uitgegeven om de stabiliteit, de veiligheid en de beveiliging van het (publieke) blockchainnetwerk te verbeteren (Simal et al., 2018).
OMA	Operationele misdrijfanalisten
Open source	Open source of open bron beschrijft de praktijk die in productie en ontwikkeling vrije toegang geeft tot de bronmaterialen (de source) van het eindproduct. Hierbij komen eindproducten en de daar aan ten grondslag liggende basismaterialen (bijvoorbeeld ontwerpen, beschrijvende documentatie en dergelijke), vrij ter beschikking voor het publieke domein.
OpenBazaar	OpenBazaar is een andere manier van online zakendoen. Het is een peer-to-peer applicatie op basis van blockchaintechnologie die geen tussenpersonen nodig heeft, wat betekent dat er geen kosten zijn en geen beperkingen. OpenBazaar verbindt mensen rechtstreeks via blockchain.

	Gegevens worden verspreid over het netwerk in plaats van opgeslagen in een centrale database. Niemand heeft controle over OpenBazaar. Elke gebruiker draagt evenveel bij aan het netwerk en heeft de controle over zijn eigen privégegevens.
OPS / REM	Operationele personeelsleden politie / Recherchemanagement
OPSEC	Operations security (OPSEC) is een term uit de militaire wereld. Het verwijst naar tactieken die worden gebruikt om privacy en anonimiteit te beschermen.
Peer-to-peer netwerk	Peer-to-peernetwerken zijn een special soort gedistribueerde systemen. Ze bestaan uit afzonderlijke computers (ook wel knooppunten genoemd), die hun resources (verwerkingskracht, opslagcapaciteit, data- of netwerkbandbreedte) direct ter beschikking stellen aan alle andere leden in het netwerk, zonder tussenkomst van enig centraal coördinatiepunt. De knooppunten in het netwerk zijn elkaars gelijke voor wat betreft hun rechten en rollen in het systeem. Bovendien zijn ze allemaal zowel leverancier als consument van resources. Peer-to-peersystemen kennen interessante toepassingen, zoals het delen van bestanden, contentdistributie en privacybescherming. De meeste van deze toepassingen gaan daarbij uit van een eenvoudig maar krachtig idee, namelijk de computers van de gebruikers omvormen tot knooppunten die het hele gedistribueerde systeem vormen. Alle gebruikers tezamen vormen één groot netwerk. Het resultaat is dat hoe meer gebruikers of klanten gebruikmaken van de software, hoe groter en krachtiger het systeem wordt.
PGP (Pretty Good Privacy)	Pretty Good Privacy (meestal afgekort tot PGP) is een van de veel gebruikte vercijferingsmethodes op internet die ook gebruik maakt van een public en een private key. PGP combineert traditionele encryptie met asymmetrische cryptografie om berichten onleesbaar te maken. Een PGP-key bestaat uit drie onderdelen: een publieke sleutel, een privésleutel en een wachtwoord. De publieke sleutel mag met iedereen worden gedeeld: deze wordt gebruikt om berichten of bestanden te verzenden. De privésleutel moet de eigenaar geheimhouden, want deze maakt het, in combinatie met het wachtwoord, mogelijk om berichten te ontsleutelen.

	Door deze encryptie zijn berichten niet te ontcijferen door overheden en de politie.
PLUK	Een plukteam is verantwoordelijk voor de inventaris van het crimineel vermogen met oog op inbeslagneming en ontneming, een buitgerichte aanpak.
Privacy-focused cryptocurrencies (“privacy coins”)	Altcoins die zich vooral op (nog) meer anonimiteit toespitsen.
Proof-of-Work (PoW) (=consensusmechanisme)	Consensus in een (publieke) blockchain wordt bereikt wanneer meer dan de helft (51%) van het netwerk akkoord is met een handeling (transactie) en deze aanvaardt. Er zijn verschillende methodes voor dit proces. De bekendste is de Proof-of-Work. Dat wordt onder andere voor Bitcoin gebruikt. De werking van het consensusmechanisme Proof-of-Work is als volgt: Proof-of-Work wordt verkregen nadat deelnemers in het netwerk met elkaar concurreren in het oplossen van een complexe mathematische puzzel, wat ook wel *mining* wordt genoemd (Cai et al., 2018). De winnaar zal het voorrecht hebben om een blok te creëren en dit uit te zenden naar de andere deelnemers. De deelnemers die met succes enkele blokken hebben gemaakt, krijgen daar een beloning voor (in de Bitcoin-blockchain is dit een kleine hoeveelheid van de betreffende cryptomunt). Omdat we om te selecteren wie het volgende blok creëert niet op de identiteit van de ‘miners’ kunnen vertrouwen, creëren we in plaats daarvan een puzzel die moeilijk op te lossen is (d.w.z. er is heel wat *werk* voor nodig), maar gemakkelijk te verifiëren is (d.w.z. alle anderen kunnen het antwoord snel controleren). Deelnemers zijn het erover eens dat degene die het probleem als eerste oplost het volgende blok creëert. Miners moeten hulpmiddelen gebruiken (computerhardware, elektriciteit et cetera) om de puzzel op te lossen, want ze moeten op zoek naar de juiste *hash,* een soort unieke vingerafdruk voor een tekst of een gegevensbestand (Tapscott & Tapscott, 2016). De puzzel is wiskundig van opzet, zodat er onmogelijk een ‘shortcut’ kan worden gevonden om hem op te lossen. Daarom vertrouwt, terwijl de rest van het netwerk het antwoord ziet, iedereen erop dat het veel werk heeft gekost om hem op te lossen. Het vinden van de juiste hashwaarde is erg moeilijk. Als de

	hashwaarde niet klopt, verandert de *miner* de invoergegevens licht en probeert hij het opnieuw. Om de oplossing te vinden is veel rekenkracht vereist. Vergelijk het met een hangslot met cijfercode. De miners proberen telkens door andere codes in te vullen, via 'trial en error', het slot open te krijgen (Straub, 2018). Na miljoenen pogingen is de juiste cijfercombinatie eindelijk gevonden, die vervolgens door de rest wordt gecontroleerd. De computer die als eerste de hashpuzzel weet op te lossen heeft gewonnen en krijgt een beloning. De beloning is de incentive om je computerkracht ter beschikking te stellen voor de opbouw en beveiliging van de blockchain. Het blok is dan compleet en wordt toegevoegd aan de bestaande keten. Door dit Proof-of-Work–mechanisme bereikt het netwerk consensus omtrent de authenticiteit van de gegevens vervat in het blok. De blokken worden nu aan elkaar gekoppeld. Elk blok moet naar het voorafgaande blok verwijzen om geldig te zijn. 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. Dit is praktisch en technisch onmogelijk. De geschiedenis van transactiegegevens wordt aldus beveiligd tegen manipulatie en vervalsing door deze op te slaan in een onveranderbare *append-only* blockchaingegevensstructuur, waarvoor de oplossing van een hashpuzzel vereist is voor elk blok dat wordt toegevoegd of herschreven. Na de aaneenkoppeling van de blokken door de miners zijn de gegevens zo goed als permanent in de blockchain vastgelegd op versleutelde wijze (Simal et al., 2018). Samengevat: Proof-of-Work is een stukje data dat erg moeilijk te produceren is, omdat het duur en tijdrovend is. Deze vorm van data is eenvoudig te controleren door anderen en moet aan bepaalde eisen voldoen. Het produceren van Proof-of-Work kan een willekeurig proces zijn met een lage waarschijnlijkheid. Er zal dus over het algemeen veel 'trial and error' moeten worden toegepast, voordat er een geldige Proof-of-Work is gegenereerd.
Recherchemanagement (ReM)	De wisselwerking tussen het (zo ideaal mogelijk) afstemmen van de recherchecapaciteit op de beleidsprioriteiten.
Technology-led policing	Technologie heeft altijd een belangrijke rol gespeeld bij de taakuitvoering van de politie. Die rol is de laatste jaren niet alleen uitgebreid maar ook vernieuwd.

Tor	Tor is de afkorting van The Onion Router, een speciaal netwerk dat gebruikers anonimiseert. Er is een browser beschikbaar, de Tor Browser, waarmee toegang tot dit netwerk wordt verkregen (om anoniem te surfen). Het wordt onder meer gebruikt om toegang te krijgen tot het dark web.
VCLP	De Vaste Commissie van de Lokale Politie werd opgericht bij artikel 91 van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Zij is voornamelijk samengesteld uit korpschefs van de lokale politie en is belast met het onderzoeken van of het geven van adviezen over alle problemen met betrekking tot de lokale politie op verzoek of op eigen initiatief.
Whitepaper	Een witboek, white paper of whitepaper is een document dat beschrijft hoe overheidsbeleid, een technologie, en/of product een specifiek probleem oplost. Witboeken worden gebruikt om de lezer van objectieve relevante informatie te voorzien die wordt gebruikt voor het nemen van een beslissing. Witboeken worden zowel in de politiek als in het bedrijfsleven gebruikt. Witboeken, wanneer deze objectief geschreven zijn, worden vaak beschouwd als een betrouwbare bron van informatie.
Zwarte markt	Is de handel in goederen of diensten die illegaal zijn of verdeeld worden via illegale kanalen. Enkele voorbeelden van een zwarte markt zijn: het verkopen van gestolen goederen, drugs of wapens.