Cybercrime en witwassen

319

Onderzoek en beleid

Cybercrime en witwassen

Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware

J.J. Oerlemans

B.H.M. Custers

R.L.D. Pool

R. Cornelisse

Boomcriminologie

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Onderzoek en beleid

De reeks Onderzoek en beleid omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Veiligheid en Justitie weergeeft.

Exemplaren van dit rapport kunnen worden besteld bij het distributiecentrum van Boom juridisch:
Boom distributiecentrum te Meppel
Tel. 0522-23 75 55
Fax 0522-25 38 64
E-mail budh@boomdistributiecentrum.nl

De integrale tekst van de WODC-rapporten is gratis te downloaden van www.wodc.nl.
Op www.wodc.nl is ook nadere informatie te vinden over andere WODC-publicaties.

ISBN 978-94-6236-728-9

NUR 741

Voorwoord

Cybersecurity-experts waarschuwden ons een paar jaar geleden al: ransomware zal de komende tijd explosief toenemen. Daarna verschenen aan de lopende band nieuwsberichten over ransomware-besmettingen. Bij ransomware worden computers besmet en (deels) onbruikbaar, waarna slachtoffers zich weer kunnen vrijkopen door betaling van losgeld. Het gaat daarbij steeds vaker om cryptoware varianten, die computerbestanden versleutelen en losgeld eisen in de vorm van virtuele valuta, meestal bitcoins. Voor consumenten kan het vervelend zijn dat de vakantie- en familiefoto's gegijzeld worden, maar voor het bedrijfsleven kan de versleuteling van gegevens in bedrijfsnetwerken nog grotere gevolgen hebben. In de Verenigde Staten worden ziekenhuizen na besmetting met cryptoware afgeperst, opdat ze losgeld in bitcoins betalen.
Een andere vorm van cybercrime waarmee criminelen geld verdienen is banking malware, waarmee via nepschermen tegoeden van bankrekeningen worden weggesluisd. Hoewel banking malware de laatste jaren op zijn retour lijkt te zijn door verschillende effectieve detectiemaatregelen die zijn genomen door banken, is dit nog steeds een veelvoorkomende vorm van cybercrime.
Achter deze beide vormen van cybercrime gaat in veel gevallen een criminele organisatie schuil. Een deel van de criminele organisatie houdt zich bezig met het technische gedeelte en een deel met het witwassen van de criminele winsten. Over het witwassen van contant geld door onder meer drugscriminelen is via de monitor georganiseerde criminaliteit die het WODC al jaren uitvoert veel kennis beschikbaar.[1]

Het nu voorliggende rapport legt echter een compleet nieuwe wereld bloot van processen achter het witwassen van cybercrimegelden, in het bijzonder de verdiensten uit banking malware en ransomware. Daarbij worden nog relatief nieuwe fenomenen als e-wallet-diensten, virtuele prepaid cards, virtuele valuta, bitcoin exchanges, en mixing services, uitvoerig beschreven. Het rapport biedt daarmee achtergrondinformatie en nieuwe inzichten die onontbeerlijk zijn voor het analyseren, maar zeker ook het bestrijden, van het witwassen van geld dat wordt verkregen uit cybercrime.

Graag wil ik bijzondere dank uitspreken naar de voorzitter en de leden van de begeleidingscommissie (zie bijlage 1), de respondenten van de interviews (bijlage 2), en collega's bij het WODC die hebben bijgedragen aan de totstandkoming van het rapport.

Prof. dr. F.L. Leeuw
Directeur WODC

1 Zie www.wodc.nl/onderzoek/cijfers-en-prognoses/Georganiseerde-criminaliteit/index.aspx. Het laatste rapport is beschikbaar via: www.wodc.nl/onderzoeksdatabase/monitor-georganiseerde-criminaliteit-vierde-ronde.aspx.

Inhoud

Samenvatting

Aanleiding, vraagstelling en scope

Over het witwassen bij cybercrime is, vergeleken met witwassen bij andere delicten, relatief weinig bekend. Bij veel delicten verdienen criminelen geld in contanten. Bij het witwassen van verdiensten uit cybercrime lijken echter in toenemende mate andere digitale betalingsmiddelen te worden gebruikt dan contant geld dat bijvoorbeeld uit drugshandel wordt verkregen. Met de groei van cybercrime in de laatste jaren neemt de urgentie toe om zicht te krijgen op het witwasproces en de betrokken actoren in dit proces. Dit onderzoek richt zich om die reden op het witwasproces, en het in kaart brengen van de betrokken actoren bij banking malware en ransomware. Banking malware is, kort gezegd, kwaadaardige software die bedoeld is om slachtoffers geld afhandig te maken via betalingen met internetbankieren. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist om het systeem te ontsleutelen. Sinds een paar jaar is een variant van ransomware in opkomst, genaamd cryptoware, waarbij bestanden op een computer versleuteld worden en het losgeld in de virtuele valuta Bitcoin wordt geëist.

De centrale vraagstelling in dit onderzoek is: *op welke wijze en door welke actoren wordt geld verkregen uit banking malware en ransomware (al dan niet digitaal) witgewassen?* Voor de beantwoording van deze vraag zijn zes deelvragen geformuleerd:

1 Wat wordt verstaan onder het witwassen van door banking malware en ransomware verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?
2 Wat zijn digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, en hoe werken deze digitale betalingsmiddelen?
3 Op welke wijze en door welke actoren wordt geld witgewassen dat:
   a door middel van banking malware wordt verkregen?
   b door middel van ransomware wordt verkregen?
4 Wat zijn de kenmerken van actoren die betrokken zijn bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?
5 Welke informatie over de modus operandi van actoren, die betrokken zijn het bij het witwassen van geld dat verkregen wordt uit banking malware en ransomware, is beschikbaar op het dark web?
6 Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?

Methodologie

De onderzoeksvragen zijn beantwoord met behulp van de volgende onderzoeksmethoden: (1) deskresearch, (2) interviews, (3) dossieronderzoek, (4) een 'experiment' met bitcoins en mixing services, en (5) een kwantitatieve analyse van transactiegegevens van de grote Nederlandse banken die zijn gerelateerd aan banking malware en phishing. De deskresearch bestond uit een analyse van de beschikbare literatuur en mediaberichten over cybercrime, witwassen, en digitale betalingsmiddelen. Daarnaast zijn verdiepende interviews afgenomen met behulp met een semigestructureerde vragenlijst bij twintig experts op het gebied van cybercrime, witwassen en het gebruik van digitale betalingsmiddelen. De deskresearch en de interviews leverden kennis op over het gebruik van digitale betalingsmiddelen en het digitaal witwassen van geld dat wordt verkregen uit cybercrime. Tevens zijn vier zaken van het High Tech Crime Team van de Nationale Politie onderzocht die betrekking hebben op cybercrime en witwassen. Door middel van een empirische oefening, waarbij bitcoins werden aangeschaft en door mixing services werden gehaald, is inzicht verkregen in de online dienstverleners op het gebied van witwassen van bitcoins. Ten slotte is een kwantitatieve analyse uitgevoerd van transactiegegevens die zijn gerelateerd aan banking malware en phishing. Deze gegevens hebben inzicht verschaft in de kenmerken van money mules die betrokken zijn in het witwasproces bij banking malware.

Resultaten en conclusies

Het geld dat wordt verkregen uit banking malware en ransomware is doorgaans digitaal van aard. Bij banking malware wordt elektronisch geld buitgemaakt en bij ransomware wordt het losgeld veelal betaald met vouchers of (in toenemende mate en vooral bij cryptoware) met bitcoins. Het witwassen van deze opbrengsten bestaat uit het verbergen of verhullen van de criminele herkomst van het geld. De typologieën die zijn ontwikkeld om opzet bij opzetwitwassen te bewijzen, hebben vooral betrekking op contant geld bij (veelal) drugsdelicten. In de praktijk bestaat daardoor regelmatig onduidelijkheid over de vraag op welke moment bij transacties of bezit van grote sommen virtuele betalingsmiddelen kan worden gesproken van opzet bij witwassen.

Veel typen digitale betalingsmiddelen kunnen worden gebruikt om de verdiensten uit cybercrime wit te wassen. In dit onderzoek wordt een onderscheid gemaakt tussen elektronisch geld en virtueel geld. Elektronisch geld is de digitale weergave van echt geld, terwijl virtueel geld niet door de overheid is gefiatteerd. Virtueel geld kan op zijn beurt centraal of decentraal beheerd zijn en wel of niet inwisselbaar zijn tegen echt geld. Inwisselbaar, centraal

beheerd virtueel geld betreft bijvoorbeeld tegoeden op websites, niet-inwisselbaar centraal beheerd virtueel geld betreft bijvoorbeeld speelgeld in online games en virtuele werelden. Inwisselbaar, decentraal beheerd virtueel geld betreft cryptocurrencies. Veruit de bekendste cryptocurrency is de Bitcoin, met 90% van de totale marktwaarde van virtuele valuta.

In dit onderzoek zijn verschillende modellen beschreven die criminelen gebruiken om geld dat wordt buitgemaakt uit banking malware en ransomware wit te wassen. De onderzoeksresultaten laten zien dat gelden die zijn verkregen uit banking malware en ransomware op zeer veel verschillende manieren kunnen worden witgewassen. Daarbij wordt vaak een combinatie gemaakt van digitale betalingsmiddelen.

Bij banking malware wordt vaak gebruikgemaakt van money mules. Het geld wordt in dat geval vanaf de rekening van het slachtoffer van banking malware overgemaakt naar een rekening van een money mule. Vervolgens neemt de money mule het bedrag zo snel mogelijk op bij een geldautomaat (de zogenoemde 'cash-out'). Deze wijze van witwassen kan deels worden verklaard door de voorkeur van criminelen om contant geld in bezit te hebben. Toch wordt uit het dossieronderzoek en de kwantitatieve analyse ook helder dat direct vanaf de rekening van slachtoffers van banking malware goederen, diensten en/of bitcoins worden aangekocht met behulp van de financiële gegevens van het slachtoffer. Daarbij kan van meerdere online dienstverleners gebruik worden gemaakt.

Bij ransomware wordt het losgeld doorgaans in online vouchers of bitcoins geëist. Bij vouchers wordt de waarde van de vouchers doorgaans bijgeschreven op een online account van een e-wallet-dienst, waarna het geld verder kan worden witgewassen. Het is ook mogelijk de vouchers door te verkopen of direct te besteden bij een online dienstverlener. Doorgaans wordt van een combinatie van witwasmethoden gebruikgemaakt. Indien het geld in bitcoins is geëist, kan de organisatie achter de malware trachten de herkomst van de bitcoins te verhullen door gebruikmaking van een mixing service. Uit de empirische oefening is tevens meer informatie verkregen over mixing services en online witwasdiensten die hun diensten beschikbaar stellen via het 'dark web'. Mixing services maken het mogelijk om bitcoins tegen een commissie om te wisselen tegen andere bitcoins. De bitcoins kunnen vervolgens direct worden besteed of worden omgewisseld bij een fysieke bitcoin-handelaar of Bitcoin exchange. Ten slotte zijn er ook gespecialiseerde illegale online dienstverleners die bereid zijn digitale en virtuele betalingsmiddelen tegen een commissie om te ruilen voor een betaling naar keuze.

Uit deze modellen kunnen de volgende actoren worden geïdentificeerd die op enigerlei wijze betrokken zijn bij het witwasproces van crimineel verkre-

gen geld uit banking malware en ransomware: (1) banken, (2) money mules, (3) geldtransfer kantoren, (4) Payment Service Providers, (5) webwinkels, (6) voucherdiensten, (7) e-wallet-diensten, (8) Bitcoin exchanges, (9) mixing services, en (10) Bitcoin-handelaren. Om in kaart te brengen met welke partijen de politie tijdens opsporingsonderzoeken in aanraking zou kunnen komen zijn in dit rapport de kenmerken van deze actoren beschreven. Met behulp van de transactiegegevens over phishing en banking malware is het mogelijk geweest op de meest gedetailleerde wijze de kenmerken van money mules in Nederland in kaart te brengen. Het beeld dat uit de analyses van de datasets naar voren komt, maakt duidelijk dat money mules voornamelijk jongvolwassenen tussen de 18 en 22 jaar zijn uit armere wijken die zich laten ronselen om tegen betaling hun pinpas af te staan. Hoewel jongeren in de achterstandswijken van de drie grote steden (Amsterdam, Rotterdam en Den Haag) oververtegenwoordigd zijn, komen money mules uit alle gemeenten in Nederland. De jongeren hebben relatief vaak een Oost-Europese nationaliteit.

Uit dit onderzoek komt naar voren dat criminelen er in veel gevallen nog steeds voor kiezen om contant geld te gebruiken. Dit komt omdat contant geld snel en anoniem verplaatst kan worden. Daarmee is en blijft contant geld voor hen aantrekkelijk om ongestoord van de opbrengsten van criminaliteit te genieten, ook bij cybercrime. De omvang van witwassen met contant geld is dan ook vele malen groter dan die van witwassen met digitale betalingsmiddelen, waar in deze studie de nadruk op ligt. Of dat in de toekomst zal veranderen, hangt sterk af van de ontwikkelingen rondom digitale betalingsmiddelen en maatregelen die bedrijven en instellingen nemen om witwassen te bestrijden. Daarbij moeten verschillende expertises van politie en justitie worden ingezet om het witwassen met digitale betalingsmiddelen te bestrijden.

Het verdient aanbeveling te overwegen om Nederlandse Bitcoin exchanges te reguleren. Nederlandse Bitcoin exchanges hebben op vrijwillige basis al een uitgebreid palet aan maatregelen genomen om witwassen tegen te gaan. Maar door regulering zouden zij bijvoorbeeld ook een melding aan de Financial Intelligence Unit (FIU) kunnen doen, hetgeen kan bijdragen aan de opsporing van witwassen met virtuele valuta. Het reguleren van bitcoin exchanges blijft echter een uitdaging, gezien het feit dat online betalingsdiensten wereldwijd hun diensten kunnen aanbieden en daarbij gevestigd kunnen zijn in jurisdicties met minder strenge regelgeving of een gebrek aan toezicht of handhaving. Bovendien zijn er ook andere online betalingsdiensten die het mogelijk maken digitale betalingsmiddelen en virtuele om te zetten en zich in jurisdicties vestigen met meer coulante regelgeving en gebrekkig toezicht. Het blijft noodzakelijk dat betalingsdienstverleners technische maatregelen nemen om verdachte transacties zo goed mogelijk te detecteren

en blokkeren. Daarnaast moeten ook andere partijen, inclusief burgers, technische maatregelen nemen om de kwaadaardige software al aan de voorkant van het proces aan te pakken. Concreet kan daarbij gedacht worden aan het monitoren van netwerkverkeer (ook op phishing e-mails). Burgers en organisaties zouden daarbij in de basis een goede cyberhygiëne moeten aanhouden en regelmatig back-ups moeten maken. Daarnaast is het ook van belang het bewustzijn bij computergebruikers over cybercrime, in het bijzonder ransomware, verder te intensiveren door voorlichting te geven.

1 Inleiding

1.1 Aanleiding voor het onderzoek

Dit onderzoek richt zich op het witwassen van de verdiensten die uit cybercrime zijn verkregen. Over het witwassen bij cybercrime is, vergeleken met witwassen bij andere delicten, relatief weinig bekend. De huidige literatuur op het gebied van witwassen richt zich vooral op het witwassen van (contant) geld dat wordt verkregen uit traditionele georganiseerde misdaad, in het bijzonder drugshandel (zie bijvoorbeeld Kleemans et al., 2002; Custers, 2006; Kruisbergen et al., 2012; Soudijn & Akse, 2012; Kruisbergen & Soudijn, 2015). Deze onderzoeksrichting is niet verwonderlijk, aangezien verreweg de meeste verdiensten uit criminaliteit nog steeds in contanten worden verkregen (Europol, 2015a). De vraag is echter of witwassen bij cybercrime hetzelfde werkt als bij andere delicten. In toenemende mate zijn er namelijk aanwijzingen dat bij het witwassen van uit cybercrime verkregen gelden (en overigens ook bij het witwassen van andere criminele opbrengsten) digitale betalingsmiddelen worden gebruikt.

De focus in dit onderzoek ligt op banking malware en ransomware, omdat dit twee van de voornaamste vormen van financiële cybercrime zijn waarmee grote bedragen zijn gemoeid.[2]

Banking malware[3] is, kort gezegd, kwaadaardige software die bedoeld is om geld van slachtoffers afhandig te maken via gemanipuleerde betalingen met internetbankieren. Dit is al jaren een prominente bedreiging op het gebied van cybercrime voor zowel burgers als bedrijven. Cybercriminelen verdienen grote geldbedragen met banking malware (Europol, 2015b, p. 7). In juli 2015 werd bijvoorbeeld bekend dat een groep cybercriminelen met banking malware tussen 2005 en 2014 een bedrag van 100 miljoen euro had verdiend (Sandee, 2015, p. 3).[4] Hoewel de schade uit banking malware in Nederland de afgelopen jaren sterk is gedaald liggen klanten van banken nog dagelijks onder vuur van cybercriminelen.

Ransomware is een andere vorm van cybercrime waarmee steeds meer geld wordt verdiend door cybercriminelen. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist. Sinds 2014 is in Nederland en op mondiaal niveau een sterke stijging in het aantal slachtoffers van ransom-

2 Bovendien is, afgezien van wat banken en opsporingsdiensten vanuit de praktijk hebben onderzocht, tot dusver in Nederland nog betrekkelijk weinig wetenschappelijk onderzoek gedaan naar deze vormen van cybercrime en het witwassen van de daaruit verkregen opbrengsten.

3 De term 'malware' is een samentrekking van de Engelse woorden 'malicious' en 'software'.

4 Zie ook Brian Krebs, 'Inside the $100M 'Business Club' Crime Gang', *Krebsonsecurity.com*, 5 augustus 2015. Beschikbaar op: http://krebsonsecurity.com/2015/08/inside-the-100m-business-club-crime-gang (laatst bezocht op 6 augustus 2015).

ware te zien (CSBN 6, 2016, p. 17).[5] Cryptoware is een bijzonder vervelende variant van ransomware, waarbij niet de computer zelf, maar de bestanden op de besmette computer worden versleuteld.[6] Zodra de versleuteling is voltooid, zijn de bestanden op de geïnfecteerde computer niet meer toegankelijk. Bij ransomware en meer in het bijzonder bij cryptoware, vindt de betaling van het 'losgeld' veelal via de virtuele valuta Bitcoin[7] plaats.

Net als bij andere vormen van criminaliteit is er ook bij cybercrime een behoefte of noodzaak bij daders om de uit criminaliteit verkregen gelden wit te wassen. Immers, als het geld niet is witgewassen, is het minder eenvoudig te besteden aan legale goederen en diensten. Tevens is dan de kans groter voor een crimineel om tegen de lamp te lopen, omdat de herkomst van de gelden kan worden getraceerd. Kenmerkend voor het witwassen van geld dat afkomstig is uit cybercrime is dat het geld door middel van het gebruik van het internet wordt verkregen. Daarna moet dit geld worden witgewassen om het te kunnen besteden. Het verhullen van de illegale oorsprong van het verdiende geld – de essentie van witwassen – brengt daarmee digitale geldstromen op gang die tot op heden nog niet goed in kaart zijn gebracht.

In dit onderzoek wordt nagegaan hoe geld verkregen uit cybercrime wordt witgewassen, welke actoren daarbij een rol spelen en welke rol digitale betalingsmiddelen daarbij spelen. Daarbij wordt nadrukkelijk gekeken of bitcoins en andere virtuele betalingsmiddelen een rol spelen en, zo ja, welke rol dat is. Europol signaleert bijvoorbeeld een verschuiving van de meer traditionele betaalmiddelen naar digitale betalingsmiddelen, zoals Bitcoin, die meer anonimiteit bieden (Europol, 2015b, p. 30).

Dit onderzoek beoogt de werkwijze (modus operandi) en de betrokken actoren bij het witwassen van geld dat wordt verkregen uit cybercrime, in het bijzonder banking malware en ransomware, bloot te leggen. Als het gaat om betrokken actoren, kan niet alleen aan daders en slachtoffers worden gedacht, maar ook aan actoren die het witwassen, al dan niet bewust, faciliteren. Dit zijn onder meer *money mules* ('geldezels' die hun bankrekening ter beschikking stellen) en online financiële dienstverleners, zoals PayPal, Ukash

5 Zie bijvoorbeeld ook: www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise, https://blogs.mcafee.com/mcafee-labs/ransomware-will-rise-2015, https://blog.kaspersky.com/ask-expert-ransomware-epidemic/9332 en www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/the-reign-of-ransomware (laatst geraadpleegd op 23 augustus 2016).

6 Er bestaat dus ook ransomware die geen cryptoware is. In die gevallen blokkeert de ransomware doorgaans de toegang tot het computersysteem zonder dat de bestanden op het computersysteem worden versleuteld.

7 Het is in de literatuur gebruikelijk een hoofdletter te gebruiken voor het woord 'Bitcoin' indien naar het (betalings)systeem zelf wordt verwezen. Een kleine letter voor 'bitcoin' wordt gebruikt indien naar de individuele eenheden van het betalingsmiddel wordt verwezen (zie ook Christopher, 2013, p. 11). Wij sluiten ons bij deze gewoonte aan.

en Bitcoin-handelaren. Deze actoren worden ook wel aangeduid als 'financial facilitators'.[8]

1.2 Onderzoeksvragen

De hoofdvraag van dit onderzoek luidt:

Op welke wijze en door welke actoren wordt geld dat wordt verkregen uit banking malware en ransomware (al dan niet digitaal) witgewassen?
De deelvragen van het onderzoek luiden als volgt:

1 Wat wordt verstaan onder het witwassen van door banking malware en ransomware verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?
2 Wat zijn digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, en hoe werken deze digitale betalingsmiddelen?
3 Op welke wijze en door welke actoren wordt geld witgewassen dat:
   a door middel van banking malware wordt verkregen?
   b door middel van ransomware wordt verkregen?
4 Wat zijn de kenmerken van actoren die betrokken zijn bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?
5 Welke informatie over de modus operandi van actoren, die betrokken zijn het bij het witwassen van geld dat verkregen wordt uit banking malware en ransomware, is beschikbaar op het dark web?
6 Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals bitcoins, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?

Inzicht in het digitaal witwassen van uit cybercrime verkregen geld draagt bij aan het ontwikkelen van strategieën van handhavingsinstanties om cybercrime én witwassen beter te bestrijden. De primaire doelgroep van dit onderzoek bestaat uit degenen die bezig zijn met het opsporen en vervolgen van cybercrime en witwassen, onder meer bij politie, Openbaar Ministerie en banken.[9] Daarnaast is dit onderzoek ook bedoeld voor beleidsmakers, wetenschappers en professionals werkzaam in het domein van cybercrime en witwassen. Om deze bredere doelgroep te faciliteren wordt in hoofdstuk 2 en 3 het fenomeen van banking malware, ransomware, witwassen en digitale betalingsmiddelen (waaronder bitcoins) onderzocht.

8 Merk op dat de term financial facilitators soms enkel wordt gebruikt voor dienstverleners die onder toezicht staan van de financiële toezichthouders. Omdat virtuele valuta doorgaans juist niet onder dit toezicht vallen (zie hoofdstuk 3), is in dit onderzoek een ruimer bereik aan de term financial facilitators toegekend. In het buitenland staan Bitcoin exchanges en/of gecentraliseerde virtuele valuta soms wel onder toezicht.
9 Voor deze doelgroep bevatten hoofdstuk 2 en 3 van dit rapport informatie die mogelijk grotendeels reeds bekend is.

1.3 Onderzoeksmethoden

Het beantwoorden van de bovenstaande hoofdvraag vergt de toepassing van verschillende onderzoeksmethodieken. In dit onderzoek wordt daarom van de volgende onderzoekmethodieken gebruikgemaakt: (1) deskresearch, (2) interviews, (3) dossieronderzoek, (4) het uitvoeren van een experiment waarbij bitcoins zijn aangeschaft en door mixing services zijn gehaald, en (5) een kwantitatieve analyse van transactiegegevens die zijn gerelateerd aan banking malware en phishing.

Door middel van deskresearch, dat wil zeggen een analyse van de beschikbare literatuur en relevante mediaberichten, is de benodigde achtergrondkennis vergaard over (en de onderlinge relatie tussen) (1) cybercrime, (2) witwassen, en (3) digitale betalingsmiddelen. Daarbij is nadrukkelijk ook Amerikaanse literatuur bestudeerd. De reden hiervoor is dat opsporingsautoriteiten in de Verenigde Staten ruime ervaring hebben met zaken waarbij geld verkregen uit cybercrime wordt witgewassen. De literatuuranalyse is tevens bedoeld om de resultaten uit de andere onderzoeksmethoden te valideren.

Daarnaast zijn er twintig interviews afgenomen met experts op het gebied van cybercrime, witwassen en het gebruik van digitale betalingsmiddelen. Deze experts zijn afkomstig uit de opsporingspraktijk, het bankwezen en de sector van digitale betalingsdiensten. In bijlage 2 is een lijst opgenomen met de namen en organisaties van de geïnterviewde personen. De resultaten uit interviews leveren kennis op over het gebruik van digitale betalingsmiddelen voor het digitaal witwassen van geld dat wordt verkregen uit cybercrime.

Ten behoeve van het dossieronderzoek zijn vier zaken onderzocht die betrekking hebben op cybercrime en witwassen. De dossiers zijn beschikbaar gesteld door het Team High Tech Crime en het Openbaar Ministerie. De informatie die uit opsporingsdossiers is verkregen, verschaft de nodige inzichten over daderkenmerken en modi operandi. In bijlage 3 is een lijst opgenomen met een korte beschrijving van de (geanonimiseerde) zaken. Daarbij is ook een overzicht gemaakt van de gebruikte betaalmethoden voor het witwassen van de crimineel verkregen gelden.

Tevens is een 'experiment'[10] uitgevoerd waarbij is nagegaan op welke wijze bitcoins via mixing services op het dark web geanonimiseerd kunnen worden en via online witwasdiensten kunnen worden omgezet in andere valuta. De opzet en resultaten van de empirische oefening zijn in hoofdstuk 4 uiteengezet.

10 Hier moet geen experiment in termen van de Maryland Scientific Methods Scale onder worden verstaan. Daarom wordt het experiment tevens beschreven als 'empirische oefening'.

Ten slotte is een kwantitatieve analyse uitgevoerd op banking malware en phishing-gerelateerde transactiegegevens[11] die door het samenwerkingsverband Electronic Crimes Task Force (ECTF, 2013) beschikbaar zijn gesteld. De dataset betreft transactiegegevens van de vier grootste Nederlandse banken over de jaren 2012-2015. Deze analyse geeft onder meer inzicht in de kenmerken van money mules die betrokken zijn bij het witwassen van verdiensten verkregen uit banking malware. De onderzoeksmethode is beschreven in hoofdstuk 5.

1.4 Opbouw

Het doel van dit onderzoek is om inzicht te verschaffen in de werkwijzen (modi operandi) en de betrokken actoren bij het witwassen van digitaal geld bij verschillende typen van cybercrime. Dit onderzoek richt zich specifiek op twee vormen van cybercrime, namelijk banking malware en ransomware. Het rapport is als volgt opgebouwd.

In hoofdstuk 2 wordt allereerst de benodigde achtergrondinformatie over cybercrime en witwassen gegeven. Tevens wordt uitgebreid ingegaan op de wijze waarop criminelen op illegale wijze geld verkrijgen door middel van banking malware en ransomware.
In hoofdstuk 3 wordt nader ingegaan op de terminologie van digitale betalingsmiddelen en wordt een typologie van virtuele betalingsmiddelen gegeven. Tevens wordt de werking van cryptocurrencies, zoals Bitcoin, uitgelegd.
In hoofdstuk 4 wordt onderzocht op welke wijze geld wordt witgewassen dat door middel van banking malware en ransomware is verkregen. Modellen voor verschillende modi operandi worden in kaart gebracht.
Hoofdstuk 5 richt zich op de kenmerken van de actoren die geïdentificeerd kunnen worden op basis van de in hoofdstuk 4 omschreven modellen. Daarbij wordt in het bijzonder ingegaan op de (achtergrond)kenmerken van money mules, die geïdentificeerd worden als actoren in het witwasproces.
Tot slot wordt in hoofdstuk 6 de hoofdvraag beantwoord en worden de belangrijkste onderzoeksbevindingen besproken. Tevens worden aanbevelingen geformuleerd om het witwassen van gelden die worden verkregen uit banking malware en ransomware tegen te gaan.

11 In de dataset konden de gegevens gerelateerd aan phishing niet worden gescheiden van de gegevens gerelateerd aan banking malware. Zie meer hierover in hoofdstuk 5 en bijlage 5.

2 Cybercrime en witwassen

In dit hoofdstuk wordt nader ingegaan op de fenomenen cybercrime en witwassen. Daarbij wordt bovendien de onderlinge relatie tussen cybercrime en witwassen geanalyseerd. De eerste onderzoeksvraag staat dan ook in dit hoofdstuk centraal: *Wat wordt verstaan onder het witwassen van door cybercrime verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?* Dit hoofdstuk is hoofdzakelijk bedoeld om basiskennis te verschaffen over banking malware, ransomware en witwassen, hetgeen noodzakelijk is om het witwasproces te doorgronden.

Dit hoofdstuk is als volgt opgebouwd. In paragraaf 2.1 wordt kort geanalyseerd wat in de literatuur wordt verstaan onder cybercrime. Paragraaf 2.2 gaat dieper in op wat banking malware is en hoe het werkt. In paragraaf 2.3 wordt ingegaan op wat ransomware is en hoe het werkt. Daarna wordt in paragraaf 2.4 een typologie van witwassen gegeven, waarbij rekening wordt gehouden met cybercrime als onderliggend misdrijf. In paragraaf 2.5 wordt de onderlinge relatie tussen cybercrime en witwassen beschreven. Het hoofdstuk wordt afgesloten met paragraaf 2.6, waarin de eerste onderzoeksvraag wordt beantwoord.

2.1 Typologie van cybercrime

Cybercrime kan als volgt worden gedefinieerd: 'misdrijven gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen'.[12] Door deze definitie van cybercrime te gebruiken, komt goed naar voren dat cybercrime in dit onderzoek beperkt is tot de zogenoemde 'computergerichte delicten' en 'computergerelateerde delicten' (Koops, 2014, p. 214).[13] Computergerichte delicten, in het Engels 'target cybercrimes' genoemd, zijn misdrijven die zijn gericht op de integriteit, vertrouwelijkheid en beschikbaarheid van computersystemen.[14] De onderzochte target cybercrimes in dit onderzoek, het gebruik van banking malware en ransomware, worden in paragraaf 2.3 en 2.4 verder belicht. Bij computergerelateerde delicten, in het Engels 'tool cybercrimes' genoemd, spelen internet en computers een faciliterende rol. Het kan daarbij ook gaan om traditionele delicten die een nieuwe verschijningsvorm

12 Zie Mededeling van de Commissie aan het Europees Parlement van 22 mei 2007, 'Naar een algemeen beleid voor de bestrijding van cybercriminaliteit', COM(2007) 267. Zie bijvoorbeeld Hulst en Van der Neve (2008) voor een overzicht van andere definities van cybercrime.

13 Charney (1994, p. 489) heeft de driedeling gemaakt tussen (1) computergerichte criminaliteit, (2) computergerelateerde criminaliteit en (3) computercriminaliteit waarbij computers incidenteel zijn aan de criminaliteit. Deze categorisering is op haar beurt geïnspireerd door het onderscheid in computercriminaliteit zoals dat is aangebracht door Parker (1976, p. 17-22). De derde categorie van computercriminaliteit heeft betrekking op misdrijven waarbij digitaal bewijs dat kan worden gevonden op computers of het internet slechts een incidentele rol speelt. Deze derde categorie wordt in dit onderzoek dus niet nadrukkelijk meegenomen.

14 Zie bijvoorbeeld Koops, 2007, p. 35 en titel 1 van het Cybercrimeverdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken), ondertekend te Boedapest op 23 november 2001 (*Trb.* 2002, 18).

op internet krijgen, zoals drugshandel, bedreiging, afpersing of smaad. Het witwassen van digitaal of virtueel geld, waarbij het geld wordt omgezet in andere digitale of virtuele valuta, kan ook worden beschouwd als een tool cybercrime. Het delict witwassen wordt in paragraaf 2.4 verder onderzocht.

De Nederlandse wetgever lijkt sinds de jaren negentig de term 'computercriminaliteit' te prefereren (Koops, 2014, p. 214). Dat is te verklaren doordat in de jaren tachtig en negentig de nadruk lag op computers zelf, terwijl inmiddels de nadruk ligt op computernetwerken (idem). Wij prefereren daarom de term 'cybercrime'. Het voorvoegsel 'cyber' illustreert goed dat computers en het internet als netwerk een nadrukkelijke rol spelen bij deze vorm van criminaliteit.[15] Bovendien is de term cybercrime breed geaccepteerd in de Nederlandse en internationale literatuur en wordt deze ook in het invloedrijke Cybercrimeverdrag van de Raad van Europa gebruikt (Clough, 2010, p. 9; Kaspersen, 2007, p. 180-182).

Zoals hierboven is opgemerkt, beperkt de aangehouden definitie van cybercrime zich tot de target cybercrimes en de tool cybercrimes. Deze twee vormen van cybercrime worden hieronder kort toegelicht.

2.1.1 Target cybercrimes

Computervredebreuk, in het Engels ook wel 'hacken' genoemd, vormt het meest voor de hand liggende voorbeeld van een target cybercrime.[16] Bij het delict computervredebreuk wordt zich kortgezegd ongeautoriseerd toegang verschaft tot computers.[17] Bij de term computer moet niet alleen worden gedacht aan een pc of laptop. Steeds meer apparaten met enige rekenkracht worden aan het internet verbonden. Deze tendens wordt ook wel het 'internet of things' genoemd.[18] Als gevolg van deze tendens zijn ook steeds meer apparaten kwetsbaar voor aanvallen van buitenaf (CSBN 4, 2014, p, 77-80).

Het zich ongeautoriseerd toegang verschaffen tot computers kan op veel verschillende manieren plaatsvinden. Daarbij kan worden gedacht aan verschillende tactieken: men kan zich toegang verschaffen door met een slimme list het slachtoffer inloggegevens afhandig te maken, door met computerkracht een wachtwoord te kraken, of door misbruik te maken van kwetsbaarheden in software op computers (Bernaards, Monsma & Zinn, 2012, p. 29-34).

15 Het Oxford woordenboek definieert het voorvoegsel cyber ook wel als: '*Relating to or characteristic of the culture of computers, information technology, and virtual reality: the cyber age*' (zie www.oxforddictionaries.com/us/definition/english/cyber, laatst geraadpleegd op 7 oktober 2015).

16 Computervredebreuk is strafbaar gesteld in artikel 138ab Sr.

17 Binnen het strafrecht wordt de term 'geautomatiseerd werk' aangehouden voor computers. Het begrip is gedefinieerd in artikel 80sexies Sv. Wij houden de term 'computer' aan, omdat deze term in het normale taalgebruik wordt gebezigd.

18 Zie bijvoorbeeld Atzoria, Ierab en Morabito (2010) voor meer informatie over het 'internet of things'.

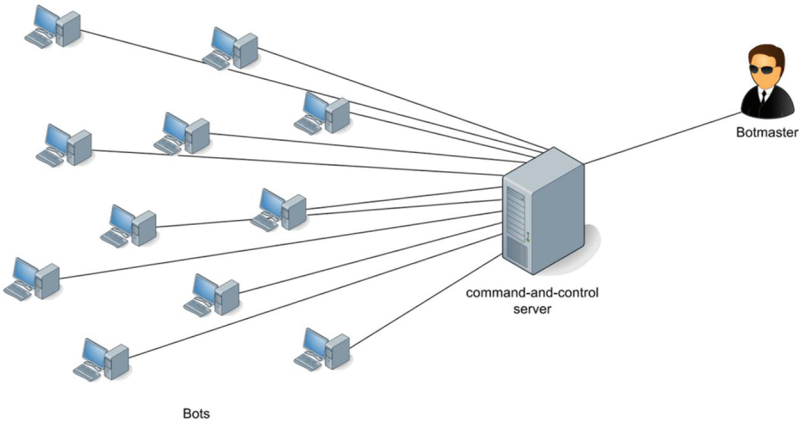
Daders kunnen ook gebruikmaken van kwaadaardige software om zich op afstand ongeautoriseerd toegang te verschaffen tot een computer. Deze kwaadaardige software wordt vaak omschreven met de Engelse term 'malware', een samenvoeging van de Engelse termen 'malicious' en 'software' (Bernaards, Monsma & Zinn, 2012, p. 35). Het maken en verspreiden van kwaadaardige software, alsmede het bezit ervan teneinde de software te gebruiken voor criminele doeleinden, is strafbaar gesteld in Nederland.[19]

Malware kan worden geprogrammeerd met veel verschillende functionaliteiten. Met name kan gedacht worden aan (1) het vastleggen van toetsaanslagen (de 'keylogging'-functie), (2) het zich op afstand via een achterdeurtje toegang verschaffen tot de computer (de 'backdoor'-functie) en (3) het aanzetten van verschillende functionaliteiten van de computers, zoals de webcam of microfoon (Bernaards, Monsma & Zinn, 2012, p. 36). Ook kan met zogeheten Remote Administration Tools (RATs) een computersysteem op afstand (totaal) worden overgenomen. In paragraaf 2.3 en paragraaf 2.4 wordt verder ingegaan op de functionaliteiten van twee specifieke vormen van malware, namelijk banking malware en ransomware. Deze typen cybercrime zijn geselecteerd omdat dit twee van de voornaamste vormen van financiële cybercrime zijn, waarmee criminelen grote bedragen verdienen die ze vervolgens willen witwassen.

Computers die besmet zijn met malware en door een derde op afstand via een andere computer kunnen worden aangestuurd, worden onderdeel van een botnet (Bernaards, Monsma & Zinn, 2012, p. 45). Figuur 2.1 visualiseert een (eenvoudige) infrastructuur van een botnet.

19 Zie artikel 350a Sr voor de strafbaarstelling van het verspreiden van malware en installeren van malware op geautomatiseerde systemen. In artikel 139c Sr is het aftappen en/of opnemen van gegevens strafbaar gesteld. Het produceren van malware is strafbaar op grond van artikel 139d lid 2 sub a Sr. In artikel 139d lid 2 sub b en lid 3 Sr wordt ten slotte ook het bezit of verspreiden van de apparatuur strafbaar gesteld.

Figuur 2.1 Visualisatie van een eenvoudig botnet



Bron: Hogben (2011, p. 16)

Botnets kunnen worden omschreven als de werkpaarden van cybercriminelen. Botnets maken het mogelijk voor criminelen om de besmette computers te besturen en bieden via het 'command & control-centrum' snel overzicht van de besmette computers en vergaarde gegevens.

2.1.2 Tool cybercrimes

Tool cybercrimes vormen een categorie van cybercrime waarbij computers en internet een faciliterende functie hebben. Computers en internet vormen daarbij het instrument van de dader om het delict te plegen.

Het plegen van oplichting en fraude vindt bijvoorbeeld in toenemende mate via internet plaats (Clough, 2010, p. 372-373). Oplichting via internet vindt ook geregeld plaats via 'phishing'. Phishing is een vorm van oplichting waarbij criminelen hengelen naar de persoonlijke gegevens van mensen om deze later te misbruiken (Bernaards, Monsma & Zinn, 2012, p. 58).[20] Respondenten van ons onderzoek gaven aan dat phishing in de loop der jaren is geprofessionaliseerd (zie ook CSBN 4, 2014, p. 34; CSBN 5, 2015, p. 51; CSBN 6, 2016, p. 45).[21] Mensen wordt al jaren via goed nagemaakte e-mails van banken bijvoorbeeld verzocht een kopie van de bankwebsite te bezoeken en hun account te verifiëren. Nadat mensen hun naam en rekeninggegevens hebben ingevoerd, worden ze opgebeld door zogenaamde bankmedewerkers. In dit

20 Phishing is ook strafbaar gesteld als een vorm van oplichting (art. 326 Sr). Zie ook *Kamerstukken II,* 2015/16, 34 372, nr. 3, p. 62-64.

21 Zie ook het persbericht 'Criminelen perfectioneren phishingmethodes' van 29 september 2015. Beschikbaar op www.nvb.nl/nieuws/2015/4344/criminelen-perfectioneren-phishingmethodes.html (laatst geraadpleegd op 9 oktober 2015).

gesprek bewegen de criminelen die zich voordoen als bankmedewerkers hun slachtoffers tot het noemen van hun pincode of zelfs het verrichten van de (frauduleuze) betalingstransactie.[22] Deze modus operandi wordt *social engineering* genoemd. 'Spear-phishing' is een variant op phishing waarbij een gerichte aanval op een individu of bedrijf wordt uitgevoerd met behulp van persoonlijke informatie die al bij de aanvallers bekend is (Bernaards, Monsma & Zinn, 2012, p. 58-59). Aangezien hier meestal geen malware in het spel is, wordt deze vorm van bankfraude verder niet specifiek onderzocht in dit onderzoek, maar enkel als onderdeel van een ruimere modus operandi, bijvoorbeeld in het geval dat eerst banking malware wordt geïnstalleerd en vervolgens met behulp van social engineering bankgegevens worden ontfutseld aan slachtoffers.[23] Het witwassen van digitaal of virtueel geld, waarbij het geld wordt omgezet in andere digitale or virtuele valuta, kan ook worden beschouwd als een tool cybercrime, omdat computers en internet in dat geval het instrument vormen om het delict te plegen. Uit jurisprudentie blijkt ook dat criminelen die door middel van malware frauduleuze overboekingen maken, worden veroordeeld voor het traditionele delict diefstal.[24]

2.2 Banking malware

Banking malware is kwaadaardige software die is gericht op het uitvoeren van frauduleuze banktransacties via de computer van het slachtoffer. Door middel van een korte analyse van de kenmerken van een van de populairste soorten banking malware die in de afgelopen jaren in omloop was, genaamd ZeuS, kan een algemeen beeld worden gegeven van de werking en functionaliteiten van banking malware.

De ZeuS-malware werd in 2006 op webfora voor het eerst aangeboden door een crimineel met de nickname 'Slavik'. Sinds 2006 heeft de malware verschillende evoluties doorgemaakt en zijn functionaliteiten toegevoegd (Sandee, 2015). ZeuS-malware is in het recente verleden bijzonder succesvol geweest in het uitvoeren van frauduleuze transacties op online banking websites (Falliere & Chien, 2009).

De kwaadaardige software was in het bijzonder zo succesvol door gebruikmaking van de zogenoemde 'webinject'-techniek. Met de webinject-techniek

22 Zie bijvoorbeeld: Rb. Den Haag, 15 juli 2016, ECLI:NL:RBDHA:2016:7981.

23 Respondenten geven aan dat steeds vaker het midden- en kleinbedrijf (mkb) slachtoffer wordt van spear-phishing-aanvallen. Daarbij is denkbaar dat bijvoorbeeld uit naam van een manager van een bedrijf een phishing e-mail wordt gestuurd naar medewerkers van dat bedrijf met het verzoek een bijlage te openen of een website te bezoeken. Vervolgens wordt de computer van een slachtoffer besmet met een zogenoemde 'Remote Administration Tool' (RAT). Een RAT is een kwaadaardige vorm van software waarbij de dader op afstand de computerhandelingen van het slachtoffer kan volgen (zie ook Europol, 2015b, p. 21-25).

24 Zie ook Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041, Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.

maakt de ZeuS-malware het mogelijk om de webbrowser van besmette computers te manipuleren (Sandee, 2015, p. 16-18).[25] Op het moment dat het slachtoffer bijvoorbeeld de naam van een grote Nederlandse bank invoert, herkent de malware de URL en wordt het slachtoffer doorgestuurd naar een website die door de crimineel is gebouwd (zie ook Bernaards, Monsma & Zinn, 2012, p. 43). Deze websites zijn nauwelijks te onderscheiden van de echte websites voor internetbankieren (online bankieren).[26] Op het moment dat het slachtoffer geld overmaakt, worden op de achtergrond het geldbedrag en de ontvanger door de crimineel gewijzigd.[27] Dit type aanval wordt ook wel een 'man in the browser'-aanval genoemd.[28] Met een wachtscherm wordt het slachtoffer virtueel aan het lijntje gehouden, terwijl de criminelen een andere transactie klaarzetten en uitvoeren met de afgevangen inloggegevens. Daarbij kunnen zelfs authenticatiecodes worden gestolen door criminelen. Naast een inlognaam of wachtwoord is ook een tweede ondertekeningscode noodzakelijk om in te loggen op de online bankieromgeving bij Nederlandse banken. De ondertekeningscode verschilt per bank. Het kan bijvoorbeeld een sms-code betreffen of een cijfercode die wordt gegenereerd op een speciaal daarvoor bestemd apparaat.[29] Om het afvangen van de extra authenticatie te bewerkstelligen moet daarbij soms wel direct contact worden gezocht met de slachtoffers. De criminelen maken daarvoor gebruik van een chatscherm of een ander pop-upscherm, teneinde het slachtoffer zo ver te krijgen de benodigde authenticatiegegevens over te dragen aan de criminelen (Sandee, 2015, p. 17-18).[30] De webinjects en nep-e-mails zijn vaak lastig van echt te onderscheiden wanneer mensen gaan internetbankieren.

Net als veel andere banking malware was ZeuS niet alleen gericht op het afhandig maken van inloggegevens voor online bankieren (Binsalleeh et al., 2010, p. 31). De software kon ook andere persoonsgegevens vergaren door het uitvoeren van aanvallen op basis van bepaalde sleutelwoorden, zoals de namen van populaire elektronische communicatiediensten en betalingsdiensten (Binsalleeh et al., 2010, p. 32).[31] Bovendien bood ZeuS de functionaliteit om – tegen betaling – andere malware van andere criminelen op de besmette computer te plaatsen voor verdere exploitatie van de slachtoffers (Sandee, 2015, p. 4-5).

25 Zie voor de werking van de ZeuS-malware ook Tajalizadehkoob, 2013.
26 Vaak is de URL (het webadres) in de adresbalk wel een aanwijzing of een internetgebruiker op de juiste website zit, maar verschillen kunnen erg klein zijn, bijvoorbeeld robobank.nl versus rabobank.nl.
27 Deze werkwijze wordt in twee recente uitspraken over banking malware bevestigd. Zie: Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.
28 Zie meer uitgebreid Tajalizadehkoob, 2013, p. 25.
29 Bij ING gaat het bijvoorbeeld om een TAN-code via de sms en bij de Rabobank om een code via een random reader of raboscanner: een apparaatje waarin de pinpas wordt gestoken.
30 Mensen bewegen zulke informatie te verstrekken kan onder andere plaatsvinden door hen te misleiden, hen te bedreigen, medelijden op te wekken of hen nieuwsgierig te maken.
31 Zie voor de selectie van de diensten die worden aangevallen ook uitgebreid Tajalizadehkoob (2013).

Uniek aan het ZeuS-onderzoek is dat een beeld is verkregen van de organisatiestructuur achter de banking malware.[32] De ZeuS-organisatie werd geleid door twee individuen, waarvan één de eerder genoemde 'Slavik' was, die is geïdentificeerd als Jevgeni Michailovitsj Bogatsjev (Sandee, 2015, p. 6). Slavik was tevens de vermoedelijke schrijver van de kwaadaardige software. Voor de exploitatie van de software bestond de organisatie uiteindelijk (in 2014) uit meer dan vijftig personen (Sandee, 2015, p. 5). De organisatie bestond niet uit een hiërarchisch model van criminelen die fysiek bij elkaar samenkwamen. In plaats daarvan kwamen de criminelen online samen op basis van de werkzaamheden die op dat moment uitbesteed moesten worden.[33] De organisatie achter ZeuS was zeer professioneel (Sandee, 2015, p. 6-7). De exploitatie van malware werd uitbesteed aan mensen die de individuele botnets bestuurden (de 'botherders') (zie Hogbenet al., 2011, p. 21). Het infecteren van de computers zelf werd uitbesteed aan andere criminelen. Daarnaast werd veel geld uitgegeven aan bullet proof hosting providers om de servers waarop de command & control-servers van de botnets draaiden zoveel mogelijk onzichtbaar en stabiel te houden (Sandee, 2015, p. 15). Met een efficiënt werkproces wisten de criminelen over de gehele wereld slachtoffers te maken en frauduleuze transacties uit te voeren met online bankieren. Door zich in het oosten van Rusland te vestigen, kon de werkdag worden begonnen met het aanvallen van banken in Australië en worden afgesloten met het aanvallen van banken in de Verenigde Staten.[34] Op die manier werd in totaal een geschatte hoeveelheid van 100 miljoen dollar tussen 2006 en 2014 door de criminelen 'verdiend'. De operatie werd beëindigd door het ontmantelen van de complexe botnetinfrastructuur door de FBI in samenwerking met private partijen in de zomer van 2014. Slavik, zoals gezegd een van de leiders van de organisatie, is nog voortvluchtig.[35]

Verschillende auteurs wijzen op een trend waarbij sprake is van toenemende professionaliteit van de organisaties achter de exploitatie met malware, waarbij de daders gespecialiseerde rollen hebben binnen deze '*malware economy*' (Bauer et al., 2008, p. 8; Hogben et al., 2011, p. 21; De Graaf, Shosha & Glady-

32 Inzicht in de organisatie achter het ZeuS-netwerk werd onder andere verkregen uit de chatlogs tussen criminelen. De criminelen die het ZeuS-netwerk exploiteerden, communiceerden in dit geval via het chatprogramma Jabber. Het netwerkverkeer wordt in dat geval ook versleuteld, waardoor het lastig of onmogelijk is de inhoud van het verkeer te ontsleutelen. Echter, aangezien in dit geval toegang werd verschaft tot logs van de chatgesprekken, kon wel bewijs worden verzameld op basis van de communicaties tussen de criminelen.

33 Of, in de woorden van Brian Krebs, 'Inside the $100M 'Business Club' Crime Gang', *Krebsonsecurity.com*, 5 augustus 2015: *'In true Oceans 11 fashion, each Business Club member brought a cybercrime specialty to the table, including 24/7 tech support technicians, third-party suppliers of ancillary malicious software, as well as those engaged in recruiting 'money mules' — unwitting or willing accomplices who could be trained or counted on to help launder stolen funds.'*

34 Zie Brian Krebs, 'Inside the $100M 'Business Club' Crime Gang', *Krebsonsecurity.com*, 5 augustus 2015. Beschikbaar op: http://krebsonsecurity.com/2015/08/inside-the-100m-business-club-crime-gang (laatst geraadpleegd op 6 augustus 2015).

35 Zie FBI press release, 'U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator', 2 juni 2014. Beschikbaar op: www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator (laatst geraadpleegd op 9 maart 2016).

shev, 2012, p. 1; Soudijn & Zegers, 2012, p. 114-115). In Nederland zijn in juni en juli 2016 tevens verdachten veroordeeld voor lidmaatschap van een criminele organisatie waarbij banking malware werd gebruikt om frauduleuze transacties uit te voeren en het geld vervolgens werd witgewassen. De rechters spraken hier ook wel van een samenwerking tussen criminelen waarbij enkelen het technische gedeelte (het ontwikkelen van de malware, de infectie en onderliggende infrastructuur) voor hun rekening nemen en anderen het financiële gedeelte (het witwassen van de overboekingen) voor hun rekening nemen.[36] Europol beschrijft in haar toekomstbeeld van georganiseerde criminaliteit een trend waarbij losse netwerken van individuen tijdelijk samenkomen in een gedeelde digitale omgeving om samen te werken en criminaliteit te plegen (Europol, 2015c, p. 11). Dit beeld wordt ook bevestigd in de interviews die zijn afgenomen met cybercrime-experts.

2.3 Ransomware

Ransomware is een verzamelnaam voor kwaadaardige software die toegang tot een computer of bestanden daarop blokkeert, waarna criminelen losgeld eisen van de slachtoffers. Slechts na betaling wordt de software – als de criminelen daartoe bereid zijn – verwijderd van de geïnfecteerde computer.

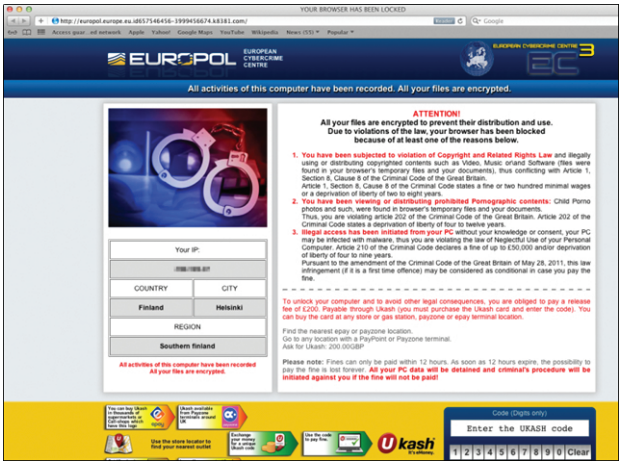
Computers worden doorgaans besmet met ransomware door het bezoeken van een website. Een computergebruiker kan bijvoorbeeld via een link in een phishing e-mail of socialemediadienst worden verwezen naar de besmette website. Bij het bezoek aan de website wordt een computergebruiker op de achtergrond naar een pagina doorgeleid waarop een zogenaamde exploit-kit de kwetsbaarheden op de computer van die gebruiker verkent (CSBN 5, 2015, p. 36). Kwetsbaarheden komen bijvoorbeeld veelvuldig voor op verouderde versies van Java-software of Adobe-software. Vervolgens wordt de malware op de achtergrond door middel van een '*drive-by-download*' op de computer geïnstalleerd. Ook is het mogelijk dat een computergebruiker direct via een bijlage in e-mails met ransomware wordt besmet.

Sinds 2015 is in Nederland een grote toename waarneembaar van de cryptoware-varianten van ransomware (CSBN 5, 2015, p. 9; CSBN 6, 2016, p. 17). Bij cryptoware worden de bestanden op de geïnfecteerde computer versleuteld via encryptie. Zodra de encryptie is voltooid, wordt de computer geblokkeerd. Met name bij cryptoware kan de toegang tot bestanden moeilijk worden verkregen zonder betaling van het losgeld – de malware is doorgaans wel te verwijderen, maar de encryptie is vaak lastig te kraken.

36 Zie Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.

Een inmiddels verouderd type ransomware vergrendelt alleen het besturingssysteem van het slachtoffer. Het slachtoffer wordt vervolgens met een dreigende tekst onder druk gezet om een betaling te verrichten om van de kwaadaardige software af te komen.[37] Het komt voor dat het bericht van de ransomware verwijst naar websites die door het slachtoffer bezocht zijn, waarbij vooral pornosites worden weergegeven. Daarbij wordt ingespeeld op het schuld- en schaamtegevoel van slachtoffers (CSBN 4, 2014, p. 84). Ook komt het voor dat de criminelen het slachtoffers beschuldigen van het bezit van kinderporno, waarbij zelfs een kinderpornoafbeelding wordt getoond. Door middel van een betaling zouden gebruikers van de software af kunnen komen. Figuur 2.2 is een illustratie van een ransomware-variant die een nepbericht laat zien dat zogenaamd van Europol afkomstig is. Door middel van een betaling via een vouchercode van Ukash zou de besmetting ongedaan kunnen worden gemaakt.

Figuur 2.2 Voorbeeld van ransomware door middel van misbruik van naam politieorganisatie



Bron: https://malwaretips.com/blogs/wp-content/uploads/2013/07/Europol-MAC-OS-X-virus.png

Na infectie met *cryptoware* worden enkele bestanden of de gehele harde schijf door de kwaadaardige software met een sterke encryptie versleuteld. Ook gedeelde netwerkmappen op geïnfecteerde computers worden geïnfecteerd. Merk op dat het belangrijkste verschil tussen ransomware en cryptoware is dat cryptoware gebruikmaakt van sterke versleutelingstechnieken, terwijl bij ransomware 'slechts' een besturingssysteem of webbrowser tijdelijk onbruikbaar wordt gemaakt. Cryptoware maakt meestal gebruik van asymmetrische encryptie. Dat betekent dat een sleutel gebruikt wordt voor

37 Overigens kan de ransomware ook slechts een vervelende screenlocker betreffen, die bij het opnieuw opstarten van de computer al is verdwenen.

het versleutelen van bestanden en een andere sleutel nodig is voor het ontsleutelen van bestanden. Toegepast op malware betekent dit dat de sleutels uniek worden gegenereerd voor een slachtoffer en dat de sleutel die wordt gebruikt om de computer te ontsleutelen slechts beschikbaar is op de computer van de dader (Intel Security, 2015, p. 16). Zonder de sleutel om de computer te ontsleutelen staan de slachtoffers vaak met lege handen.

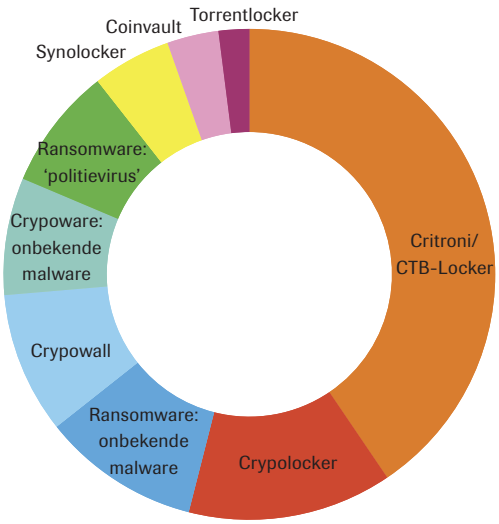
De vraag is uiteraard waarom slachtoffers het losgeld zouden betalen. Als slachtoffers geen back-up hebben van hun bestanden en ze toch veel waarde hechten aan de bestanden (bijvoorbeeld in het geval van financiële gegevens of familiefoto's), blijkt er vaak een zekere bereidheid te bestaan het losgeld te betalen. Uit onderzoek blijkt dat circa 10% van de Nederlandse aangevers zegt betaald te hebben om toegang tot bestanden terug te krijgen (CSBN 5, 2015, p. 12). Uiteraard biedt betaling van het losgeld geen garantie dat de toegang tot de computer of de bestanden wordt vrijgegeven, hoewel de decryptiesleutel in de regel daadwerkelijk wordt afgegeven.[38] De politie raadt het betalen van losgeld na besmetting met ransomware af om zo het verdienmodel van cybercriminelen tegen te gaan en nieuwe aanvallen te voorkomen.[39]

Een voorbeeld van een populaire en relatief geavanceerde vorm van cryptoware is CTB-Locker. CTB-Locker wordt verspreid via internet sinds medio 2014. Het Nationaal Cyber Security Centrum (NCSC) geeft in zijn Cyber Security Beeld Nederland (CSBN) 5 een overzicht van de verschillende typen ransomware in Nederland (figuur 2.3).

38 Indien dit niet standaard zou gebeuren, zou het verdienmodel van de cybercriminelen niet werken.

39 Zie ook het artikel 'ransomware' op de website van de politie, beschikbaar op: www.politie.nl/themas/ransomware.html (laatst geraadpleegd op 19 februari 2016). Zie ook de website www.nomoreransom.org/ransomware-qa.html (laatst geraadpleegd op 4 augustus 2016). Op deze website wordt burgers tevens de mogelijkheid geboden om de decryptiesleutels van bepaalde typen ransomware te downloaden om hun computers te ontsleutelen.

Figuur 2.3 Diagram van ransomware-typen in Nederland



Bron: CSBN 5, 2015, p. 35

Het overzicht in figuur 2.3 is in 2015 door het NCSC geproduceerd op basis van 87 aangiftes die bij de politie zijn gedaan. De slachtoffers van cryptoware variëren sterk. Het NCSC geeft aan dat kantoorautomatiseringsomgevingen vaak worden getroffen door de malware. Infecties hebben onder andere plaatsgevonden bij de gemeentes Dronten, Lochem en Den Haag en Rijkswaterstaat (CSBN 5, 2015, p. 17). Uit het bovenstaande diagram blijkt dat de meeste aangiftes betrekking hadden op infecties met het type CTB-Locker. Daarom wordt dit type van cryptoware hieronder apart toegelicht.

CTB-Locker verspreidt zich net als andere cryptoware via e-mail, waarbij de verzender zich voordoet als een financiële instelling met een zogenaamd betalingsformulier als bijlage.[40] Direct na de infectie wordt een bericht aan de computergebruikers gepresenteerd met een eis voor losgeld dat moet worden betaald via de virtuele valuta Bitcoin.[41]

40 Zie Klijnsma, Y. (2015). 'The state of ransomware in 2015', 7 september 2015, Blog Fox-IT. Beschikbaar op: http://blog.fox-it.com/2015/09/07/the-state-of-ransomware-in-2015 (laatst geraadpleegd op 14 september 2015). Zie ook voor een technische beschrijving van de malware 'TR-33 Analysis – CTB-Locker / Critroni', van het Computer Incident Response Center Luxembourg. Beschikbaar op: www.circl.lu/pub/tr-33/#ctb-locker-commands-and-states (laatst geraadpleegd op 14 september 2015). Intel Security geeft aan dat CTB-Locker ook is verspreid via IRC-chat, peer-to-peer netwerken en nieuwsgroepen (Intel Security, 2015, p. 5).

41 Zie bijvoorbeeld Goodin, D. (2013). 'You're infected — if you want to see your data again, pay us $300 in Bitcoins', 17 oktober 2013, *Ars Technica*. Beschikbaar op: http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/ (laatst geraadpleegd op 14 september 2015), Krebs, B. (2014). '2014: The Year Extortion Went Mainstream', 14 juni 2014, *Krebs on Security*. Beschikbaar op: www.krebsonsecurity.com/2014/06/2014-the-year-extortion-went-mainstream (laatst geraadpleegd op 14 september 2015), en redactie Blauw, 'Bits en bytes in plaats van vuisten', *Blauw,* nr. 2, 2015, p. 39.

Het bericht met de eis voor losgeld bij CTB-Locker is weergegeven in figuur 2.4. Op het scherm is te lezen dat binnen 96 uur een betaling moet worden gedaan en staat een link voor verdere instructies voor de betaling van het losgeld.

Figuur 2.4 Een voorbeeld van het computerscherm dat een slachtoffer van de CTB-Locker-malware te zien krijgt

Bron: www.circl.lu/pub/tr-33/#ctb-locker-commands-and-states

Gebruikers van computers die besmet zijn met cryptoware hebben soms nog wel de mogelijkheid door te surfen naar een website om de betaling uit te voeren. Bij CTB-Locker wordt daarvoor verbinding gemaakt via het Tor-netwerk naar een instructiepagina om de betaling tot stand te brengen (CSBN 5, 2015, p. 36).

Bij CTB-Locker wordt het instructiescherm voor de betaling weergegeven in figuur 2.5. In het geval van CTB-Locker wordt afhankelijk van het land waar het slachtoffer verbinding met het internet maakt een bericht in het Russisch, Engels, Italiaans, Nederlands, Duits, Spaans, Frans of Lets gepresenteerd.[42]

42 De computer wordt versleuteld met een bijzonder sterk algoritme. Zie de blog van Massimiliano Felici, 'CTB-Locker encryption/decryption scheme in details', 27 februari 2015. Beschikbaar op: https://zairon.wordpress.com/2015/02/17/ctb-locker-encryptiondecryption-scheme-in-details (laatst geraadpleegd op 14 september 2015). Opvallend is dat de CTB-Locker-malware geen internetverbinding nodig heeft om na infectie de computer te versleutelen.

Figuur 2.5 Een voorbeeld van het betalingsscherm van de CTB-Locker-malware met daarin het Bitcoin-adres waarnaar het losgeld moet worden overgemaakt

Bron: www.circl.lu/pub/tr-33/#ctb-locker-commands-and-states

Slechts na betaling met bitcoins kan de decryptiesoftware worden gedownload en de computer worden ontsleuteld. Indien geen betaling plaatsvindt of de criminelen hun belofte niet nakomen, hebben consumenten na infectie bijvoorbeeld geen toegang meer tot hun documenten en foto's op geïnfecteerde computers en gegevensdragers. Bedrijven en overheidsinstellingen kunnen zelfs tijdelijk niet meer hun werkzaamheden uitvoeren indien de werkcomputers en netwerkschijven zijn versleuteld.[43] Cryptoware kan namelijk ook virtuele harde schijven, externe harde schijven, USB-sticks en backupschijven infecteren (CSBN 6, 2016, p. 11).[44]

Waar het NCSC in 2014 nog kon stellen dat geen grootschalige infecties met cryptoware hadden plaatsgevonden, is dat nu niet meer mogelijk. Infecties met cryptoware bij Nederlandse overheidsinstellingen zijn sinds 1 januari 2015 regelmatig in het nieuws gekomen.[45] In het meest recente Cyber Security Beeld wijst het NCSC op een sterke groei van het probleem van ransom-

43 Zie Hartholt, S. (2015). 'Friese gemeenten getroffen door ransomware', *Binnenlands Bestuur*, 9 juni 2015. Beschikbaar op: www.binnenlandsbestuur.nl/digitaal/nieuws/friese-gemeenten-getroffen-door-ransomware.9478427.lynkx (laatst geraadpleegd op 16 juni 2015).

44 Het NCSC merkt daarbij op dat het bereik van de versleuteling afhangt van de privileges van de getroffen gebruikers binnen een netwerk.

45 Zie ANP, 'Steeds meer besmettingen met cryptoware in Nederland', Nu.nl, 16 maart 2015. Beschikbaar op www.nu.nl/internet/4011877/steeds-meer-besmettingen-met-cryptoware-in-nederland.html (laatst geraadpleegd op 18 augustus 2015); ANP, 'Overheid vaker doelwit cyberaanval', 13 augustus 2015, NU.nl. Beschikbaar op: www.nu.nl/internet/4105537/overheid-vaker-doelwit-cyberaanval.html (laatst geraadpleegd op 18 augustus 2015). Zie ook CSBN 5 (2015, p. 17).

ware en in het bijzonder cryptoware in Nederland (CSBN 5, 2016, p. 17). Respondenten van de interviews geven ook aan dat het probleem van cryptoware zal groeien, omdat de technologie van versleuteling inmiddels is geperfectioneerd en relatief eenvoudig geld kan worden verdiend met de malware.

2.4 Typologie van witwassen

In de literatuur bestaat geen eenduidige definitie voor witwassen. Uit literatuuronderzoek van Unger (2006, p. 30-35) blijkt bijvoorbeeld dat er 18 definities te vinden zijn (Van Koningsveld, 2008, p. 88-104; Gelemerova, 2011, p. 59 e.v.). Dit geeft aan hoe onduidelijk het begrip is. Er zijn echter wel twee kernaspecten, namelijk het verbergen of verhullen van de illegale herkomst van gelden of voorwerpen en het uitgeven van die opbrengsten (deels) in de bovenwereld. Om confiscatie te voorkomen zullen criminelen via het witwasproces het geld willen onttrekken aan het zicht van politie, justitie en de Belastingdienst (Kleemans et al., 2002, p. 127).[46]

Voordat kan worden ingegaan op de relatie tussen cybercrime en witwassen, is het van belang om een beeld te krijgen van de verschillende witwasmethoden. Op deze manier wordt de werkwijze van criminelen duidelijker en kan een onderscheid worden gemaakt tussen de fysieke en digitale wereld. Om deze reden volgt hieronder een overzicht van witwasmethoden die regelmatig voorkomen in de opsporingspraktijk. Wij maken daarbij een onderscheid tussen eenvoudige en complexe witwasconstructies (Kruisbergen et. al., 2012, p. 187-213; Kruisbergen & Soudijn, 2015, p. 12; Europol, 2015a, p. 18 e.v.). Onderstaande vormen van witwassen kunnen in beginsel ook een rol spelen bij het witwassen van uit cybercrime verkregen gelden.

2.4.1 De eenvoudige witwasconstructies

Het verplaatsen van geld met als doel te verhullen is een methode die in veel zaken voorkomt (Kruisbergen et. al., 2012, p. 190-203; Soudijn & Akse, 2012). Binnen deze witwasconstructie wordt geld bijvoorbeeld omgezet naar een andere valuta of verplaatst naar een ander land, waarin het geld wordt geïnvesteerd in onroerend goed of andere zaken. Dit kan op twee manieren, door middel van het fysiek smokkelen van het geld, waarbij een persoon het in zijn bagage meeneemt of als postpakket opstuurt. Het kan ook als een girale verplaatsing door middel van bijvoorbeeld money-transfer. Het toezicht is sinds de jaren negentig verscherpt. Eerst werd de Wet melding ongebruikelijke transacties (Wet MOT) en de Wet identificatie bij dienstverlening (Wid) ingevoerd. Later, in 2008, werden deze wetten opgevolgd door de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Centraal in deze

46 *Kamerstukken II*, 1999/2000, 27 159, nr. 3, p. 1.

wetgeving staan het identificeren van klanten ('Know Your Customer' (hierna: KYC) en de meldplicht ongebruikelijke/afwijkende transacties (Custers, 2006, 2007). Melding moet worden gedaan bij de Financial Intelligence Unit – Nederland (FIU-Nederland). Dit alles betekent niet dat money-transfer en vergelijkbare diensten niet meer worden gebruikt door criminelen. Door bijvoorbeeld bedragen op te splitsen in kleine bedragen wekken ze geen argwaan en wordt veel geld verplaatst (Kruisbergen & Soudijn, 2015, p. 13). Criminelen zoeken bovendien naar locaties en/of instellingen die hen bewust of onbewust faciliteren bij het witwassen van vermogen.

Een andere vorm van witwassen is het afgeschermd consumeren van het misdaadgeld. Betalen in het buitenland is een makkelijke vorm van afgeschermd consumeren. Een crimineel kan ook in Nederland geld uitgeven zonder dat het de aandacht trekt van de autoriteiten. Criminelen kunnen dure auto's of registergoederen laten registeren op naam van iemand anders (bijvoorbeeld een katvanger), waardoor de besteding niet is te herleiden naar de crimineel. Uit de literatuur komen voorbeelden naar voren van autobedrijven die contante betalingen aannemen en de auto op een andere naam registreren. Dit kan ook gedaan worden bij de aankoop van een huis (Kruisbergen & Soudijn, 2015, p. 13).

2.4.2 De complexere witwasconstructies

Daarnaast zijn er verschillende andere methoden om crimineel geld wit te wassen die vaker in literatuur worden besproken (Soudijn & Akse, 2012, p. 28 e.v.; Europol, 2015a, p. 18 e.v.; Kruisbergen & Soudijn, 2015, p. 15). Het gaat hier onder meer om gefingeerde omzet, gefingeerde gokwinsten, en de loan-back-constructie.

Het fingeren van omzet is een witwasmethode waarbij de omzet van een legale onderneming wordt gemanipuleerd door criminele gelden op te voeren als omzet. Op deze manier kunnen legale inkomsten worden vermengd met de criminele gelden. Een casus uit de Monitor Georganiseerde Criminaliteit die tot de verbeelding spreekt, betreft een dadergroep die geld verdiende met drugshandel. Op de rekening van het autobandenbedrijf van een van de verdachten werd € 150 tot € 6.000 per keer gestort (Kruisbergen et al., 2012). Op deze manier werden de gelden uit drugshandel als legale inkomsten opgevoerd. In de praktijk zijn er voor criminelen ook wel risico's en nadelen verbonden aan deze constructie. Een risico is dat de Belastingdienst bij een controle onjuistheden in de administratie aantreft. Een nadeel voor daders is bijvoorbeeld dat er belasting moet worden betaald over de inkomsten.

Een andere manier om hetzelfde resultaat te bereiken is om het geld daadwerkelijk in het bedrijf te houden. Deze constructie staat bekend als Trade

Based Money Laundering (TBML). Het criminele geld wordt gebruikt om legale internationale transacties te verrichten, waarbij in een land goederen worden ingekocht en vervolgens in een ander land worden verkocht. De Financial Action Task Force on Money Laundering (FATF, 2008, p. 1) heeft het misbruik als volgt gedefinieerd: *'the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities'*.[47] Het geld is op deze manier verplaatst door wat lijkt een legitieme reden, maar het proces gaat echter vaak gepaard met valse facturen. Uit verschillende Nederlandse opsporingsonderzoeken blijkt dat bij TBML regelmatig wordt betaald met contanten. Het is van belang op te merken dat dit doorgaans een teken is dat er iets verdachts aan de hand is. Het is namelijk zeer uitzonderlijk voor bedrijven om grote bedragen met contanten te betalen (Europol, 2015a, p. 30).

Geld kan ook worden witgewassen via (online) kansspelen. Er is een aantal manieren waarop gokwinsten de herkomst van criminele gelden kunnen verhullen. In 2009 stelde een rapport van AGP-FATF dat het volume en de omzetsnelheid van de transacties die in casino's plaatsvinden een aanzienlijk risico voor witwassen vormen. De eenvoudigste manier is door zwart geld in speelfiches om te wisselen en deze vervolgens (na al dan niet gespeeld te hebben) op een bankrekening te laten boeken. Op het moment dat de omschrijving 'speelwinst' bij de overboeking staat, is het zwarte geld daarmee legaal geld geworden. Het kan ook zo zijn dat achteraf een verklaring wordt aangedragen voor het anders onverklaarbare vermogen als speelwinst. Feit is dat deze verklaring snel te weerleggen is, want bewijs van een overboeking ontbreekt. Daarnaast kan met gegevens zoals het aantal casinobezoeken en een kansberekening worden bepaald of het realistisch is dat er sprake is van gokwinsten.[48] De komst van online casino's heeft het witwassen gemakkelijker gemaakt doordat twee of meer accounts kunnen worden gecreëerd. Zo kan de crimineel met beide accounts spelen en door expres slecht te spelen op het ene account, het vermogen oversluizen naar het andere account.

De loan-back-constructie is, zoals de naam al doet vermoeden, een manier voor criminelen om crimineel verdiend geld via een omweg aan zichzelf terug te lenen. De methode is vaak redelijk doordacht en er wordt gebruikgemaakt van buitenlandse rekeningen. Zo kan er een huis worden gekocht met geld geleend van een particulier in het buitenland. De particulier is in werkelijkheid de crimineel zelf, onder valse naam, of een familielid of katvanger aan wie het geld eerst is overgemaakt. Op deze manier lijkt er sprake te zijn van een rechtmatige leningsovereenkomst en wordt het financiële spoor moeilijker te volgen. Soudijn en Akse (2012, p. 34) geven aan dat het wel

47 Zie ook Soudijn en Akse (2012, p. 49).
48 Gerechtshof Arnhem, 27 februari 2007, ECLI:NL:GHARN:2007:AZ9398.

mogelijk is om met een aantal controlevragen te achterhalen of er sprake is van witwassen. De geldstroom is vaak niet verklaarbaar. Verder ontbreken in veel gevallen de zekerheden en het aflossingsplan en wijkt de rente soms erg af van de rente voor een marktconforme leningsovereenkomst. Daarnaast worden soms ondoorzichtige constructies gebruikt zoals trustkantoren (trusts) en offshore-banken. Een trust is een kantoor dat zich bezighoudt met het beheren van vennootschappen. Een offshore-bank is een bank die om fiscale redenen (lagere of afwezige belastingtarieven) of administratieve redenen (minder of geen administratieve verplichtingen) in bepaalde landen is gepositioneerd. Soms worden deze landen aangeduid als 'belastingparadijzen'. Ook trustkantoren worden om deze redenen vaak in zulke landen gepositioneerd. Als een trustkantoor nauwelijks of geen inhoudelijke activiteiten ontplooit, wordt ook wel gesproken van een brievenbusvennootschap. Omdat in bepaalde landen weinig of geen toezicht is, kan deze constructie (soms gestapeld via een keten of netwerk van trustkantoren in verschillende landen) aantrekkelijk zijn om de herkomst van criminele gelden te verhullen (Custers, 2006).

Merk op dat al deze methoden bepaalde kenmerken gemeen hebben. Deze kenmerken zijn (1) het verhullen van de herkomst van de gelden; (2) het direct en indirect controle houden over de gelden; (3) het veranderen van de vorm van de gelden, zodat ze niet aan de criminele activiteit kunnen worden gekoppeld (Europol 2015a, p. 9). Contant geld heeft een belangrijk voordeel ten opzichte van andere vormen van geld (zie hoofdstuk 3), omdat het moeilijker is om de oorsprong van het geld vast te stellen. De rol van contant geld is daarom veel groter dan vaak wordt gedacht. Sterker nog, een recent Europol-rapport over witwassen geeft duidelijk aan dat vrijwel alle criminelen ergens gedurende het witwasproces gebruikmaken van contant geld. Zij komen dan ook tot de conclusie dat '*Cash still king*' is in het witwasproces. Het is van belang in het achterhoofd te houden dat de omvang van witwassen met 'cash' geld vele malen groter is dan het witwassen met digitale betalingsmiddelen waar in deze studie de nadruk op ligt.

2.4.3 Strafbaarstelling witwassen in Nederland

Witwassen is in 2001 strafbaar gesteld ter implementatie van verschillende internationale verdragen.[49] De ratio van de strafbaarstelling voor witwassen is gelegen in de bescherming van de integriteit van het financieel-economisch verkeer en bescherming van de openbare orde.[50] Het economisch ver-

49 *Stb.* 2001, 606. In het wetsvoorstel wordt verwezen naar het Verdrag van de Verenigde Naties tegen de sluikhandel in verdovende middelen en psychotrope stoffen (Wenen, 20 december 1988, *Trb.* 1990, 94), het Verdrag inzake het witwassen, de opsporing, de inbeslagneming en de confiscatie van opbrengsten van misdrijven (Straatsburg, 8 november 1990, *Trb.* 1990, 172) en Richtlijn nr. 91/308/EEG van de Raad van de Europese Gemeenschappen van 10 juni 1991 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld (*PbEG* L 166).

50 *Kamerstukken II*, 1999/2000, 27 159, nr. 3, p. 5.

keer kan door het strafbaar stellen van witwassen worden beschermd door illegale geldstromen in de schaduweconomie tegen te gaan en daarmee legale geldstromen te beschermen. De openbare orde wordt indirect beschermd door het tegengaan van witwassen, omdat criminele gelden worden verkregen uit misdrijven die daaraan voorafgaan en tevens misdrijven kunnen worden gepleegd om de criminele geldstroom te blijven verhullen.[51] Tevens is met de harmonisatie van de witwasbepalingen de rechtshulp vereenvoudigd.[52] Een veroordeling voor witwassen kan gepaard gaan met verbeurdverklaring (art. 33 Sr), een bijkomende (vermogens)straf, en beschermende en reparatoire maatregelen als onttrekking aan het rechtsverkeer (art. 36b Sr), ontneming (art. 36e Sr) en schadevergoeding aan het slachtoffer (art. 36f Sr).

De strafbaarstelling van witwassen vindt haar oorsprong in de bestrijding van drugshandel. Voor het witwassen kan tegenwoordig echter ieder misdrijf als gronddelict fungeren. Deze Nederlandse omzetting van de witwasbepalingen voor alle misdrijven is verstrekkend. Enige buurlanden hebben ervoor gekozen witwassen slechts voor bepaalde misdrijven strafbaar te stellen.[53]

De Nederlandse regering en het Openbaar Ministerie zetten sterk in op het afpakken van crimineel verkregen vermogen.[54] Door het afpakken van crimineel verkregen vermogen van verdachten, hebben zij geen profijt of geldelijk gewin van hun criminele gedragingen en wordt duidelijk gemaakt dat misdaad niet loont. Bovendien wordt met het afpakken van criminele winsten voorkomen dat nieuwe criminaliteit wordt gefinancierd. Daarnaast zijn de maximumstraffen verhoogd, voor het gronddelict 'witwassen' van vier naar zes jaar gevangenisstraf en voor gewoontewitwassen naar acht jaar gevangenisstraf.

Witwassen is strafbaar gesteld als opzetwitwassen (art. 420bis Sr), gewoontewitwassen (art. 420ter Sr) en schuldwitwassen (art. 420quater Sr).[55] Bij opzetwitwassen worden de versluierhandelingen (het verbergen of verhullen) van de oorsprong van het 'voorwerp', de plaatsingshandelingen (verwerven, voorhanden hebben, overdragen of omzetten) en de omzettingshandelingen (omzetten en gebruikmaken) van een voorwerp uit misdrijf verkregen strafbaar gesteld. Bij schuldwitwassen gaat het om de versluierhandelingen en verplaatsingshandelingen van een voorwerp, waarbij de verdachte redelijkerwijs moet vermoeden dat het voorwerp uit misdrijf afkomstig is. Bij gewoon-

51 Zie ook *Kamerstukken II*, 1999/2000, 27 159, nr. 3, p. 5.
52 *Kamerstukken II*, 1999/2000, 27 159, nr. 3, p. 3 en p 7-8.
53 Zie commentaar strafrecht onderdeel C.4.1.
54 Zie www.om.nl/onderwerpen/afpakken (laatst geraadpleegd op 19 oktober 2015).
55 Merk op dat de witwasbepalingen veel overeenkomsten vertonen met de helingsbepalingen. Het belangrijkste verschil is dat een witwasser ook strafbaar is als het gaat om criminele opbrengsten van een door hemzelf gepleegd misdrijf.

tewitwassen (art. 420ter Sr) worden zwaardere strafmaxima gesteld voor degenen die een gewoonte maken van het plegen van witwassen.[56]

Onder het witwassen van een 'voorwerp' kan (uiteraard) ook geld worden verstaan. In 2006 heeft de Hoge Raad ook wel aangenomen dat met valse Bahreinse dinars kan worden witgewassen, omdat de biljetten met reguliere gelden waren gekocht.[57] Daarom kan ook worden aangenomen dat met virtuele valuta als Bitcoin kan worden witgewassen, omdat die tevens op geld waardeerbaar zijn en met reguliere valuta kunnen worden aangekocht (zie hoofdstuk 3).

Het Openbaar Ministerie moet het opzet bij witwassen bewijzen.[58] Daarbij moet worden bewezen dat de verdachte willens en wetens de versluierhandelingen of verplaatshandelingen heeft uitgevoerd of (in geval van voorwaardelijk opzet) willens en wetens de kans heeft aanvaard dat versluierhandelingen of verplaatshandelingen zouden plaatsvinden. Afhankelijk van de omstandigheden van het geval kan het opzet uit de handelingen van de verdachte worden afgeleid. Het Openbaar Ministerie maakt ook wel gebruik van verschillende typologieën om het opzet af te leiden. Voorbeelden van deze typologieën zijn:[59]

- het feit dat er geen legale economische verklaring is voor de gewisselde valutasoorten en de frequentie van de wisselingen;[60]
- de transacties staan niet in verhouding tot de inkomsten;[61]
- het contant omwisselen in een witwascyclus wordt vaak gedaan ter onderbreking van de 'paper trail';[62]
- bij grote hoeveelheden contant geld in diverse valuta: het is een feit van algemene bekendheid dat diverse vormen van criminaliteit gepaard gaan met grote hoeveelheden contant geld in diverse valuta;[63]
- het feit dat ten aanzien van de verdachte geen economische activiteit bekend is in relatie tot de verschillende landen waarmee transacties werden verricht;[64]
- het feit dat meerdere wisseltransacties op één dag bij verschillende wisselkantoren/banken dan wel bij verschillende vestigingen van deze wisselkantoren/banken zijn uitgevoerd;

56 Merk op dat hier een verschil bestaat met recidive van (gewoon) witwassen, waarbij geen verband tussen de afzonderlijk gepleegde misdrijven van witwassen hoeft te bestaan.
57 HR 11 april 2006, ECLI:NL:HR:2006:AV2349.
58 In de uitspraak van het Gerechtshof Amsterdam van 11 januari 2013, ECLI:NL:GHAMS:2013:BY8481, zijn de stappen om witwassen te bewijzen samengevat. Zie ook Rozemeijer, 2015.
59 HR 9 december 2014, Conclusie, ECLI:NL:PHR:2014:2832.
60 Rechtbank Groningen 17 december 2009, ECLI:NL:RBGRO:2009:BK6970, Hof Arnhem 23 november 2011, ECLI:NL:GHARN:2012:BY5404.
61 Hof 's-Hertogenbosch 25 maart 2015, ECLI:NL:GHSHE:2015:1181, Rb. Overijssel 9 juni 2015, ECLI:NL:RBOVE:2015:2771.
62 Rb. Overijssel 9 juni 2015, ECLI:NL:RBOVE:2015:2771.
63 Rb. Oost-Brabant 30 juli 2013, ECLI:NL:RBOBR:2013:4278, Hof Arnhem 23 november 2011, ECLI:NL:GHARN:2012:BY5404, Rb. Leeuwarden 7 juni 2011, ECLI:NL:RBLEE:2011:BQ8623, Rb. Amsterdam 18 juni 2015, ECLI:NL:RBAMS:2015:6616.
64 Rb. Groningen 17 december 2009, ECLI:NL:RBGRO:2009:BK6970.

- het feit dat de handel in verdovende middelen veel geld in kleine coupures oplevert;[65]
- het feit dat door de verdachte veel contacten werden (worden) onderhouden met personen met criminele antecedenten;[66]
- het feit dat de verdachte iets weigert te verklaren over de herkomst van het geld;[67]
- het feit dat het kennelijk de bedoeling was om de meldgrens te ontduiken;[68]
- het feit dat er een beloning werd verkregen voor de door verdachte uitgevoerde wisseltransacties;[69]
- bij (veelvuldig) gebruik van money transfers (het is een feit dat het aanmerkelijk duurder is om geld over te maken naar het buitenland via money transfers dan via girale transacties);[70]
- het voorhanden hebben van grote hoeveelheden contant geld zonder noodzaak daartoe op grond van bedrijf of beroep.[71]

Respondenten van onze interviews geven aan dat er onduidelijkheid bestaat, onder meer als gevolg van het ontbreken van jurisprudentie, over de omstandigheden waaruit een 'redelijk vermoeden' van witwassen of een gronddelict voor witwassen kan worden afgeleid indien gebruik wordt gemaakt van cryptocurrencies, zoals Bitcoin. Een financiële dienstverlener kan bijvoorbeeld vaststellen dat ongebruikelijke Bitcointransacties plaatsvinden op een rekening van een klant. Meer concreet kan het voorkomen dat een bank vaststelt dat er veel uitbetalingen van Bitcoin exchanges op een bankrekening plaatsvinden, maar hier geen reguliere inkomsten tegenover staan. Andersom kan een klant continu bitcoins aankopen, waarbij de rekening continu wordt aangevuld met stortingen in contant geld. De vraag is dan of er een redelijk vermoeden kan bestaan voor witwassen, waardoor een opsporingsonderzoek kan worden gestart. Naar analogie van het melden van ongebruikelijke transacties en het KYC-beleid (zie paragraaf 2.4.1) zou daarbij onderscheid gemaakt kunnen worden tussen ongebruikelijke transacties en klanten met een verhoogd risico enerzijds en verdachte transacties en verdachte klanten anderzijds. Hierbij wordt gewerkt met een trechtermodel, waarbij de FIU (Financial Intelligence Unit) ongebruikelijke transacties analyseert en daaruit verdachte transacties selecteert. Hiervoor kunnen verschillende aanleidingen zijn, zoals een match met subjecten in een politieonderzoek of met gegevens

65 Rb. Leeuwarden 7 juni 2011, ECLI:NL:RBLEE:2011:BQ8623, Rb. Rotterdam 30 mei 2008 ECLI:NL:RBROT:2008:BD3415.
66 Rb. Oost-Brabant 30 juli 2013, ECLI:NL:RBOBR:2013:4278.
67 HR 25 maart 2014, ECLI:NL:HR:2014:697, Rb. Leeuwarden 7 juni 2011, ECLI:NL:RBLEE:2011:BQ8623.
68 Rb. Noord-Holland 1 december 2014, ECLI:NL:RBNHO:2014:11716, Rb. Groningen 17 december 2009, ECLI:NL:RBGRO:2009:BK6970.
69 Rb. Groningen 17 december 2009, ECLI:NL:RBGRO:2009:BK6970, Hof Arnhem 23 november 2011, ECLI:NL:GHARN:2012:BY5404.
70 Rb. Overijssel 9 juni 2015, ECLI:NL:RBOVE:2015:2771, Rb. Groningen 17 december 2009, ECLI:NL:RBGRO:2009:BK6970.
71 Hof 's-Hertogenbosch 25 maart 2015, ECLI:NL:GHSHE:2015:1181, Hof Amsterdam 14 december 2010, ECLI:NL:GHAMS:2010:BO9255.

van het Openbaar Ministerie of FIU zelf (Van der Knoop, 2015). Voorop staat in elk geval dat er een verschil is tussen ongebruikelijke en verdachte transacties: niet alle ongebruikelijke transacties zijn verdacht.[72] Om van een ongebruikelijke tot een verdachte transactie te komen, zou bij voorkeur informatie uit meerdere bronnen een rol moeten spelen. Uiteraard kan informatie uit andere bronnen ook ontlastend zijn, bijvoorbeeld wanneer een verdachte een afdoende verklaring verstrekt voor een transactie die in eerste instantie als ongebruikelijk werd aangemerkt.

Voor de opsporingspraktijk is het tevens van belang dat de Hoge Raad in enkele recente arresten zogenoemde 'kwalificatie-uitsluitingsgronden' voor het witwassen door middel van plaatsingshandelingen heeft geformuleerd.[73] Deze kwalificatie-uitsluitingsgronden brengen met zich mee dat (opzet)witwassen niet automatisch is bewezen indien wordt vastgesteld dat een verdachte onmiddellijk crimineel verkregen voorwerpen uit een zelf begaan misdrijf voorhanden heeft. Daarmee beoogt de Hoge Raad te voorkomen dat een verdachte die een bepaald misdrijf heeft begaan en die daarbij door dat misdrijf verkregen voorwerpen voorhanden heeft, zich automatisch ook schuldig maakt aan witwassen (Bogers & Kooijman, 2015). Voor witwassen is dus, ten opzichte van het gronddelict, nog een extra handeling (de plaatsings- of versluieringshandeling) nodig. Daarbij kan nog worden opgemerkt dat crimineel verkregen gelden (ongeacht een veroordeling wegens witwassen) kunnen worden afgepakt via de verbeurdverklaring of ontnemingsmaatregel naar aanleiding van het gronddelict.[74]

Indien sprake is van een kwalificatie-uitsluitingsgrond, moet het Openbaar Ministerie bewijzen dat er sprake is van het verbergen of verhullen van de criminele herkomst van het verkregen voorwerp. De politie kan hiermee rekening houden door bij een verhoor al te vragen om welke reden geld dat wordt aangetroffen bij een huiszoeking niet op de bank is gezet. Daarbij moet rekening worden gehouden met het feit dat een verklaring op zichzelf nog niet voldoende is om witwassen te bewijzen; er moet ook sprake zijn van een daadwerkelijke gedraging.[75] Het Openbaar Ministerie moet dus motiveren dat verhullingshandelingen of verplaatshandelingen hebben plaatsgevonden, terwijl het onder omstandigheden evident kan zijn dat de voorwerpen uit criminele activiteiten zijn verkregen.[76] In de handhavingspraktijk worden deze motiveringseisen als een belemmering ervaren.

72 Ter illustratie: de laatste jaren ontvangt FIU-Nederland jaarlijks circa 200.000 meldingen over ongebruikelijke transacties, waarvan er sinds 2011 circa 23.000 verdacht werden verklaard (Knoop, 2015, p. 7).

73 Zie o.a. HR 8 januari 2013, ECLI:HR:2013:BX6910, HR 25 maart 2014, ECLI:NL:HR:2014:702, HR 16 juni 2015, ECLI:NL:HR:2015:1655, HR 13 oktober 2015, ECLI:NL:HR:2015:3028, De kwalificatie-uitsluitingsgronden zijn gericht op artikel 420bis lid 1 sub b Sr en artikel 420quater lid 1 sub b Sr.

74 Dit onderzoek gaat verder niet in op de voorwaarden voor onttrekking aan het rechtsverkeer of de ontnemingsmaatregel.

75 Zie bijvoorbeeld HR 9 december 2008, ECLI:NL:HR:2008:BF5557 en HR 28 januari 2014, ECLI:NL:HR:2014:188.

76 Zie verder over de kwalificatie-uitsluitingsgronden: Van Leeuwen, 2011; Borgers, 2013; Verbaan & Nan, 2014; en Borgers & Kooijmans, 2015.

Het onderstaande voorbeeld is illustratief voor de belemmering van de kwalificatie-uitsluitingsgrond in cybercrimezaken. Op 8 mei 2014 heeft de Rechtbank Rotterdam een verdachte partieel vrijgesproken van witwassen, maar wel een vijfjarige gevangenisstraf opgelegd voor de 'grootschalige en grensoverschrijdende handel in XTC-pillen' via internet.[77] Tijdens de huiszoeking van de verdachte voor drugshandel werd een contant geldbedrag van € 82.900 aangetroffen, waarvoor de verdachte voor witwassen is veroordeeld. Ontslag van alle rechtsvervolging volgde echter voor een hoeveelheid van ongeveer 325 bitcoins op de Bitcoin wallet op een USB-stick die in het bezit was van de verdachte. De desbetreffende officier van justitie schatte in dat de verdachte ongeveer € 160.000 had verdiend aan de handel van XTC op internet tegen betaling in bitcoins. Echter, omdat de USB-stick te vinden was op de eettafel van de verdachte en verder *'niet gebleken [is] dat verdachte handelingen heeft verricht die erop neerkomen dat hij de aard, herkomst of vindplaats van de Bitcoins heeft verhuld'* kon de rechtbank niet komen tot de kwalificatie van witwassen.[78] Borgens en Kooijmans (2015) wijzen erop dat *'het feit dat een verdachte in het bezit is van zowel drugs als geld, niet per definitie de vaststelling rechtvaardigt dat de verdachte zelf het gronddelict heeft begaan waarvan het aangetroffen geld de (directe) opbrengst belichaamt'*.[79]

Bij zaken waarbij (virtueel) geld wordt witgewassen door middel van bitcoins is kennis over de inbeslagname van bitcoins onontbeerlijk.[80]

Een eerste vraag die daarbij gesteld moet worden, is of bitcoins als een *goed* gekwalificeerd kunnen worden en daarmee vatbaar zijn voor inbeslagname. In de regel worden gegevens binnen het strafrecht niet gekwalificeerd als een goed.[81] Echter, in de afgelopen jaren is uit jurisprudentie af te leiden dat gegevens wel degelijk als een goed kunnen worden beschouwd voor zover zij uniek zijn en waarde hebben in het economische verkeer.[82] Het Openbaar Ministerie neemt dan ook de positie in dat bitcoins als een goed kunnen worden beschouwd en vatbaar zijn voor inbeslagname.[83] In 2014 bevestigde de Rechtbank Overijssel dat bitcoins geen geld maar een ruilmiddel zijn.[84] In ieder geval is helder dat een computer als voorwerp wordt gekwalificeerd dat

77 Rb. Rotterdam, 8 mei 2014, ECLI:NL:RBROT:2014:3504.
78 Zie Rb. Rotterdam, 8 mei 2014, ECLI:NL:RBROT:2014:3504.
79 Met verwijzing naar HR 21 januari 2014, ECLI:NL:HR:2014:127, NJ 2014/78, m.nt. M.J. Borgers.
80 Zie ook het interview met landelijk officier van justitie cybercrime Martijn Egberts door Thea van der Geest, 'Misbruik van bitcoins', *Opportuun*, jrg. 21, nr. 6, 2015. Beschikbaar op: om.nl.
81 Zie *Kamerstukken II*, 1989/90, 21 551, nr. 3, p. 3 en HR 3 december 1996, NJ 1997, 574.
82 Zie HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (Runescape), HR 31 december 2012, ECLI:NL:HR:2012:BQ6575 (diefstal van belminuten), Hof 's-Gravenhage 3 december 2015, ECLI:NL:GHDHA:2015:3355 (diefstal van eindexamens op de Ibn Ghaldoun school). Zie Koops (2014) voor een kritische analyse van deze trend in de rechtspraak en Schermer & Nan in hun noot bij Rb. Rotterdam, 13 februari 2014, ECLI:NL:RBROT:2014:976, *Tijdschrift voor Internetrecht* 2014, nr. 3, p. 83-86. Merk op dat in de memorie van toelichting van de Wet computercriminaliteit III wordt opgemerkt dat gegevens als goed worden aangemerkt indien zij uniek zijn en een individu gegevens uit zijn beschikkingsmacht kan verliezen (*Kamerstukken II* 2015/16, 24 372, nr. 3, p. 63).
83 Zie ook het interview met landelijk officier van justitie cybercrime Martijn Egberts door Thea van der Geest, 'Misbruik van bitcoins', *Opportuun*, *21*(6), 2015, p. 9. Beschikbaar op: om.nl.
84 Rb. Overijssel, 14 mei 2014, ECLI:NL:RBOVE:2014:2667.

vatbaar is voor inbeslagname. Op dit moment gelden afhankelijk van de locatie van de computer andere voorwaarden voor de inbeslagname (Conings & Oerlemans, 2013, p. 24).[85]

Een tweede vraag die gesteld moet worden, is *op welke wijze* bitcoins in beslag kunnen worden genomen. Uit het rapport van het UNODC (2014) over opsporingsonderzoeken met betrekking tot witwassen en het gebruik van digitale betalingsmiddelen wordt de volgende procedure als standaard verondersteld voor de inbeslagname van bitcoins. Als eerste stap moet de computer van de verdachte in beslag worden genomen waar bitcoins op zijn opgeslagen. De mogelijkheid bestaat dat een Bitcoin wallet lokaal is opgeslagen op de inbeslaggenomen computer.[86] Een Bitcoin wallet is software waarmee verbinding wordt gemaakt met het Bitcoin-netwerk en waar bitcoins van de gebruiker in worden beheerd (UNODC, 2014, p. 101).[87] Als tweede stap kunnen de bitcoins naar een ander adres worden overgemaakt, bijvoorbeeld naar een Bitcoin-adres dat is aangemaakt door opsporingsambtenaren en in het beheer is van het Openbaar Ministerie (UNODC, 2014, p. 155). Als derde en laatste stap kunnen de 'inbeslaggenomen' bitcoins via Bitcoin exchanges worden omgezet in euro's en op een rekening van het Openbaar Ministerie worden gestort. Indien de bitcoins spoedig worden omgezet in euro's wordt een snelle potentiële waardevermindering voorkomen. Deze wijze van inbeslagname komt overeen met de wijze waarop bitcoins in Nederland in beslag worden genomen.[88]

Het kabinet vindt nieuwe wetgeving noodzakelijk teneinde het voorhanden hebben van crimineel verkregen gelden beter te kunnen bestraffen.[89] Daartoe is recentelijk een wetsvoorstel ingediend dat het eenvoudiger moet maken

85 Merk op dat in het kader van het project modernisering strafvordering wordt overwogen de regeling tot inbeslagname ten opzichte van geautomatiseerde werken te wijzigen. Zie p. 79 van de Kamerbrief van Minister van der Steur van 30 september 2015 over de Modernisering van het Wetboek van Strafvordering.

86 De wallet is in de regel slechts een klein bestand, vaak kleiner dan 100 bytes (UNODC, 2014, p. 103). Echter, merk op dat bitcoins niet noodzakelijk beschikbaar zijn op een wallet via een computer. Digitale en virtuele valuta kunnen ook online via browser worden beheerd. In dat geval kunnen websites die staan aangemerkt als favoriet, te vinden zijn in de browser geschiedenis of tijdelijke internetbestanden de vindplaats van deze betalingsmiddelen aanwijzen (zie UNODC, 2014, p. 102). Dat betekent overigens wel dat mogelijk andere dwangmiddelen of opsporingsbevoegdheden dan inbeslagname ingezet moeten worden.

87 Door het uitlezen van het .wallet bestand kunnen de bitcoin-transacties die zijn uitgevoerd in de blockchain worden nagegaan (zie UNODC, 2014, p. 107).

88 Zie ook het interview met landelijk officier van justitie cybercrime Martijn Egberts door Thea van der Geest, 'Misbruik van bitcoins', *Opportuun*, *21*(6), 2015, p. 9–10. Beschikbaar op: www.om.nl. Zie ook het persbericht 'Hackers plunderen bankrekeningen' van 24 oktober 2013. Beschikbaar via: www.om.nl/vaste-onderdelen/zoeken/@32220/hackers-plunderen (laatst geraadpleegd op 3 juli 2016). In het persbericht wordt aangegeven dat 56 bitcoins in beslag zijn genomen en zijn omgezet in meer dan € 7.700. Overigens koos de FBI in de Silk Road zaak voor de verkoop van bitcoins door middel van veiling. Zie bijvoorbeeld 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 januari 2014. Beschikbaar op: www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php (laatst geraadpleegd op 14 januari 2015).

89 Zie *Kamerstukken II*, 2015/16, 34 294, nr. 3, p. 2. Borgers en Kooijmans (2015) wijzen er echter op dat de jurisprudentie van de Hoge Raad voor het delict witwassen nog in ontwikkeling is. In de nabije toekomst raken de witwasbepalingen met de daarbij ontwikkelde kwalificatie-uitsluitingsgronden wellicht meer uitgekristalliseerd.

voor witwassen te vervolgen.[90] Het voorstel is om een nieuw lid 2 bij artikel 420bis Sr (nieuw) toe te voegen, waarbij duidelijk wordt gesteld dat het verwerven of voorhanden hebben van een voorwerp dat onmiddellijk afkomstig is uit een misdrijf dat de verdachte heeft gepleegd als witwassen wordt verstaan. Daarmee zouden de kwalificatie-uitsluitingsgronden die de Hoge Raad heeft geformuleerd teniet worden gedaan, hetgeen volgens Borgers en Kooijmans (2015) een aantal nieuwe problemen in het leven roept die nu juist goeddeels door de Hoge Raad waren geëcarteerd.

2.5 Relatie tussen cybercrime en witwassen

Cybercrime heeft vaak (hoewel zeker niet altijd) een financieel motief, zeker wanneer het banking malware en ransomware betreft (Europol, 2015b). Het geld dat wordt verkregen via banking malware en ransomware is doorgaans digitaal van aard.[91] Het geld dat via banking malware giraal wordt verkregen van het slachtoffer moet vervolgens worden witgewassen teneinde de herkomst te verbergen en vervolgens te kunnen besteden.[92] Geld dat uit cryptoware wordt verkregen, is doorgaans virtueel van aard, omdat het losgeld vaak (maar niet altijd) in bitcoins of vouchers moet worden betaald. Ook deze bitcoins en vouchers zullen criminelen vervolgens willen besteden en buiten beeld van de fiscus willen houden. Criminelen werken daarbij niet alleen, maar vaak in georganiseerd verband.

Op welke wijze criminelen dit witwasproces bij banking malware en ransomware veelal inrichten, zal in hoofdstuk 4 worden beschreven. Hierbij is het van belang op te merken dat de juridische omschrijving van witwassen (zie vorige paragraaf) veel ruimer is dan wat in veel criminologische literatuur onder witwassen wordt verstaan (Kruisbergen & Soudijn, 2015). In veel gevallen wordt witwassen in criminologische literatuur uitgelegd als een model met drie opeenvolgende fasen: plaatsing, verhulling en integratie (Unger 2007):

– *Placement* (plaatsing): in deze fase wordt (uit misdrijf afkomstig) chartaal geld in het financiële stelsel gebracht.
– *Layering* (versluiering): in deze fase vindt een opeenvolging van soms complexe financiële transacties plaats, met als doel de oorsprong van het ingebrachte vermogen te verhullen. Door achtereenvolgende omzettingen in giraal en in chartaal geld wordt daarbij vaak getracht de zogenoemde '*paper trail*' te doorbreken.

90 Zie het Wetsvoorstel van 1 oktober 2015 tot Wijziging van het Wetboek van Strafrecht met het oog op het verbeteren van de mogelijkheden tot bestrijding van het verwerven en voorhanden hebben van uit misdrijf afkomstige voorwerpen (aanpassing witwaswetgeving).

91 Bij banking malware gaat het doorgaans om elektronisch geld, bij ransomware wordt het losgeld steeds vaker in bitcoins opgeëist.

92 Zie ook Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.

– *Integration* (bestemming): in deze fase wordt het crimineel verkregen vermogen, dat nu een legale schijn heeft, geïnvesteerd in het legale economische (inter)nationale verkeer.[93]

Dit 'klassieke' driefasenmodel is inmiddels deels achterhaald, omdat het impliceert dat pas van witwassen kan worden gesproken als de drie fasen zijn doorlopen en het uit misdrijf afkomstige geld uiteindelijk onderdeel is geworden van de legale economie.[94] Het doel van witwassen (ongestoord genieten van de opbrengsten van criminaliteit) kan namelijk ook worden bereikt zonder dat alle drie de fasen worden doorlopen (Soudijn & Akse, 2012; Kruisbergen et al. 2012; Verrest, 2006, p. 45; Akse, 2003; Kleemans et al., 2002, p. 108).

Bij de analyses in dit onderzoek zal niet bij het bovengenoemde klassieke driefasenmodel worden aangesloten. Ook bij witwassen met digitale betalingsmiddelen is het model grotendeels achterhaald. Een belangrijke reden daarvoor is dat bij cybercrime de plaatsingsfase veelal wordt overgeslagen, omdat het crimineel verkregen geld meteen digitaal van aard is, waarna het geld versluierd of omgezet kan worden (Tropina, 2014, p. 71). Bitcoins verkregen uit criminaliteit kunnen bijvoorbeeld enerzijds worden omgezet in 'echt geld' (euro's, dollars, etc.), maar anderzijds ook worden besteed als geld waarmee direct producten en diensten kunnen worden afgenomen. Juridisch gezien is in beide gevallen sprake van witwassen, maar volgens het driefasenmodel is in het tweede geval geen sprake van witwassen, omdat de plaatsingsfase wordt overgeslagen. Naarmate bitcoins op meer en meer plekken in de legale economie kunnen worden gebruikt als betalingsmiddel, nemen de mogelijkheden voor afgeschermd consumeren (zonder omzetting in andere betalingsmiddelen) toe. Meer hierover volgt in hoofdstuk 3. Bij de analyses wordt steeds uitgegaan van de juridische kwalificaties voor witwassen in het Wetboek van Strafrecht.

2.6 Tussenconclusie

In dit hoofdstuk is een typologie gegeven van cybercrime en is nagegaan hoe geld door criminelen wordt verdiend met banking malware en ransomware. Tevens is een typologie gegeven van witwassen en is de relatie tussen cybercrime en witwassen onderzocht. Daarmee wordt een antwoord gegeven op de eerste onderzoeksvraag: *Wat wordt verstaan onder het witwassen van door banking malware en ransomware verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?*

93 Deze omschrijving is overgenomen uit *Kamerstukken II* 1999/2000, 27 159, nr. 3, p. 4.

94 Het overslaan van de plaatsingsfase heeft niet alleen een theoretische implicatie voor het model, maar ook praktische consequenties voor de opsporing: het is in zulke gevallen niet mogelijk uit cybercrime afkomstig geld op te sporen door te kijken naar waar chartaal geld in het financiële stelsel wordt ingebracht. De opsporing dient dan gericht te zijn op versluierings- en bestemmingsfasen.

De twee voorbeelden van ZeuS banking malware en CTB-Locker cryptoware laten zien dat criminelen relatief complexe kwaadaardige software kunnen maken om geld te verdienen. Bij banking malware wordt elektronisch geld naar cybercriminelen overgemaakt, hetgeen vervolgens kan worden witgewassen. Bij ransomware wordt geld via vouchers of de cryptocurrency Bitcoin overgemaakt, hetgeen vervolgens kan worden witgewassen. Witwassen omvat in de kern het verbergen of verhullen van de illegale herkomst van gelden of voorwerpen, doorgaans met de bedoeling het geld te kunnen gebruiken in het normale handelsverkeer.[95] Het meest gebruikte criminologische model, het klassieke driefasenmodel, lijkt grotendeels achterhaald aangezien het doel van witwassen kan worden bereikt zonder alle fasen te doorlopen. Onze analyse heeft laten zien dat dit juist bij het witwassen met digitale betalingsmiddelen mogelijk is. Een belangrijke reden daarvoor is dat bij cybercrime de plaatsingsfase veelal wordt overgeslagen, omdat het crimineel verkregen geld meteen digitaal van aard is waarna het geld versluierd of omgezet kan worden. Bij de analyses in dit onderzoek zal niet bij het bovengenoemde model worden aangesloten; uitgegaan wordt van de juridische kwalificaties voor witwassen in het Wetboek van Strafrecht. Juridisch is witwassen strafbaar gesteld als opzetwitwassen (art. 420bis Sr), gewoontewitwassen (art. 420ter Sr) en schuldwitwassen (art. 420quater Sr). Overigens hebben wij geconstateerd dat de omvang van witwassen met 'cash' geld vele malen groter is dan die van het witwassen met digitale betalingsmiddelen waar in deze studie de nadruk op ligt. Of dat in de toekomst zal veranderen, hangt sterk af van de mogelijkheden die digitale betalingsmiddelen bieden voor criminelen (zie hoofdstuk 3).

95 Het gaat niet om het verhullen van gelden of voorwerpen zelf, maar om de illegale herkomst ervan.

3 Digitale betalingsmiddelen

In dit hoofdstuk worden digitale betalingsmiddelen onderzocht. Digitale betalingsmiddelen omvatten zowel digitale bankrekeningen in nationale valuta (bijvoorbeeld internetbankieren in euro's of dollars) als virtueel geld (bijvoorbeeld bitcoins).[96] In dit hoofdstuk wordt de tweede onderzoeksvraag van dit onderzoek beantwoord, namelijk: *Wat zijn digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, en hoe werken deze digitale betalingsmiddelen?* Daartoe wordt in paragraaf 3.1 eerst de belangrijkste terminologie rondom digitaal geld, elektronisch geld en virtueel geld uiteengezet. De meeste lezers zullen bekend zijn met internetbankieren, maar virtueel geld behoeft voor de niet-ingewijde lezer meer toelichting. Om deze reden worden in paragraaf 3.2 de verschillende typen virtueel geld geanalyseerd wordt en een korte beschrijving gegeven van de virtuele betalingsvormen die door cybercriminelen worden gebruikt. In paragraaf 3.3 wordt beschreven hoe virtueel geld werkt, zowel in technisch opzicht als in gebruikersopzicht. Daarbij wordt ingegaan op de vraag hoe virtueel geld wordt verhandeld (gekocht en verkocht) en hoe er betalingen mee worden verricht. In paragraaf 3.4 komt de juridische status van virtueel geld aan bod en het (eventuele gebrek aan) toezicht op virtueel geld. In paragraaf 3.5 wordt de onderzoeksvraag beantwoord. De werking van digitale betalingsmiddelen wordt in dit hoofdstuk onderzocht vanuit een legaal perspectief. Hoe digitale betalingsmiddelen kunnen worden gebruikt om geld wit te wassen, komt in de volgende hoofdstukken aan bod. Dit hoofdstuk is hoofdzakelijk bedoeld om de benodigde basiskennis te verschaffen over digitale betalingsmiddelen en hun werking.

3.1 Terminologie

Geld bestaat al duizenden jaren (Davies, 2002). In feite maakt geld als ruilmiddel de directe ruil van goederen en diensten overbodig. Bovendien heeft het gebruik van geld als voordeel dat de waarde van producten en diensten benoemd kan worden. Het eerste gebruik van geld bestond uit waardevolle materialen, zoals schelpen, zout en (edel)metalen. Het maken van munten uit metalen, met name zilver en goud, is in de geschiedenis het meest populair gebleken. In eerste instantie was de waarde van een munt gelijk aan de waarde van het materiaal van de munt, maar later kregen munten een zogeheten fiduciaire waarde. Hiermee wordt niet gedoeld op de waarde van het materiaal maar op het vertrouwen dat producten en diensten kunnen worden gekocht met het geld. Tegenwoordig zijn de meeste munten niet langer van edelmetalen als zilver en goud en met de invoering van papiergeld verdween de intrinsieke waarde van geld vrijwel helemaal.[97]

96 Betaalmethoden betreffen de manier van betalen en betaalmiddelen betreffen hetgeen wordt overgedragen. In dit hoofdstuk komen ook verschillende digitale betaalmethoden aan bod.

97 Hoewel in China al in de zevende eeuw papiergeld werd gebruikt, werd papiergeld pas in de dertiende eeuw in Europa geïntroduceerd. In Nederland werd in 1574 in Leiden het eerste papiergeld gemaakt (Singh 2009, p. 21).

Naast het betalen met papiergeld ontstond halverwege de twintigste eeuw ook de mogelijkheid te betalen met betaalkaarten, ook wel 'plastic geld' genoemd. Zulke betaalkaarten zijn meestal gekoppeld aan een bankrekening, zoals creditcards en debitcards, maar niet altijd (denk bijvoorbeeld aan chipkaarten als de OV-chipkaart, de inmiddels afgeschafte Chipknip en kaarten met prepaid beltegoed).[98] Creditcards ontstonden in de jaren vijftig van de twintigste eeuw. Bedrijven als American Express, MasterCard en VISA hebben wereldwijd uitgebreide netwerken voor hun kredietkaarten. Door het tonen van een kaart in combinatie met een handtekening en/of pincode kan met deze kaarten worden betaald. Creditcards moeten niet worden verward met andere betaalkaarten, zoals debitcards.[99] Deze passen kunnen worden gebruikt om bedragen af te schrijven van een betaalrekening bij een betaling of geldopname. Bij een pinpas moet doorgaans vooraf geld worden gestort op de bankrekening, terwijl met een creditcard pas achteraf hoeft worden betaald. Doordat veel bankrekeningen tegenwoordig toestaan dat iemand 'rood staat', vervaagt het verschil tussen creditcards en pinpassen.

In dit verband is het ook relevant *prepaid cards* te noemen. Dit zijn debet- noch creditcards. Bij prepaid cards wordt namelijk, zoals de naam al aangeeft, vooraf betaald, terwijl bij debitcards en creditcards verrekening pas achteraf (dat wil zeggen na een transactie) plaatsvindt.[100] Prepaid cards zijn onder meer interessant voor personen die (bijvoorbeeld als gevolg van beperkte kredietwaardigheid) geen creditcard en/of bankrekening kunnen verkrijgen. De monetaire waarde van prepaid cards staat ofwel op de kaart zelf of in een database op afstand. Voorbeelden van prepaid cards zijn de OV-chipkaart, waarop vooraf tegoed moet worden geladen en cadeaukaarten (*giftcards*) van winkelketens. Sommige prepaid cards zijn herlaadbaar, maar dit is niet altijd het geval. Prepaid cards kunnen worden gebruikt bij witwassen (Sienkiewiz, 2007). Achter bepaalde prepaid cards zit een bankrekening die geopend moet worden met een identiteitsbewijs. Echter, er zijn ook prepaid cards die anoniem zijn of minder streng gereguleerd zijn (bijvoorbeeld in het buitenland) en dat kan voor criminelen aantrekkelijk zijn.

In de geschiedenis van betalingsmiddelen komt 'plastic geld' pas zeer kort voor. De ontwikkeling van plastic geld ging redelijk gelijk op met die van elektronisch geld (e-geld, e-money).[101] Hiermee wordt gedoeld op een digitale weergave van 'echt geld', dat wil zeggen door de overheid gefiatteerd geld (fiat money, nationale valuta), zoals een digitale bankrekening in dollars of

98 Omdat sommige kaarten, zoals de OV-chipkaart, slechts in een beperkte omgeving kunnen worden gebruikt als betaalmiddel, worden ze juridisch niet gezien als geld. Zie http://blog.iusmentis.com/2009/05/10/ov-chipkaart-toch-geen-elektronisch-geld (laatst geraadpleegd op 19 oktober 2015).

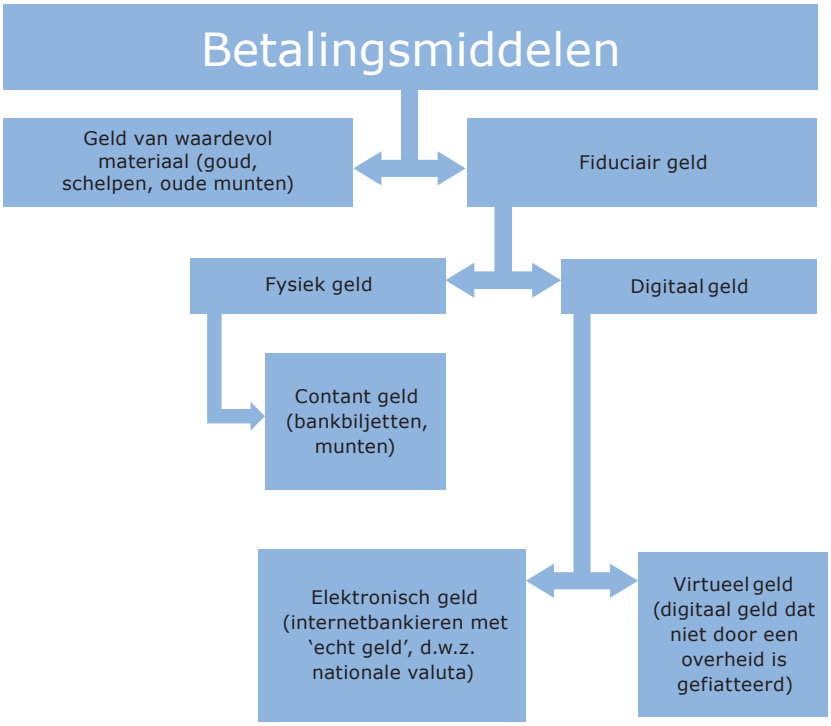
99 Gewoonlijk 'pinpas' genoemd in Nederland en 'bankkaart' in België.

100 Prepaid cards '*pay early*', debitcards '*pay now*' and creditcards '*pay later*'. Zie Berger, Molyneux & Wilson 2015, p. 279.

101 Zie bijvoorbeeld UNODC, 2014, p. 10.

euro's (vaak aangeduid als internetbankieren).[102] Van veel recentere datum is het ontstaan van zogeheten virtueel geld. Onder virtueel geld wordt begrepen een digitale weergave van geld dat niet door een overheid is gefiatteerd. Voorbeelden hiervan zijn geld in online games en cryptocurrencies, zoals Bitcoin.[103] Digitale betalingsmiddelen omvatten zowel elektronisch geld als virtueel geld, dus een digitale weergave van geld dat wel of niet door de overheid is gefiatteerd. In figuur 3.1 worden de verschillende vormen van betalingsmiddelen schematisch weergegeven.

Figuur 3.1 Indeling van de verschillende vormen van betalingsmiddelen



Bovenstaande indeling is grotendeels gebaseerd op de definities van de Financial Action Task Force (FATF), een internationale organisatie die standaarden ontwikkelt om witwassen en terrorismefinanciering tegen te gaan (UNDOC, 2014, p. 9). In Nederland kent de Wet op het financieel toezicht (Wft) chartaal (contant), giraal en elektronisch geld.[104] Chartaal geld is contant geld. In de definitie van de Wft kan ook een elektronische cadeaukaart met daarop een tegoed worden gezien als elektronisch geld.[105] Wanneer het

102 Internetbankieren via de mobiele telefoon wordt ook wel aangeduid als mobiel bankieren.
103 Zie paragraaf 2.4 en 3.2.
104 Artikel 1:1 Wft. Zie ook paragraaf 2.4.1 voor meer informatie over gerelateerde wetgeving zoals de Wwft.
105 Zie www.toezicht.dnb.nl/2/50-227911.jsp (laatst geraadpleegd op 19 oktober 2015).

tegoed echter alleen bij de eigen winkel kan worden gebruikt, is de vrijstellingsregeling Wft van toepassing. Zoals in de volgende paragraaf uiteengezet zal worden, zijn verschillende vormen van virtueel geld, de zogeheten cryptocurrencies, geen elektronisch geld in de zin van de Wft. Uitgevers van virtuele valuta die niet over een vergunning beschikken, kunnen formeel ook geen elektronisch geld uitgeven.

Zoals aangegeven in hoofdstuk 1, richt dit onderzoek zich op digitale betalingsmiddelen omdat cybercriminelen enerzijds via banking malware en ransomware hun geld verdienen in de vorm van digitale betalingsmiddelen en anderzijds mogelijk digitale betalingsmiddelen gebruiken om hun crimineel verdiende opbrengsten (verder) wit te wassen. De European Banking Authority (EBA) heeft verschillende voordelen van digitale betalingsmiddelen geïdentificeerd als aantrekkelijk voor criminelen en deze aangemerkt als hoge risico's voor onder meer gebruikers, financiële markten en toezichthouders:[106]

- De geldstroom is niet in alle gevallen geheel te traceren, bijvoorbeeld wanneer transacties gestapeld worden via online betaalplatformen en/of plaatsvinden via landen met strikte bankgeheimen of beperkt toezicht. Het principe '*follow the money*' vervalt dan.
- Bepaalde omzettingen kunnen redelijk anoniem plaatsvinden, als zij bijvoorbeeld online internationaal worden verhandeld of als geld via een pinautomaat in het buitenland wordt opgenomen.
- Geld kan op een snelle manier over de wereld verplaatst worden.
- Complexe infrastructuren kunnen onduidelijkheid veroorzaken over wie verantwoordelijk kan worden gehouden voor het toezicht.

In paragraaf 3.3.3 wordt nader ingegaan op de specifieke voor- en nadelen van virtueel geld, een subcategorie van digitaal geld.

Dit onderzoek heeft betrekking op digitaal witwassen, waarbij ook digitale betalingsmiddelen een rol kunnen spelen. Zowel elektronisch geld als virtueel geld vallen dus binnen de reikwijdte van dit onderzoek. Ook andere betalingsmiddelen, zoals contant geld en betaalkaarten, kunnen onderdeel uitmaken van het witwasproces. Bij de meeste vormen van witwassen speelt contant geld nog steeds een (grote) rol (Europol, 2015a). Ook bij witwassen met behulp van digitale betalingsmiddelen komt het vaak voor dat er een *cash-out* in contant geld of met betaalkaarten plaatsvindt (zie hoofdstuk 4).

106 EBA (2014), 'Opinion on Virtual Currencies', 4 juli 2014, beschikbaar op: www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n (laatst geraadpleegd op 9 oktober 2015).

3.2 Virtueel geld

Omdat de meeste consumenten tegenwoordig digitale betaalrekeningen hebben bij hun bank via een of andere vorm van internetbankieren, wordt de werking van elektronisch geld en internetbankieren hier niet verder uitgelegd. Door de toenemende digitalisering bieden banken in toenemende mate hun diensten aan via internet. Betalen via de bankwebsite op de computer (internetbankieren) of een app op de smartphone of tablet (mobiel bankieren) is meer de norm dan de uitzondering.

Virtueel geld behoeft voor de niet-ingewijde lezer daarentegen enige toelichting. Het gebruik van virtueel geld is immers minder wijdverbreid dan het gebruik van fysiek geld en elektronisch geld. In paragraaf 3.2.1 wordt de typologie van virtueel geld nader uitgewerkt. In paragraaf 3.2.2 worden de belangrijkste verschijningsvormen van virtueel geld beschreven. Daarbij ligt de nadruk op verschijningsvormen van virtueel geld die ook daadwerkelijk door criminelen worden gebruikt bij cybercrime en/of witwassen. Daarnaast worden ook enkele verschijningsvormen beschreven die weliswaar niet in de dossiers voorkwamen maar mogelijk toch interessant zijn voor cybercriminelen.

3.2.1 Typologie

Virtueel geld kan op basis van twee criteria worden onderscheiden. In de eerste plaats betreft dat de vraag of het geld (de unit) kan worden omgezet in nationale valuta en in de tweede plaats of er een centraal systeem/centrale autoriteit achter de werking (het netwerk of protocol) van het virtuele geld zit.

Wanneer virtueel geld kan worden omgezet in nationale valuta (door de overheid gefiatteerd geld), wordt gesproken van inwisselbaar (*convertible*) virtueel geld of open virtueel geld. Kan dat niet, dan is sprake van niet-inwisselbaar (*non-convertible*) virtueel geld of gesloten virtueel geld. Inwisselbaar virtueel geld heeft een equivalente waarde in echt geld. Niet-inwisselbaar virtueel geld is specifiek bedoeld voor een bepaalde virtuele omgeving, zoals een online game of website. Niet-inwisselbaar virtueel geld kan niet worden ingeruild voor echt geld, ook al moet het in veel gevallen wel worden gekocht met echt geld. Daarbij dient opgemerkt te worden dat er soms een zwarte markt kan ontstaan rondom niet-inwisselbaar virtueel geld. Zo kunnen bijvoorbeeld spelers van een online game doorgaans hun speelgeld niet inruilen voor echt geld, maar niettemin proberen ze soms hun spelidentiteiten of gewonnen objecten en eigenschappen door te verkopen, ook buiten de spelomgeving zelf en ook als dit in strijd is met de algemene voorwaarden (Schermer et al., 2008, p. 46). Een voorbeeld van een populair betaalmiddel in online games is ‘World of Warcraft gold’. In 2014 speelden meer dan 10 mil-

joen spelers World of Warcraft. Eind 2015 was het aantal spelers echter gezakt naar 5,6 miljoen.[107] Binnen de spelomgeving is 'World of Warcraft gold' het virtuele betaalmiddel, maar het is niet toegestaan om het spelgoud te kopen of verkopen met echt geld.[108] Niettemin is er een actieve, officieuze handel in World of Warcraft-goud.[109] Daarmee is het de facto inwisselbaar virtueel geld geworden (UNDOC, 2014, p. 15). Opgemerkt moet worden dat unieke, op geld waardeerbare identiteiten, objecten en eigenschappen in deze spellen kunnen worden gestolen (Schermer et al., 2008, p. 49).[110] Omdat niet-inwisselbaar virtueel geld niet goed bruikbaar is voor witwasdoeleinden, wordt hieronder vooral ingegaan op inwisselbaar virtueel geld.

Het andere relevante onderscheid is of er sprake is van een centrale autoriteit die het virtuele geld beheert of dat het geld gedecentraliseerd in omloop is. Bij gecentraliseerd virtueel geld is sprake van een enkele autoriteit voor het beheer, dat wil zeggen een *third party* die het systeem beheert en controleert. Deze autoriteit stelt de regels vast voor het gebruik van het virtuele geld en heeft de mogelijkheid virtueel geld aan het systeem te onttrekken of juist aan het systeem toe te voegen. De centrale autoriteit kan de wisselkoers van het virtuele geld vastzetten of juist laten variëren.

Gedecentraliseerd virtueel geld wordt ook wel aangeduid met de term *cryptocurrencies*.[111] Dit is virtueel geld dat is gebaseerd op cryptografische software, waarbij er geen centrale autoriteit is die toeziet op het beheer van het geld.[112]

In tabel 3.1 is de indeling van virtueel geld weergegeven aan de hand van enkele verschijningsvormen.

Tabel 3.1 Indeling van virtueel geld

	Inwisselbaar	Niet-inwisselbaar
Centraal beheer	Vouchers, tegoeden op websites	Speelgeld
Decentraal beheer	Cryptocurrencies	[Non-existent]*

* In de praktijk zou een cryptocurrency niet-inwisselbaar kunnen blijken wanneer niemand deze wil hebben. Hier wordt echter gedoeld op de mogelijkheid tot inwisselen en niet of dat ook feitelijk plaatsvindt.

107 www.forbes.com/sites/insertcoin/2015/08/05/world-of-warcraft-has-lost-44-of-its-subscribers-in-six-months-but-thats-okay (laatst geraadpleegd op 18 april 2016).

108 Zie http://eu.battle.net/wow/en/shop/anti-gold (laatst geraadpleegd op 10 oktober 2015). Merk op dat bijvoorbeeld in Zuid-Korea alle vormen van speelgeld verhandelen voor echt geld illegaal zijn, ongeacht de regels van de game zelf. A. Yoon, 'Selective Bombing of RMT in Korea', *TerraNova*, 13 mei 2007.

109 Zie www.wikihow.com/safely-buy-gold-in-world-of-warcraft (laatst geraadpleegd op 10 oktober 2015).

110 Zie ook *NOS Journaal*, 'Dief uit Habbo-hotel gearresteerd', november 2007.

111 Merk op dat niet alle vormen van virtueel geld cryptografie gebruiken.

112 Merk op dat het protocol hier de belangrijkste innovatie is, niet zozeer de eenheid, zie bijvoorbeeld 'The trust machine: The promise of the blockchain', *The Economist*, 31 oktober 2015. Beschikbaar op: www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine (laatst geraadpleegd op 26 februari 2016).

Centraal beheerd, inwisselbaar virtueel geld komt vooral voor in de vorm van fiches in casino's of als vouchers, coupons en tegoeden bij webwinkels en andere websites. Zulke tegoeden worden soms wel als geld aangeduid door webwinkels, maar het is de vraag of het grote publiek dit ook als geld ziet. Ter vergelijking: een VVV-bon of boekenbon vertegenwoordigt een waarde in euro's en kan als betalingsmiddel worden gezien, maar wordt doorgaans niet als geld beschouwd, zelfs als deze bonnen terug te wisselen zijn voor euro's.

Cryptocurrencies daarentegen worden (in de media en maatschappelijk gezien, niet juridisch) wel vaker als geld beschouwd, omdat er steeds meer betalingen mee kunnen plaatsvinden die in de maatschappij ook met 'echt geld' worden verricht. Daarmee lijken cryptocurrencies wat betreft toepassingsmogelijkheden en gebruik nog het meest op 'echt geld'. Het laatste type geld is decentraal beheerd, niet-inwisselbaar virtueel geld. Dit type virtueel geld bestaat niet: alle vormen van niet-inwisselbaar virtueel geld zijn gecentraliseerd. Per definitie is er een centrale autoriteit die dit type virtueel geld uitgeeft en de regels vaststelt waardoor het geld niet-inwisselbaar is (UNODC, 2014, p. 13).

3.2.2 Verschijningsvormen

In deze paragraaf worden kort voorbeelden beschreven van de hierboven genoemde varianten van inwisselbaar virtueel geld die wij in ons literatuuronderzoek en dossieronderzoek veel zijn tegengekomen. Enkele valuta bestaan inmiddels niet meer, maar omdat bij die valuta sprake was van witwassen en cybercriminaliteit worden ze toch benoemd. Daarnaast is in bijlage 4 een uitgebreider overzicht gepresenteerd met de kenmerken van de betalingsvormen die wij in ons onderzoek specifiek zijn tegengekomen.

Doordat het onderstaande overzicht chronologisch is opgebouwd, wordt tevens de ontwikkeling van het gebruik van verschillende virtuele valuta weergegeven. Allereerst komen enkele centraal beheerde vormen van virtueel geld aan bod, daarna komende de decentraal beheerde vormen van virtueel geld (de cryptocurrencies, met name Bitcoin) aan bod.

E-Gold was een van de eerste populaire virtuele valuta. In 1996 werd E-Gold opgericht door het bedrijf Gold & Silver Reserve Inc. (G&SR) in de Verenigde Staten. Dit bedrijf was officieel gevestigd in Saint Kitts and Nevis, een eilandstaat in de Caraïben en opereerde vanuit Florida. Gebruikers konden een rekening openen via de website ter waarde van een bedrag in grammen goud of andere edelmetalen. Van deze rekening konden overal ter wereld bedragen worden overgemaakt naar andere E-Gold rekeningen (Bronk, Monk & Villasenor, 2012, p. 131). In 2005 waren er 2,5 miljoen rekeningen en in 2009 waren er vijf miljoen rekeningen. Tijdens het hoogtepunt in 2006 verwerkte E-Gold

voor een bedrag van meer dan 2 miljard dollar aan transacties per jaar (UNODC, 2014, p. 7). Echter, in 2007 werd E-Gold in de Verenigde Staten beschuldigd van witwassen en het opereren als financiële dienstverlener zonder vergunning.[113] Als gevolg hiervan werd E-Gold uiteindelijk platgelegd in 2009.

WebMoney is in 1998 opgericht in Moskou door het bedrijf WebMoney Transfer Ltd. Om een WebMoney rekening te openen, is geen bankrekening of creditcard nodig. Tienduizenden online winkels accepteren betalingen van WebMoney. De eenheden waarin WebMoney rekent, zijn verschillend. Zo zijn er rekeningen in euro's (WME), Amerikaanse dollars (WMZ), in Russische roebels (WM) en in Bitcoins (WMX). Het verdienmodel van WebMoney is gebaseerd op een commissie: voor elke transactie wordt een bedrag van 0,8% in rekening gebracht. Het aanmaken van een rekening en het ontvangen van geld is gratis. Het storten op een WebMoney rekening kan via een overboeking van een gewone bankrekening of van een rekening met virtueel geld, zoals een Bitcoin-rekening.[114]

Liberty Reserve was een digitale financiële dienstverlener uit Costa Rica. Met behulp van enkel een naam, e-mailadres en geboortedatum konden gebruikers een rekening aanmaken en geld overmaken naar andere gebruikers (UNODC, 2014, p. 7). Omdat de identiteiten van gebruikers niet werden gecontroleerd, was Liberty Reserve aantrekkelijk voor cybercriminelen voor fraude en witwassen. Bedragen konden worden gestort in dollars en euro's. Geld werd verdiend door voor elke transactie een kleine commissie te rekenen, ongeveer 1% per transactie (Richet, 2013). In 2013 beschuldigde het Amerikaanse ministerie van Justitie Liberty Reserve van het opereren als financiële dienstverlener zonder vergunning en het witwassen van meer dan 6 miljard dollar uit illegaal verkregen geld.[115] Datzelfde jaar werd Liberty Reserve ontmanteld. In 2014 werd de eigenaar van Liberty Reserve uitgeleverd vanuit Spanje aan de Verenigde Staten.[116] Er waren in deze zaak verschillende verbanden met Nederland. Zo leefde de topman van Liberty Reserve in Nederland en speelden politie en OM in Nederland een belangrijke rol in het opsporingsonderzoek.[117]

113 Zie ook het persbericht van de U.S. Department of Justice, 'Over $56.6 Million Forfeited In E-Gold Accounts Involved In Criminal Offenses', 23 april 2014. Beschikbaar op : www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses (laatst geraadpleegd op 19 oktober 2015).

114 Zie www.wmtransfer.com/eng/inout/topup.shtml (laatst geraadpleegd op 10 augustus 2016).

115 Zie Santora, M., Rashbaum, W.K. & Perlroth, N. (2013). *Online Currency Exchange Accused of Laundering $6 Billion*, 28 mei 2013. Beschikbaar op: www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html (laatst geraadpleegd op 19 oktober 2015).

116 Zie het persbericht van het Amerikaanse ministerie van Justitie, 'Liberty Reserve Founder Extradited from Spain', 10 oktober 2014. Beschikbaar op: www.justice.gov/opa/pr/liberty-reserve-founder-extradited-spain (laatst geraadpleegd op 19 oktober 2015).

117 ANP, 'Topman Liberty Reserve leefde in Nederland'. *Trouw*, 30 mei 2013. Beschikbaar op: www.trouw.nl/tr/nl/4492/Nederland/article/detail/3449885/2013/05/30/Topman-Liberty-Reserve-leefde-in-Nederland.dhtml (laatst geraadpleegd op 19 oktober 2015).

PayPal is een online betaalsysteem dat onderdeel was van eBay maar medio 2015 is afgesplitst als zelfstandig, beursgenoteerd bedrijf. Betalingen worden verricht via een bankrekening, creditcard of PayPal-rekening. Geld kan worden overgeschreven van/naar een eigen bankrekening. In de VS is PayPal wettelijk gezien geen bank, maar in de EU heeft PayPal een EU-banklicentie. PayPal had 2,7 miljoen rekeninghouders in Nederland in 2010. Betalen met PayPal is voor de betaler gratis, maar de ontvanger moet een provisie betalen van € 0,35 plus 3,4% van het transactiebedrag.[118]

Ukash was een online betaalsysteem dat gebruikers de mogelijkheid bood contant geld in te wisselen voor een voucher (eigenlijk een code) waarmee ze online betalingen konden verrichten.[119] De code kon gebruikt worden voor online betalingen, om betaalkaarten op te laden, e-wallets te vullen of om geld over te boeken. De codes werden gedistribueerd door deelnemende winkeliers, kiosken en betaalautomaten. Gebruikers kregen een unieke code bestaande uit 19 karakters die ze konden invoeren bij een betaling of transactie. Wanneer een betaling een kleiner bedrag betrof dan die van de gebruikte code, werd een nieuwe code aangemaakt voor het restbedrag. De vouchers hadden maximumbedragen, maar gebruikers konden zoveel vouchers aanschaffen als ze wilden. Eind 2015 hield Ukash op te bestaan omdat het werd overgenomen door Skrill. Skrill biedt de Paysafecard[120] aan, een vergelijkbare prepaid voucher waarmee in verschillende landen met verschillende valuta kan worden betaald. De Paysafecard kan gekocht worden (eventueel met contanten) via aangesloten winkeliers, tankstations en kiosken.

Neteller is een in 1999 opgericht online betaalsysteem uit Canada. In 2004 werd het hoofdkwartier verplaatst naar Isle of Man. Het bedrijf maakt deel uit van de Paysafe Group Plc.[121] Een Neteller wallet wordt aangemaakt in één valuta. Hierbij kan gekozen worden uit 26 verschillende landelijke valuta. Geld uit een Neteller e-wallet kan gebruikt worden om voor producten en diensten te betalen. Verder is het mogelijk om bitcoins te kopen met Neteller. Daarnaast biedt Neteller ook een virtuele en prepaid Mastercard aan. De provisie voor het opwaarderen van de wallet verschilt per methode, van 0% tot 8%.[122]

Perfect Money is een digitale financiële dienstverlener uit Panama. Het is mogelijk om vier soorten rekeningen te openen bij Perfect Money. Zo is er een rekening in Amerikaanse dollars (U-wallet), euro's (E-wallet), Gold (G-wallet), en Bitcoins (B-wallet). Bij Perfect Money wordt 4% rente uitbetaald

118 www.paypal.com/nl/webapps/mpp/paypal-fees (laatst geraadpleegd op 10 juli 2016).
119 https://en.wikipedia.org/wiki/Ukash (laatst geraadpleegd op 10 juli 2016).
120 Lange tijd was Paysafecard zelfstandig.
121 Zie het artikel 'Neteller' op Wikipedia. Beschikbaar op: https://en.wikipedia.org/wiki/Neteller (laatst geraadpleegd op 10 juli 2016).
122 Zie www.neteller.com/nl (laatst geraadpleegd op 10 juli 2016).

per jaar. Perfect Money biedt gebruikers de mogelijkheid om hun rekening te verifiëren met een ID-bewijs en een mobiel telefoonnummer. Een geverifieerd account heeft lagere kosten met extra opties voor accountbeveiliging.[123] Perfect Money heeft drie verschillende soorten accounts: een Normal account, Premium account, en Partner account. Voor transacties via de dienst wordt een commissie in rekening gebracht. Dit varieert van 2% voor een ongeverifieerde rekening tot 0,5% voor een geverifieerde Premium-rekening. Met een Perfect Money-rekening is het ook mogelijk om een prepaid card aan te vragen.

Bovengenoemde virtuele valuta worden allemaal centraal beheerd. De decentraal beheerde virtuele valuta zijn de cryptocurrencies. Veruit de bekendste cryptocurrency is *Bitcoin*. Ongeveer 90% van de totale marktwaarde van virtuele valuta wordt vertegenwoordigd door bitcoins (Trautman, 2014, p. 46). Deze cryptocurrency, met een open source protocol, werd in 2009 opgezet door Satoshi Nakamoto (Nakamoto, 2008). Dit is het pseudoniem van een onbekend persoon, vermoedelijk zelfs een groep onbekende personen. Bij Bitcoin is er geen centrale autoriteit of bank: het gehele netwerk van Bitcoin-gebruikers verifieert tezamen of een transactie legitiem is of niet (Engelfriet, 2014). Een nieuwe transactie wordt aan het gehele netwerk van gebruikers gemeld. Via het netwerk van gebruikers wordt de juiste versie van de blockchain gesynchroniseerd.

Bitcoins worden opgeslagen op een computer[124] in een bestand, de zogeheten Bitcoin wallet of Bitcoin-portemonnee.[125] Dit is niet zonder risico's: als het bestand wordt verwijderd of beschadigd, bijvoorbeeld door een computercrash, kan ook de toegang tot het geld in de wallet verdwenen zijn. De Bitcoin wallet kan ook worden gestolen, zowel door het bestand te stelen, bijvoorbeeld door hackers die inbreken op de computer, als door de computer zelf te stelen. De Bitcoin wallet kan ook in de cloud worden opgeslagen, maar ook daaraan zijn risico's verbonden. Het is immers maar de vraag of de betreffende clouddienst adequate beveiliging en bescherming biedt.

Bitcoin is zo opgezet dat er uiteindelijk 21 miljoen bitcoins in omloop zullen zijn. De verwachtingen over wanneer de laatste nieuwe bitcoin wordt geproduceerd lopen enigszins uiteen, van 2033 (FBI, 2012) tot 2040 (Baukema, 2013). Doordat er daarna geen nieuwe bitcoins meer bijkomen, wordt inflatie tegengegaan.[126] In 2013 waren er ongeveer 12 miljoen bitcoins in omloop

123 Zie https://perfectmoney.is/features.html (laatst geraadpleegd op 10 juli 2016).
124 Dat kan zijn op de eigen pc, maar ook in de cloud. Ook opslag op een smartphone is mogelijk.
125 Om precies te zijn: eigenlijk worden niet de bitcoins zelf opgeslagen in de Bitcoin wallet, maar bevat de Bitcoin wallet de sleutels/rechten om gebruik te kunnen maken van een Bitcoin-adres. Zonder deze rechten kan een gebruiker het Bitcoin-adres niet meer gebruiken om zijn of haar bitcoins te verplaatsen. Hierbij wordt gebruikgemaakt van asymmetrische encryptie. Dit houdt in dat de sleutel die wordt gebruikt voor het versleutelen van bestanden een andere sleutel is dan die wordt gebruikt voor het ontsleutelen van bestanden.
126 Merk op dat bij een andere cryptocurrency (Dogecoins) uiteindelijk werd besloten de initiële limiet te laten vervallen toen het maximum dichtbij kwam.

met een totale waarde van circa 10 miljard euro (Baukema, 2013, p. 413). De koers van de Bitcoin stond in januari 2013 op ongeveer $ 14 en in maart 2015 op ongeveer $ 250.[127]

Bitcoins zijn volgens de Europese en de Nederlandse wetgeving geen officieel geld (Engelfriet, 2014). De Wet op het financieel toezicht (Wft) kent, zoals hierboven al werd aangegeven, chartaal (contant), giraal en elektronisch geld.[128] Omdat bitcoins geen fysieke verschijningsvorm hebben, is het geen chartaal geld.[129] Bitcoins zijn echter ook geen elektronisch geld, omdat geen sprake is van een vordering op een uitgever.[130] Dit is ook door de Minister van financiën[131] en door de rechter[132] bevestigd. Ook zijn bitcoins geen financieel product, hetgeen wordt bevestigd door de Europese Centrale Bank (ECB, 2012, 2015). Daarmee kan de conclusie worden getrokken dat bitcoins en het gebruik van bitcoins ongereguleerd zijn en niet onderhevig zijn aan enige vorm van financieel toezicht.[133] Meer hierover in paragraaf 3.4. Bitcoins worden wel beschouwd als vermogen, waardoor er belasting over dient te worden betaald.

Bitcoins bieden volgens de FBI (2012) de gelegenheid tot het genereren, overboeken, witwassen en stelen van illegaal verkregen geld met enige anonimiteit. Alle transacties zijn openbaar en iedereen die dat wil, kan de transacties volgen. In principe zijn gebruikers anoniem, maar het is wel zo dat transacties van een (anonieme) gebruiker aan elkaar kunnen worden gekoppeld. Als de identiteit van een gebruiker bekend raakt, bijvoorbeeld omdat de gebruiker die zelf prijsgeeft op internet, kan diens gehele transactiehistorie worden achterhaald. Wel is het mogelijk als gebruiker meerdere Bitcoin wallets aan te maken en per wallet meerdere Bitcoin-adressen. Slechts per Bitcoin wallet kunnen transacties worden gekoppeld.

De technische werking van Bitcoin wordt nader beschreven in paragraaf 3.3.1. Het gebruik van bitcoins, waaronder het verkrijgen, overdragen en verkopen van bitcoins, wordt nader beschreven in paragraaf 3.3.2.

Naast Bitcoin bestaan er nog zo'n 600 andere cryptocurrencies, die vaak als groep worden aangeduid met de term '*altcoins*', als alternatief voor Bitcoin, die veruit het meest worden gebruikt. Bekende voorbeelden van andere cryp-

127 Zie www.koersbitcoins.net (laatst geraadpleegd op 10 oktober 2015).
128 Artikel 1:1 Wft.
129 Merk op dat er in het verleden wel fysieke bitcoin-munten zijn geslagen, zogeheten Casascius Bitcoins. Deze munten bevatten een code om ze te kunnen gebruiken op het internet. Na gebruik zijn het vooral verzamelobjecten. Zie www.casascius.com (laatst geraadpleegd op 10 oktober 2015). De Amerikaanse toezichthouder heeft dit echter verboden omdat er geen vergunning was voor deze praktijk. Zie: www.coindesk.com/us-regulators-bitcoin-mint-casascius-shut (laatst geraadpleegd op 10 oktober 2015).
130 Artikel 1:1 Wft (elektronisch geld).
131 Antwoord op Kamervragen, 7 juni 2013, 2013D18614.
132 Rb. Overijssel, 14 mei 2014, ECLI:NL:RBOVE:2014:2667.
133 Zie ook *Kamerstukken II*, 2012/13, Aanhangsel van de Handelingen, nr. 216.

tocurrencies zijn Litecoin[134] en Dogecoin.[135] Sommige altcoins zijn serieus bedoeld, andere lijken niet al te serieus. Litecoin is na Bitcoin de grootste cryptocurrency, met een totale waarde van ongeveer 880 miljoen euro in 2013. *Dogecoin* lijkt minder serieus bedoeld en begon in 2013 als een grap. Doge is een bekende internetmeme[136] die bestaat uit de afbeelding van een hond van het Japanse hondenras Shiba Inu. Deze afbeelding staat ook op Dogecoins. Andere relatief vaak genoemde cryptocurrencies zijn Namecoin en Peercoin (ook wel PPCoin genoemd).

In toenemende mate ontstaan er ook nieuwe modaliteiten, waarbij online betaalsystemen en exchanges naast betaal- en wisseldiensten ook hun eigen valuta aanbieden. Hieronder wordt het voorbeeld van Ripple beschreven om deze ontwikkeling te illustreren. Ripple kwam in dit onderzoek niet naar voren tijdens de interviews en in de onderzochte strafdossiers, maar wordt hier toch kort aangestipt als nieuwe ontwikkeling.

Ripple is een online betaalsysteem en wisselkantoor dat is ontwikkeld en opgezet in 2004 in Canada. Het systeem ondersteunt enerzijds echt geld als dollars, yens en euro's en anderzijds cryptocurrencies als Bitcoin en Litecoin. Ripple is een populair forum om bitcoins te verhandelen en in te wisselen. Omdat Ripple echter ook een eigen interne valuta heeft (ook Ripple geheten, afgekort XRP), kan het tevens worden gezien als virtueel geld. Ripple is gebaseerd op een openbaar register met saldi en informatie over aanbiedingen om valuta te kopen en verkopen. Bij elke wijziging in het register moet consensus in het netwerk van deelnemers worden bereikt. Dat gebeurt elke 2-5 seconden.[137] Ripple is opgezet om sneller en goedkoper (wat betreft rekentijd) transacties te verrichten dan Bitcoin. Waar bij Bitcoin voor elke transactie een complete (her)berekening moet plaatsvinden (zie volgende paragraaf), is Ripple gebaseerd op vertrouwen. Dit houdt in dat elke gebruiker aangeeft welke andere gebruikers te vertrouwen zijn. Bij een transactie wordt dan gekeken naar het vertrouwen in de omgeving van de betrokken gebruikers, waardoor sneller berekend kan worden of een transactie wel of niet kan worden geaccepteerd. Door deze opzet wordt Ripple ook wel het digitale hawala genoemd.[138] In tegenstelling tot bij Bitcoin is er geen miningproces bij Ripple. Er waren 100 miljard XRP in omloop bij de start van het systeem en geleidelijk neemt dit aantal af wanneer transactiekosten worden betaald. Daarmee kent Ripple een snelle deflatie. Ripple wordt door een deel van de financiële sector als innovatief beschouwd en wordt al door een paar

134 Zie https://litecoin.org/nl (laatst geraadpleegd op 10 oktober 2015).
135 Zie http://dogecoin.com (laatst geraadpleegd op 11 april 2016).
136 Een internetmeme is een concept dat zich via het internet van persoon tot persoon verspreidt. Het kan gaan om afbeeldingen, geruchten, broodjeaapverhalen, hoaxes, reclame, etc.
137 Zie http://en.wikipedia.org/wiki/Ripple_(payment_protocol) (laatst geraadpleegd op 10 oktober 2015).
138 Hawala is een informeel banksysteem voor het verplaatsen van geld dat veel gebruikt wordt in Pakistan, India en het Midden-Oosten. Wanneer bij het ene steunpunt contant geld op tafel wordt gelegd, kan dat bij een ander steunpunt worden opgehaald. Hawala is afgeleid van het Hindi-woord voor vertrouwen. Zie http://nl.wikipedia.org/wiki/Hawala (laatst geraadpleegd op 10 oktober 2015).

banken in de Verenigde Staten en Europa gebruikt.[139] Voor criminelen biedt Ripple vergelijkbare kansen als andere virtuele valuta. In 2015 kreeg Ripple in de Verenigde Staten een boete van 700.000 dollar voor het schenden van regelgeving op het gebied van antiwitwassen.[140]

3.3 Hoe werken cryptocurrencies?

In deze paragraaf zal worden ingegaan op de werking van decentraal beheerd (inwisselbaar) virtueel geld, ofwel cryptocurrencies. Eerst zal (kort en niet al te technisch) uiteengezet worden hoe cryptocurrencies werken vanuit een technisch perspectief. Daarna zal uiteengezet worden hoe cryptocurrencies werken vanuit een gebruikersperspectief. In deze paragraaf zal de nadruk liggen op de werking van Bitcoin, de meest populaire cryptocurrency.

3.3.1 Technische werking

Iemand die Bitcoins wil gebruiken heeft een Bitcoin wallet en een of meer Bitcoin-adressen nodig. Een Bitcoin wallet aanmaken kan via www.blockchain.info. Bij dit proces wordt een Bitcoin-adres verstrekt. Een gebruiker kan zoveel adressen/Bitcoin wallets aanmaken als nodig. De adressen worden gebruikt om het eigendom van een bitcoin weer te geven.[141] Elke overboeking vindt plaats naar een Bitcoin-adres, dus niet naar een bankrekening of een persoon. Voor cryptocurrencies als Bitcoin is het bij elke transactie noodzakelijk om te kunnen nagaan dat iemand echt eigenaar is van de betreffende bitcoins en dat die persoon de bitcoins niet eerder heeft uitgegeven.[142] Daartoe houdt het Bitcoin-netwerk een zogeheten block chain bij. Dit is een register dat alle transacties uit het verleden bevat. Elke gebruiker heeft toegang tot dit register, zodat de eigendom van bitcoins na te gaan is. Nieuwe transacties worden verzameld in blokken en de blokken tezamen vormen de block chain. Alle transacties in een bepaald blok krijgen hetzelfde tijdstip (timestamp) mee. Elk blok verwijst naar het vorige blok in de keten. Zolang transacties nog niet in een blok zitten, zijn ze onbevestigd. Een voorgesteld blok moet de oplossing bevatten van een complex wiskundig probleem dat lastig te berekenen is. Gemiddeld wordt ongeveer elke tien minuten een nieuw blok aan de keten toegevoegd (UNODC, 2014, p. 35).

139 Zie D. Proctor, 23 juni 2015, 'The Ripple effect: what's the impact on banking?'. Beschikbaar via: www.temenos.com/en/blog/2015/june/the-ripple-effect-whatstheimpact-on-banking (laatst geraadpleegd op 10 juli 2016).

140 Zie: www.capco.com/insights/capco-blog/facing-the-risks-of-crypto-regulators-take-on-virtual-payments (laatst geraadpleegd op 10 juli 2016).

141 Een adres is een combinatie van een publieke en een private cryptografische sleutel. Het ontvangende adres is de publieke sleutel en de private sleutel wordt gebruikt om transacties digitaal te ondertekenen, zodat transacties geauthentiseerd kunnen worden.

142 Dit is ook om 'valsemunterij' te voorkomen.

Omdat voor elk blok nieuwe berekeningen nodig zijn om het wiskundig probleem op te lossen, kost dit rekencapaciteit (en dus elektriciteitskosten). Daarom is er voor iedereen die een krachtige computer heeft, de mogelijkheid om nieuwe bitcoins te introduceren en daarvan eigenaar te worden (Engelfriet, 2014). Dit proces wordt mining (delven) genoemd. In feite zijn de nieuw geproduceerde bitcoins een vergoeding voor de beschikbaar gestelde rekencapaciteit (in het bijzonder de elektriciteitskosten) die nodig is voor het oplossen van het wiskundige probleem. Naarmate er meer rekencapaciteit in het Bitcoin-netwerk beschikbaar komt (in de vorm van meer of krachtigere computers), wordt het wiskundige probleem complexer en vergt het meer rekencapaciteit. Daarmee worden de kosten voor mining van nieuwe bitcoins in beginsel ook hoger.[143] Zoals aangegeven in de vorige paragraaf, houdt het proces van mining op als er 21 miljoen bitcoins in omloop zijn. Vanaf dat moment moet het beschikbaar stellen van rekencapaciteit volledig worden vergoed door het heffen van transactiekosten.[144]

3.3.2 Gebruik van bitcoins in het dagelijks verkeer

Een groeiend aantal bedrijven en personen accepteert betalingen in bitcoins, zowel in een fysieke omgeving als online. Dagelijks worden voor miljoenen dollars transacties in bitcoins verricht. Inmiddels kan ook in Nederland op diverse plaatsen met bitcoins worden betaald, niet alleen op het internet, maar bijvoorbeeld ook in bepaalde cafés en restaurants, hotels, interieurwinkels en modezaken.[145] Arnhem profileert zich bijvoorbeeld als meest bitcoinvriendelijke stad van Nederland, met meer dan honderd punten waar met bitcoins betaald kan worden.[146]

Voor winkeliers zijn er voordelen van betalingen door middel van bitcoins. Ten eerste zijn betalingen met bitcoins onomkeerbaar, zodat er geen risico is dat een transactie ongedekt is of gestorneerd wordt. Fraude zoals die voorkomt met betaalkaarten, komt niet voor bij bitcoins. Ten tweede zijn de kosten voor het verwerken van bitcoins lager dan de kosten die verbonden zijn aan betaalkaarten en bijbehorende betaalsystemen. Ten derde zijn er mogelijk internationale klanten of toeristen die graag gebruikmaken van betalingen middels bitcoins. Hieronder wordt uiteengezet hoe het aankopen en verkopen van bitcoins in zijn werk gaat (dus het converteren van bitcoins van en naar echt geld) en hoe het betalen met bitcoins in zijn werk gaat (dus iets aankopen met bitcoins).

143 Om de zoveel tijd wordt ook de beloning gehalveerd, waardoor de uitgifte van nieuwe bitcoins afneemt.
144 De transactiekosten gaan dan naar de miner die als eerste de oplossing heeft.
145 Zie bijvoorbeeld een lijst met winkels en horecagelegenheden op: www.watisbitcoin.nl/uitgeven.php (laatst geraadpleegd op 19 oktober 2015).
146 www.arnhembitcoinstad.nl.

Bitcoins kunnen worden aangekocht of verkocht via tussenpersonen, zogeheten Bitcoin-wisselkantoren, die bitcoins aan- en verkopen tegen commissie.[147] De commissie kan bestaan uit een vast bedrag per transactie, een percentage van het transactiebedrag of een combinatie van beide. Daarnaast zijn er ook Bitcoin-platformen waar gebruikers zonder tussenpersonen met elkaar kunnen handelen. Hier worden vraag en aanbod bij elkaar gebracht. Ook bij Bitcoin exchanges wordt vaak een commissie gerekend die kan bestaan uit een vast bedrag per transactie, een percentage van het transactiebedrag of een combinatie van beide. Veel online Bitcoin-platformen beheren ook online wallets voor gebruikers, waaraan verschillende betaalmethoden kunnen zijn gekoppeld voor het omzetten van digitaal geld in contant geld.[148] Bij Bitcoin-wisselkantoren worden zelden voor particulieren wallets beheerd. Bij Bitcoin-platformen dient men zich doorgaans te registreren en soms ook identificerende persoonsgegevens te verstrekken. In de praktijk noemen zowel Bitcoin-platformen als Bitcoin-wisselkantoren zichzelf een Bitcoin exchange en er zijn ook Bitcoin exchanges die beide diensten aanbieden, waardoor het onderscheid tussen Bitcoin-platformen en Bitcoin-wisselkantoren soms lastig te maken is.

Populaire Bitcoin exchanges zijn onder meer CleverCoin,[149] Kraken[150] en BitStamp.[151] In Nederland is Bitonic[152] een populaire Bitcoin exchange. Transacties kunnen plaatsvinden van de ene naar de andere virtuele valuta.[153] Transacties kunnen ook plaatsvinden via iDEAL danwel overboekingen via een bank,[154] een betaalkaart,[155] contant[156] of PayPal.[157] Ook het aanschaffen van bitcoins via sms is mogelijk.[158]

Inmiddels zijn ook de eerste Bitcoin-geldautomaten opgedoken, de eerste in Canada[159] en in Stockholm.[160] Op de website http://bitcoinatmmap.com is te zien waar zoal Bitcoin-geldautomaten beschikbaar zijn. Deze automaten werken met een zogeheten QR-code. Het aankopen van bitcoins vindt plaats

147 Zie http://debitcoin.org/hoe-verkrijg-je-bitcoins (laatst geraadpleegd op 19 oktober 2015).
148 Het omzetten van digitaal geld in contant geld wordt in het witwasproces ook wel de 'cash-out' genoemd. Zie paragraaf 4.1.1.
149 Zie www.clevercoin.com (laatst geraadpleegd op 19 oktober 2015).
150 Zie www.kraken.com (laatst geraadpleegd op 19 oktober 2015).
151 Zie https://nl.bitstamp.net (laatst geraadpleegd op 19 oktober 2015).
152 Zie www.bitonic.nl (laatst geraadpleegd op 19 oktober 2015).
153 Zie https://firstmetaexchange.com/home, www.virwox.com/?stage=1, en https://howtobuybitcoins.info. (laatst geraadpleegd op 19 oktober 2015).
154 Zie www.bitstamp.net/help/how-to-buy en http://portal.bitcoinschile.cl (laatst geraadpleegd op 19 oktober 2015).
155 Zie http://btc-delaer.com (laatst geraadpleegd op 19 oktober 2015).
156 Zie www.tradebitcoin.com en https://localbitcoins.com (laatst geraadpleegd op 19 oktober 2015).
157 Zie www.virwox.com/?stage=1 (laatst geraadpleegd op 19 oktober 2015).
158 Zie http://sms.btc-com (laatst geraadpleegd op 19 oktober 2015).
159 Zie Nu.nl, 'Canada komt met 's werelds eerste bitcoin-pinautomaat', 27 oktober 2013. Beschikbaar op: www.nu.nl/tech/3612448/canada-komt-met-s-werelds-eerste-bitcoin-pinautomaat.html (laatst geraadpleegd op 19 oktober 2015).
160 Zie www.telegraaf.nl/tv/dft/nieuws/22136934/__Eerste_Europese_bitcoin-geldautomaat__.html (laatst geraadpleegd op 19 oktober 2015).

door de gekochte bitcoins bij te schrijven op de persoonlijke Bitcoin wallet. Het systeem geeft tegelijkertijd een QR-code uit waarmee omgekeerd ook weer dollars kunnen worden gekocht voor de bitcoins. De code moet worden gescand door de mobiele telefoon.[161]

Transacties uitvoeren met bitcoins gaat via de Bitcoin wallet (zie vorige paragraaf) en lijkt vanuit gebruikersperspectief min of meer op het versturen van een e-mailbericht. Om bitcoins over te kunnen maken naar een andere gebruiker is enkel diens ontvangstadres nodig. Het overboeken komt in de praktijk neer op het invullen van het adres van de ontvanger (de begunstigde), het invullen van het aantal bitcoins (het transactiebedrag) en klikken op verzenden.[162] Er is geen verdere verificatie of authenticatie nodig, zoals een pincode.[163] Het versturen is een onomkeerbaar proces. Wanneer te veel is overgemaakt of naar het verkeerde adres is overgemaakt, is dit niet meer ongedaan te maken.

3.3.3 Voor- en nadelen van virtueel geld

Virtueel geld biedt voor gebruikers een aantal voordelen ten opzichte van elektronisch geld. Bij overboekingen naar het buitenland hoeft de ontvanger bijvoorbeeld geen bankrekening te hebben en hoeven geen buitenlandse valuta of wisselkoersen aangevraagd te worden. Ook zijn vaak de transactiekosten vele malen lager dan bij traditionele manieren van overboeken, in het bijzonder overboekingen naar het buitenland. Verder kunnen (met name internationale) transacties in bepaalde gevallen veel sneller worden afgehandeld. Dit hangt overigens wel af van het type virtueel geld: bij centrale virtuele valuta kunnen transacties soms ook langer duren en bij Bitcoin is het netwerk tegenwoordig dusdanig belast dat het valideren van transacties steeds langer duurt. Dit kan onpraktisch zijn voor real time afrekenen voor producten of diensten. Virtueel geld kent doorgaans geen maximale transactiebedragen (UNODC, 2014 p. 47). Virtuele valuta kunnen ook worden aangeschaft als investering of belegging. Tot slot is ook een voordeel dat transacties met bitcoins en andere valuta die een block chain (zie vorige paragraaf) gebruiken onomkeerbaar zijn. Daardoor kan geld niet worden teruggeboekt en kan verlies door fraude (in tegenstelling tot bijvoorbeeld een betaalkaart die geen dekking blijkt te hebben) worden voorkomen.

161 Zie banken.nl, 'Canada lanceert eerste Bitcoin pinautomaat ter wereld', 30 oktober 2013. Bescihkbaar op: www.banken.nl/nieuws/1506/canada-lanceert-eerste-bitcoin-pinautomaat-ter-wereld (laatst geraadpleegd op 19 oktober 2015).

162 Zie www.bitcoinspot.nl/hoe-kan-je-met-bitcoins-betalen.html (laatst geraadpleegd op 19 oktober 2015). Merk op dat het ook mogelijk is een vrijwillige toeslag te betalen waardoor transacties sneller worden opgenomen in de blockchain.

163 Wel is een private key (cryptografische sleutel) nodig om transacties te kunnen verrichten. Deze zit in de Bitcoin wallet.

Nadelen van virtueel geld voor gebruikers zijn er ook. Het toezicht op cryptocurrencies en andere virtuele valuta ontbreekt in veel landen (waaronder Nederland), waardoor gebruikers maar moeten afwachten hoe betrouwbaar andere partijen zijn. Bij fraude of oplichting is er daardoor meestal ook geen bescherming of schadevergoeding. Naast vertrouwen in specifieke andere partijen met wie zaken wordt gedaan, is vertrouwen in het gehele systeem een gevoelig punt: gelet op het gebrek aan regulering en financieel toezicht is rechtszekerheid een probleem. Mede daardoor kennen veel cryptocurrencies stevige koersschommelingen, waardoor virtueel geld aanzienlijk in waarde kan dalen (Chambers-Jones & Hillman, 2014, p. 141). Verder kunnen transacties niet ongedaan gemaakt worden (zie vorige paragraaf over de block chain). Dit kan een voordeel zijn (zie hierboven) als het gaat om de zekerheid voor de ontvangende partij, maar ook een nadeel voor de betalende partij, bijvoorbeeld wanneer een vergissing wordt gemaakt (verkeerde ontvanger) of wanneer producten niet worden geleverd.

3.3.4 Anonimiteit

Het gebruik van bitcoins biedt enige anonimiteit, maar helemaal anoniem is het niet. Door het gebruik van Bitcoin-adressen gaan de identiteiten van Bitcoin-gebruikers feitelijk schuil achter pseudoniemen.[164] Transacties vanaf een Bitcoin-adres kunnen aan elkaar gerelateerd worden, maar pseudoniemen kunnen niet zonder meer gerelateerd worden aan de identiteit van de gebruiker. Omdat transacties vanaf een Bitcoin-adres aan elkaar gekoppeld kunnen worden, kan het voor criminelen gunstig zijn om veel Bitcoin-adressen tegelijk te gebruiken en/of regelmatig van Bitcoin-adressen te wisselen. Op die manier wordt voorkomen dat al te veel herleidbaarheid ontstaat. In hoofdstuk 5 komen verdere manieren aan bod die criminelen gebruiken om hun anonimiteit te waarborgen en de herkomst van crimineel verkregen geld verder te verhullen.[165]

Bij het overmaken van bitcoins gaan deze van het ene pseudoniem naar het andere. Als een gebruiker met meerdere Bitcoin-adressen bitcoins naar zichzelf overmaakt, kunnen de verschillende adressen van een gebruiker in potentie aan elkaar gerelateerd worden. Dit werd bij het ontwerp van Bitcoin al erkend (zie Nakamoto, 2008). Omdat niet duidelijk is of achter het betalende en het ontvangende Bitcoin-adres dezelfde gebruiker schuilt, is dit in eerste instantie slechts een aanwijzing. Maar door het analyseren van transactiegegevens met meer geavanceerde methoden, kunnen pseudoniemen geclusterd worden tot verschillende gebruikers (Meiklejohn et al., 2013; Ron & Shamir, 2013).

164 Meer specifiek gaat het om de publieke sleutel in het Bitcoin-adres.
165 Zie bijvoorbeeld de rol van mixing services (paragraaf 5.2.3) en de rol van Bitcoin-handelaren (paragraaf 5.2.4).

Vervolgens blijft het nog steeds de uitdaging om de pseudoniemen te koppelen aan hun echte identiteiten. Dit kan bijvoorbeeld door de transactiegegevens en geclusterde Bitcoin-adressen te koppelen aan andere bronnen. Wanneer bijvoorbeeld iemand op een forum zijn of haar Bitcoin-adres noemt, is een koppeling mogelijk (Meiklejohn et al., 2013; Reid & Harrigan, 2013). Ook via informatie over betalingen bij webwinkels kunnen bijvoorbeeld afleveradressen en e-mailadressen en andere informatie worden achterhaald. Criminelen zullen wellicht niet snel de Bitcoin-adressen prijsgeven waarmee ze geld witwassen, maar soms minder voorzichtig zijn met Bitcoin-adressen waarmee ze legale bestedingen willen doen.

Meer voorzichtige criminelen zullen gebruikmaken van anonimiseringsdiensten als Tor. Biryukov et al. presenteren een methode om Bitcoin-adressen aan IP-adressen te koppelen en anonimiseringsmethoden te omzeilen (Biryukov, Khovratovich & Pustogarov, 2014). Ook daartegen zijn weer maatregelen te bedenken, waaronder enkele tegenmaatregelen die Biryukov et al. (2014) zelf voorstellen. Anonimiseren en identificeren is een kat-en-muisspel tussen criminelen en opsporingsdiensten, maar het gebruik van digitale betalingsmiddelen laat altijd digitale sporen achter en is dus niet geheel anoniem.

3.4 Juridische status en toezicht

Zoals hierboven al is aangegeven, kent de Wet op het financieel toezicht (Wft) chartaal (contant), giraal en elektronisch geld (Baukema, 2013, p. 413), en zijn bitcoins volgens de Europese en de Nederlandse wetgeving geen officieel geld (Engelfriet, 2014). Omdat bitcoins geen fysieke verschijningsvorm hebben, is het geen chartaal geld.[166] Bitcoins zijn echter ook geen elektronisch geld, omdat geen sprake is van een vordering op een uitgever.[167] Dit is ook door de Minister van Financiën[168] en door de rechter[169] bevestigd. Ook zijn bitcoins geen financieel product, hetgeen wordt bevestigd door de Europese Centrale Bank (ECB, 2012, 2015). Daarmee kan de conclusie worden getrokken dat bitcoins en het gebruik van bitcoins ongereguleerd zijn en in Nederland niet onderhevig zijn aan enige vorm van financieel toezicht.[170] Teneinde meer zicht te krijgen op de mogelijke (juridische) aanpak van witwassen met behulp van digitale betalingsmiddelen,[171] wordt in deze paragraaf gekeken naar de juridische status van virtueel geld, in het bijzonder bitcoins, in

166 Merk op dat in het verleden wel fysieke bitcoin-munten zijn geslagen, zogeheten Casascius Bitcoins. Deze munten bevatten een code om ze te kunnen gebruiken op het internet. Na gebruik zijn het vooral verzamelobjecten. Zie www.casascius.com (laatst geraadpleegd op 10 oktober 2015). De Amerikaanse toezichthouder heeft dit echter verboden omdat er geen vergunning was voor deze praktijk. Zie: www.coindesk.com/us-regulators-bitcoin-mint-casascius-shut (laatst geraadpleegd op 10 oktober 2015).

167 Artikel 1:1 Wft (elektronisch geld).

168 Antwoord op Kamervragen, 7 juni 2013, 2013D18614.

169 Rb. Overijssel, 14 mei 2014, ECLI:NL:RBOVE:2014:2667.

170 Zie ook *Kamerstukken II*, 2012/13, Aanhangsel van de Handelingen, nr. 2162 (Handelingen 2012/2013).

171 Zie paragraaf 6.2.

andere landen (paragraaf 3.4.1) en naar toezicht op het gebruik van virtueel geld, met eveneens focus op bitcoins (paragraaf 3.4.2).

3.4.1 Juridische status

Deze paragraaf gaat in op hoe virtueel geld, in het bijzonder bitcoins, juridisch kan worden gezien.[172] In verschillende landen wordt verschillend aangekeken tegen de juridische status van virtueel geld. In de eerste plaats is het gebruik van en de handel in bitcoins en andere virtuele valuta in verschillende landen verboden.[173] Voorbeelden van landen waar bitcoins zijn verboden, zijn: Argentinië, Bangladesh, Bolivia, Indonesië, Kirgizië, Rusland, Thailand en Vietnam. In Vietnam bijvoorbeeld stelt de overheid zich op het standpunt dat het gebruik van bitcoins veel risico's met zich meebrengt waarvoor de overheid niet garant kan staan of bescherming kan bieden, en dat het de economie kan ontwrichten. Andere landen plaatsen restricties aan het gebruik van bitcoins. Zo mogen in China bitcoins niet worden gebruikt door banken en andere financiële instellingen. In IJsland wordt het aankopen van bitcoins uit het buitenland gezien als uitgaand kapitaalverkeer, hetgeen niet is toegestaan. Hoe het zit met binnenlandse Bitcoin-transacties is onduidelijk, maar Bitcoin mining is wel toegestaan. In Taiwan mogen wel bitcoins worden verhandeld, maar zijn Bitcoin-geldautomaten verboden.[174] In de EU en andere Westerse landen, waaronder Australië, Canada, de Verenigde Staten en Zwitserland is het gebruik van en de handel in bitcoins gewoon toegestaan. In Zuid-Korea is virtueel geld wel toegestaan, maar is speelgeld in online games gereguleerd: het is er verboden speelgeld uit games te kopen of verkopen met echt geld.[175]

Zoals hierboven is aangegeven, wordt virtueel geld in Nederland en de Europese Unie niet gezien als geld en ook niet als financieel product. Bitcoins en andere vormen van virtueel geld zouden gelet op hun aard en functie uiteraard wel gezien kunnen worden als geld of financieel product. In de landen waar bitcoins zijn toegestaan, is echter (tot dusver) nergens sprake van officiële erkenning van bitcoins als wettig betaalmiddel.[176] Duitsland is het eerste land dat bitcoins min of meer als rechtmatig betaalmiddel beschouwt: in augustus 2015 gaf het ministerie van Financiën aan dat bitcoins een betaalmiddel zijn.[177] Daarmee is de officiële juridische status van bitcoins in Duitsland echter nog niet helder. In de meeste landen worden bitcoins en ander

172 Hoe virtueel geld economisch wordt gezien valt buiten het bereik van dit onderzoek.
173 Zie https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country (laatst geraadpleegd op 19 oktober 2015).
174 J. Horwitz, 'Now you can buy bitcoin along with your snacks and sodas in 3,000 Taiwanese convenience stores', *Tech in Asia*, 8 oktober 2014. Beschikbaar via: www.techinasia.com (laatst geraadpleegd op 19 oktober 2015).
175 Yoon, A. (2007). 'Selective Bombing of RMT in Korea', *TerraNova*, 13 mei 2007.
176 Bij betalingen anders dan met een wettig betaalmiddel dienen partijen akkoord te gaan met het betreffende betaalmiddel. Zie Bollen, 2012, p. 34.
177 Zie Nu.nl, 'Duitsland eerste land dat Bitcoin erkent als valuta'. Beschikbaar op: www.nu.nl/tech/3553479/duitsland-eerste-land-bitcoin-erkent-als-valuta.html (laatst geraadpleegd op 19 oktober 2015).

virtueel geld gezien als een ruilmiddel (bijvoorbeeld in Australië) of een goed of gebruiksvoorwerp ('commodity').[178] Dit laatste is het geval in de Verenigde Staten.[179] Een belangrijke reden om bitcoins juridisch gezien als een bezit van waarde te beschouwen, lijkt te zijn dat het daarmee mogelijk wordt belasting te heffen.[180] Zulke belasting kan onder meer vermogensbelasting en inkomstenbelasting betreffen (Bal, 2013). Het mag duidelijk zijn dat handhaving een grote uitdaging is voor belastingdiensten wereldwijd (Gruber, 2013). Daarmee zijn cryptocurrencies interessant voor belastingontduikers die niet of niet meer terecht kunnen in traditionele belastingparadijzen (Marian, 2013).

3.4.2 Toezicht en strafrechtelijke handhaving

Op basis van de analyse in de vorige paragraaf kan worden geconcludeerd dat virtueel geld in veel landen niet als geld of financieel product wordt gezien. Dit heeft als gevolg dat het buiten de scope van financiële toezichthouders valt, al zal in het geval van centraal beheerd virtueel geld in veel landen de uitgever een licentie moeten aanvragen als betaaldienst, waarna deze onder toezicht staat en moet voldoen aan antiwitwasverplichtingen. Bitcoins en andere cryptocurrencies worden veelal niet genoemd in wetgeving op nationaal en internationaal niveau (Chambers-Jones & Hillman, 2014, p. 164). Gelet op mogelijke misstanden zou regulering wenselijk kunnen zijn, maar regulering en de bijbehorende handhaving en controlemechanismen ontbreken veelal (Tropina, 2014, p. 77).

Toezicht op virtueel geld is ook ingewikkelder dan het traditionele toezicht op banken en andere financiële instellingen, eenvoudigweg omdat bij decentraal virtueel geld als bitcoins strikt genomen geen banken nodig zijn om transacties te verrichten (Weimer, 2000, p. 199). Hoewel centrale banken in veel landen waarschuwen voor de risico's van bitcoins, houden ze zich verder niet bezig met toezicht. Ook gewone banken en andere financiële instellingen zijn nauwelijks betrokken bij virtueel geld (UNODC, 2014, p. 55). Daarmee staat virtueel geld als bitcoins vrijwel helemaal los van het reguliere betalingssysteem met bijbehorend toezicht en handhaving. Veel banken

178 Forbes, S. (2013). 'Bitcoin: Whatever it is, it's not money!' *Forbes*, 16 april 2013. Beschikbaar op: www.forbes.com/sites/steveforbes/2013/04/16/bitcoin-whatever-it-is-its-not-money (laatst geraadpleegd op 19 oktober 2015). Zie ook CFTC, 'CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering', 17 september 2015. Beschikbaar op: www.cftc.gov/PressRoom/PressReleases/pr7231-15 (laatst geraadpleegd op 19 oktober 2015).

179 Clinch, M. (2015). 'Bitcoin now classed as a commodity in the US'. *CNBC*, 18 september 2015. Beschikbaar op: www.cnbc.com/2015/09/18/bitcoin-now-classed-as-a-commodity-in-the-us.html (laatst geraadpleegd op 19 oktober 2015).

180 Zie ook: Lederman (2007, p. 1670-1672) en Seto (2009). Ook in Nederland is de opgave van bitcoins voor belastingdoeleinden verplicht, omdat ze als vermogen worden beschouwd.

monitoren wel het girale verkeer van hun klanten (bij aankoop en verkoop) van Bitcoin-gerelateerde transacties.[181]

Naast de eerder genoemde legitieme voordelen van onder meer hoge snelheid, lage transactiekosten en landsgrenzen die niet langer een hindernis vormen, is virtueel geld voor criminelen aantrekkelijk omdat (FBI, 2012; Tropina, 2014, p. 69-84):

- toezicht vanuit financiële instellingen/toezichthouders in veel landen ontbreekt (waaronder Nederland);[182]
- transacties tot op zekere hoogte anoniem kunnen plaatsvinden;[183]
- transacties mondiaal kunnen worden uitgevoerd zonder uitgebreide bankinfrastructuur en zonder bankrekening (Europol, 2015c, p. 30);[184]
- meerdere transacties vanaf meerdere Bitcoin-accounts kunnen worden gestapeld om de herkomst en routering van geld te verhullen (UNODC, 2014, p. 47);[185]
- virtueel geld een betrekkelijk nieuw fenomeen is; daarom ontbreekt kennis en ervaring bij verschillende (delen) van opsporingsinstanties (UNODC, 2014, p. 60);[186]
- verschillende landen verschillend beleid of helemaal geen beleid voeren met betrekking tot virtueel geld (Chambers-Jones & Hillman, 2014, p. 155);
- zich vanwege het internationale karakter van virtueel geld jurisdictieproblemen bij politie en justitie kunnen voordoen waardoor criminelen moeilijker te pakken zijn (UNODC, 2014, p. 145).[187]

Aanpassingen in de wetgeving om cryptocurrencies als bitcoins wel te reguleren en onder het reguliere financiële toezicht onder te brengen, zouden onder meer de rechtszekerheid en consumentenbescherming kunnen verstevigen.[188] De vraag is echter op welke wijze dit zou moeten gebeuren, want het identificeren van klanten (Know Your Customer) is lastig af te dwingen bij Bitcoin exchanges wanneer deze in het buitenland zijn gevestigd. In elk geval

181 Ook andere payment service providers kunnen een rol hebben bij de aankoop en verkoop van bitcoins en daarom betrokken worden in het toezicht, zie hieronder.

182 Zie ook Meuzelaar, D. & Wely, M. van (2015). 'De moderne boef gaat voor anonieme bitcoin; geen bank of andere tussenpersoon nodig'. *De Telegraaf*, 24 augustus 2015. Merk op dat Bitcoin exchanges soms wel onder toezicht staan en/of een meldplicht hebben en een KYC-beleid voeren. Zie paragraaf 2.4.1 voor meer hierover.

183 Transacties zijn anoniem, maar via een Bitcoin-adres wel aan elkaar te linken. Wanneer bekend wordt wie achter een bepaalde transactie zit, kunnen alle andere transacties vanaf dat Bitcoin-adres ook aan die persoon worden toegeschreven.

184 Merk op dat dit ook een voordeel kan zijn voor legitieme gebruikers, bijvoorbeeld in ontwikkelingslanden.

185 Hierbij kan onder meer gebruik worden gemaakt van zogeheten *mixing services* of *tumblers.* Zulke diensten vermengen de Bitcoin-tegoeden van verschillende eigenaren opdat de herkomst van de bitcoins wordt verhuld. In veel gevallen zijn deze diensten overigens onbetrouwbaar en retourneren ze de tegoeden helemaal niet.

186 In sommige landen is beperkt of geen toezicht, zodat ook geen sprake is van klantenidentificatieplicht (Know Your Customer) of meldplicht van ongebruikelijke transacties.

187 Specifiek bij cloud computing kan jurisdictie een probleem zijn. Zie ook: Koops et al. (2012).

188 Zie bijvoorbeeld Haverkort, H. (2013). 'Pvda wil beter toezicht op nieuwe digitale betaalmiddelen', *NU.nl*, 28 oktober 2013. Beschikbaar op: www.nu.nl/politiek/3613337/pvda-wil-beter-toezicht-nieuwe-digitale-betaalmiddelen.html (laatst geraadpleegd op 9 maart 2016).

zou de wetgeving hiervoor tot op zekere hoogte technologieonafhankelijk moeten worden geformuleerd om te voorkomen dat nieuwe technologieën meteen al buiten de reikwijdte komen te vallen (Vandezande, 2014). Bitcoin exchanges zouden in de toekomst een rol kunnen spelen in het toezicht, maar daarvan is tot dusver slechts beperkt sprake.

Het gebrek aan regulering en toezicht zou de verdere ontwikkeling van virtueel geld in de weg kunnen staan, omdat er (rechts)onzekerheid bestaat over wat wel en niet is toegestaan. Tegelijkertijd kan een overvloed aan regulering verdere innovatie in de kiem smoren. Een gebalanceerde aanpak kan zijn 'smart regulation', die gericht is op aanwezige risico's: daar waar risico's groter zijn, worden steviger interventies ingezet (Tropina, 2014, p. 81).

Daarbij moet wel rekening worden gehouden met het feit dat Bitcoin exchanges eenvoudig van jurisdictie kunnen wisselen waardoor het lastig wordt lokale (Nederlandse) normen af te dwingen (Christopher, 2013, p. 23). Zelfs wanneer het mogelijk is door middel van rechtshulp bewijs – zoals registratiegegevens en transactiegegevens – te verkrijgen, is rechtshulp een relatief traag instrument vergeleken met de snelle verplaatsing van het geld via internet (Trautman, 2014, p. 41). Christopher (2013, p. 29) stelt daarom een alternatieve benadering voor door meer intensief samen te werken met de dienstverleners van nieuwe online betalingsdiensten om meer ernstige delicten als witwassen tegen te gaan in plaats van direct over te gaan tot regulering en handhaving van regelgeving met betrekking tot financieel toezicht. Samenwerking bij handhaving en het verzamelen van bewijs zijn daarbij cruciaal. Indien toch tot regulering wordt overgegaan, moet rekening worden gehouden met verplaatsingseffecten. Om deze reden ligt het tevens voor de hand eventuele regulering in EU-verband te laten plaatsvinden om een gefragmenteerd juridisch kader en 'free havens' binnen de Europese Unie tegen te gaan.

3.5 Tussenconclusie

In dit hoofdstuk is antwoord gegeven op de vraag: *Wat zijn digitale betalingsmiddelen en hoe werken ze?* Digitaal geld kan daarbij worden omschreven als de tegenhanger van fysiek geld (contant geld en plastic geld in de vorm van creditcards, pinpassen en chipkaarten) en kan bestaan uit elektronisch geld (de digitale weergave van echt geld) of virtueel geld (zoals vouchers, speelgeld in online games of cryptocurrencies).

Veruit de bekendste cryptocurrency is Bitcoin, met 90% van de totale marktwaarde van virtuele valuta. Naast de voordelen die ook voor legitieme gebruikers gelden, heeft Bitcoin ook voordelen specifiek voor criminelen. Voorbeelden hiervan zijn het ontbreken van toezicht vanuit financiële instellingen,

een beperkte of afwezige klantenidentificatieplicht (Know Your Customer), afwezigheid van een meldplicht voor ongebruikelijke transacties, het stapelen van accounts en transacties om de herkomst van geld te verhullen en een lagere pakkans ten gevolge van beperkte kennis, ervaring en internationale samenwerking van opsporingsinstanties ten gevolge van niet-geharmoniseerd beleid en jurisdictieproblemen.[189] Cryptocurrencies kunnen ook worden gebruikt om geld te stallen teneinde belasting te ontduiken/ontwijken.

Bitcoin-transacties hebben een bepaalde mate van anonimiteit. Het is echter wel zo dat via de block chain in beginsel de herkomst van elke bitcoin kan worden getraceerd en transacties van een bepaald Bitcoin-adres aan elkaar kunnen worden gekoppeld.[190] Wanneer iemands identiteit dan bekend wordt voor een bepaalde transactie of Bitcoin-adres, is voor alle transacties de anonimiteit verdwenen. Bitcoins laten dus in vergelijking met contant geld relatief veel (digitale) sporen achter, die in opsporingsonderzoek van belang kunnen zijn om de transacties na te gaan.

Vanuit het perspectief van politie en justitie zou regulering van virtueel geld, met name van cryptocurrencies als Bitcoin, een bijdrage kunnen leveren aan de criminaliteitsbestrijding. Daarbij kan in het bijzonder in overweging worden genomen Bitcoin exchanges te reguleren. Echter, juist bij cryptocurrencies is het door het decentrale beheer zeer eenvoudig om uit te wijken naar landen waar toezicht ontbreekt. Omdat bitcoins niet als geld of financieel product worden beschouwd, is de rol van banken en financiële toezichthouders enigszins beperkt. Zij kunnen weliswaar waarschuwen voor de risico's van virtueel geld, en doen dat ook, maar kunnen op dit punt niet hun volledige arsenaal aan toezicht- en handhavingsmaatregelen inzetten. Zo kunnen zij slechts beperkt een bijdrage leveren aan de opsporing en vervolging van witwaspraktijken.

189 In het buitenland spelen vergelijkbare, maar niet altijd dezelfde problemen. Bijvoorbeeld in de Verenigde Staten staan grote bitcoin exchanges wel onder toezicht en moeten zij verdachte transacties melden aan FINCEN.
190 Bovendien kunnen Bitcoin-adressen behorende bij dezelfde Bitcoin wallet worden geclusterd.

4 Witwassen van geld verkregen uit banking malware en ransomware

In dit hoofdstuk wordt onderzocht op welke wijze het geld dat wordt verkregen uit banking malware en ransomware wordt witgewassen.[191] Daarmee wordt antwoord gegeven op de deelvraag: *Op welke wijze en door welke actoren wordt geld witgewassen dat door middel van banking malware en ransomware wordt verkregen?* Tevens wordt ingegaan op de rol van digitale betalingsmiddelen, in bijzonder bitcoins, in de witwasprocessen. Daarmee wordt tevens de deelvraag beantwoord: *Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?*

In dit onderzoek ligt de nadruk op witwasmethoden waarbij digitale betalingsmiddelen zijn betrokken.[192] In veel gevallen zullen, ook bij het witwassen van opbrengsten van cybercrime, in het witwasproces 'klassieke witwasmethoden' worden gebruikt.[193] De modi operandi die in dit hoofdstuk worden beschreven, kunnen daarom voornamelijk worden beschouwd als bouwstenen van het witwasproces. In de praktijk worden de methoden die hieronder worden beschreven en de 'klassieke methoden' in allerlei volgordes en varianten gecombineerd, met als doel de herkomst van het crimineel verkregen geld verder te verhullen. De daadwerkelijk gebruikte ketens zijn in de praktijk vaak langer en complexer dan de modellen die in dit hoofdstuk worden gepresenteerd.

In paragraaf 4.1 wordt nagegaan op welke wijzen het verkregen geld uit banking malware wordt witgewassen. In paragraaf 4.2 wordt het witwasproces van geld dat wordt verkregen uit ransomware onderzocht. In beide witwasprocessen wordt specifiek ingegaan op de rol van digitale betalingsmiddelen, in het bijzonder bitcoins, in het witwasproces. In de tussenconclusie in paragraaf 4.3 wordt antwoord gegeven op de twee deelvragen.

4.1 Witwasproces bij banking malware

Het geld dat met banking malware wordt verdiend door cybercriminelen is in eerste instantie elektronisch geld – digitale euro's, dollars of andere fiatvaluta[194] – omdat ze van een digitale bankrekening worden gehaald via internetbankieren. Cybercriminelen zullen op zoek gaan naar manieren om het verkregen geld om te zetten in besteedbaar geld, goederen of diensten.

191 Merk op dat er juridisch gezien al sprake kan zijn van witwassen voordat cybercriminelen de opbrengsten tot hun beschikking hebben. De term 'verkregen' duidt hier vooral op het feit dat het geld afhandig is gemaakt van het slachtoffer.

192 Zie hoofdstuk 1.

193 Zie paragraaf 2.4.

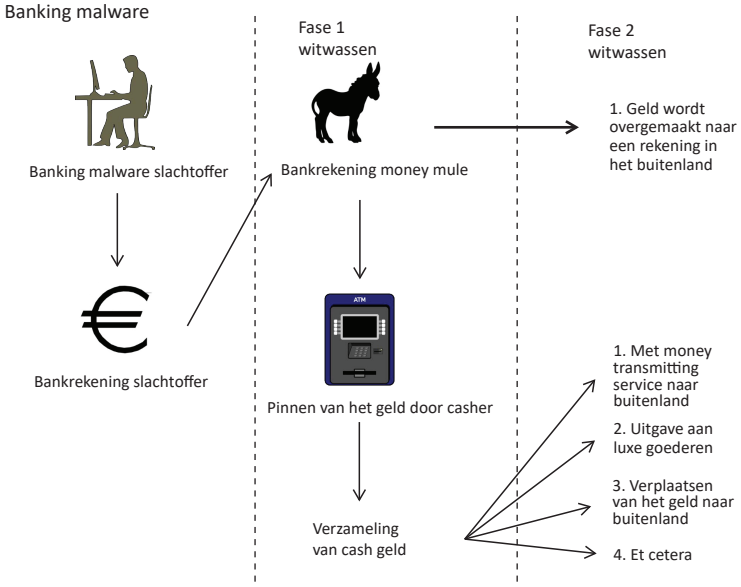
194 Fiatvaluta is een betaalmiddel of geldsoort waarvan de overheid verplicht dat mensen het accepteren als betaalmiddel of geldsoort en waarvan de waarde niet wordt gedekt die het als gebruiksgoed heeft.

Uit het door ons uitgevoerde literatuuronderzoek, dossieronderzoek en de afgenomen interviews blijkt dat twee terugkerende modellen onderscheiden kunnen worden. Het eerste model beschrijft hoe geld wordt witgewassen met behulp van money mules, waarbij de nadruk ligt op het omzetten van het elektronische geld in contant geld, dat vervolgens kan worden besteed of naar het buitenland worden weggesluisd. Het tweede model beschrijft hoe het elektronische geld direct wordt uitgegeven aan goederen of diensten. Hoewel het ook mogelijk is dat cybercriminelen het verkregen geld uit banking malware op andere wijzen witwassen, zoals bijvoorbeeld door een combinatie van klassieke methoden en de hieronder beschreven methoden, zijn de hieronder beschreven modellen de modi operandi die wij in ons onderzoek hoofdzakelijk zijn tegengekomen.

4.1.1 Witwassen via money mules en directe 'cash-out'

Het eerste model van het witwassen van geld dat wordt verkregen uit banking malware is opgedeeld in twee fasen (zie figuur 4.1). Fase 1 betreft het omzetten van het elektronische geld in contant geld. Fase 2 betreft de besteding van het contante geld. In de praktijk lopen deze twee fasen in elkaar over. Echter, voor het bewijzen van witwassen van geld verkregen uit banking malware als delict is fase 1 voldoende. Fase 2 bestaat in de praktijk uit (lange ketens van) allerlei witwasmethoden, teneinde de herkomst van crimineel verkregen gelden verder te verhullen.

Figuur 4.1 Model 1 betreft het witwassen van geld met money mule



Fase 1
De cybercriminelen achter de banking malware infecteren computers van slachtoffers, waarna op de achtergrond een frauduleuze transactie wordt uitgevoerd naar een andere rekening. Op basis van jurisprudentie, ons literatuuronderzoek, de afgenomen interviews met experts en ons dossieronderzoek, komt duidelijk het beeld naar voren dat in de meeste gevallen het geld wordt overgemaakt naar een *money mule*.[195] In figuur 4.1 is de money mule afgebeeld als een (geld)ezel. De money mule kan daarmee worden gekwalificeerd als een belangrijke actor in het witwasproces. De kenmerken van money mules worden uitgebreid in paragraaf 5.1 beschreven.

Uit ons dossieronderzoek en uit gepubliceerde uitspraken komt een beeld naar voren dat money mules in Nederland worden geronseld.[196] De ronselaar speelt dus indirect een rol in het witwasproces. Zoals in figuur 4.1 is weergegeven, krijgt de money mule het geld direct van het slachtoffer op zijn (internet)rekening. In de praktijk wordt het geld vervolgens kort na dat moment gepind (dit betreft de *cash-out*). De cash-out vindt vaak niet plaats door de money mule zelf, omdat deze de bankpas aan de ronselaar of een ander individu – de *casher* – heeft afgegeven.[197] De money mule krijgt een commissie (meestal rond de 5%) van het bedrag voor het beschikbaar stellen van de rekening.[198]

De modus operandi in dit model is de meest eenvoudige en meest gangbare. Echter, deze werkwijze heeft een belangrijk nadeel voor cybercriminelen: er zijn maxima voor de bedragen die per dag gepind kunnen worden door de money mule en zodra slachtoffers aangifte doen en/of hun bank informeren, worden de bankrekeningen van money mules snel geblokkeerd. Daardoor kan per money mule slechts een beperkt bedrag worden witgewassen. Money mules worden dus snel gedetecteerd door banken. Tegen hen kan eventueel aangifte worden gedaan van witwassen en hun rekening kan worden geblokkeerd. Voor het witwassen van grote bedragen zijn dus vele money mules nodig. Daar hoort een complexe organisatie bij waar voor criminelen kosten aan zijn verbonden. In interviews, uit jurisprudentie en uit ons dossieronderzoek komt overigens naar voren dat het ook mogelijk is dat het geld direct naar een begunstigde of bedrijf in het buitenland wordt overgemaakt, waarna het geld vervolgens daar wordt opgenomen, besteed of verdere verhullingshandelingen plaatsvinden.[199]

195 Zie bijvoorbeeld UNODC 2014, p. 20. Zie Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041, Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.
196 Zie Europol, 2015a, p. 10 en Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041 en Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877.
197 Zie bijvoorbeeld Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041 en Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877
198 Zie Europol, 2015a, p. 41. Zie ook UNODC, 2014, p. 52 met verwijzing naar COE-CMF, par. 168.
199 Zie bijvoorbeeld ook Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.

Aangezien het geld op criminele wijze is verkregen en door het gebruik van een money mule en direct pinnen van het geld duidelijk verhullingshandelingen worden verricht, is op dat moment juridisch gezien al sprake van witwassen. De Rechtbank Rotterdam heeft recentelijk in een uitspraak opgemerkt dat de overboeking zelf, van de rekening van een slachtoffer naar de money mule, kan worden aangemerkt als diefstal maar nog niet als witwassen. Het is de daarop volgende versluiering van de criminele herkomst van het geld die de gedraging als witwassen kwalificeert.[200] In de literatuur en in interviews wordt opgemerkt dat criminelen graag contant geld in handen hebben. 'Cash is still king', concludeert Europol in haar witwasrapport van 2015. Contant geld is anoniem en kan eenvoudig worden verplaatst of besteed aan goederen (Europol, 2015c, p. 7). Met deze conclusie zijn we bij fase 2 van het beschreven witwasproces bij banking malware aangekomen.

Fase 2 (optioneel)
Hoewel in fase 1 het geld juridisch gezien al is witgewassen, worden daarna vaak nog andere transacties gepleegd met het geld teneinde de herkomst van het geld verder te verhullen. Door meerdere verhullingstransacties te stapelen en te combineren wordt het spoor naar de illegale herkomst immers lastiger te volgen. Het gepinde geld wordt in fase 2 verder witgewassen, onder andere via de 'klassieke' methoden die in hoofdstuk 2 zijn beschreven, maar ook door middel van nieuwe witwasmethoden, waaronder het gebruik van bitcoins (zie paragraaf 4.2.2). Uit jurisprudentie, ons literatuuronderzoek, de interviews en het dossieronderzoek is een gefragmenteerd en divers beeld van witwasmethoden naar voren gekomen. Toch zijn we in ons onderzoek enkele witwasvormen vaker tegengekomen dan andere.

Een veelvoorkomende modus operandi is het gebruik van geldtransferkantoren voor het verder witwassen van het crimineel verkregen geld. Uit literatuur en enkele gepubliceerde uitspraken met betrekking tot banking malware komt nadrukkelijk het gebruik van geldtransferkantoren zoals Western Union en MoneyGram naar voren.[201] Mensen kunnen via deze kantoren volledig legitiem en eenvoudig geld overmaken naar bijvoorbeeld familieleden in het buitenland. Een persoon kan in Nederland bijvoorbeeld geld overmaken naar een familielid in Suriname. De verzender geeft daarvoor enkele gegevens van de begunstigde in Suriname op. Het uit te betalen bedrag met de gegevens van de begunstigde en referentienummer wordt vervolgens in een gegevensbestand ingevoerd.[202] In Suriname kan de begunstigde vervolgens na legitimatie en het geven van het referentienummer het geld in de gewenste valuta

200 Zie Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m. nt. J.J. Oerlemans.
201 Zie ook bijvoorbeeld UNODC, 2014, p. 20: 'Previous work studying criminal money flows on the Internet has indicated that the use of money remittance providers is the most common technique for laundering criminal money derived from cybercrime.' Zie ook Europol, 2015a, p. 41 en Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041.
202 Eventueel kan nog een boodschap bij het uitbetaalde bedrag worden meegegeven.

opnemen. De politie geeft in haar rapport over witwassen aan dat het geld naar een andere rekening kan worden overgemaakt of dat via het kantoor het geld contant kan worden opgenomen (Soudijn & Akse, 2012, p. 116).

Het beeld dringt zich op dat veelal van deze kantoren gebruik wordt gemaakt voor het verplaatsen van het geld naar het buitenland. Het gepinde geld wordt daarbij door de money mule of ronselaar, die het geld van verschillende money mules heeft verzameld door middel van deze geldwisselkantoren naar het buitenland overgeboekt.[203] Daar wordt het geld vervolgens door een ander individu opgehaald.

Het beeld van het witwasproces dat kon worden verkregen uit de interviews en literatuuronderzoek hield daarmee op. Het UNODC beschrijft het proces echter verder en merkt in zijn rapport op dat het geld vaak wordt overgemaakt naar Oost-Europese landen. Het geld wordt daar door lokale money mules opgehaald die geen kennis hebben over de herkomst van het geld (UNODC, 2014, p. 54).[204] Vervolgens wordt het geld verzameld en overgemaakt naar de geldverzamelaar. In het beschreven geval wordt het verzamelde geld vervolgens omgezet en gestort op een WebMoney-account (UNODC, 2014, p. 54).[205] Het witwassen met deze digitale betalingsdienst wordt verder onderzocht in paragraaf 4.2.1.

4.1.2 Witwassen via aankoop van goederen of diensten van webdienstverleners

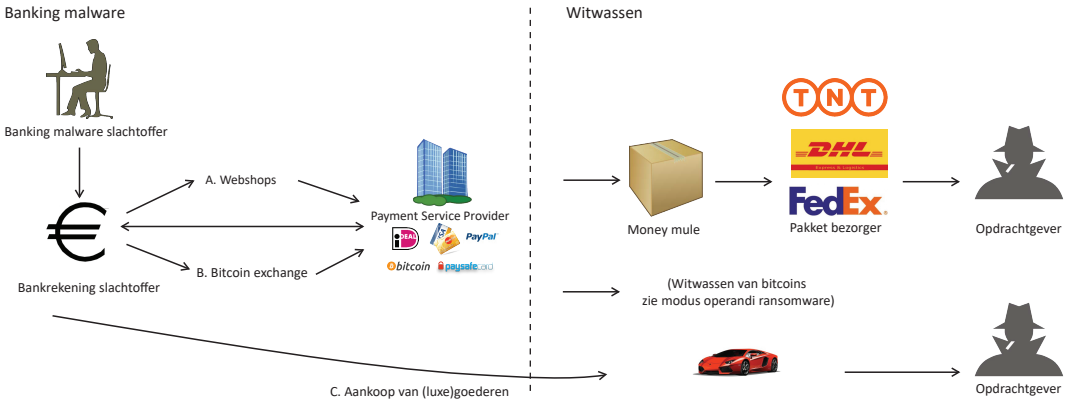
In het tweede model van het witwassen van geld dat wordt verkregen uit banking malware wordt het geld direct besteed aan goederen en diensten. Deze modus operandi is weergegeven in figuur 4.2. In dit model wordt een onderscheid gemaakt tussen (A) de aankoop van goederen via webshops, (B) de aankoop van bitcoins via Bitcoin exchanges en (C) de directe aankoop van (luxe)goederen.

203 Zie ook UNODC, 2014, p. 20, 53-54. Zie bijvoorbeeld ook Brian Krebs, 'MoneyGram Fined $100 Million for Wire Fraud', 19 november 2012: 'In nearly every case, the sequence of events is virtually the same: The organization's controller opens a malware-laced email attachment, and infects his or her PC with a Trojan that lets the attackers control the system from afar. The attackers then log in to the victim's bank accounts, check the account balances – and assuming there are funds to be plundered — add dozens of money mules to the victim organization's payroll. The money mules are then instructed to visit their banks and withdraw the fraudulent transfers in cash, and wire the money in smaller chunks via a combination of nearby MoneyGram and Western Union locations.' Beschikbaar op: http://krebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud.

204 Met verwijzing naar COE-CMF, p. 49.

205 In die zaak ging het om een bedrag van 150.000 dollar binnen twee maanden.

Figuur 4.2 Model 2 betreffende het witwassen van geld door directe uitgave



Aanschaf van producten via webshops

Uit ons dossieronderzoek en de interviews is duidelijk geworden dat criminelen die gebruikmaken van banking malware om frauduleuze transacties uit te voeren regelmatig producten bij webwinkels kopen. In Nederland wordt daarbij in de meeste gevallen gebruikgemaakt van de betalingsdienst iDeal. In veel gevallen faciliteren Payment Service Providers zoals Global Collect of Adyen de betalingen bij de webshop voor de aankoop van de goederen. Payment Service Providers bieden naast iDeal ook de mogelijkheid om te betalen met bijvoorbeeld creditcard en PayPal. De kosten voor de aankoop worden afgeschreven van de rekening van het slachtoffer. De levering van het pakketje resulteert mogelijk in een spoor naar de opdrachtgever. Om die reden wordt vaak het adres van een money mule gebruikt voor de levering van pakketjes.[206] In sommige zaken komt het voor dat tijdens een huiszoeking veel ongeopende pakketjes met bijvoorbeeld spelcomputers werden aangetroffen. Uit interviews komt naar voren dat pakketten veelal naar Oost-Europese landen worden verscheept. Uit ons dossieronderzoek blijkt ook dat via online winkels prepaidkaarten, cadeaukaarten en zelfs beltegoeden worden aangekocht.[207] Deze waardeproducten kunnen vervolgens tegen een commissie online worden doorverkocht of worden besteed. Dit gebeurt overwegend via illegale kanalen maar er kan ook gedacht worden aan besteding van tegoed bij grote webwinkels.

206 Eigenlijk gaat het in deze situatie strikt genomen niet om een money mule maar om een 'katvanger' of een 'drop'. Immers een money mule stelt zijn of haar bankrekening ter beschikking, terwijl in deze situatie niet de bankrekening maar het adres ter beschikking wordt gesteld.

207 Zie ook het hierna beschreven Mega Server-onderzoek (Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7038).

Aankoop bitcoins
In banking malware-zaken van de laatste twee jaar is het opvallend dat veelvuldig direct bitcoins zijn aangekocht vanaf de bankrekening van slachtoffers.[208] In de onderzochte zaken werd voor de aankoop van de bitcoins gebruikgemaakt van Bitcoin exchanges die iDeal accepteren.

De kosten van de aangekochte bitcoins, inclusief commissie, worden afgeschreven van de rekening van het slachtoffer. Wat er verder met de bitcoins gebeurt, om de herkomst ervan verder te verhullen, wordt beschreven in paragraaf 4.2.2.

Directe aanschaf (luxe)producten
Indien het slachtoffer een aanzienlijk bedrag op zijn rekening heeft staan, is het via een overboeking voor criminelen mogelijk luxegoederen aan te kopen, zoals een auto. Eerder is vastgesteld dat criminelen zich ook richten op het besmetten van computers uit het bedrijfsleven. Het is bekend dat criminelen met behulp van *Remote Administration Tools* (RATs) het computergedrag van medewerkers van een bedrijf met toegang tot de betaalrekeningen monitoren (CSBN 5, 2015, p. 39-40). In deze gecombineerde aanval worden de computers in eerste instantie besmet door een gerichte phishing mail, die vaak uit naam van een bekende lijkt te zijn verstuurd. Dit in tegenstelling tot algemene phishing mails, die veelal uit naam van een bepaald bedrijf worden verstuurd. Het NCSC merkt op dat het gebruik van RATs toeneemt (CSBN 6, 2016, p. 18).

Op een uitgekiend moment, bijvoorbeeld tijdens de lunchpauze van de medewerker, wordt vervolgens op afstand een betaling uitgevoerd. Als de betaling goed kan worden gepland, is het mogelijk de betaling te laten samenvallen met de aankoop van het luxeproduct. Indien de verkoper de rekeninggegevens niet zorgvuldig controleert, wordt de verkoop afgerond. Het luxeproduct, bijvoorbeeld een auto, wordt vervolgens meteen naar het buitenland vervoerd, waardoor de politie onvoldoende tijd heeft om in te grijpen wanneer de fraude eenmaal aan het licht komt. Uit ons dossieronderzoek is ook gebleken dat ook andere producten direct worden aangekocht vanuit een bankrekening van het slachtoffer. Het ging daarbij om de aankoop van onder andere prepaidkaarten.

De directe aankoop van (luxe)producten vanuit de bankrekening van het slachtoffer van banking malware (de besmette bankrekening) is een modus operandi die is vastgesteld naar aanleiding van interviews en dossieronderzoek. Deze witwasmethode lijkt vooralsnog niet bijzonder vaak voor te

208 Zie Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7038, Rb. Zeeland, 29 juni 2016, ECLI:NL:RBZWB:2016:3877 en Rb. Rotterdam, 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m.nt. J.J. Oerlemans.

komen, maar niet is uit te sluiten dat deze modus operandi in de toekomst meer gebruikt gaat worden. Duidelijk is dat criminelen die van (banking) malware gebruikmaken voor het uitvoeren van frauduleuze transacties voortdurend de modus operandi aanpassen om het verkregen geld succesvol wit te wassen.

Met model 2 winnen criminelen meer tijd (in vergelijking met model 1), omdat de money mules/katvangers minder snel getraceerd kunnen worden. Daardoor kunnen money mules/katvangers iets langer worden gebruikt dan de money mule in model 1. Echter, voor cybercriminelen zit aan model 2A het nadeel vast dat er nog steeds gebruikgemaakt wordt van money mules/katvangers die moeten worden geronseld. Bovendien is uiteraard een bezwaar van model 2A dat de winsten niet in de vorm van geld worden verdiend maar in de vorm van goederen. Voor zover deze goederen niet door cybercriminelen ter consumptie worden gebruikt, dienen ze dus geheeld/doorverkocht te worden. Het nadeel van model 2C is voor cybercriminelen dat het zeer bewerkelijk is. Model 2B biedt voor cybercriminelen wel opbrengsten in de vorm van besteedbaar geld. Op de vervolgstappen voor opbrengsten in bitcoins wordt in de volgende paragraaf nader ingegaan.

Zoals in de inleiding van deze paragraaf is opgemerkt, wordt in de praktijk vaak een combinatie van beide modellen gebruikt voor het witwassen van geld dat is verkregen uit banking malware. Om dit te illustreren volgt een korte beschrijving van de Mega Server-zaak, waarover de Rechtbank Rotterdam op 2 oktober 2015 een uitspraak is gewezen.[209]

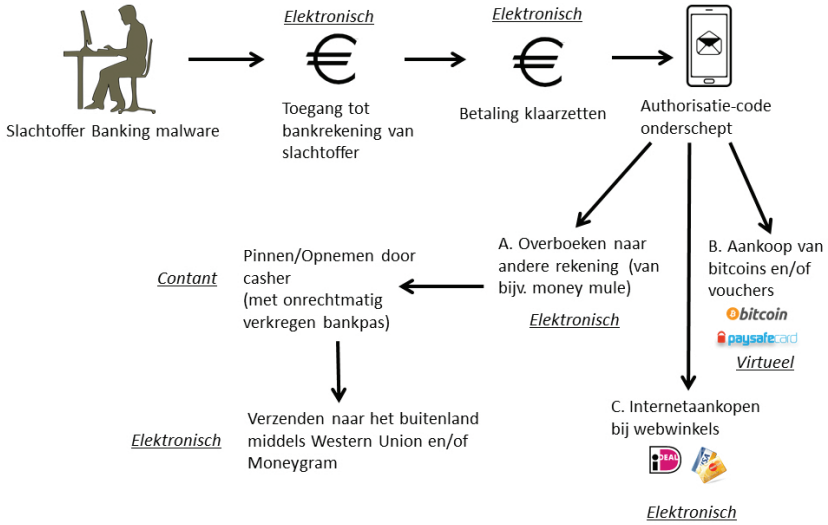
De Mega Server-zaak
Op 2 oktober 2015 werden vier verdachten door de Rechtbank Rotterdam veroordeeld voor het voorhanden hebben en verwerven van malware, het plegen van computervredebreuk, diefstal, oplichting en (gewoonte) witwassen. In de uitspraak wordt uitgelegd hoe de gebruikte banking malware via een botnet werd verspreid en computers heeft besmet. Deze malware zorgde ervoor dat met webinjects (zie paragraaf 2.2 over de werking van webinjects) een ogenschijnlijk authentieke website van de bank aan de slachtoffers werd getoond. Nadat de slachtoffers hun inloggegevens hadden ingevoerd op deze nepwebsite, beschikten de daders over de ingevoerde gegevens van de rekeninghouders. Daarnaast werden ook de mobiele telefoons van rekeninghouders geïnfecteerd met op maat gesneden malware. Op deze manier konden de sms-berichten van de bank worden afgevangen teneinde de benodigde (TAN-)codes te bemachtigen waarmee vervolgens geld kon worden overgeboekt.

209 Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7038, ECLI:NL:RBROT:2015:7039, ECLI:NL:RBROT:2015:7041, en ECLI:NL:RBROT:2015:7044. Zie ook Oerlemans, J.J. (2015). Uitspraak Mega Server zaak. *Computerrecht* 2015, (6), 356-357.

In de uitspraken wordt ook besproken op welke wijze het geld na de overboeking via het online bankiersysteem is witgewassen. Het geld is bijvoorbeeld overgemaakt naar de bankrekening van money mules, waarna het bedrag direct werd opgenomen door een money mule of casher (zie ook model 1). Daarnaast hebben verdachten met behulp van valse identiteitsbewijzen en documenten bij verschillende banken rekeningen geopend en pinpassen aangevraagd, waarvandaan na de overboeking het geld werd gepind of doorgesluisd. Het crimineel verkregen geld dat werd gepind, is vervolgens via Western Union naar het buitenland overgemaakt. De verdachten hebben ook vanaf de rekening van het slachtoffer bitcoins en betaalkaarten (zoals Ukash) gekocht via het internet (zie ook model 2). In totaal is voor € 13.000 aan bitcoins aangekocht. De rechters in deze zaken geven aan dat bovenstaande handelingen te kwalificeren zijn als witwassen. In de uitspraak komt naar voren dat de verdachten ook op verschillende andere manieren hebben bijgedragen aan het witwassen van het verworven geld. Een van de verdachten is bijvoorbeeld verweten dat hij een nepbedrijf heeft opgezet om het geld heimelijk te ontvangen. Een andere verdachte wordt aangerekend dat hij op naam van een slachtoffer een creditcard heeft aangevraagd. Een derde andere verdachte zou geld hebben witgewassen in een casino.
De rechter kwalificeerde de delicten als ernstige feiten, omdat het Nederlandse systeem van internetbanken op grove wijze is aangevallen. Daardoor zou het vertrouwen in de integriteit van het elektronische betalingsverkeer zijn geschaad en het maatschappelijk en economisch verkeer zou kunnen worden ontwricht. Gemiddeld zijn de verdachten veroordeeld tot twee jaar gevangenisstraf, waarvan zes maanden voorwaardelijk. Bij de straffen hield de rechter rekening met de jonge leeftijd van de verdachten.

Op basis van de feiten uit de bovengenoemde Mega Server-zaak kan het volgende model worden afgeleid. Het is wezen een combinatie van model 1 en 2.

Figuur 4.3 (Eenvoudig) witwasmodel op basis van de feiten uit de Mega Server-zaak



Figuur 4.3 illustreert de verschillende wijzen waarop cybercriminelen met gebruik van banking malware het verkregen geld van slachtoffers hebben witgewassen.

4.2 Witwasproces bij ransomware

Uit literatuuronderzoek, dossieronderzoek en interviews komen twee verschillende modellen van witwassen voor geld verkregen via ransomware naar voren. Het is goed om hier te benadrukken dat losgeld van ransomware soms wordt opgeëist in de vorm van vouchers en in toenemende mate in de vorm van bitcoins (Europol, 2015b, p. 11; Cyber Threat Alliance, 2015, p. 4.). De twee modellen voor witwassen van geld verkregen uit ransomware worden hieronder nader omschreven. Het ene model ziet op het witwassen via vouchers, het andere model op het witwassen via bitcoins.

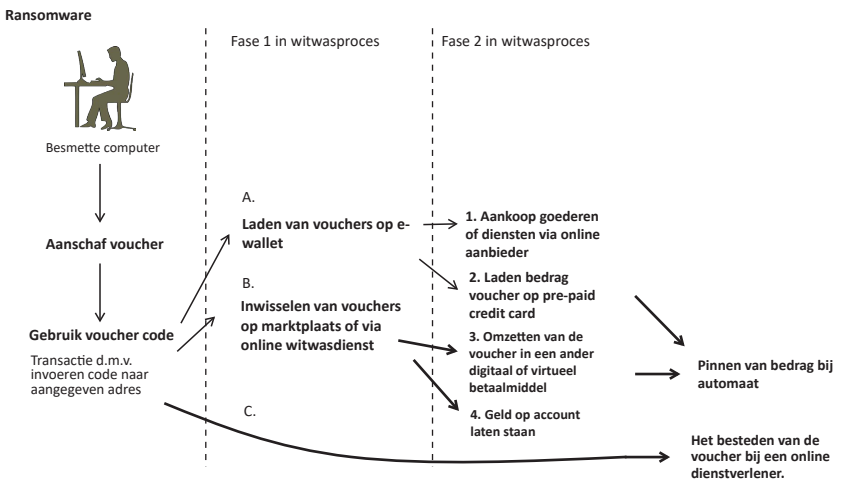
Het ene witwasmodel wordt beschreven in paragraaf 4.2.1. In dit model wordt uitgelegd hoe het geld verkregen met ransomware wordt witgewassen wanneer het losgeld met vouchers is betaald. Deze vouchers zijn bij verschillende fysieke winkels te verkrijgen. Het gaat dan bijvoorbeeld om Paysafecards (voorheen Ukash). Het *politievirus* is hier een voorbeeld van, waarbij slachtoffers werd gevraagd om een bedrag van € 100 te betalen om weer toegang te krijgen tot de computer.

In het andere model voor het witwassen van geld verkregen via ransomware staat het witwassen van bitcoins centraal. Dit model wordt beschreven in paragraaf 4.2.2. Met name bij cryptoware wordt de betaling van het losgeld vaak opgeëist in de vorm van bitcoins. In dit model worden de bitcoins overgemaakt naar een ander Bitcoin-adres of een serie van Bitcoin-adressen, waarna vaak (maar niet altijd) een cash-out volgt. Bovendien wordt soms gebruikgemaakt van *mixing services* om de herkomst van de illegaal verkregen bitcoins verder te verhullen.

4.2.1 Witwassen van vouchers

Het eerste model voor het witwassen van geld verkregen uit ransomware betreft geld dat is verkregen in de vorm van vouchers. Het proces in dit model kan worden opgedeeld in twee fasen van witwassen (figuur 4.4). Fase 1 gaat over het proces nadat het losgeld in de vorm van vouchers door het slachtoffer aan de dader is overgedragen. Merk op dat juridisch gezien in fase 1 al sprake is van (strafbare) witwashandelingen.[210] Fase 2 betreft vervolgens de verdere verhulling en/of besteding van het virtuele geld. In de meeste gevallen worden de vouchers omgezet in contant geld door middel van een cash-out.

Figuur 4.4 Model 3 betreft het witwassen van losgeld in de vorm van vouchers



210 Strafbaarstelling op grond van artikel 420bis lid 1 sub b Sr, waarin het verwerven, voorhanden hebben, omzetten en gebruikmaken van zaken en vermogensrechten afkomstig uit enig misdrijf strafbaar worden gesteld.

Fase 1
Nadat het losgeld in de vorm van vouchers is ontvangen, kan de organisatie achter de ransomware op verschillende manieren te werk gaan. Uit interviews met financieel rechercheurs blijkt dat er twee varianten zijn te onderscheiden: (A) bijschrijven van de waarde van de voucher op een account van een e-wallet en (B) het doorverkopen van de voucher. Bij een derde variant (C) wordt de voucher niet overgedragen aan de cybercriminelen, maar wordt deze direct besteed bij een online dienstverlener.

Laden van vouchers op de e-wallet
Voor het bijschrijven van het tegoed van een voucher op een online account kan gebruik worden gemaakt van digitale betalingsdienstverleners. Voorbeelden van deze betalingsdienstverleners zijn Skrill en Netteller (zie hoofdstuk 5). Op deze manier is het mogelijk om bijvoorbeeld Ukash/Paysafecard-vouchers van Skrill over te zetten naar de e-wallet van de online betalingsdienst. Uit ons dossieronderzoek komt naar voren dat verdachten vaak van verschillende diensten gebruikmaken om de criminele gelden wit te wassen, zodat de gelden verder worden verspreid en het spoor naar de herkomst van het geld verder wordt verhuld. Hierbij moet gedacht worden aan een combinatie van zowel buitenlandse betalingsdiensten en vouchersystemen. In één zaak is bijvoorbeeld gebruikgemaakt van zowel PayPal, Western Union, bitcoins als vouchers. Vervolgens kunnen verdere verhullingshandelingen plaatsvinden in fase 2. Merk op dat de transacties met een voucher kunnen worden gevorderd bij de uitgever. Als dit lukt, wordt bekend waar de voucher is uitgegeven en kan dat bijdragen aan het opsporingsonderzoek. Als er een katvanger, fysieke overdracht of valse identiteit is gebruikt, kan het spoor echter doodlopen.

Inwisselen/doorverkopen van vouchers
Het doorverkopen gebeurt doorgaans op criminele online fora. Respondenten van interviews geven aan dat via advertenties op deze fora vouchers ondergronds worden verkocht in ruil voor dollars of cryptocurrencies, zoals Bitcoin. Daarnaast is het mogelijk om de vouchers in te wisselen voor andere vouchers. Ook daarmee wordt het spoor naar de herkomst van het geld verder verhuld. Op online fora kunnen bijvoorbeeld Paysafecards worden geruild voor cadeaukaarten. Het doorverkopen van vouchers via een online dienst is ook een mogelijkheid. Er zijn verschillende legale diensten, zoals Zeek,[211] die het mogelijk maken om vouchers te kopen en te verkopen voor contant geld.

Direct besteden van vouchers
Soms worden vouchers niet overgedragen en verder omgezet, geruild of verkocht, maar direct besteed. Dit besteden gebeurt bij een online dienstverle-

211 www.zeek.me (laatst geraadpleegd op 20 april 2016).

ner die de betreffende vouchers accepteert als betaalmiddel. Wanneer de producten die worden aangeschaft direct naar de cybercriminelen zouden gaan, zouden zij betrekkelijk eenvoudig traceerbaar zijn via bijvoorbeeld het afleveradres of andere bestelgegevens. Daarom wordt in deze variant doorgaans gebruikgemaakt van money mules als tussenpersonen. Zij kunnen dan de producten (soms via een keten van tussenpersonen) bij de cybercriminelen bezorgen. Deze variant lijkt sterk op model 2A in figuur 4.2.

Fase 2
In fase 2 wordt het geld verder witgewassen, door middel van het verder verhullen en/of het besteden van het omgezette geld. Uit ons literatuur- en dossieronderzoek komt een breed scala aan witwasmethoden naar voren. Meestal betreft het combinaties van methoden. Hieronder worden vier methoden besproken die in combinaties (en in combinaties met andere methoden die in dit rapport worden besproken) voorkomen.

Een eerste methode (3A1) betreft het direct uitgeven van de voucher bij een online dienstverlener. Vouchers kunnen immers rechtstreeks worden ingewisseld voor producten of diensten. In een recente zaak kwam bijvoorbeeld een methode van witwassen naar voren waarbij tegoeden van een Paysafecard werden omgezet in beltegoeden.[212]

Een tweede methode (3A2) is dat de tegoeden van een voucher vanuit een account met gekoppelde e-wallet op prepaid creditcards worden gestort. Veel online betalingsdiensten bieden prepaid creditcards aan om eenvoudig geld uit te geven. Daarnaast bestaan er ook uitgevers van volledig anonieme prepaid cards, die bovendien hoge of helemaal geen limieten hebben (UNODC, 2014, p. 16).[213] Bij geldautomaten kan het geld vervolgens worden opgenomen met deze prepaid cards.

Een derde methode (3B3) die veel voorkomt is het overzetten van het tegoed van een voucher op een online account met een daaraan gekoppelde e-wallet. Deze e-wallet wordt vervolgens gebruikt voor de aankoop van producten of diensten bij webwinkels. Op deze manier kan de waarde van een voucher worden besteed. Maar het tegoed kan uiteraard ook worden omgezet in andere valuta en bijvoorbeeld via een cash-out worden omgezet in contant geld.

Een vierde methode (3B4) is simpelweg niets met het tegoed doen en het tegoed, als ware het spaargeld, op het account laten staan. Als het geld immers voldoende is witgewassen, dat wil zeggen als de illegale herkomst van

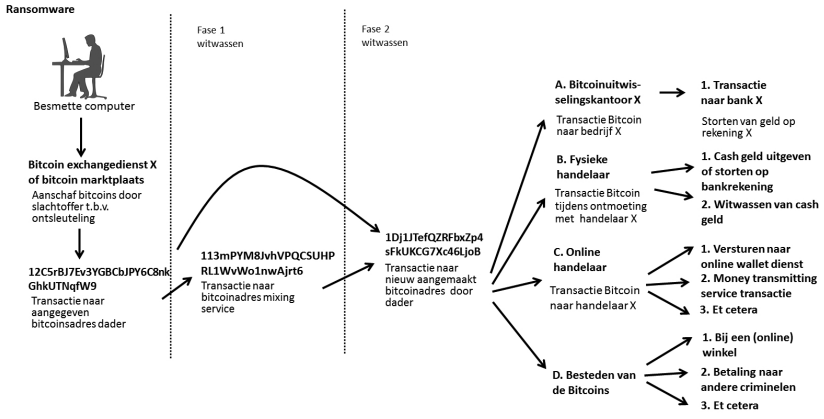
212 Op een gegeven moment gaat het hier om accounts met honderdduizenden euro's aan Skype-tegoeden.
213 Zie ook: 'Money Laundering using New Payment Methods', FATF-GAFI, October 2010. Zie bijvoorbeeld www.megaspyshop.nl/shop/anonymous-credit-card-high-limit en www.podex.nazwa.pl/card (laatst geraadpleegd op 20 april 2016).

het geld voldoende is verhuld, kan het geld door cybercriminelen eenvoudig worden besteed in de legale economie. Dat is doorgaans wel pas het geval nadat het geld vele malen is verplaatst van de ene naar de andere betaaldienst en meerdere malen is omgezet van het ene naar het andere betalingsmiddel. Het Europol-rapport benadrukt dat criminelen simpelweg geld van de ene (online) betaaldienst naar de andere verplaatsen (Europol, 2015b, p. 47). Dit kan plaatsvinden via onder andere online fora of door gebruik van verschillende exchanges. Exchange-diensten in de breedste zin van het woord zijn een van de meest gebruikte methoden om virtuele valuta te verhandelen. Ten slotte kan ook gebruik worden gemaakt van een Payment Service Provider om een overboeking naar bijvoorbeeld PayPal of Western Union te realiseren (UNODC, 2014, p. 17).

4.2.2 Witwassen van bitcoins

Het andere model voor het witwassen van geld verkregen uit ransomware betreft losgeld dat is verkregen in de vorm van bitcoins. Dit model (figuur 4.5) kent twee fasen van witwassen. In fase 1 vindt (eventueel) een verhullingshandeling plaats door de bitcoins door een 'mixing' dienst te halen. Als gebruik wordt gemaakt van een dergelijke mixing service, is juridisch gezien naar alle waarschijnlijkheid reeds sprake van witwassen, omdat het een verhullingshandeling betreft. In fase 2 worden de bitcoins overgemaakt naar een Bitcoin-adres van een of meerdere tussenpersonen, waarna de dader het geld kan besteden.

Figuur 4.5 Model 4 betreffende het witwassen van geld in de vorm van Bitcoin



Fase 1
Alvorens de bitcoins naar een Bitcoin-adres van de dader worden overgemaakt, al dan niet via een of meerdere tussenpersonen, kunnen criminelen gebruikmaken van mixing services (CSBN 6, 2016, p. 26).[214] Mixing services hebben als doel om het gebruik van bitcoins anoniemer te maken. Het idee achter mixing services is dat bitcoins tegen andere bitcoins worden gewisseld (tegen betaling van een commissie),[215] zodat de herkomst van de bitcoins verder wordt verhuld.[216] Uit de door ons onderzochte dossiers en de interviews met opsporingsambtenaren blijkt dat verdachten niet altijd gebruikmaken van mixing services. Om die reden is in figuur 4.5 ook de optie aangegeven dat de bitcoins direct worden overgemaakt naar een Bitcoin-adres van de dader of een tussenpersoon, waarna de bitcoins verder worden witgewassen.

In juli 2015 is in het kader van dit onderzoek een 'experiment' uitgevoerd om na te gaan hoe mixing services precies werken. Tevens is nagegaan op welke wijze de cash-out van bitcoins mogelijk kan plaatsvinden. Om deze empirische oefening mogelijk te maken is eerst op basis van reviews van dark web-websites[217] nagegaan van welke Bitcoin mixing services in de praktijk gebruik wordt gemaakt. Een selectie is gemaakt op basis van reviews van gebruikers van zowel betrouwbare als onbetrouwbare mixing services. Op deze manier kon worden nagegaan of de reviews een betrouwbare beoordeling geven van de diensten. Vervolgens zijn vijf aangekochte bitcoins via iDeal en een Bitcoin exchange door de mixing services gehaald om na te gaan of de bitcoins daadwerkelijk naar het aangegeven adres werden overgemaakt. Uit het 'experiment' werd helder dat sommige mixing services betrouwbaar zijn en tegen een commissie weer bitcoins terug hebben overgemaakt. Mixing services die slechte reviews van gebruikers hadden ontvangen, keerden de verstuurde bitcoins echter niet uit. [218]

Mixing services maken het mogelijk om de keten van transacties tussen het slachtoffer en de dader verder te verhullen. Mixing services werken in drie stappen:
1 De klant moet zijn bitcoins naar de mixing service sturen.

214 Mixing services worden ook wel '*tumbling*-' of '*blending services*' genoemd of kortweg *mixers*, *tumblers* en *blenders*.
215 Feitelijk worden een heleboel transacties uitgevoerd: de bitcoins worden niet een-op-een gewisseld, maar in een grotere pool gezet (vandaar de term mixing).
216 Zoals in paragraaf 3.3.4 is uitgelegd, worden Bitcoin-transacties gelogd en zijn ze daarmee raadpleegbaar via publiek toegankelijke websites zoals blockchain.info. Transacties die zijn uitgevoerd in het verleden kunnen daarom worden herleid tot een Bitcoin-adres van zowel de zender als de ontvanger, inclusief de hoeveelheid bitcoins die op een bepaald Bitcoin-adres staan. Het systeem wordt daarom ook wel beschreven als pseudo-anoniem.
217 Websites op het dark web zijn websites waarvan de webservers niet geïndexeerd zijn en dus niet vindbaar zijn via reguliere zoekmachines zoals Google. De desbetreffende websites waren alleen vindbaar via de anonimiseringsdienst Tor. Door gebruikmaking van de TNO DarkWeb MoniTOR was het eenvoudiger om reviews van mixing services te lezen.
218 Zie voor een volledig overzicht van de resultaten: Wegberg, Oerlemans en Van Deventer (2016,in voorbereiding).

2 De mixing service verwerkt de bitcoins. De mixing service verzamelt de bitcoins uit verschillende bronnen en stuurt vervolgens de bitcoins terug. Een klant krijgt als het ware bitcoins van een andere (willekeurige, onbekende) gebruiker. Tevens is het mogelijk dat mixing services (als Bitcoin miners, zie paragraaf 3.3.2) geheel nieuwe bitcoins aanmaken die vervolgens naar een klant worden verstuurd.[219]
3 De bitcoins worden naar een door de klant aangegeven adres teruggestuurd. Voor deze dienstverlening wordt een commissie ingehouden, bijvoorbeeld een percentage van 3% van de verstuurde hoeveelheid bitcoins (Möser, Böhme & Breuker, 2013, p. 4). Mixing services zijn in de regel alleen bereikbaar via het Tor-netwerk om de anonimiteit van de dienstverlener en zijn klanten te waarborgen (Europol, 2014).[220] Ook blijft daarmee onduidelijk in welke jurisdictie de dienstverleners zich begeven.

De werkwijze van mixing services is alleen succesvol indien de herkomst van de bitcoins zodanig wordt verhuld dat de bitcoins van het slachtoffer niet meer te traceren zijn naar de cybercriminelen en vice versa.[221] In die gevallen waarin, binnen de test, de bitcoins door de mixing service waren overgemaakt, waren de bitcoins niet herleidbaar tot eerdere Bitcoin-transacties.[222] De test ondersteunt dus de stelling dat mixing services de herkomst van bitcoin verder kunnen verhullen.

Het gebruik van mixing services voor bitcoins die uit criminele doeleinden zijn verkregen, levert naar alle waarschijnlijkheid het delict witwassen op. Door de ingehouden commissie en het doel van de dienst (het verhullen van de oorsprong van uit criminaliteit verkregen bitcoins) kan waarschijnlijk het bewijs voor het vereiste opzet voor het witwassen worden geleverd.[223] Er is echter nog geen jurisprudentie beschikbaar met betrekking tot het gebruik van deze diensten. Merk op dat de inbeslagname van een server van een mixing service bijzonder waardevol kan zijn in een opsporingsonderzoek. De analyse van de gegevens die zijn opgeslagen op de server maakt het mogelijk bitcoin-transacties te koppelen, hetgeen kan bijdragen aan de identificatie van de oorspronkelijke verzender(s).

219 Zie bijvoorbeeld Deepdotweb, 'Introducing Grams Helix: Bitcoins Cleaner', 22 juni 2014. Beschikbaar op: www.deepdotweb.com/2014/06/22/introducing-grams-helix-bitcoins-cleaner (laatst geraadpleegd op 3 februari 2016).
220 Websites die alleen via anonimiseringsnetwerken als Tor beschikbaar zijn, worden ook wel 'hidden services' genoemd.
221 Slechts twee van de vijf geselecteerde mixing services stuurden de bitcoins terug. Deze teruggestuurde bitcoins waren niet meer terug te traceren naar de bitcoins die eerder werden verstuurd naar de mixing service.
222 Om dit na te kunnen gaan is gebruikgemaakt van Numisight blockchain explorer. Zie Wegberg, Oerlemans en Van Deventer, 2016 (in voorbereiding).
223 Mixing services met namen als 'BitLaundry' maken overigens ook geen geheim van het doel van hun dienstverlening (zie ook Möser, Böhme & Breuker, 2013, p. 3).

Fase 2
In fase 2 van model 4 komen de bitcoins van het slachtoffer bij een adres van de cybercriminelen terecht, doorgaans via een of meerdere tussenpersonen, waarna de cybercriminelen de bitcoins verder kunnen omzetten en/of besteden.[224] Vier vormen van verder witwassen en/of besteden worden in het model uitgelicht. Dit zijn (A) het direct omwisselen van bitcoins in elektronisch geld via een Bitcoin exchange, (B) het besteden na gebruikmaking van een fysieke Bitcoin-handelaar, (C) het besteden na gebruikmaking van een online witwasdienst en (D) het direct besteden van bitcoins.

Het omwisselen van bitcoins via een Bitcoin exchange
Ten eerste kunnen bitcoins eenvoudig en direct via een Bitcoin exchange worden omgewisseld voor fiatvaluta zoals euro's of dollars.[225] Bij het gebruik van een Bitcoin exchange worden de bitcoins naar een gespecifieerd Bitcoinadres van de Bitcoin exchange overgemaakt.[226] Tegen betaling van een commissie wordt vervolgens een bedrag in euro's of dollars, vaak binnen één dag, op een door de klant gekozen bankrekening overgemaakt.

Witwassen via een fysieke Bitcoin-handelaar
Een (fysieke) Bitcoin-handelaar kan worden ingeschakeld om de verworven bitcoins wit te wassen. Uit ons dossieronderzoek en uit de interviews blijkt dat daarvoor een fysieke ontmoeting plaatsvindt tussen de handelaar en de klant. Tegen een hoge commissie accepteert de handelaar bitcoins, waarbij vervolgens contant geld wordt uitgekeerd aan de klant (in dit model is de klant de dader achter ransomware of een tussenpersoon).[227]

Nadat de bitcoins zijn ingeruild bij de handelaar vraagt een cybercrimineel er vaak contant geld voor terug of wordt het geld gestort op de rekening van de cybercrimineel.

Witwassen via online witwasdienstverleners
Criminele dienstverleners bieden ook witwasdiensten via internet aan (CSBN 6, 2016, p. 26). In dat geval kunnen bitcoins worden overgemaakt naar een bedrijf. Het bedrijf betaalt vervolgens de bitcoins op een manier naar keuze uit. figuur 4.6 geeft een voorbeeld van betalingsvormen die via internet door dergelijke bedrijven worden aangeboden.

224 Zoals ook in paragraaf 4.2.1 is opgemerkt ten aanzien van vouchers, is het ook mogelijk dat een dader het geld (in dit geval bitcoins) enige tijd op een bepaald account bewaart alvorens het te besteden.
225 Zie ook paragraaf 3.3.2.
226 Ten behoeve van het hierboven genoemde experiment zijn de bitcoins die door een Bitcoin Exchange-dienst gehaald ook weer teruggestort op een bankrekening bij verschillende banken. Dit leverde geen problemen op. Dat wil overigens niet zeggen dat een transactie met hogere bedragen niet wordt tegengehouden door banken.
227 Zie ook Nos.nl, 'Tien aanhoudingen in grootschalige bitcoinszaak', 20 januari 2016. Beschikbaar op: http://nos.nl/artikel/2081511-tien-aanhoudingen-in-grootschalige-bitcoinszaak.html.

Figuur 4.6 Een overzicht van 'cash-out'-vormen zoals aangeboden door een online dienstverlener. De afbeelding is verkregen uit de empirische oefening

Sell BTC

You may sell BTC by completing the below form.

Fee Schedule

Payment Method	Minimum	Maximum	Fee	Processing Time
PayPal	$50.00 USD	$2,000.00 USD	6.000%	24hrs or Less
SEPA Transfer	$250.00 USD	$2,000.00 USD	7.000%	3 Days or Less
Virtual Visa Card	$100.00 USD	$500.00 USD	$15.00 USD + 8.00%	24hrs or Less
Wire Transfer	$800.00 USD	$10,000.00 USD	7.000%	5 Days or Less
Check / Money Order	$250.00 USD	$2,000.00 USD	$20.00 USD + 7.00%	7 Days or Less
MoneyPak	$250.00 USD	$1,000.00 USD	10.000%	24hrs or Less
Western Union	$250.00 USD	$2,000.00 USD	$50.00 USD + 10.00%	24hrs or Less
Cash by Mail (DHL Express)	$500.00 USD	$1,000.00 USD	$90.00 USD + 7.00%	5 Days or Less
Interac E-Transfer	$150.00 USD	$1,000.00 USD	9.000%	Up to 24hrs
Cash Deposit to USA Bank	$500.00 USD	$2,000.00 USD	8.000%	Up to 24hrs
Cash Deposit to Canadian Bank	$500.00 USD	$2,000.00 USD	7.000%	Up to 24hrs
MoneyGram	$200.00 USD	$2,000.00 USD	$25.00 USD + 11.00%	Up to 24hrs
Dwolla	$100.00 USD	$1,000.00 USD	10.000%	Up to 24hrs
Vanilla Reload	$100.00 USD	$500.00 USD	8.000%	Up to 24hrs
CoinChimp Debit Card	$100.00 USD	$200.00 USD	6.000%	24hrs
Gold by Mail (DHL Express)	$1,500.00 USD	$500,000.00 USD	$90.00 USD + 7.00%	2-3 Days

Tevens is nagegaan op welke manieren de cash-out van bitcoins kan plaatsvinden (Wegberg, Oerlemans & Van Deventer, 2016). In het kader van de empirische oefening is daarbij succesvol gebruikgemaakt van het uitbetalen van de bitcoins op een PayPal-rekening en het ophalen van contant geld bij Western Union. In beide gevallen moesten de bitcoins worden verstuurd naar een aangegeven Bitcoin-adres van een Russische dienstverlener.[228] Vervolgens werd de actuele waarde van de bitcoins, minus de commissie van 6%, naar een door ons aangegeven PayPal-rekening overgemaakt. Binnen een paar dagen werd ons bericht dat het bedrag kon worden opgehaald bij Western Union in Den Haag. Dat bedrag werd door een Amerikaan, hoogstwaarschijnlijk een money mule, overgemaakt. De bitcoins die voor de test waren aangeschaft en door een mixing service zijn gehaald, zijn uiteraard niet uit enig misdrijf verkregen, maar legitiem aangekocht. Wegens het ontbreken van een gronddelict is er in dit geval dus geen sprake van witwassen. Indien de bitcoins echter door een delict, zoals via ransomware, zouden zijn verkregen, zouden de transacties waarschijnlijk als verhullings- en omzethandelingen kunnen worden aangemerkt.

In de interviews werd door respondenten opgemerkt dat bitcoins via online witwasdiensten tevens kunnen worden omgezet in de virtuele valuta WebMoney (zie ook Odinot et al., 2017).[229] In het bijzonder cybercriminelen in

228 De namen van de mixing services worden hier niet genoemd. Door aan te geven welke mixing services wel en niet goed bruikbaar zijn voor witwassen, zou dit rapport als handleiding voor criminelen kunnen dienen.
229 Zie hoofdstuk 3.

Oost-Europa zouden gebruikmaken van WebMoney voor het betalen van diensten die onderling worden geleverd (Europol, 2016, 16). Het gebruik van WebMoney komt ook in de onderzochte zaaksdossiers voor, maar niet met betrekking tot ransomware.[230] Europol vermoedt dat op grotere schaal van WebMoney gebruik wordt gemaakt dan de aangeleverde cijfers van nationale politiediensten binnen de Europese Unie doen vermoeden (Europol, 2016, p. 16). Tevens werd in de interviews opgemerkt dat relatief vaak gebruik wordt gemaakt van prepaidkaarten. Dit blijkt ook uit een ander WODC-onderzoek naar georganiseerde cybercriminaliteit (Odinot et al., 2017). Zoals in het overzicht in figuur 4.6 is te zien, is het ook mogelijk de virtuele valuta direct te laten uitbetalen op een prepaid creditcard. Met de prepaid creditcard kan vervolgens het geld bij een geldautomaat worden opgenomen.

Het direct besteden van bitcoins
Daders kunnen er ook voor kiezen de bitcoins direct uit te geven. Zoals uitgelegd in paragraaf 3.3.2, kunnen bitcoins onder andere worden uitgegeven in online casino's, voor hosting-diensten en voor aankopen in webwinkels. Maar ook allerlei bedrijven in de fysieke wereld, zoals cafés en restaurants en winkels accepteren bitcoin als betaalmiddel.

Criminelen kunnen daarom eenvoudig de – eventueel geanonimiseerde bitcoins – uitgeven aan producten of diensten. Uiteraard kan daarbij gebruik worden gemaakt van money mules om de directe link met de dader te verhullen.

Ten slotte is het denkbaar (en ook in een van de onderzochte dossiers voorgekomen) dat criminelen de verkregen bitcoins uitgeven aan criminele producten en diensten die worden aangeboden door andere criminelen. Een Europol rapport over het gebruik van betalingsmethoden in cybercrimezaken geeft aan dat in 33% van de gevallen transacties tussen criminelen onderling met bitcoins worden betaald (Europol 2016, p. 11). Met bitcoins worden bijvoorbeeld ook hosting- diensten of drugs op online fora betaald (Europol, 2016, p. 12).[231]

4.3 Tussenconclusie

In dit hoofdstuk zijn witwasprocessen in beeld gebracht die plaatsvinden bij respectievelijk banking malware en ransomware. Daarmee wordt antwoord

230 Zie bijlage 4. Uit interviews bleek dat in dossiers van Europol het gebruik van WebMoney met betrekking tot ransomware wel voorkomt.

231 Het is opvallend dat de onderzoeksresultaten van Europol aangeven dat voor de aankoop van drugs op zwarte markten op het dark web in 70% van de gevallen met bitcoins werd betaald. Het is ook opvallend dat voor de aankoop van malware door criminelen om computers te infecteren volgens het onderzoek WebMoney werd gebruikt in 67% van de gerapporteerde zaken.

gegeven op de deelvraag: *Op welke wijze en door welke actoren wordt geld witgewassen dat door middel van banking malware en ransomware wordt verkregen?* Tevens wordt ingegaan op de rol van digitale betalingsmiddelen, in het bijzonder bitcoins, in de witwasprocessen. Daarmee wordt tevens de deelvraag beantwoord: *Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals bitcoins, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?*

In het eerste model is beschreven hoe geld dat is verkregen met banking malware wordt witgewassen met behulp van money mules. De frauduleuze transactie wordt vanaf de rekening van het slachtoffer van banking malware overgemaakt naar een rekening van een money mule. Vervolgens neemt de money mule het bedrag zo snel mogelijk op bij een geldautomaat. Het geld wordt dan vaak via geldtransferkantoren naar het buitenland overgemaakt, waarna het geld eventueel door een money mule in het buitenland wordt opgenomen.

Het tweede model beschrijft het proces waarmee direct goederen en diensten worden aangekocht met elektronisch geld dat is verkregen uit banking malware. Daarbij kan van veel verschillende online dienstverleners gebruik worden gemaakt, zoals (1) de aankoop van goederen bij webwinkels, (2) de aankoop van bitcoins via Bitcoin exchanges[232] en (3) de directe aankoop van (luxe)goederen in fysieke winkels.

In het derde model wordt uiteengezet op welke wijze crimineel verkregen vouchers uit ransomware worden witgewassen. In de tweede fase van het witwasproces worden de volgende modus operandi beschreven:
(1) de (online) aankoop van goederen, (2) het laden van de voucher op een prepaid creditcard en het pinnen van het contante geld, (3) het omzetten van het geld in een ander digitaal betalingsmiddel, en ten slotte (4) het laten staan van het geld op een account.

In het vierde model wordt uiteengezet op welke wijze crimineel verkregen bitcoins uit ransomware worden witgewassen. In de eerste fase van het witwasproces vindt eventueel een verhullingshandeling plaats door de bitcoins door een mixing service te halen. Vervolgens kunnen bitcoins in de tweede fase worden omgezet of besteed via: (1) Bitcoin exchange-diensten, (2) fysieke Bitcoin-handelaren, (3) online witwasdiensten, en (4) dienstverleners die bitcoins als betaalmiddel accepteren.

232 Bitcoins kunnen ook van particulieren worden gekocht. Vaak gaat dat via een Bitcoin-platform/marktplaats. In dit onderzoek worden zulke fora ook aangeduid als Bitcoin exchanges.

5 Kenmerken van actoren bij het witwassen van opbrengsten uit banking malware en ransomware

In dit hoofdstuk wordt onderzocht op welke wijze het geld dat wordt verkregen[233] uit banking malware en ransomware wordt witgewassen en welke kenmerken de betrokken actoren in dit proces hebben. Daarmee wordt de volgende deelvraag beantwoord: *Wat zijn de kenmerken van actoren die betrokken zijn het bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?*

Op basis van de beschreven modellen in paragraaf 4.1 en 4.2 kunnen naast de cybercriminelen zelf de volgende actoren worden onderscheiden: (1) banken, (2) money mules, (3) geldtransfer kantoren, (4) Payment Service Providers, (5) webwinkels, (6) voucherdiensten, (7) e-wallet-diensten, (8) Bitcoin-exchanges, (9) mixing services, en (10) Bitcoin-handelaren.

Wat betreft de cybercriminelen zelf komt uit het literatuuronderzoek een beeld naar voren dat ze in toenemende mate professionaliseren en dat zij verschillende taken, waaronder het schrijven van malware, de infectie met malware, het vergaren van gegevens en het ronselen van money mules, regelmatig uitbesteden of onderling verdelen. Het voorbeeld van de ZeuS-malware (zie paragraaf 2.2) illustreert hoe cybercriminelen in georganiseerd verband samenwerken. In dit hoofdstuk wordt vooral ingegaan op de kenmerken van de andere actoren die betrokken zijn bij het witwasproces.

Aan de hand van een analyse van de verzamelde data bij de vier grootste Nederlandse banken kan een goed beeld worden geschetst van de kenmerken van de money mules die betrokken zijn bij het witwassen van de verkregen gelden. Bij de andere actoren die in dit hoofdstuk worden behandeld is een dergelijke dataset niet voorhanden om kenmerken af te leiden. Bij hen gaat het vooral om een typering en een beschrijving van hun werkwijze voor het faciliteren van betalingen die ook door criminelen kunnen plaatsvinden.

Alle tien geïdentificeerde actoren worden afzonderlijk onderzocht in paragraaf 5.1 tot en met paragraaf 5.10. In de tussenconclusie in paragraaf 5.11 wordt antwoord gegeven op bovengenoemde onderzoeksvraag.

233 Merk op dat er juridisch gezien al sprake kan zijn van witwassen voordat cybercriminelen de opbrengsten tot hun beschikking hebben. De term 'verkregen' duidt hier vooral op het feit dat het geld afhandig is gemaakt van het slachtoffer.

5.1 De banken

De rol van banken als actor bij banking malware is evident, aangezien gebruik wordt gemaakt van de omgeving voor internetbankieren voor het uitvoeren van delicten. De rol van banken bij ransomware is zeer beperkt. Om dit contrast te benadrukken bespreken we in paragraaf 5.1.1 de rol van banken bij banking malware en in paragraaf 5.1.2 hun rol bij ransomware.

5.1.1 Rol bij banking malware

Banken zijn in het kader van de Wft verplicht om een actieve rol te spelen in de preventie en bestrijding van digitale bancaire criminaliteit.[234] Hierdoor hebben de banken een goed inzicht in de omvang en ontwikkelingen van onder andere banking malware. Al enige jaren is een daling in de schade uit fraude bij internetbankieren en in het bijzonder schade uit banking malware te bespeuren. Deze trend is duidelijk te zien in tabel 5.1, opgemaakt uit de gepubliceerde schadecijfers uit internetbankieren in de periode van 2011-2016.[235]

Tabel 5.1 Schadecijfers uit internetbankieren in de periode van 2011–2016

Periode	Schade door fraude internetbankieren (incl. banking malware)	Deel schade uit banking malware
2011	€ 35 miljoen	onbekend
2012	€ 34,8 miljoen	onbekend
2013	€ 9,7 miljoen	+- € 950.000
2014	€ 4,7 miljoen	< € 500.000
2015	€ 3,7 miljoen	< € 700.000
2016	€ 148.000*	onbekend

* Dit betreft de eerste helft van 2016. Zie: 'Nauwelijks fraude bij internetbankieren', 16 september 2016. Beschikbaar op: www.nvb.nl/nieuws/2016/5447/nauwelijks-fraude-bij-internetbankieren.html (laatst geraadpleegd september 2016).

Uit tabel 5.1 wordt duidelijk dat de schade door fraude met internetbankieren zeer sterk is gedaald in de afgelopen vier jaar. De schade uit banking malware met internetbankieren lijkt in de jaren 2011-2012 het grootst te zijn

234 Zie www.nvb.nl/verhaal-van-de-banken/4870/veiligheid-en-fraude.html (laatst geraadpleegd in april 2016)

235 Zie persbericht NVB.nl, 'Scherpe daling fraude internetbankieren', 2 april 2013. Beschikbaar op: www.nvb.nl/nieuws/2013/1812/scherpe-daling-fraude-internetbankieren.html, 'Fraude met internetbankieren gehalveerd', 18 maart 2015. Beschikbaar op: www.nvb.nl/nieuws/2015/4033/fraude-met-internetbankieren-gehalveerd.html, 'Criminelen perfectioneren phishingmethodes', 29 september 2015. Beschikbaar op: www.nvb.nl/nieuws/2015/4344/criminelen-perfectioneren-phishingmethodes.html en 'Daling fraude met internetbankieren zet door', 8 april 2016. Beschikbaar op: www.nvb.nl/nieuws/2016/4991/daling-fraude-met-internetbankieren-zet-door.html (laatst geraadpleegd april 2016). Het grootste aandeel van de schade is de laatste jaren overigens gelegen in phishing-activiteiten van criminelen.

geweest.[236] Tevens is een daling te bespeuren specifiek met betrekking tot fraude met banking malware. Respondenten geven aan dat deze sterke daling duidelijk is veroorzaakt door investeringen door de banken in het detecteren en blokkeren van fraudeleuze transacties die door middel van banking malware worden uitgevoerd.[237] Ook geven sommige respondenten aan dat de daling deels te verklaren is door acties die zijn uitgevoerd met betrekking tot het ontmantelen van money mule-organisaties en de recente internationale acties tegen de ZeuS-bende.[238] Tegelijkertijd wordt benadrukt dat het financiële bankverkeer nog dagelijks onder vuur ligt en criminelen constant innoveren om te proberen frauduleuze transacties uit te voeren. De Nederlandse Vereniging van Banken (NVB) geeft zelf in verschillende persberichten op haar website aan dat ook de samenwerking met andere instanties, in het bijzonder het ECTF en het Nationaal Cyber Security Centrum, een belangrijke bijdrage heeft geleverd.[239] Het aanpakken van banking malware lijkt echter gelijk op te gaan met het opkomen van andere vormen van cybercrime, zoals ransomware (Europol, 2015b, p. 7). Of hier een verband tussen is, is onduidelijk. Daarnaast is het ook niet duidelijk of de fraude verschoven is naar andere landen. In tegenstelling tot Nederlandse banken, hebben banken in het buitenland niet standaard tweestaps authenticatie, hetgeen de banken extra kwetsbaar maakt voor banking malware.

5.1.2 Rol bij ransomware

In het witwasproces van gelden die worden verkregen door ransomware spelen banken geen directe rol. De betaling van het 'losgeld' geschiedt vaak in de vorm van vouchers of bitcoins. Banken spelen hooguit een indirecte rol, omdat slachtoffers via hun bankrekening bijvoorbeeld vouchers (via een kiosk) of bitcoins (bij een Bitcoin exchange) aanschaffen. Tevens kunnen banken aan het einde van de witwasketen nog een rol spelen wanneer de crimineel verkregen bitcoins weer worden omgezet naar elektronisch geld (waarna het eventueel wordt opgenomen als contant geld). Dit kan worden gesignaleerd door de banken. Verdachte stortingen via Bitcoin exchanges

236 Onbekend is of de schade door fraude met internetbankieren vóór 2011 nog groter is geweest. Uit de persberichten van de NVB wordt tevens helder dat de meeste schade uit internetbankieren wordt veroorzaakt door fraude uit phishing. In 2014 was de schade uit phishing bijvoorbeeld 3,9 miljoen euro en in 2015 3,7 miljoen euro.

237 Zie ook het persbericht op nvb.nl 'Fraude met internetbankieren gehalveerd', 18 maart 2015. Beschikbaar op: www.nvb.nl/nieuws/2015/4033/fraude-met-internetbankieren-gehalveerd.html: 'Doordat Nederlandse banken fraude met malware steeds beter geautomatiseerd kunnen detecteren en voorkomen, is de schade door malware zelfs met 90% gedaald, tot minder dan € 500.000' (laatst geraadpleegd op 9 oktober 2015).

238 Zie ook Europol 2015b, p. 26: 'Although some variants remain a threat, the investigation rates of ZeuS (plus its variants Ice IX and Citadel), Torpig, Spyeye and Carberp have either plateaued or are in decline. Many of these products have had their development and support discontinued by the developer either voluntarily or as a result of arrest.'

239 Zie ook de persberichten 'Scherpe daling fraude internetbankieren', 2 april 2013. Beschikbaar op: www.nvb.nl/nieuws/2013/1812/scherpe-daling-fraude-internetbankieren.html en 'Fraude met internetbankieren gehalveerd', 18 maart 2015. Beschikbaar op: www.nvb.nl/nieuws/2015/4033/fraude-met-internetbankieren-gehalveerd.html (laatst geraadpleegd op 9 oktober 2015).

kunnen vervolgens aanleiding vormen voor een witwasonderzoek.[240] Daarbij zal het in eerste instantie niet altijd helder zijn om wat voor een gronddelict het gaat.[241] In verband met de verplichte registratie van rekeninghouders bij banken (met identificatiemiddel op locatie of eventueel door middel van 1-centverificatie), kunnen opsporingsinstanties relevante gebruikersgegevens vorderen. Indien daartoe aanleiding is (en met de juiste vordering), kunnen eventueel ook relevante transactiegegevens worden gevorderd.

5.2 Money mules

Uit ons dossieronderzoek en de interviews komt het beeld naar voren dat de money mule vaak wordt gerekruteerd door een ronselaar. Money mules worden soms ingezet voor het doorsturen van pakketjes[242] die met het frauduleus verkregen geld zijn gekocht, maar meestal voor het beschikbaar stellen van een bankrekening en voor het opnemen van geld wanneer daartoe de instructie wordt gegeven. De money mule mag vervolgens een kleine commissie op het geld behouden. Daarentegen komt het via een money mule doorsluizen van geld naar een andere rekening veel minder vaak voor.

Uit de gepubliceerde Mega Server-zaak blijkt dat mensen tevens zijn geronseld om met een valse identiteit een rekening te openen en pinpassen te verkrijgen.[243] Na het opnemen van het geld werd in deze zaak getracht het geld via een geldtransferkantoor van MoneyGram over te maken naar Rusland. In de literatuur wordt ook wel genoemd dat money mules zich niet bewust zijn van het feit dat ze meewerken aan witwassen. Daarbij zijn de money mules in de veronderstelling dat via internetadvertenties een baan als 'financial manager' wordt aangeboden waarbij de mensen vanuit huis kunnen werken (UNODC 2014, p. 53-54). Uit ons onderzoek bleek dat het echter in de meeste gevallen ging om money mules die op straat geronseld werden en bewust tegen een vergoeding aan het witwassen meewerkten.

In paragraaf 5.1 kwam de actieve rol van de banken in de bestrijding van digitale bancaire criminaliteit aan bod. Dankzij de identificatieplicht is het mogelijk om een goed inzicht te verkrijgen in de kenmerken van de money mules. Met deze gegevens is het mogelijk gebleken de kenmerken van de money mules in kaart te brengen. De frauduleuze transacties zelf hebben daarnaast

240 Zie het persbericht van de FIOD, '10 aanhoudingen in internationaal bitcoins onderzoek', 20 januari 2016. Beschikbaar op: www.belastingdienst.nl/wps/wcm/connect/nl/fiod/nieuws/10_aanhoudingen_in_internationaal_bitcoins_onderzoek (laatst geraadpleegd april 2016).

241 Het is bijvoorbeeld ook mogelijk dat de transacties afkomstig zijn van drugshandel op het dark web. Het is ook mogelijk dat veel transacties via Bitcoin exchanges plaatsvinden, omdat het om een (mogelijk legale) Bitcoin-handelaar gaat.

242 Merk op dat het hier strikt genomen eigenlijk gaat om een katvanger, aangezien een adres en geen bankrekening ter beschikking wordt gesteld.

243 Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041.

bijgedragen aan het in kaart brengen van de meest populaire witwaskanalen voor banking malware en phishing (zie Bijlage 5).

Via het ECTF-samenwerkingsverband hebben de vier grootste Nederlandse banken (ABN-AMRO, ING, Rabobank en SNS bank) voor dit onderzoek gegevens beschikbaar gesteld over alle transacties die betrekking hadden op banking malware (en phishing) over de periode 2012 tot en met 2015. Dit maakte het mogelijk om het onderzoek naar money mules van Mauritz (2014), dat alleen op 2012 is gebaseerd, voor een langere tijdsperiode uit te voeren en de bevindingen daarin verder uit te diepen. In deze paragraaf worden de resultaten van deze nieuwe gegevensset over money mules in Nederland besproken. Meer informatie over de gegevensset zelf en andere resultaten die hieruit zijn verkregen, worden in bijlage 5 gepresenteerd. Let wel, dankzij deze gegevensset van de banken is het mogelijk om gedetailleerde kenmerken van money mules in kaart te brengen, zeker in vergelijking met de andere actoren die worden besproken in dit hoofdstuk. Dit betekent uiteraard niet dat de money mule een belangrijkere rol speelt in het witwasproces, maar vooral dat relatief veel over deze actor bekend is.

5.2.1 Omgevingskenmerken

De omgevingskenmerken zijn afgeleid uit de opgegeven woonplaatsen van de rekeninghouders. Hoewel money mules door heel Nederland verspreid wonen (zie ook Mauritz, 2014), laat figuur 5.1 zien dat negen van de tien gemeenten met het hoogste aantal money mules behoren tot de top vijftien grootste gemeenten van Nederland.[244] De enige uitzondering is Schiedam, de 44e gemeente van Nederland, die op de vijfde plaats staat. Zeer waarschijnlijk komt deze hoge notering door de nabijheid van Rotterdam.

Tabel 5.2 geeft voor elk jaar de top vijf steden aan en het percentage van de money mules dat daar woonachtig is. Hierdoor wordt duidelijk dat de drie grootste gemeenten (Amsterdam, Rotterdam, en Den Haag) elk jaar de gegevensset domineren. Samen huisvesten ze jaarlijks meer dan 40% van het totaal aan money mules, terwijl maar 12% van de Nederlandse bevolking in deze drie steden woont. Daarnaast is het ook duidelijk dat de overige gemeenten in de top vijf nauwelijks veranderen.

244 https://nl.wikipedia.org/wiki/Lijst_van_grootste_gemeenten_in_Nederland.

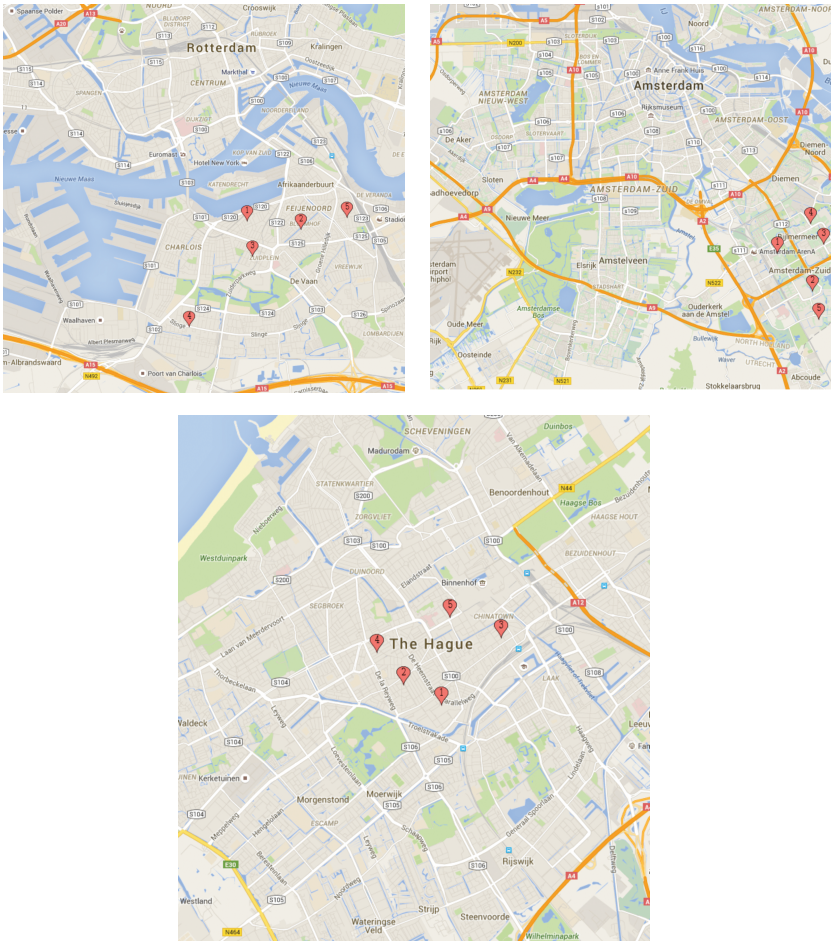
Figuur 5.1 **Top tien gemeenten met het hoogste aantal money mules in de periode van 2012 tot en met 2015**

Tabel 5.2 **Top vijf gemeenten met het hoogste aantal money mules per jaar**

2012	2013	2014	2015
Rotterdam (18%)	Rotterdam (17%)	Rotterdam (20%)	Rotterdam (14%)
Den Haag (12%)	Amsterdam (16%)	Amsterdam (19%)	Amsterdam (14%)
Amsterdam (11%)	Den Haag (10%)	Den Haag (10%)	Den Haag (12%)
Almere (3,5%)	Almere (3,5%)	Almere (2,9%)	Almere (3,7%)
Schiedam (3,5%)	Schiedam (1,6%)	Utrecht (1,9%)	Utrecht (2,7%)

Met behulp van de opgegeven postcode van rekeninghouders is het ook mogelijk om na te gaan in welke wijk de money mule woont. Figuur 5.2 toont voor Rotterdam (links), Amsterdam (rechts) en Den Haag (linksonder) de top vijf wijken met meest voorkomende money mules. Na deze top vijf is voor alle drie de steden een sterke afname in het aantal money mules in een wijk te zien. Waar in de top vijf wijken gemiddeld nog 103 money mules wonen, is dit voor de wijk op de zesde plaats nog ongeveer de helft.

Figuur 5.2 Top vijf wijken met het hoogste aantal money mules voor Rotterdam (Links), Amsterdam (Rechts) en Den Haag (Linksonder)

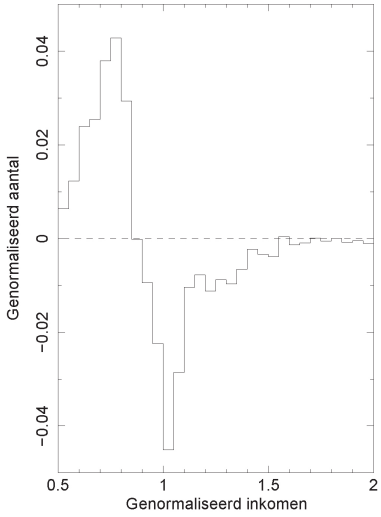


Figuur 5.2 laat zien dat voor de drie grote gemeenten de money mules zich voornamelijk in achterstandswijken bevinden (Amsterdam-Zuidoost, Rotterdam-Zuid, en de Schilderswijk). Dit suggereert dat money mules voornamelijk in armere buurten wonen. Om deze hypothese te toetsen, kan de verdeling van het gemiddelde inkomen van de wijken waarin money mules wonen, worden vergeleken met het gemiddelde inkomen van alle wijken in Nederland. Hiervoor zijn de cijfers over het aantal inwoners, het gemiddelde inkomen in een wijk en de meest voorkomende postcode in de wijk uit het bestand 'Kerncijfers wijken en buurten 2009-2012' (CBS, 2012a[245]) gebruikt.

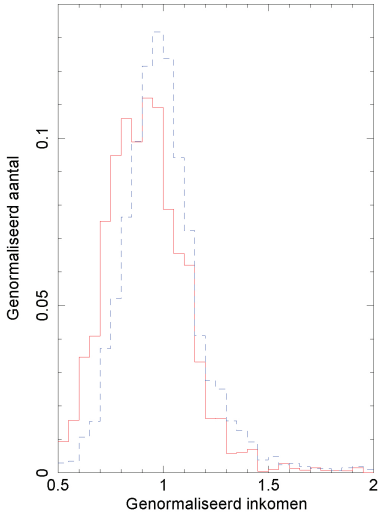
245 Beschikbaar op: http://statline.cbs.nl (laatst geraadpleegd in februari 2016).

Figuur 5.3

Verschil tussen het gemiddelde inkomen van de wijken waarin money mules wonen en dat van alle Nederlandse wijken



Verdeling van het gemiddelde inkomen in de wijken waarin de money mules wonen (vaste lijn) en van alle Nederlanders (gestreepte lijn)



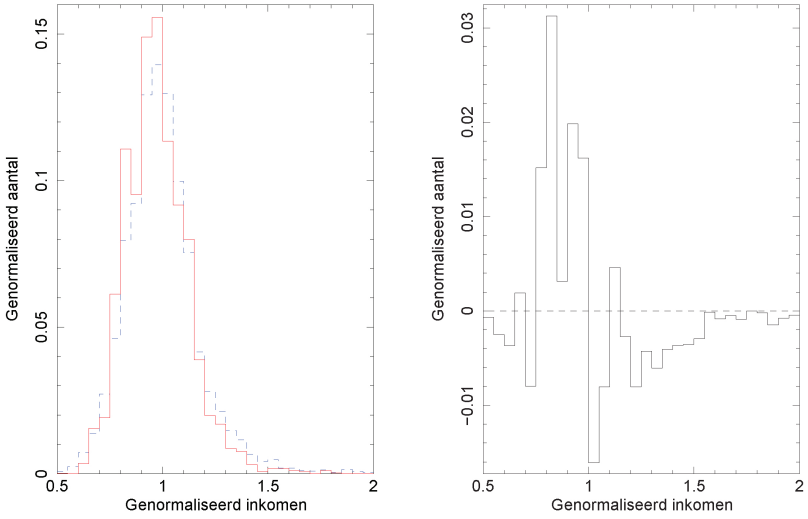
De resulterende verdelingen worden getoond in figuur 5.3 (links), waarbij de gestreepte lijn het gemiddelde inkomen voor alle wijken laat zien en de vaste lijn die van de wijken waarin de money mules wonen. De vaste lijn, die de verdeling van de money mules weergeeft, ligt voor de laagste inkomens altijd hoger dan voor de verdeling voor alle Nederlanders. Dit betekent dat money mules typisch in armere wijken wonen. Ditzelfde beeld wordt op andere wijze gevisualiseerd in figuur 5.3 (rechts), waar het verschil tussen beide verdelingen uit figuur 5.3 (rechts) wordt getoond. Hier ligt bij de lagere inkomens het verschil tussen de verdelingen altijd boven de gestreepte lijn (die het nulniveau aangeeft), wat ook betekent dat money mules voornamelijk in armere wijken wonen.

Uit de combinatie van tabel 5.2 en figuur 5.3 is duidelijk dat armere wijken in de drie grote steden de set van money mules domineren. Om na te gaan waar de money mules in overige gemeenten wonen, is ook de verdeling van het gemiddelde inkomen voor de wijken van de money mules die niet in de drie grote steden wonen gemaakt.

Figuur 5.4

Verschil tussen het gemiddelde inkomen van de wijken waarin money mules wonen en dat van alle Nederlandse minus de drie grote steden.

Verdeling van het gemiddelde inkomen in de wijken waarin de money mules wonen (vaste lijn) en van alle Nederlanders (gestreepte lijn) minus de drie grote steden



Het linkerpaneel van figuur 5.4 toont de resulterende verdeling (vaste lijn), die wordt vergeleken met de verdeling van de CBS gegevens waarin de drie grote steden ook niet zijn meegenomen (gestreepte lijn). Het rechterpaneel van figuur 5.4 laat ook deze keer het verschil tussen beide verdelingen zien. Hoewel er een verandering is in vergelijking met de verdeling waar de grote steden wel worden meegenomen, wonen ook hier de money mules voornamelijk in armere wijken. Het grote verschil met de verdeling voor alle gemeenten in Nederland (figuur 5.3) is dat de money mules buiten de drie grote steden voornamelijk in wijken wonen waar het gemiddeld inkomen tussen 0,75 en 1,0 keer modaal is, terwijl dit voor de totale set tussen de 0,5 en 1,0 keer modaal is. Dit betekent dat buiten de grote steden de money mules ook in armere wijken wonen, maar dat deze wijken minder arm zijn dan in de drie grote steden.

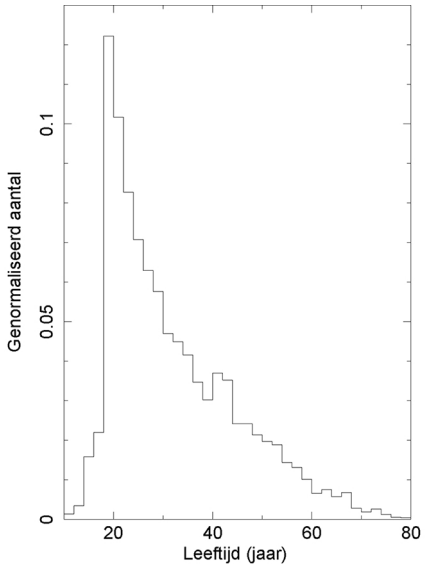
Om te controleren of er veranderingen over tijd plaatsvinden, is de verdeling van het gemiddelde inkomen van de wijk waarin de money mules wonen, voor elk jaar gemaakt. Hierbij worden geen significante veranderingen waar-

genomen.[246] Dat betekent dat money mules tussen 2012 en 2015 uit vergelijkbare wijken worden gerekruteerd. Andere dwarsdoorsneden van de data (bijvoorbeeld geslacht, bank, leeftijd, etc.) laten ook geen significante veranderingen zien.

5.2.2 Leeftijd, geslacht en nationaliteit

De gegevensset van de banken laat verder zien dat 66% van de money mules man is. Daarnaast laat de verdeling van de leeftijd van de money mules op het moment van de transactie zien (zie figuur 5.5) dat er een sterke piek is tussen de 18 en 22 jaar. Slechts een kleine fractie van de money mules is jonger dan 18 jaar, maar wel is er een lange staart met money mules die ouder zijn dan 22 jaar. Ook voor verdeling van de leeftijd wordt er geen significante verandering over de jaren 2012 tot 2015 waargenomen (evenmin als voor enige andere dwarsdoorsnede zoals geslacht, woonplaats of bank).

Figuur 5.5 Verdeling van de leeftijd van de money mules ten tijde van de transactie



Zoals aangegeven aan het begin van deze paragraaf zijn er aanwijzingen dat veel geld uiteindelijk naar Oost-Europese landen verdwijnt (UNODC 2014). Het is daarom goed mogelijk dat personen met een Oost-Europese achtergrond een grotere kans hebben om hun bankrekening ter beschikking te stellen voor witwassen, omdat ze bijvoorbeeld makkelijker te ronselen zijn of de

246 Dit kan bijvoorbeeld worden getest met een Chi-kwadraattest. Voor meer informatie zie Bevington en Robinson (2003).

bankrekening doelbewust voor witwasactiviteiten hebben geopend. Om deze hypothese te toetsen zijn de statistieken over het aantal Oost-Europeanen in Nederland gebruikt (CBS, 2012b)[247] voor zowel de drie grote steden als geheel Nederland minus de drie grote steden.

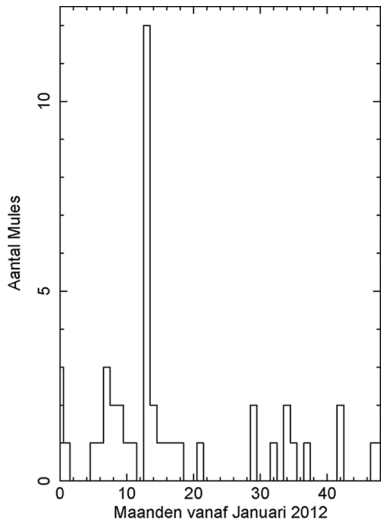
In Amsterdam heeft tussen de 7,9% en 12,9% van de money mules een Oost-Europese nationaliteit, terwijl volgens cijfers van het CBS (2012) dit 1,4% van de inwoners zou moeten zijn. Vergelijkbare percentages worden ook voor andere grote steden gevonden. Voor geheel Nederland minus de drie grote steden wordt een percentage van Oost-Europese money mules gevonden tussen 2,7% en 3,4%, terwijl ook hier het verwachte percentage veel lager is (namelijk 0,9%). Daar de percentages van Oost-Europese money mules veel groter zijn dan verwacht op basis van het aantal inwoners met een Oost-Europese nationaliteit, is het aannemelijk dat de hypothese correct is.

5.2.3 Ronselen

Door te controleren of in een gemeente een groot aantal money mules in dezelfde periode werd gebruikt, kan worden nagegaan of ronselen heeft plaatsgevonden. De gedachte hierachter is dat de bankrekeningen van de money mules die in dezelfde periode worden geronseld ook in eenzelfde periode worden gebruikt voor een frauduleuze transactie. Hiervoor is voornamelijk naar de middelgrote gemeenten gekeken waar gemiddeld twee tot vijf frauduleuze transacties per maand plaatsvinden. In 75% van deze gemeenten vindt een groot deel van de transacties in één en dezelfde maand plaats. Een voorbeeld daarvan wordt getoond in figuur 5.6. In deze figuur is te zien dat in de meeste maanden twee of minder transacties plaatsvonden, maar dat er in januari 2013 (maand 13) plotseling twaalf transacties waren. Omdat de kans dat er twaalf of meer transacties in één maand voorkomen zo klein is (veel kleiner dan 1%)[248], lijkt het waarschijnlijk dat de money mules die bij deze transacties betrokken waren allen in dezelfde periode zijn gerekruteerd.

247 Beschikbaar op: http://statline.cbs.nl (laatst geraadpleegd in februari 2016).
248 Om te berekenen wat de kans is op meer dan 12 gebeurtenissen in een maand, is een binomiale verdeling aangenomen met 38 gebeurtenissen een kans van 1/48 dat een gebeurtenis voorkomt.

Figuur 5.6 Tijdlijn over een periode van 4 jaar (48 maanden) waarin het aantal transacties per maand in een middelgrote gemeente in Nederland wordt getoond



5.2.4 Antecedenten

Voor circa 600 money mules die actief waren in 2012 is naar mogelijke antecedenten (t/m september 2015) gezocht in het politie-informatiesysteem Blueview. Hieruit blijkt dat 40% van de money mules geen antecedenten heeft, 19% één antecedent heeft en 12% kan worden geclassificeerd als veelpleger (en met dus meer dan tien antecedenten). Wat opvalt, is dat er in 2012 in veel gevallen geen aangifte werd gedaan tegen money mules en dat dus 69% niet of nauwelijks bekend is bij de politie. In tabel 5.3 wordt voor verschillende groepen de top vijf van meest voorkomend delicttype getoond. De tabel laat zien dat money mules voornamelijk betrokken waren bij diefstal- en/of geweldsdelicten. Slechts een kleine fractie was betrokken bij oplichting, fraude of heling (in de tabel aangeduid met 'Opium').

Tabel 5.3 Top vijf meest voorkomend delict type voor verschillende groepen money mules

Allen*	Één antecedent	Veelplegers*
Diefstal (48%)	Diefstal (25%)	Diefstal (133%)†
Mishandeling (17%)	Opium (17%)	Mishandeling (52%)
Opium (14%)	Mishandeling (11%)	Geweld (49%)
Geweld (14%)	Oplichting (9%)	Heling (38%)
Bedreiging (11%)	Fraude (6%)	Bedreiging (36%)

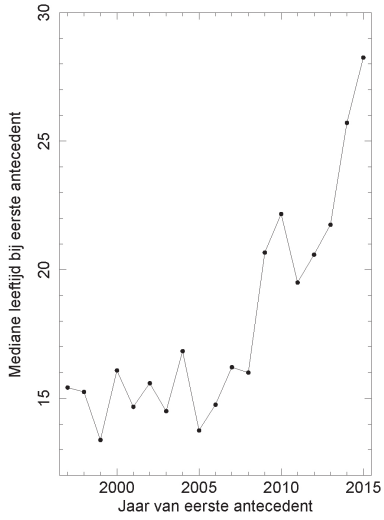
* Omdat een money mule meerdere antecedenten kan hebben, die kunnen bestaan uit verschillende delicten, is totaal groter dan 100%.

† Deze categorie bevat verschillende typen diefstal waardoor het percentage groter dan 100% is.

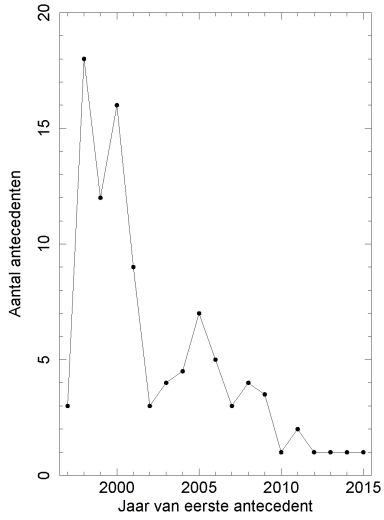
Daarnaast is voor elke money mule bepaald in welk jaar het eerste antecedent was. Figuur 5.7 (links) toont de mediane[249] leeftijd van de money mules per jaar van eerste antecedent. Opvallend is dat tot 2008 de leeftijd van de money mules rond de 15 jaar was en dat dit daarna naar ongeveer 21 jaar springt. Een vergelijkbare trend is zichtbaar als het mediane aantal antecedenten wordt uitgezet tegen het jaar van het eerste antecedent in figuur 5.7 (rechts). Voor 2001 wordt de set gedomineerd door veelplegers, maar van 2001 tot 2008 is het mediane aantal antecedenten gedaald naar ongeveer vier. Ook in 2008, hetzelfde jaar als de sprong in het linkerpaneel van figuur 5.7, is een tweede daling waar te nemen en is het mediane aantal antecedenten van de money mules minder dan vijf geworden.

Figuur 5.7

Mediane leeftijd ten tijde van het eerste antecedent ten opzichte van het jaar van eerste antecedent



Mediane aantal antecedenten als functie van het jaar van eerste antecedent



Het lijkt erop dat in totaal vier verschillende groepen van money mules kunnen worden onderscheiden. Allereerst is er de grootste groep van money mules die geen antecedenten hebben. Daarna zijn er de mules die gemiddeld 20 jaar oud zijn en één of twee antecedenten hebben. Ze komen vaak voor het eerst in aanraking met de politie nadat ze money mule zijn geweest. De derde groep komt al op 15-jarige leeftijd in aanraking met de politie en heeft vier tot acht antecedenten. Tot slot is er nog de groep van veelplegers, die

249 Leeftijd waarop precies de helft van de mules jonger (en de andere helft van de mules dus ouder) is. Er is voor de mediaan in plaats van het gemiddelde gekozen om te voorkomen dat uitschieters naar hogere leeftijden het beeld domineren.

over het algemeen ook op 15-jarige leeftijd al in aanraking komt met de politie.

5.3 Geldtransferkantoren

Uit ons dossieronderzoek komt naar voren dat geldtransferkantoren vaak worden gebruikt voor het witwassen van geld dat wordt verkregen uit banking malware.[250] Deze observatie is ook in interviews door respondenten uit de bancaire sector genoemd.[251] Ten slotte is uit gepubliceerde jurisprudentie op www.rechtspraak.nl af te leiden dat de bekende geldtransferkantoren ook worden gebruikt voor het witwassen van geld dat is verkregen uit drugshandel.[252]

Het is eenvoudig om geld over te maken bij een lokale vestiging van een geldtransferkantoor. Bij een geldtransferkantoor kan tevens (onder andere voorwaarden) via internet, een automaat, telefoon en e-mail geld worden overgemaakt. Voor het ophalen van geld op een locatie moet een identificatiemiddel worden vertoond. Ter plekke kunnen ook andere gegevens worden geregistreerd. Online worden ook registratiegegevens vereist, zoals de volledige naam, geboortedatum en telefoonnummer. Europol geeft aan dat deze gegevens echter niet geverifieerd worden (Europol 2016, p. 29). Om een geverifieerd account te krijgen moet wel een kopie van het identiteitsbewijs worden nagestuurd. Door middel van registratie van de klanten en het monitoren van transacties houden geldtransferkantoren een antiwitwasbeleid aan. Afhankelijk van het soort account is het versturen van geld via internet bovendien gebonden aan een maximumbedrag. Voor niet-geverifieerde accounts ligt deze drempel op $ 1.000 binnen een termijn van twaalf maanden, voordat gevraagd wordt om de identiteit te bevestigen. Het versturen van geld op een fysieke locatie is beperkt tot 10.000 dollar. Ook voor bedragen onder de 10.000 dollar bestaat een meldplicht als het ongebruikelijke of afwijkende transacties betreft. Meldingen moeten worden gedaan bij de FIU,[253] maar het UNODC merkt op dat door de grote hoeveelheid transacties niet altijd goed is te achterhalen welke transacties (onder de € 10.000-grens) nu precies als verdacht aan te merken zijn (UNODC 2014, p. 20).

250 Dit resultaat wordt echter slechts ondersteund door één gepubliceerde uitspraak: Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7041.

251 Merk op dat in het Criminaliteitsbeleid Witwassen 2012 wordt opgemerkt: 'Het is al twintig jaar bekend dat moneytransfers niet alleen legaal wordt gebruikt, maar ook door criminelen' (Soudijn, 2012, p. 117).

252 Zie bijvoorbeeld Rb. 's-Gravenhage, 9 maart 2007, ECLI:NL:RBSGR:2007:BA0370, Gerechtshof Amsterdam, 6 mei 2010, ECLI:NL:GHAMS:2010:BM6067, Rb. Breda, 11 oktober 2010, ECLI:NL:RBBRE:2010:BO0034, Rb. Noord-Holland, 6 maart 2014, ECLI:NL:RBNHO:2014:1968, Gerecht in eerste aanleg van Curaçao, 30 oktober 2015, ECLI:NL:OGEAC:2015:18. Zie ook Soudijn, 2012, p. 117.

253 Zie paragraaf 2.4.

5.4 Payment Service Providers

Payment Service Providers faciliteren op grote schaal betalingen voor online dienstverleners, zoals webwinkels. Een Payment Service Provider (PSP) aggregeert verschillende betaalmiddelen en doet dienst als tussenschakel tussen de betaler, de webwinkel en de dienstverlener van een financieel product. Een webwinkel kan bijvoorbeeld met één technische koppeling met een PSP verschillende betaalmethoden aanbieden. Met deze koppelingen kunnen bijvoorbeeld betalingen worden verricht via iDeal, creditcards en PayPal, maar ook met bijvoorbeeld Bitcoin en Paysafecards. Het is mogelijk dat de PSP de gelden voor de begunstigde van de betaling verzamelt en vervolgens op grond van een raamovereenkomst doorbetaalt (Voerman & Baukema, 2015). PSP's faciliteren slechts de betaling tussen de consument, webshops en banken. Zij faciliteren niet, althans niet bewust, het witwasproces (afgezien van enkele criminele PSP's).[254]

Uit interviews komt naar voren dat PSP's zelf ook monitoring toepassen om fraude tegen te gaan. Over het algemeen worden bedragen die via een PSP worden afgerekend op een rekening gestort van de PSP. Uitbetaling aan de webwinkel kan worden gepauzeerd als er indicaties zijn dat er sprake is van fraude. In sommige gevallen zal het bedrag dan direct worden teruggestort op de rekening van de consument. Om het risicoprofiel zo laag mogelijk te houden, eisen PSP's in veel gevallen van de webwinkel bij de registratie de volgende gegevens: Kamer van Koophandel-gegevens, een kopie van identiteitsbewijs en verificatie van de betaalrekening. Daarnaast is het mogelijk voor PSP's om het faciliteren van bekende witwasroutes te weigeren en extra te monitoren op risicobetalingen. Sommige PSP's kiezen er voor betalingen met een combinatie van betaalmethoden niet te faciliteren.

Er is een onderscheid te maken tussen gereguleerde en ongereguleerde PSP's. PSP's hebben een vergunning nodig van De Nederlandsche Bank als zij de gelden voor begunstigden verzamelen en doorbetalen. Kort gezegd zijn sommige PSP's in Nederland vrijgesteld van deze vergunning, omdat zij deze dienst niet leveren en onder een bepaalde grens van betalingstransacties blijven (Voerman & Baukema, 2015). Er is minder zicht op de handelingen van PSP's zonder vergunning. Bovendien zijn er vele buitenlandse PSP's actief op de Nederlandse markt. Deze betaaldiensten zijn soms gevestigd in jurisdicties met minder strenge of niet actuele regelgeving. Het kan ook zijn dat lokale handhavingsinstanties niet altijd de capaciteit hebben voor handhaving binnen deze sector of dat niet prioriteren. Dit alles zorgt voor grote verschillen in antifraude- en antiwitwasmaatregelen tussen PSP's en mogelijke

254 Tijdens het onderzoek kwam een geval naar voren waarin een derdenrekening van een Payment Service Provider werd gebruikt om criminele transacties te faciliteren, maar dit betrof geen banking malware of ransomware.

witwasroutes die criminelen kunnen nemen. Overigens is op 8 oktober 2015 de nieuwe Betalingsrichtlijn door het Europees Parlement goedgekeurd.[255] Deze richtlijn heeft tot gevolg dat meer online betalingsdiensten een vergunning moeten hebben of geregistreerd moeten zijn. De regelgeving leidt tot meer harmonisatie van regelgeving van deze nieuwe betalingsdiensten.[256] Daarmee worden de handhavingsproblemen echter niet automatisch opgelost.

5.5 Webwinkels

Uit ons dossieronderzoek en de afgenomen interviews is gebleken dat webwinkels later in de witwasketen een rol kunnen spelen. Via de bankrekening van slachtoffers van banking malware kunnen namelijk producten worden gekocht.

Webwinkels van grote omvang zoals Bol.com en Wehkamp.nl nemen zelf ook maatregelen om fraude en witwassen tegen te gaan. Uit onze interviews is duidelijk geworden dat de beveiligingsafdelingen van banken samenwerken met webwinkels om de levering van producten die met fraudeleus verkregen geld zijn betaald tegen te gaan. Indien snel wordt gehandeld, kan door middel van deze private samenwerking de schade uit banking malware worden beperkt.

5.6 Voucherdiensten

Uit ons onderzoek is gebleken dat de op zichzelf legale voucherdiensten met name bij ransomware een rol spelen binnen het witwasproces van criminelen. Voucherdiensten maken het onder andere mogelijk om de waarde van de voucher bij te schrijven op een e-wallet of direct te besteden bij een online dienstverlener. Het is eenvoudig om geld te verspreiden tussen verschillende diensten en zodoende de herkomst van het geld verder te verhullen. Bovendien kan geld uit een voucher worden geparkeerd op een online account en vanuit dat online account worden omgezet naar een andere vorm van geld.

De werking van voucherdiensten en enkele kenmerken ervan zijn reeds beschreven in hoofdstuk 3.[257] Vouchers kunnen worden gekocht (eventueel met contanten) via aangesloten winkeliers, tankstations en kiosken. Een voorbeeld van een voucher is een Paysafecard (voorheen Ukash) van Skrill.

255 Zie Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt van 23 december 2015, L 337/35.
256 Wel blijven er enige uitzonderingen van toepassing. Het ligt buiten het bestek van dit onderzoek om dieper op dit onderwerp in te gaan.
257 Zie paragraaf 3.2.2 en bijlage 4.

Voor het kopen van vouchers in Nederland bestaat een limiet om witwassen tegen te gaan. Naast de aankoop van vouchers in de fysieke wereld is het ook mogelijk om een account aan te maken teneinde voucherbedragen bij te schrijven op een e-wallet. Om gebruik te maken van dit account wordt meestal gevraagd om een naam, geboortedatum, adres, telefoonnummer en e-mailadres. Het telefoonnummer en e-mailadres worden tijdens het registratieproces geverifieerd om witwassen tegen te gaan. Zodra het account is aangemaakt is het ook mogelijk om een prepaid creditcard aan te vragen. De creditcard moet worden opgeladen met tegoed uit het account, vaak tot een maximum van € 5.000. Het is mogelijk om bij verschillende online dienstverleners direct met het tegoed op vouchers te betalen, zoals Skype, Deezer, Spotify en de PlayStation Store. Met deze aanvullende diensten vormen de voucherdiensten een uitgebreid betaalsysteem. Uit ons onderzoek blijkt dat de verschillende conversievormen mogelijkheden bieden voor cybercriminelen om geld wit te wassen (Europol, 2016, p. 8-13).[258]

5.7 E-wallet-diensten

Onder e-wallet-diensten worden in deze studie online betalingsdiensten verstaan, waarbij geld op een persoonlijk account kan worden geparkeerd. Dit account is alleen beschikbaar via internet. Een voorbeeld van een e-wallet-dienst is PayPal.[259] Met de e-wallet-dienst kunnen vervolgens betalingen worden gedaan bij aangesloten webwinkels en kunnen transacties worden verricht met andere gebruikers van de e-wallet-dienst. Indien de online portemonnee is gekoppeld aan een bankrekening kan ook geld worden af- en bijgeschreven van/op een bankrekening. Het koppelen van een e-wallet-dienst aan een bankrekening is natuurlijk een extra verificatiemiddel voor de dienst en kan een bron van gegevens zijn voor opsporingsdiensten, indien een e-wallet-dienst wordt misbruikt voor witwasdoeleinden.

Binnen de e-wallet-diensten is er een onderscheid te maken tussen e-wallet-diensten met een hoofdkantoor binnen de Europese Unie en e-wallet-diensten met een hoofdkantoor buiten de Europese Unie (Soudijn & Akse 2012, p. 160). Van deze laatste categorie e-wallet-diensten zouden criminelen vaker gebruikmaken, omdat daar minder strenge regels op het gebied van witwassen gelden. Deze regels hebben voornamelijk betrekking op het KYC-beleid en monitoring van de transacties om witwassen tegen te gaan. Bovendien hebben nationale toezichthouders in andere landen weinig zicht op de activiteiten van deze betalingsdiensten (Soudijn & Akse, 2012, p. 161). Uit interviews kwam naar voren dat de naleving van Nederlandse financiële toezicht-

258 Het gebruik van vouchersystemen ten behoeve van cybercrime wordt ook veelvuldig bevestigd in interviews en blijkt uit enkele dossiers die zijn onderzocht tijdens ons dossieronderzoek.
259 Zie paragraaf 3.3.2.

wetgeving op de activiteiten van e-wallet-diensten gecompliceerd is. De reden daarvoor is dat veel van deze betalingsdienstverleners in het buitenland gevestigd zijn en niet altijd onder de reikwijdte van de wetgeving vallen. Criminelen kunnen gebruik- en misbruik maken van financiële diensten die via internet op de Nederlandse markt worden aangeboden, terwijl de handhaving van Nederlandse regelgeving problematisch is.

Europol geeft aan dat e-wallet-diensten buiten de EU, zoals WebMoney, veel gebruikt worden door Russisch sprekende cybercriminelen (Europol 2016, p. 21). Het gebruik van dergelijke diensten door cybercriminelen wordt in onze interviews en in twee van de onderzochte dossiers bevestigd. Gebruikers moeten zich registreren met onder andere een kopie van hun identiteitsbewijs. Respondenten van interviews geven aan dat daarvoor ook valse of gestolen identiteitsbewijzen worden gebruikt. Om een rekening te openen is geen bankrekening of creditcard nodig. De betalingsdrempel wisselt per gekozen wallet en status van het account. Tegelijkertijd geeft Europol aan dat ook door de aangeboden e-wallet-diensten buiten de EU steeds meer wordt geïnvesteerd in antiwitwasmaatregelen, waardoor de diensten minder aantrekkelijk worden door cybercriminelen (Europol 2016, p. 22). De diensten worden namelijk ook gebruikt voor legitieme doeleinden en op die doelgroep willen veel van deze diensten zich richten. In onder meer Rusland, maar ook in andere landen, horen pinautomaten met toegang tot e-wallets en andere betaaldiensten bij het straatbeeld.

5.8 Bitcoin exchanges

Uit ons dossieronderzoek, de interviews met respondenten en enkele rechtszaken is af te leiden dat bitcoins door criminelen worden aangeschaft vanaf de rekening van een slachtoffer van banking malware.[260] Wanneer een transactie met bitcoins eenmaal heeft plaatsgevonden, kan de transactie niet meer worden teruggedraaid. De onderliggende infrastructuur voor de handel in bitcoins laat dit niet toe (zie hoofdstuk 3). Wel is het mogelijk om beschikbare gegevens van Bitcoin exchanges te vorderen met de juiste wettelijke grondslag.

Bitcoin exchanges in Nederland[261] zijn niet gereguleerd en zijn daarom niet verplicht een KYC-beleid aan te houden en monitoring van de betalingen toe te passen (zie hoofdstuk 3). Transacties met Bitcoins gaan doorgaans via de blockchain, maar het wisselen van Bitcoins tegen fiatvaluta gaat vaak via Bitcoin exchanges. Zoals in hoofdstuk 3 is uitgelegd, worden bitcoins niet

260 Rb. Rotterdam, 2 oktober 2015, ECLI:NL:RBROT:2015:7038.

261 In het buitenland zijn Bitcoin exchanges soms wel gereguleerd, bijvoorbeeld in de VS via FINCEN, het Financial Crimes Enforcement Network van het Amerikaanse ministerie van Financiën.

erkend als geld, waardoor Bitcoin exchanges in Nederland op dit moment niet onder de wetgeving voor financieel toezicht vallen (Voerman & Baukema, 2015). Toch nemen veel Bitcoin exchanges in Nederland in de praktijk op vrijwillige basis maatregelen om gebruikers van hun diensten te identificeren en transacties te monitoren om witwassen tegen te gaan.[262] Voor het aankopen van bitcoins is bijvoorbeeld een verificatie van de rekening noodzakelijk. Tevens moet soms een telefoonnummer worden opgegeven voordat het mogelijk is om een transactie te verrichten. Door deze maatregelen kan witwassen voor een deel worden tegengegaan. Het voorkomt echter niet dat slachtoffers van ransomware bij Bitcoin exchanges bitcoins kunnen aanschaffen om er losgeld mee te betalen.[263] Een groep Bitcoin exchanges heeft zich inmiddels verenigd in de Verenigde Bitcoinbedrijven Nederland (VBNL). De vereniging stelt een richtlijn op voor een uniform antiwitwasbeleid. Respondenten van Bitcoin exchanges gaven aan dat geen melding kan worden gedaan van ongebruikelijke transacties aan de FIU, waardoor verdachte transacties die door monitoring vanuit Bitcoin exchanges worden opgemerkt niet doorkomen. In tegenstelling tot de Nederlandse situatie, melden in de VS grote Bitcoin exchanges verdachte transacties direct aan het Amerikaanse FINCEN.

5.9 Mixing services

Zoals in paragraaf 3.3.4 is uitgelegd, is het Bitcoin-systeem pseudo-anoniem. De Bitcoin-transacties zelf zijn openbaar, maar de identiteit van de zender en ontvanger niet. Bitcoin-transacties worden gelogd en kunnen worden herleid tot een Bitcoin-adres van zowel de zender als ontvanger, inclusief de hoeveelheid bitcoins die op een bepaald Bitcoin-adres staan. Het gebruik van mixing services heeft als doel transacties met bitcoins anoniemer te maken. Het idee achter mixing services is dat bitcoins tegen andere bitcoins worden gewisseld (tegen betaling van een commissie), zodat de herkomst van de bitcoins verder wordt verhuld.[264] Uit de in paragraaf 4.2.2 beschreven test bleek dat mixing services, voor zover ze geen ‘scams’ zijn en de bitcoins niet voor zichzelf houden, de herkomst van bitcoins inderdaad goed kunnen verhullen. Toch is het mogelijk om met een combinatie van opsporingsmethoden, bepaalde analysesoftware en het koppelen van bekende Bitcoin-adressen en identiteiten de gebruikers van bepaalde Bitcoin-transacties te achterhalen (Möser, Böhme & Breuker, 2013, p. 4).

262 Overigens kan dit deels worden verklaard door druk vanuit banken die slechts onder bepaalde voorwaarden elektronische betalingen aan Bitcoin exchanges willen faciliteren.
263 Uiteraard kunnen Bitcoin exchanges wel hun klanten waarschuwen dat het niet verstandig is om losgeld voor ransomware te betalen.
264 Zie ook paragraaf 4.2.2.

Mixing services kunnen gevestigd zijn in jurisdicties waar minder strenge regels met betrekking tot witwassen gelden. Uit de empirische oefening komt naar voren dat op het dark web wordt geadverteerd door aanbieders van mixing services. Echter, de fysieke locatie van deze diensten is vaak onduidelijk, omdat wordt geadverteerd op websites via Tor en het vestigingsadres van het bedrijf niet wordt genoemd. Het behoeft geen betoog dat het ontbreken van kennis over de fysieke locatie van de bedrijven en het gebrek aan andere identificerende informatie over de bedrijven die mixing services aanbieden uitdagingen stellen aan de handhavingsinstanties.

5.10 Bitcoin-handelaren

Uit dossieronderzoek en interviews is gebleken dat bitcoins ook worden witgewassen door een fysieke handelaar in te schakelen. Deze handelaren komen op een afgesproken locatie samen met een klant. Tegen betaling van een relatief hoge commissie kan de klant vervolgens bitcoins inruilen bij de Bitcoin-handelaar voor contant geld (CSBN 6, 2016, p. 26).[265] Respondenten geven aan dat handelaren hun diensten aanbieden via online marktplaatsen, zoals Local Bitcoins. Het feit dat deze marktplaatsen geen strikte verificatieprocedure hanteren, is aantrekkelijk voor criminelen. Uit interviews is één zaak naar voren gekomen waarin gebruik werd gemaakt van deze methode. De zaak begon met een melding van ongebruikelijke transacties van een cliënt van een bank, waarbij grote bedragen zeer regelmatig en direct na ontvangst contant werden opgenomen. In deze zaak spraken de verdachten via een website zoals Localbitcoins.com af bij openbare eetgelegenheden (zoals McDonald's of Starbucks). Daar werden vervolgens bitcoins gekocht van personen in ruil voor contant geld tegen een commissie. Vervolgens werden de bitcoins direct verkocht via bitcoin exchanges. Het geld dat werd teruggestort op de aangegeven bankrekening werd direct na ontvangst opgenomen. Het is niet duidelijk geworden wat daarna met het geld gedaan werd, maar naar verwachting zijn daar ook nieuwe bitcoins van gekocht. In een periode van tweeënhalf jaar is minstens een paar miljoen euro witgewassen.

5.11 Tussenconclusie

In dit hoofdstuk is getracht om antwoord te geven op de vraag: *Wat zijn de kenmerken van actoren die betrokken zijn het bij het witwassen van geld dat wordt verkregen uit cybercrime?*

Aan de hand van de modellen in hoofdstuk 4 zijn, naast de cybercriminelen zelf, ook de volgende actoren geïdentificeerd: (1) banken, (2) money mules,

265 Merk op dat deze hoge commissie eventueel als een indicatie voor opzet bij witwassen zou kunnen gelden.

(3) geldtransferkantoren, (4) Payment Service Providers, (5) webwinkels, (6) voucherdiensten, (7) e-wallet-diensten, (8) Bitcoin exchanges, (9) mixing services en (10) Bitcoin-handelaren. In hoofdstuk 3 en bijlage 4 zijn reeds voorbeelden van deze diensten gegeven met daarbij bijzondere aandacht voor bepaalde kenmerken (m.b.t. de registratieverplichtingen van klanten en land van vestiging).

In dit hoofdstuk zijn de kenmerken van money mules uiteengezet die betrokken zijn geweest bij het wegsluizen van geld dat is verkregen uit phishing en banking malware. Als belangrijke schakel in de meest gangbare modus operandi voor het witwassen van geld verkregen uit banking malware is het de meest voor de hand liggende groep om als eerste te analyseren. De resultaten laten zien dat veel en gedetailleerde informatie over de kenmerken van money mules kan worden verkregen. In het kort wordt het beeld van Mauritz (2014) bevestigd, namelijk dat ze voornamelijk jongvolwassenen tussen de 18 en 22 jaar zijn die in armere wijken wonen. Echter, die gegevensset beperkte zich tot 2012, en nu kan er ook voor de daarop volgende jaren (t/m 2015) worden geconcludeerd dat de kenmerken van de money mules gelijk zijn gebleven. Daarnaast laten de resultaten zien dat het via de andere actoren die tijdens dit onderzoek in beeld zijn gekomen, zoals bijvoorbeeld Payment Service Providers of Bitcoin exchanges, ook de moeite kan lonen om een gelijksoortig onderzoek uit te voeren met de frauduleuze transacties.

De identificatie van money mules en het blokkeren van frauduleuze transacties is een effectieve manier gebleken om de schade uit banking malware te beperken. Criminelen zijn echter constant op zoek naar alternatieven om met cybercrime geld te verdienen en de oorsprong van het verkregen geld te verhullen. Uit ons onderzoek blijkt dat het verkregen geld uit banking malware regelmatig wordt weggesluisd naar het buitenland via geldtransferkantoren. Money mules kunnen daarbij tevens worden ingezet om het geld te versturen en op te halen. Money mules worden door opsporingsdiensten als het 'laaghangend fruit' beschouwd van de criminele organisatie die achter de exploitatie van banking malware zitten.

Online betalingsdiensten, zoals voucherdiensten en e-wallet-diensten bieden hun diensten vaak wereldwijd aan. Deze bedrijven vereisen tevens een vorm van registratie en doen ook aan transactiemonitoring om witwassen tegen te gaan. Een belangrijk verschil met banken is dat er minder direct contact is met klanten (met daarbij een identificatie die op locatie plaatsvindt). Bovendien kunnen de dienstaanbieders in een andere jurisdictie gevestigd zijn, hetgeen handhaving en opsporingsonderzoeken bemoeilijkt. Payment Service Providers en webwinkels nemen ook maatregelen om witwassen tegen te gaan, maar hebben minder zicht op de oorsprong van transacties, waardoor het lastiger is malafide transacties te blokkeren.

Bitcoin exchanges kunnen ook overal ter wereld gevestigd zijn. Ook zij nemen in meer of mindere mate maatregelen om witwassen te bestrijden. In Nederland hebben Bitcoin exchanges zich verenigd en nemen ze op vrijwillige basis maatregelen om witwassen via hun diensten tegen te gaan. Mixing services kunnen de herkomst van bitcoins verder verhullen. De diensten worden aangeboden via Tor, waardoor de locatie van de dienstverleners lastiger te achterhalen is, hetgeen de handhaving bemoeilijkt.

6 Conclusie

In dit onderzoek is nagegaan hoe geld verkregen uit cybercrime wordt witgewassen. Daarbij is de nadruk gelegd op twee typen van cybercrime waarmee veel geld wordt verdiend, namelijk banking malware en ransomware. Naast verschillende 'klassieke' witwasmethoden die hierbij worden gebruikt, is in het bijzonder ingegaan op witwasmethoden met behulp van Bitcoin en andere virtuele valuta en de rol van online financiële dienstverleners. De hoofdvraag van dit onderzoek is als volgt geformuleerd:

Op welke wijze en door welke actoren wordt geld dat wordt verkregen uit banking malware en ransomware (al dan niet digitaal) witgewassen?
In dit hoofdstuk zal beknopt antwoord worden gegeven op bovenstaande onderzoeksvraag door de zes deelvragen te beantwoorden (paragraaf 6.1). Deze deelvragen zijn uitgebreid aan bod gekomen in de hoofdstukken 2 tot en met 5. Vervolgens worden aanbevelingen gedaan over hoe deze vormen van cybercrime gericht kunnen worden tegengegaan en digitaal witwassen verder kan worden bestreden (paragraaf 6.2). Ten slotte worden suggesties gedaan voor verder onderzoek (paragraaf 6.3).

6.1 Antwoorden op de onderzoeksvragen

1 *Wat wordt verstaan onder het witwassen van door banking malware en ransomware verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?*

Banking malware is, kort gezegd, kwaadaardige software die bedoeld is om geld van slachtoffers afhandig te maken via betalingen met internetbankieren. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist. Het geld dat wordt verkregen uit de twee typen misdrijven is doorgaans digitaal van aard. Bij banking malware wordt doorgaans elektronisch geld verdiend/buitgemaakt en bij ransomware wordt het losgeld doorgaans betaald met vouchers of (in toenemende mate en vooral bij cryptoware) met bitcoins. Het witwassen van deze opbrengsten bestaat uit het verbergen of verhullen van de criminele herkomst van het geld.

Witwassen is strafbaar gesteld als opzetwitwassen (art. 420bis Sr), gewoontewitwassen (art. 420ter Sr) en schuldwitwassen (art. 420quater Sr). Witwassen omvat in de kern het verbergen of verhullen van de illegale herkomst van gelden of voorwerpen, doorgaans met de bedoeling het geld te kunnen gebruiken in het normale handelsverkeer.[266] De typologieën die zijn ontwikkeld om opzet bij opzetwitwassen te bewijzen, hebben vooral betrekking op contant geld bij (veelal) drugsdelicten. In de praktijk bestaat daardoor regelmatig

266 Het gaat niet om het verhullen van gelden of voorwerpen zelf, maar om de illegale herkomst ervan.

onduidelijkheid over de vraag op welke moment bij transacties met of bezit van grote sommen virtuele betalingsmiddelen gesproken kan worden van opzet bij witwassen. Ook Bitcoin en andere virtuele valuta kunnen worden gebruikt bij witwassen.

2 *Wat zijn digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, en hoe werken deze digitale betalingsmiddelen?*

Digitale betalingsmiddelen zijn betalingsmiddelen waarbij geld digitaal wordt overgedragen.[267] Digitaal geld kan bestaan uit elektronisch geld of virtueel geld. Elektronisch geld is de digitale weergave van echt geld (bijvoorbeeld euro's of dollars), terwijl virtueel geld niet door de overheid is gefiatteerd (bijvoorbeeld vouchers of tegoeden).

Virtueel geld kan centraal of decentraal beheerd zijn en wel of niet inwisselbaar zijn tegen echt geld. Inwisselbaar, centraal beheerd virtueel geld betreft bijvoorbeeld tegoeden op websites, niet-inwisselbaar centraal beheerd virtueel geld betreft bijvoorbeeld speelgeld in online games en virtuele werelden. Inwisselbaar, decentraal beheerd virtueel geld betreft cryptocurrencies. Veruit de bekendste cryptocurrency is Bitcoin, met 90% van de totale marktwaarde van virtuele valuta, maar er bestaan daarnaast honderden zogeheten altcoins, cryptocurrencies die een alternatief zijn voor Bitcoin. Via Bitcoin exchanges, een soort online wisselkantoren, kunnen bitcoins worden aangekocht en verkocht. Er zijn steeds meer aanbieders van producten en diensten die bitcoins accepteren als betaalmiddel. Betalingen met bitcoins lijken vanuit gebruikersperspectief min of meer op het versturen van een e-mailbericht.

3 *Op welke wijze en door welke actoren wordt geld witgewassen dat*
a *door middel van banking malware wordt verkregen?*

Er zijn twee methoden waarmee geld verdiend door middel van banking malware wordt witwassen. De eerste is met behulp van zogeheten money mules (personen die, doorgaans tegen een vergoeding, hun bankrekening beschikbaar stellen – ook wel geldezels genoemd). Het geld wordt vanaf de rekening van het slachtoffer van banking malware overgemaakt naar een rekening van een money mule. Vervolgens neemt de money mule of een ander individu (de *casher*) het bedrag zo snel mogelijk op bij een geldautomaat (de *cash-out*). Het geld wordt daarna bijvoorbeeld via geldtransferkantoren naar het buitenland overgemaakt, waarna het geld eventueel door een money mule in het buitenland wordt opgenomen.

267 Betaalmethoden betreffen de manier van betalen, betaalmiddelen betreffen hetgeen wordt overgedragen.

De tweede methode is met elektronisch geld direct vanaf de rekening van het slachtoffer van banking malware goederen, diensten en/of bitcoins aankopen met behulp van de financiële gegevens van het slachtoffer. Daarbij kan van meerdere online dienstverleners gebruik worden gemaakt. In de praktijk lopen deze modellen dikwijls door elkaar.

b *door middel van ransomware wordt verkregen?*

Ook voor het witwassen van geld verkregen door middel van ransomware zijn twee methoden te onderscheiden. De eerste is met behulp van vouchers: nadat het losgeld in de vorm van vouchers is ontvangen, kan de waarde van de voucher op een account van een e-wallet-dienst worden bijgeschreven of via internet worden doorverkocht. Ook kan een variant worden onderscheiden waarbij de voucher direct wordt besteed bij een online dienstverlener die vouchers accepteert. Vervolgens kan het geld verder worden witgewassen door het verder te verhullen of te besteden, bijvoorbeeld via de (online) aankoop van goederen, het laden van de voucher op een prepaid creditcard, en het pinnen van het contante geld en het omzetten van het geld in een ander digitaal betalingsmiddel.

De tweede methode is met behulp van bitcoins. Nadat het losgeld in de vorm van bitcoins is ontvangen, vindt eventueel een verhullingshandeling plaats door van een mixing service gebruik te maken teneinde de herkomst van de bitcoins verder te verhullen. Vervolgens kunnen bitcoins worden omgezet of besteed via Bitcoin exchanges, fysieke Bitcoin-handelaren, online witwasdiensten en dienstverleners die bitcoins als betaalmiddel accepteren. Gelet op het groeiend aantal mogelijkheden om bitcoins te besteden, kunnen criminelen er ook voor kiezen de bitcoins niet om te zetten, maar te laten staan op hun account.

4 *Wat zijn de kenmerken van actoren die betrokken zijn het bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?*

Naast de cybercriminelen zelf kunnen de volgende actoren betrokken zijn bij het witwasproces: banken, money mules, geldtransferkantoren, Payment Service Providers, webwinkels, voucherdiensten, e-wallet-diensten, Bitcoin exchanges, mixing services en Bitcoin-handelaren.

Money mules in Nederland zijn voornamelijk jongvolwassenen tussen de 18 en 22 jaar uit armere wijken die zich laten ronselen om tegen betaling hun pinpas af te staan. Hoewel de jongeren in de achterstandswijken van de drie grote steden (Amsterdam, Rotterdam en Den Haag) oververtegenwoordigd zijn, komen money mules uit alle gemeenten in Nederland. De jongeren hebben relatief vaak een Oost-Europese nationaliteit. Money mules worden door

opsporingsdiensten als het 'laaghangend fruit' beschouwd van de criminele organisatie die achter de exploitatie van banking malware zitten.

Van de andere actoren kunnen door een gebrek aan onderzoeksgegevens geen uitgebreide kenmerken worden beschreven. Een beknopt overzicht van de kenmerken van betalingsdiensten die worden gebruikt door criminelen om geld verkregen uit cybercrime wit te wassen (WebMoney, PayPal, Ukash/Paysafecard, Neteller, Skrill, PerfectMoney, Western Union en banken) is te vinden in bijlage 4.

5 *Welke informatie over de modus operandi van actoren die betrokken zijn bij het witwassen van geld dat verkregen wordt uit banking malware en ransomware, is beschikbaar op het dark web?*

Op het dark web worden mixing services aangeboden waarbij, tegen betaling van een commissie, bitcoins kunnen worden verruild voor andere bitcoins, zodat de herkomst van de originele bitcoins verder verhuld kan worden. De bitcoins kunnen vervolgens via verschillende manieren worden omgezet in contant geld of andere valuta. Zowel mixing services als online witwasdiensten worden via het dark web aangeboden, vaak via Tor, waardoor het lastig is de locatie van deze dienstverleners vast te stellen. Dat maakt het lastig voor opsporings- en handhavingsinstanties om bewijs te verzamelen of toezicht uit te oefenen. Indien het mogelijk is een server van een mixing service met transactiegegevens veilig te stellen, zou een analyse van de opgeslagen gegevens op de server het koppelen van bitcoin transacties weer mogelijk kunnen maken.

6 *Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?*

De opbrengsten van banking malware zijn doorgaans in de vorm van elektronisch geld en de opbrengsten van ransomware zijn doorgaans in de vorm van vouchers of bitcoins. Daarmee zijn alle opbrengsten van banking malware en ransomware digitale betalingsmiddelen. Ook in het daarop volgende witwasproces komen verschillende digitale betalingsmiddelen naar voren, al is het ook belangrijk om op te merken dat criminelen in veruit de meeste gevallen ernaar lijken te streven de opbrengsten vroeg of laat om te zetten in contant geld. In drie van de vier modellen beschreven in hoofdstuk 4 spelen virtuele valuta een rol. Alleen bij het model waarbij meteen via money mules een cash-out plaatsvindt, spelen virtuele valuta geen rol. Bij de andere modellen, inclusief alle varianten voor het witwassen van gelden uit ransomware, kunnen bitcoins en vouchers een rol spelen. Het witwassen van bitcoins gaat via (offline en online) Bitcoin-handelaren of mixing services.

Duidelijk is dat criminelen een breed scala aan witwasmethoden gebruiken voor het witwassen van gelden verkregen uit cybercrime. Daarbij worden combinaties van 'klassieke' witwasmethoden en witwasmethoden met digitale betalingsmiddelen gebruikt. In hoofdstuk 4 is duidelijk geworden dat er met betrekking tot ransomware een verschuiving heeft plaatsgevonden van de betaling bij ransomware via vouchers naar de betaling van het losgeld via bitcoins. Deze verschuiving gaat samen met de opkomst van cryptoware.

Met enige regelmaat komt ook het gebruik van prepaid creditcards terug in de bestudeerde dossiers. Verschillende e-wallet-diensten bieden eigen prepaid creditcards aan waarop eenvoudig tegoeden kunnen worden geladen en daarmee de cash-out van crimineel verkregen geld kan worden gefaciliteerd. Na verhulling van het financiële spoor kan het geld worden uitgegeven in de legale economie of in het criminele circuit worden gehouden. E-wallet-diensten, zoals WebMoney, Netteller en Skrill, maken het relatief eenvoudig om digitale en virtuele betalingsmiddelen om te zetten in contant geld of andere betalingsmiddelen. Deze diensten zijn niet of nauwelijks gereguleerd en vaak gevestigd in het buitenland, waardoor het lastig is bewijs voor het witwassen te verzamelen.

6.1.1 Conclusies

De antwoorden op de onderzoeksvragen overziend, kunnen enkele conclusies worden getrokken. Onder meer wordt duidelijk dat het probleem van banking malware stevig wordt geadresseerd door banken en opsporingsdiensten, maar dat het probleem van ransomware veel lastiger aan te pakken lijkt. Ransomware, in het bijzonder de variant cryptoware, neemt stevig toe en er is een duidelijke trend het losgeld op te eisen in de vorm van bitcoins, waar dat voorheen vooral in vouchers gebeurde. Er zijn in Nederland nog geen zaken met betrekking tot cryptoware voor de rechter gekomen.

Net als bij andere vormen van criminaliteit lijkt ook bij cybercrime het witwassen erop gericht te zijn vroeg of laat contant geld op te leveren. Maar niet altijd. In sommige gevallen is het voor criminelen niet nodig hun opbrengsten om te zetten in contant geld. Daarnaast proberen criminelen door middel van het gebruik van digitaal geld, in het bijzonder via bitcoins en online financiële dienstverleners, de herkomst van hun geld verder te verhullen. De rol van digitaal geld bij witwassen lijkt dus toe te nemen.

Het gebruik van virtueel geld, in het bijzonder bitcoins, is op veel vlakken aantrekkelijk voor (cyber)criminelen. De snelheid, de lage kosten en het gemak waarmee geld naar het buitenland kan worden overgemaakt, zijn legitieme voordelen voor alle gebruikers waarop criminelen graag meeliften. Daarnaast zijn het gebrek aan toezicht, de geboden anonimiteit, gebrek aan

kennis en ervaring bij opsporingsdiensten in sommige landen en jurisdictieproblemen enkele aspecten die het gebruik van virtueel geld aantrekkelijk maken voor criminelen.

Cybercriminaliteit wordt steeds complexer. Als gevolg daarvan lijken criminelen in toenemende mate te werken in georganiseerd verband, waarbij verschillende personen elk hun eigen expertise inbrengen. Zulke samenwerkingsverbanden kunnen bestaan uit experts vanuit de hele wereld en de samenwerking vindt vaak plaats via het dark web. Onderlinge transacties worden regelmatig verrekend via bitcoins of andere virtuele valuta. Bitcoins die eerder verdiend zijn met cybercrime worden soms zonder verdere omzettingen gebruikt om te investeren in nieuwe cybercrimeprojecten.

Echter, dit alles wil niet zeggen dat in de toekomst de rol van contant geld bij witwassen zal afnemen. Juist om de herkomst van crimineel verkregen geld verder te verhullen, geld snel naar het buitenland te kunnen wegsluizen en opbrengsten ongehinderd te kunnen besteden, zullen naar verwachting steeds meer complexe combinaties van omzettingshandelingen worden gebruikt. Dit zullen combinaties zijn van zowel 'klassieke' witwasmethoden als de nieuwe digitale witwasmethoden die in dit onderzoek zijn blootgelegd.

6.2 Aanbevelingen voor een verbeterde aanpak

Uit bovenstaande antwoorden op de onderzoeksvragen wordt helder dat cybercriminelen hun gelden die zijn verkregen uit banking malware en ransomware op zeer veel verschillende manieren kunnen witwassen. Het vormt op zichzelf al een uitdaging de ontwikkelingen rond digitale betalingsmiddelen bij te houden en vervolgens na te gaan op welke manier cybercriminelen van digitale betalingsmiddelen gebruikmaken ten behoeve van witwassen. Tijdens dit onderzoek werden de eerste opsporingsonderzoeken opgestart naar witwassen waarbij bitcoins in het spel waren. Daarbij is onmisbare kennis opgedaan over het gebruik van virtuele betalingsmiddelen door cybercriminelen.

De resultaten van dit onderzoek roepen de vraag op wat opsporingsinstanties en toezichthouders kunnen doen om hun aanpak van witwassen verder te verbeteren. Duidelijk is dat er geen eenvoudige, eenduidige oplossing bestaat, maar er zijn wel verschillende aanpakken die kunnen bijdragen aan een oplossing. In dat opzicht is een zogenoemd barrièremodel bruikbaar: door het opwerpen van verschillende barrières (of deeloplossingen) kan het witwassen worden tegengegaan. Deeloplossingen kunnen zich richten op het tegengaan of moeilijk maken van het gronddelict (in dit geval banking mal-

ware of ransomware) of het witwassen zelf. Hieronder worden enkele suggesties gedaan.

1 *Know Your Customer-beleid en monitoring van transacties*
Een registratieverplichting van klanten (Know Your Customer-beleid) en monitoring van transacties draagt bij aan de bestrijding van witwassen én cybercrime. De monitoringmaatregelen van banken om specifiek fraudeleuze transacties uit banking malware tegen te gaan zijn succesvol gebleken. Het gevolg is wel dat criminelen op zoek gaan naar nieuwe businessmodellen. De sterke opkomst van ransomware in de afgelopen jaren, meer in het bijzonder cryptoware, kan daardoor deels worden verklaard. Alle geïdentificeerde betalingsdienstverleners in Nederland nemen in meer of mindere mate antiwitwasmaatregelen. Naarmate de wens groter wordt om op grote schaal legale diensten te leveren, wordt de trend helder dat meer registratiemaatregelen (ook op vrijwillige basis) worden genomen en de monitoringmaatregelen worden uitgebreid. Op deze zelfregulering zou ook de overheid verder kunnen inzetten.

2 *Regulering en toezicht*
De vraag of regulering van virtueel geld vanuit economisch perspectief wenselijk is, valt buiten de reikwijdte van dit onderzoek. Het is belangrijk op te merken dat bitcoins en ander virtueel geld niet per definitie goed of slecht zijn, maar dat vooral het illegale of onethische gebruik ervan problematisch is (Angel & McCabe, 2014). Voor het algeheel verbieden van bitcoins, zoals in sommige landen gebeurt, lijkt onvoldoende reden te zijn (nog afgezien van de vraag of deze maatregel effectief zou kunnen zijn). Nu staan financiële toezichthouders echter in zekere zin buiten spel, omdat virtueel geld niet als geld of financieel product wordt beschouwd. Zij kunnen weliswaar waarschuwen voor de risico's van virtueel geld, en doen dat ook, maar kunnen op dit punt niet hun volledige arsenaal aan toezicht- en handhavingsmaatregelen inzetten. Toezichthouders kunnen hier door de overheid verder in positie worden gebracht door digitale betalingsmiddelen binnen hun toezichtbereik te plaatsen. Wij bevelen aan te overwegen Bitcoin exchanges in Nederland als betaaldienstverlener te reguleren om het witwassen van bitcoins tegen te gaan. Nederlandse Bitcoin exchanges hebben op vrijwillige basis al een uitgebreid palet aan maatregelen genomen om witwassen tegen te gaan. Maar door regulering zouden zij bijvoorbeeld ook een melding aan het FIU kunnen doen, hetgeen kan bijdragen aan de opsporing van witwassen met de virtuele valuta.

Het blijft echter een uitdaging dat online betalingsdiensten wereldwijd hun diensten kunnen aanbieden en daarbij gevestigd kunnen zijn in jurisdicties met minder strenge regelgeving of een gebrek aan toezicht of handhaving. Voor nationale toezichthouders is het zelfs binnen de EU een uitdaging om

toezicht te houden op de regels van deze internationale partijen. De tweede betalingsrichtlijn zal enige harmonisering binnen de lidstaten van de EU met zich meebrengen. De effecten van deze richtlijn kunnen echter pas later, na implementatie in de nationale juridische raamwerken, worden nagegaan. Internationale samenwerking met toezichtsinstanties en opsporingsinstanties is noodzakelijk om successen in de bestrijding van witwassen te boeken. De kennis en ervaring van opsporingsdiensten met betrekking tot internationale samenwerking kunnen verder worden verstevigd.

Ten slotte zijn er ook online betalingsdiensten die zich geheel aan het reguliere financiële verkeer (via banken) onttrekken en clandestiene diensten aan gebruikers aanbieden via internet. Digitale en virtuele betalingsmiddelen kunnen daarbij tegen een commissie worden omgezet in andere betalingsmiddelen. Het lijkt erop dat het zicht van de opsporingsdiensten op deze digitale schaduweconomie onder cybercriminelen vooralsnog gering is. Europol heeft in haar rapport over het witwassen van geld door cybercriminelen opgemerkt dat Europese opsporingsinstanties wellicht een vertekend beeld hebben van de gebruikte (digitale) betalingsmethoden door criminelen. Europol spreekt dan ook haar vermoeden uit dat wellicht vaker van diensten zoals WebMoney door Russische cybercriminelen gebruik wordt gemaakt, dan de resultaten uit opsporingsonderzoeken doen vermoeden. Opsporingsdiensten zouden hun kennis en expertise op dit vlak verder kunnen ontwikkelen.

3 *Combinaties van expertises en internationale samenwerking*
Er geen sprake van één modus operandi voor witwassen bij ransomware. Afhankelijk van de gebruikte ransomware en de betalingsmethode voor het losgeld is sprake van een andere geldstroom. Mede hierdoor zijn opsporingsonderzoeken naar witwassen van geld dat is verkregen uit ransomware gecompliceerd en kost het veel capaciteit om voldoende bewijs te vergaren voordat tot vervolging kan worden overgegaan.

Tijdens een interview werd door één van de respondenten treffend omschreven hoe voor het uitvoeren van opsporingsonderzoeken betreffende cybercrime en witwassen een combinatie van expertises noodzakelijk is. Voor de onderliggende cybercrime en digitale bewijsvergaring is de gespecialiseerde kennis van cybercrimerechercheurs noodzakelijk, voor het witwassen is gespecialiseerde kennis van financieel rechercheren noodzakelijk en vanwege het internationale aspect van de opsporingsonderzoeken moeten de opsporingsinstanties de weg zien te vinden binnen de internationale rechtshulp. Er zijn in Nederland nog geen strafzaken met betrekking tot cryptoware voor de rechter gekomen (zowel het delict zelf als het witwassen van de opbrengsten ervan). Dit is deels te verklaren doordat cryptoware een relatief recent fenomeen is, maar ook door de internationale en de technisch en juri-

disch complexe aard van het delict, waardoor het geldspoor door criminelen verder kan worden verhuld. Door de toenemende internationalisering van banking malware en ransomware en het successievelijke witwassen van de opbrengsten ervan, lijkt verdere internationale samenwerking bovendien noodzakelijk om daders daadwerkelijk te kunnen oppakken. Kortom, naast het verder ontwikkelen van kennis en expertise zouden opsporingsdiensten er goed aan doen om nog verder personen met verschillende achtergronden (technisch, financieel, internationaalrechtelijk) in opsporingsteams te combineren.

4 *Technische maatregelen en voorlichting*
Technische maatregelen kunnen worden ingezet om geldstromen bloot te leggen en actoren te deanonimiseren. Als een gebruiker met meerdere Bitcoin-adressen bitcoins naar zichzelf overmaakt, kunnen de verschillende adressen van een gebruiker in potentie aan elkaar gerelateerd worden. Door het analyseren van transactiegegevens met meer geavanceerde methoden, kunnen pseudoniemen geclusterd worden tot verschillende gebruikers (Meiklejohn et al., 2013; Ron & Shamir, 2013). Vervolgens blijft het nog steeds de uitdaging om de pseudoniemen te koppelen aan hun echte identiteiten. Dit kan bijvoorbeeld door de transactiegegevens en geclusterde Bitcoin-adressen te koppelen aan andere bronnen. Wanneer bijvoorbeeld iemand op een forum zijn of haar Bitcoin-adres noemt, is een koppeling mogelijk (Meiklejohn et al., 2013; Reid & Harrigan, 2013). Ook via informatie over betalingen bij webwinkels kunnen bijvoorbeeld afleveradressen, e-mailadressen en andere informatie worden achterhaald. Meer voorzichtige criminelen zullen gebruikmaken van anonimiseringsdiensten als Tor. Biryukov et al. (2014) presenteren een methode om Bitcoin-adressen aan IP-adressen te koppelen en anonimiseringsmethoden te omzeilen. Ook daartegen zijn weer maatregelen te bedenken, waaronder enkele tegenmaatregelen die Biryukov et al. (2014) zelf voorstellen. Een andere technische maatregel is door bij mixing services in- en uitgaande geldstromen aan elkaar te koppelen en te detecteren wanneer criminelen een specifiek bedrag (bijvoorbeeld 3248,38 Bitcoin) proberen wit te wassen. Anonimiseren en identificeren is een kat-en-muisspel tussen criminelen en opsporingsdiensten, maar het gebruik van digitale betalingsmiddelen laat altijd digitale sporen achter en is dus niet geheel anoniem.

Technische maatregelen kunnen ook worden ingezet voor detectie van ongebruikelijke en/of verdachte transacties. Zoals al eerder is opgemerkt, zijn de monitoringmaatregelen van banken om frauduleuze transacties uit banking malware tegen te gaan succesvol gebleken, en uit dit onderzoek is naar voren gekomen dat veel van de andere actoren bereid zijn tot zulk soort monitoringmaatregelen. Daarnaast kunnen technische maatregelen bijdragen aan het tegengaan van het gronddelict (in casu banking malware en ransom-

ware), waardoor er geen opbrengsten zijn om wit te wassen. Onder meer door middel van detectie in het netwerkverkeer van bedrijven en instellingen kan wellicht een belangrijke bron van besmetting, namelijk de phishing e-mails, worden tegengegaan. Phishing is namelijk een belangrijke bron van waaruit computergebruikers kunnen worden besmet met malware, waaronder ransomware. Het is van belang dat mensen zich bewust zijn van deze aanvalsbron en meer alert zijn bij het openen van e-mails. De overheid zou kunnen overwegen een voorlichtingscampagne over phishing én cryptoware te starten om meer bewustzijn over de problematiek te creëren en handvatten voor de slachtoffers te geven. Bedrijven en instellingen kunnen, zoals het Nationaal Cyber Security Centrum recentelijk in zijn Cyber Security Beeld Nederland ook heeft aangegeven, meer maatregelen nemen om phishingmails uit het e-mailverkeer te filteren.

Het valt buiten de reikwijdte van dit onderzoek om alle technische maatregelen te beschrijven die bedrijven en overheidsinstellingen zouden moeten nemen om cryptoware tegen te gaan. Echter, het hebben van een crisis- en incidentenplan, het monitoren van netwerkverkeer (inclusief phishing e-mails), het maken van back-ups en voorlichting aan werknemers over ransomware lijken op het eerste gezicht aan de basis te liggen van een goede 'cyberhygiëne'. De overheid kan ook burgers verder voorlichten over cyberhygiëne.

6.3 Discussie en verder onderzoek

Dit onderzoek heeft een verkennend karakter: hoewel er veel onderzoek beschikbaar is over witwassen, is dit een van de eerste onderzoeken naar het witwassen van geld verkregen uit banking malware en ransomware. Verschillende nieuwe modi operandi zijn blootgelegd en de kenmerken van money mules zijn uitgebreid beschreven. Echter, door een gebrek aan onderzoeksgegevens is het niet mogelijk gebleken voor de andere actoren, de betalingsdiensten die worden gebruikt door criminelen om geld verkregen uit cybercrime wit te wassen (WebMoney, Paypal, Ukash/Paysafecard, Neteller, Skrill, PerfectMoney, Western Union en banken), verder te komen dan een beknopt overzicht van kenmerken. Zodra er onderzoeksgegevens beschikbaar komen, bijvoorbeeld wanneer meer opsporingsonderzoeken zijn afgerond op het gebied van ransomware, kan een diepgaander vervolgonderzoek worden gestart naar de kenmerken van deze actoren. Mogelijk komen daaruit ook kenmerken naar voren waarop risicoprofielen kunnen worden gebouwd die bruikbaar zijn voor opsporingsinstanties en toezichthouders.

Middels een analyse van datasets van de grote Nederlandse banken zijn de kenmerken van money mules onderzocht. Vooraf was het al bekend dat de

banken uitgebreide maatregelen treffen om frauduleuze transacties te detecteren, en dankzij bestaande connecties met het ECTF was het dan ook mogelijk om deze dataset samen te stellen. Hierdoor is in dit onderzoek de focus op deze dataset, en dus de money mules, komen te liggen. Echter, tijdens het onderzoek is ook duidelijk geworden dat andere actoren die betrokken zijn bij het witwasproces in meer of mindere mate monitoren op frauduleuze transacties. Een onderzoek van deze gegevensets (bijvoorbeeld de Bitcoin exchanges) zou inzichten in andere criminele actoren kunnen geven. Daarnaast was het voor dit doel niet zinvol de money mules zelf te interviewen. Echter, het interviewen van money mules kan wel zinvol blijken wanneer de focus ligt op ronselaars. Via money mules zou kunnen worden achterhaald hoe ze geronseld zijn en door wie. Vervolgens zouden ronselaars gevonden en bevraagd kunnen worden. Via hen is wellicht ook te achterhalen welke opdrachtgevers zij op hun beurt hebben. Een gericht onderzoek naar de ronselaars van money mules voor de cash-out bij banking malware en andere vormen van cybercrime zou om die reden van toegevoegde waarde kunnen zijn.

Omdat de ontwikkelingen volop in beweging zijn, zijn de resultaten van dit onderzoek, zeker met betrekking tot banking malware, beperkt houdbaar: banking malware lijkt alweer op zijn retour. Ransomware, in het bijzonder cryptoware, lijkt daarentegen enorm toe te nemen. Ook de schade uit phishing overstijgt de schade uit banking malware. Phishing vormt vaak ook de eerste stap om ander cyberdelicten te plegen. Het ligt daarom voor de hand meer onderzoek te doen naar phishing en de mogelijke aanpak daarvan verder te onderzoeken.

Summary

Cybercrime and money laundering
Bitcoins, payment service providers and other methods of laundering banking malware and ransomware profits

Background, research question and scope

Compared to money laundering in traditional offenses, like drug trafficking, relatively little is known about money laundering in cybercrime. The major difference is that, contrary to traditional offenses, in which criminals usually acquire money in cash, cybercrime profits increasingly appears to be made via new payment methods. With the growth of cybercrime in recent years, there is an urgency to gain insight into the money laundering process and the actors involved. This study focusses on the money laundering process and maps the actors involved in banking malware and ransomware. Banking malware, in short, is malicious software that is intended to steal money through online banking payments. Ransomware is malicious software that keeps a computer system (or all files on it) 'hostage' and demands a ransom payment to unlock the system. In recent years, a new form of ransomware has emerged. This so-called cryptoware encrypts files on a computer and demands a ransom payment, often by paying with the virtual currency Bitcoin to decrypt the files.

The key question of this research report is: *in what way and through which actors are profits of banking malware and ransomware laundered?* To answer this question, six sub-questions were formulated:

1 What is money laundering of banking malware and ransomware profits, and how can this kind of laundering be qualified in criminal law?
2 What are new payment methods, especially virtual currencies such as Bitcoin, and how do they work?
3 How and with the help of which actors is money laundered that is obtained
   a through banking malware?
   b through ransomware?
4 What are the characteristics of actors involved in the money laundering process?
5 Which information about the modus operandi of actors involved in the money laundering of banking malware and ransomware profits is available on the dark web?
6 What role do new payment methods, especially virtual currencies such as Bitcoin, have in the money laundering process of banking malware and ransomware?

Methodology

The research questions have been answered through use of the following methods: (1) desk research, (2) interviews, (3) police files analysis, (4) an 'experiment' with bitcoins and mixing services, and (5) a quantitative analysis of transaction data from Dutch banks, related to banking malware and phishing. The desk research has been conducted on the basis of an analysis of scientific literature, professional literature, and news articles with regard to money laundering, cybercrime and new payment methods. Semi-structured interviews were held with twenty experts in various relevant disciplines. The desk research and the interviews provided knowledge about the use of new payment methods and the digital laundering of cybercrime profits. In addition, four cases from the Dutch National High Tech Crime Unit were analysed with regard to cybercrime and money laundering. By means of an empirical test, in which bitcoins were purchased and submitted to a mixing service for processing, insight was gained into the world of online money laundering services. Finally, a quantitative analysis was conducted on transaction data from all large banks in the Netherlands. This data provided information on the characteristics of money mules involved in the money laundering process of banking malware.

Results and conclusions

Typically the profits of banking malware and ransomware are digital. In case of banking malware, criminals acquire electronic money and in case of ransomware the ransom is often paid with vouchers or (in case of cryptoware increasingly) with bitcoins. Laundering of the profits consists of concealing the criminal origin of the money. The legal typologies developed to prove deliberate money laundering, relate mainly to cash in drug offenses. Consequently, there is a lack of clarity as to when processing or possessing large sums of digital money can be seen as money laundering.

Many types of new payment methods can be used to launder cybercrime profits. A distinction can be made between electronic money and virtual money. Electronic money is the digital representation of real money (fiat money), i.e. national currencies, while virtual money is not endorsed by any government. Virtual money can be either centralised or decentralised, and may or may not be convertible to real money. Convertible, centralised virtual currencies includes credit on websites. Non-convertible centralised virtual currencies include money in online games and virtual worlds. Convertible, decentralised virtual currencies include cryptocurrencies. Bitcoin is by far the best-known cryptocurrency, with 90% of the total market value of all cryptocurrencies.

In this study various models of money laundering are identified and described. The research results show that banking malware and ransomware profits are laundered in several different ways.

Money mules are often, but not always, involved in the laundering of banking malware profits. The electronic money is transferred from the account of the online banking account of the victim to an online banking account of a money mule. Subsequently, the money mule performs a so-called cash-out of the money as soon as possible at an ATM. This method of money laundering can partly be explained by the preference of criminals to have cash. However, from the police file analysis and quantitative analysis it also became clear that goods, services or bitcoins are purchased directly via the account of victims of banking malware, using their financial data. Criminals typically use multiple online services in this process.

The ransom that is demanded after infection with ransomware is usually in the form of online vouchers or bitcoins. Vouchers are generally credited to an online account with an e-wallet service, after which the money can be laundered digitally. It is also possible to sell the vouchers or directly pay for an online service. Criminals tend to use a combination of money laundering methods. The origin of bitcoins can be disguised using a mixing service. Mixing services allow bitcoins to be swapped for other bitcoins in exchange for a fee. The bitcoins can then be used for purchases or converted to other currencies via Bitcoin Exchanges. Finally, there are also illegal online service providers who are prepared to exchange digital and virtual payment systems for a fee.

In these models, the following actors can be identified as part of the money laundering process: (1) banks, (2) money mules, (3) money transfer offices, (4) Payment Service Providers (5) e-commerce, (6) voucher services, (7) e-wallet services, (8) Bitcoin exchanges, (9) mixing services, and (10) bitcoin dealers. The characteristics of these actors are described in this report to identify which parties are likely to appear in police investigations. By using the transaction data with regard to phishing and banking malware, it has been possible to map the characteristics of money mules in the Netherlands. The picture that emerges from the analysis of the data sets, shows that money mules are mostly young adults between 18 and 22 years from relatively poor neighbourhoods who allow criminals to use their debit cards. While these young adults in the relatively poor areas of the three major Dutch cities (Amsterdam, Rotterdam and The Hague) are overrepresented, money mules come from all municipalities in the Netherlands. Furthermore, there is an overabundance of juveniles with an Eastern European nationality.

This study shows that criminals (still) often opt to use cash. This is probably because cash can be moved quickly and anonymously. As a result, cash remains the instrument of choice for them to enjoy the proceeds of crime, including those of cybercrime. The scale of laundering cash therefore appears much greater than money laundering using new payment methods – which is the focus of this study. Whether that will change in the future, strongly depends on the developments of new payment methods and measures taken by companies and institutions to address money laundering. Police agencies and the Public Prosecution Service should maintain and further develop their expertise to combat money laundering via new payment methods.

Based on this research, it is recommended to consider regulating the Dutch Bitcoin exchanges. Dutch Bitcoin exchanges have already voluntarily taken an extensive range of measures to combat money laundering. However, with regulation they would, for example, also be able to report to the FIU, the financial intelligence unit, which can contribute to the detection of money laundering with virtual currencies. The enforcement of anti-money laundering regulations will remain a challenge, given that online payment services can offer their services worldwide and thereby may be located in jurisdictions with less strict regulations or a lack of supervision and enforcement. Moreover, there are also other online payment services that allow digital and virtual payment methods to convert, which settle in jurisdictions with more lenient regulation or poor supervision. It remains necessary that payment service providers take technical measures to detect and block suspicious transactions. Other parties, including citizens, should adopt technical measures to address malicious software, such as monitoring network traffic (including phishing emails). Citizens and organizations would thereby have to maintain a good cyber strategy and make regular backups of systems. It is also important to raise awareness among computer users about cybercrime, in particular ransomware, by providing more information.

Literatuur

Akse, Th. (2003). *En de kleur is vuil*. Zoetermeer: KLPD.

Angel, J.J., & McCabe, D. (2014). The ethics of payments: Paper, plastic, or bitcoin? *Journal of Business Ethics*, (3), 603-611.

Atzoria, L. Ierab, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks: The International Journal of Computer and Telecommunications Networking,* (54), 2787-2805.

Bal, A. (2013). Stateless virtual money in the tax system. *European Taxation, 7*(53).

Bauer, J., Eeten, M. van, Chattopadhyay, T., & Wu, B. (2008). *ITU study on the financial aspects of network security: Malware and spam*. Genève: ITU.

Baukema, J. (2013). Bitcoin: Een (ongereguleerd) betaalmiddel van de toekomst? *Tijdschrift voor financieel recht,* (12), 411-418.

Berger, A.N., Molyneux, Ph., & Wilson, J.O.S. (2015). *The Oxford handbook of banking*. Oxford: Oxford University Press.

Bernaards, F., Monsma, E., & Zinn, p. (2012). *High tech crime: Criminaliteitsbeeldanalyse*, Rotterdam: The Media Centre.

Bevington, P.R., & Robinson, D.K. (2003). *Data reduction and error analysis*. Boston: McGraw-Hill.

Binsalleeh et al. (2010). On the analysis of the ZeuS Botnet Crimeware. In *2010 Eighth Annual International Conference on Privacy, Security and Trust (PST)* (pp. 31-38). Geraadpleegd april 2016 via: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5564352

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM* (pp. 15-29). New York: ACM.

Bollen, R. (2012). The legal status of online currencies: Are bitcoins the future? *Journal of Banking and Finance Law and Practice*.

Borgers, M.J., & Kooijmans, T. (2015), 'Van probleem naar oplossing en weer terug. Het conceptwetsvoorstel aanpassing witwaswetgeving', *Delikt en Delikwent, 8*(2), 57-74.

Borgers, M.J. (2013), 'Rechtsvorming door de Hoge Raad en de reikwijdte van de strafbaarstelling van witwassen', *Delikt en Delinkwent,* (5), 361-370.

Bronk, C., Monk, C., & Villasenor, J. (2012). The dark side of cyber finance. *Survival: Global Politics and Strategy, 54*(2), 129-142.

CBS (Centraal Bureau voor de Statistiek) (2012a). *Kerncijfers wijken en buurten 2009-2012*.

CBS (Centraal Bureau voor de Statistiek) (2012b). *Regionale spreiding van eerstegeneratieallochtonen en arbeidsmigranten uit Midden-, Oost- en Zuid-Europa*.

Chambers-Jones, C., & Hillman, H. (2014) *Financial crime and gambling in a virtual world: A new frontier in cybercrime*. Northhampton, MA: Edward Elger Publshing.

Charney, S. (1994). Computer crime: Law enforcement's shift from a corporeal environment to the intangible, electronic world of cyberspace. *Federal Bar News, 41*(7), 489-494.
Christopher, C.M. (2013). Whack-a-mole: Why prosecuting digital currency exchanges won't stop online laundering. *Lewis & Clark Law Review*, (18), 1-36.
Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press 2010.
Conings, C., & Oerlemans, J.J. (2013). Van een netwerkzoeking naar online doorzoeking: Grenzeloos of grensverleggend? *Computerrecht*, (1), 23-32.
CSBN 4 (2014). *Cyber Security Beeld Nederland 4*. Den Haag: Nationaal Cyber Security Centrum.
CSBN 5 (2015). *Cyber Security Beeld Nederland 5*. Den Haag: Nationaal Cyber Security Centrum.
CSBN 6 (2016). *Cyber Security Beeld Nederland 6. Den Haag: Nationaal Cyber Security Centrum*.
Custers, B.H.M. (2006). Risicoprofilering en identificatie van terreurfondsen. *Banking Review*, 28-33.
Custers, B.H.M. (2007). Risk profiling of money laundering and terrorism funding: Practical problems of current information strategies. *Proceedings of the 9th International Conference on Enterprise Information Systems*. Portugal: Funchal.
Cyber Threat Alliance (2015). *Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat*.
Davies, G. (2002). *History of money: From ancient times to the present day*. Cardiff: University of Wales Press.
ETCF (Electronic Crimes Task Force) (2013). *Projectdocument 'Money mules'*, Nationale politie en samenwerkende Nederlandse banken.
Engelfriet, A.F. (2014). Ontwikkeling en recht: Waar gaat het heen met Bitcoin? *Tijdschrift voor Internetrecht*, 5.
ECB (Europese Centrale Bank) (2012). *Virtual currency schemes*. Frankfurt: Frankfurt am Main.
ECB (Europese Centrale Bank) (2015). *Virtual currency schemes – a further analysis*. Frankfurt: Frankfurt am Main.
Europol (2014). *The Internet Organised Crime Threat Assessment (iOCTA)* 2014. Den Haag: Europol Police Office.
Europol (2015a). *Why is cash still king?* Den Haag: Europol Police Office.
Europol (2015b). *The internet organised crime threat assessment (iOCTA)*. Den Haag: Europol Police Office.
Europol (2015c). *The future of organised crime report 2015*. Den Haag: Europol Police Office.
Europol (2016). *An analysis of payment mechanisms used within cybercrime in the EU*. Den Haag: Europol Police Office.

Falliere, N., & Chien, C. (2009). *Zeus: King of the bots*. Symantec Security Response.

FBI (2012). *Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity*, 24 april 2012, Directorate of Intelligence, Cyber Intelligence Section and Criminal Intelligence Section.

Gelemerova, L. (2011). *The anti-money laundering system in the context of globalisation: A panopticon built on quicksand?* Nijmegen: Wolf Legal Publishers.

Graaf, D. de, Shosha, A.F., & Gladyshev, P. (2012). *EDOLAB: Shopping in the Cybercrime Underworld*. Research Paper.

Gruber, S. (2013). Trust, identity and disclosure: Are bitcoin exchanges the next virtual havens for money laundering and tax evasion? *Quinnipiac Law Review*, 32, 135-196.

Hogben, G., Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, measurement, disinfection & defence. *European Union Agency for Network and Information Security*.

Hulst, R.C., & Neve, R.J.M. van der (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 264.

Intel Security (2015). *McAfee Labs Threats Report May 2015*.

Kaspersen, H.W.K. (2007). Het Cybercrime-verdrag van de Raad van Europa. In E.J. Koops (red.), *Strafrecht & ICT: Monografieën Recht en Informatietechnologie*. Den Haag: Sdu Uitgevers.

Kleemans, E.R., Brienen, M.E.I., Bunt, H.G. van de, Kouwenberg, R.F., Paulides, G., & Barensen (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 198.

Knoop, J. van der (2015). *De bestrijding van witwassen, beschrijving en effectiviteit 2010-2013*. Groningen: Rollingswier.

Koningsveld, T.J. van (2008). Witwassen: de fasen van het witwasproces getoetst. *Tijdschrift voor Onderneming en Financiering*, 4, 88-104.

Koops, E.J. (2014). Cybercriminaliteit. *Recht en Praktijk: Informatie- en Communicatietechnologie*, 4.

Koops, E.J. (red.) (2007). *Strafrecht & ICT, Monografieën Recht en Informatietechnologie*. Den Haag: Sdu Uitgevers.

Kruisbergen, E.W., & Soudijn, M.R.J. (2015). Wat is witwassen eigenlijk? Introductie tot theorie en praktijk. *Justitiële verkenningen, 1*, 10-23.

Kruisbergen, E.W., Bunt, H.G. van de, & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma uitgevers. Onderzoek en beleid 306.

Lederman, L. (2007). Stranger than fiction: Taxing virtual worlds. *New York University Law Review, 82*, 1620-1672.

Leeuwen, D.J. van (2011). Witwassen naar Nederlands recht: Over voorhanden hebben en het bewijs van witwassen. *Delikt en Delikwent, 41*(3), 297-326.
Marian, O.Y. (2013). Are cryptocurrencies 'super' tax havens? *Michigan Law Review First Impressions, 38*, 38-48.
Maurtiz H. (2014). *De aard en omvang van Money Muling: Fraude met internetbankieren en witwassen*. Scriptie, uitgevoerd voor de Nationale Politie.
Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G., & Savage, S. (2013). A fistful of bitcoins: Characterising payments among men with no names. *Proceedings of the 2013 conference on Internet measurement conference, ACM*, 127-140.
Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. *Proceedings of the 2013 e Crime Researches Summit,* 1-14.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*.
Odinot, G., Verhoeven, M.A., Pool, R.L.D. & Poot, C.J. de (2017). *Cybercrime, Organised Crime and Organised Cybercrime in the Netherlands. Empirical Findings and Implications for Law Enforcement*. Den Haag: WODC (in voorbereiding).
Parker, D.B. (1976). *Crime by computer*. New York: Scribner.
Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. S*ecurity and privacy in social networks*, 197-223.
Richet, J.L. (2013). Laundering Money Online: A review of cybercriminals methods. *arXiv preprint arXiv:1310.2368*.
Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial cryptography and data security, 7859*, 6-24.
Rozemeijer, J.P. (2015). Witwasonderzoeken zonder aantoonbaar gronddelict: Het rechterlijk toetsingskader en efficiënt opsporen in zes stappen. *Justitiële verkenningen, 41*(1), 24-39.
Sandee, M. (2015). *Game over Zeus: Background on the Badguys and Backends*. Whitepaper for the U.S. Blackhat conference 2015.
Schermer, B.W., Marbus, R., Gerding, R., & Van Kesteren, S. (2008). *Gaming: Meer dan een spelletje. Een onderzoek naar de economische, juridische en maatschappelijke aspecten van computerspellen en online werelden in Nederland*. Leidschendam: ECP Platform voor de Samenleving.
Seto, T.P. (2009). When is a game only a game? The taxation of virtual worlds. *University of Cincinatti Law Review, 77*, 1027-1040.
Sienkiewiz, S.J. (2007). Prepaid cards: Vulnerable to money laundering? *Federal Reserve Bank of Philadelphia Payment Card Discussion Paper, 7*.
Singh, S.K. (2009). *Banking Regulation*. New Delhi: Discovery Publishing House.
Soudijn, M.R.J., & Akse, T. (2012). *Witwassen*: *Criminaliteitsbeeldanalyse 2012*. Driebergen: KLPD.

Soudijn, M.R.J., & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in organized Crime, 15*(2), 111-129.
Tajalizadehkoob, S. (2013). *Online banking fraud mitigation.* Delft: TU Delft.
Trautman, L. (2014). Virtual currencies: Bitcoin & what now after liberty reserve, silk road and Mt Gox? *Richmond Journal of Law and Technology, 20*(4), 1-108.
Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, 15(1), 69-84.
Unger, B. (2007). *The scale and impacts of money laundering.* Cheltenham: Edward Elgar.
UNODC (United Nation Of Drugs and Crime) (2014). Basic manual of the detection and investigation of the laundering of crime proceeds using virtual currencies. *United Nations Office on Drugs and Crime.*
Vandezande, N. (2014). Between Bitcoins and mobile payments: Will the European Commission's new proposal provide more legal certainty? *International Journal of Law and Information Technology, 22*, 295-310.
Verbaan, J., & Nan, J. (2014). Probleemoplossingsgericht denken bij het witwassen uit eigen misdrijf afkomstige voorwerpen. *Proces, 4*, 272-288.
Verrest, p. A.M. (2006). De strafbaarstelling van witwassen. *Justitiële verkenningen, 6*(32) 41-53.
Voerman, J.A., & Baukema, J. (2015). FinTech in de betaalketen: Wanneer ben ik een betaaldienstverlener? *Tijdschrift voor Financieel Recht, 10*, 367-374.
Wegberg, R.S., Oerlemans, J.J., & Deventer, M.O. van (2016). *Mixed Results? An explorative study on money laundering of cybercrime proceeds using Bitcoin* (in voorbereiding).
Weimer, W. (2000). Cyberlaundering: An international cache for microchip money. *DePaul Business Law Journal, 13*(199).

Bijlage 1 Begeleidingscommissie

Voorzitter

Dhr. prof. dr. A.R. Lodder	Vrije Universiteit Amsterdam

Leden

Mw. A.F. Jansen MSc	Team High Tech Crime, Nationale Politie
Dhr. R. Schaap MSc	Team High Tech Crime, Nationale Politie
Dhr. R.G.J. Ruiter	Betaalvereniging Nederland
Dhr. N. Ploeger MSc	Belastingdienst
Mw. mr. B. Perels	DG Politie, Ministerie van Veiligheid en Justitie

Bijlage 2 Lijst van respondenten

Geïnterviewde personen

Mirjam Visser	ABN AMRO
Frank Haksteeg	ABN AMRO
Derk Streunding	ABN AMRO
Ireen Lammerts	SNS Bank
Stan de Graauw	SNS Bank
Dennis van Bruchem	Rabobank
Maud Bökkerink	De Nederlandsche Bank
Jouke Hofman	Bitonic
Jennifer MacLeod	Europol
Cornelie Backer	Openbaar Ministerie
Yolanda van Setten	Openbaar Ministerie
Peter Staal	Openbaar Ministerie
Anoniem	Nationale Politie – THTC
Anoniem	Nationale Politie – THTC
Anoniem	Nationale Politie – THTC
Anoniem	Belastingdienst – FIOD
Anoniem	Belastingdienst – FIOD
Marco van Loosen	Fox-IT
Michael Sandee	Fox-IT
Remco Boer	Mollie

Aanvullende gesprekken

Anoniem	Nationale Politie

Bijlage 3 Lijst van (geanonimiseerde) zaken

Mega Server

Deze zaak betreft het besmetten van computers en mobiele telefoons met banking malware. De criminelen richtten zich op klanten van een grote Nederlandse bank die gebruikmaken van bankieren via hun mobiele telefoon. Mensen kregen via een mail het verzoek om op een (nagemaakte) website persoonsgegevens en het merk van hun mobiele telefoon in te vullen. Daarna werd een sms gestuurd om de gebruiker onder valse voorwendselen een app te laten installeren op de mobiel. Hiermee werd het mogelijk om sms-berichten van de bank te onderscheppen en te gebruiken voor overboekingen. Zo konden de criminelen een deel van het klaargezette bedrag overmaken naar een van hun rekeningen. De verdachten hebben het geld vervolgens op verschillende manieren witgewassen. Zo werden er verschillende vormen van elektronisch geld aangekocht, waaronder bitcoins, Ukash, WebMoney en vouchers. Ook werd er gebruikgemaakt van money mules die direct na de overboeking het geld contant opnamen. De laatste manier waarop werd witgewassen, is door de aankoop van elektronica bij verschillende webshops.

Rogue

Een zaak waarin een georganiseerde groep van negen Nederlandse verdachten samenwerkte en door middel van RAT banking malware geld kon stelen en vervolgens probeerde wit te wassen met behulp van vele money mules. Na aangifte door een aantal Nederlandse bankinstellingen is een onderzoek gestart. De malware heeft verschillende functionaliteiten ingebouwd, onder andere het wijzigen of verwijderen van getoonde informatie aan de gebruiker van internetbankieren. Als gevolg werden er gelden overgeboekt naar de criminelen zonder dat het slachtoffer hiervan wist. Het slachtoffer zag de fraude pas op het moment dat hij inlogde op internetbankieren op een ‘schone’ computer. Vervolgens is het geld witgewassen door voor duizenden euro’s aan bitcoins te kopen via de rekeningen van money mules. Uit tapgegevens blijkt dat er gebruik is gemaakt van een mixing service om de herkomst van de bitcoins te verhullen.

Professor-X

Dit onderzoek gaat over frauduleus geld afhandig maken middels banking malware. Diverse klanten van drie grote Nederlandse banken zijn slachtoffer geworden van deze vorm van criminaliteit. De banken zijn ook benadeeld, mede omdat zij de schade van hun klanten hebben vergoed. Deze strafbare

feiten zijn gepleegd met behulp van een banking malware-virus. De verdachten kochten vervolgens producten bij verschillende webshops, en betaalden via de rekeningen van money mules. Daarnaast blijkt uit het onderzoek dat de verdachten ook handelden in bitcoins, zo werd onder andere gebruikgemaakt van bitplaats.nl, Anycoin Direct en van Happycoins.eu.

Nightcrawler

Deze zaak betreft het verspreiden van ransomware in Nederland en in andere delen van Europa. Wanneer een computer besmet raakte met de ransomware, ging de computer van het slachtoffers 'op slot' en gaf deze een melding dat er bijvoorbeeld kinderpornografisch materiaal gevonden was op de betreffende computer en dat deze na het betalen van een geldsom van € 100 pas weer toegankelijk zou worden. In de melding werden logo's gebruikt van de opsporingsdiensten uit het betreffende land. Ook hielden daders zich bezig met witwassen. In Nederland worden drie verdachten vervolgd voor deze zaak. Uit internettaps blijkt dat er een veelheid aan virtuele valuta en buitenlandse betaaldiensten is gebruikt om het wederrechtelijk verdiende geld wit te wassen. Zo is regelmatig gebruikgemaakt van PayPal, Western Union, WebMoney, Bitonic en xmlgold.eu.

Tabel B3.1 Overzicht van gebruikte betalingsmethoden

	Rogue	MegaServer	Professor-X	Nightcrawler
Bitcoins	x	x	x	x
Webmoney		x		x
PayPal			x	x
Ukash		x		
Vouchers		x		
3v credit cards		x		x
Paysafecard				x
Western Union		x	x	
MoneyGram		x	x	

Bijlage 4 Overzicht kenmerken van betalingsdiensten

Betalingssoort	Jurisdictie	Registratie	Omzetmogelijkheid	Drempel
	NL/EU/buiten EU	Ter plekke/e-mailadres en betaling/paspoort nasturen	Bitcoin/voucher, prepaid creditcard etc.	€ 1.000, € 10.000, etc. (voor zover bekend)
WebMoney	EU – Engels recht	Online registratie vraagt telefoonnummer, geboortedatum en e-mailadres. Telefoonnummer wordt geverifieerd.	Men kan verschillende wallets aanmaken: 8 soorten – zowel fiatvaluta als goud en bitcoins.	Drempels wisselen per gekozen wallet en status van account. Zie voor overzicht: http://tinyurl.com/WMdrempel
PayPal	EU – Engels recht	Online registratie vraagt naam, adres, telefoonnummer en e-mail. Verificatie met e-mailadres en sms. Account moet gekoppeld worden aan creditcard of bankrekening.	– Overmaken van geld naar creditcard of bankrekening -> cash. – Directe betaling met PayPal-account bij webshops e.d.	Niet bekend
Ukash/ Paysafecard	NL-regelgeving, 'met uitzondering van prudentiële regels die zich richten op het principe van het herkomstland, namelijk de Engelse regelgeving'	Online registratie vraagt naam, geboortedatum, adres, telefoonnummer en e-mailadres. Telefoonnummer en e-mailadres worden tijdens registratie geverifieerd.	– Paysafecard-vouchers kunnen worden gebruikt om diensten te betalen, o.a. Skype, Deezer, Spotify, en de PlayStation Store. – Paysafecard biedt ook prepaid Mastercard aan in aantal landen.	Vouchers hebben waarde van 10, 25, 50, of 100 in GBP, EUR, of USD.
Neteller	EU – Engels recht	Online registratie vraagt naam, geboortedatum, adres, telefoonnummer en e-mailadres.	– Mogelijk om direct uit wallet te betalen bij duizenden websites. – Geld kan worden overgemaakt naar bankrekening en opgenomen bij bankautomaat/cheque in de post. – Biedt virtuele en plastic prepaid Mastercard aan.	Met de prepaid Mastercard: 2 opnames per dag van max. 500 GBP. Daarnaast: per dag max. 10 aankopen van max. 1500 GBP.
Skrill	EU – Engels recht	Personal of Business account mogelijk. Vraagt naar naam, geboortedatum, adres, telefoonnummer en e-mailadres.	– Keuze uit 40 verschillende valuta. – Prepaid MasterCard voor betalen en opnemen bij bankautomaten.	Niet bekend
Perfect Money	Niet bekend	Perfect Money stimuleert klanten om hun account te verifiëren met ID-bewijs en telefoonnummer.	– Meerdere wallets mogelijk op 1 account: keuze uit USD, EUR, Gold en Bitcoins. – Prepaid creditcard kan worden aangevraagd.	Prepaid creditcard voor bedragen van € 10 t/m € 1.000. Hier kan alleen geld uit USD, EUR en Gold wallets op worden gezet.

Betalingssoort	Jurisdictie	Registratie	Omzetmogelijkheid	Drempel
Western Union	EU – Oostenrijks recht	Online registratie vraagt naam, geboortedatum, adres, telefoonnummer en e-mailadres. GEEN verificatie van deze gegevens. Om geverifieerd account te krijgen moet kopie van ID worden nagestuurd.	– Prepaid creditcards en giftcards (alleen in VS), prepaid telefoonkaarten, en travellercheques. – Mogelijkheid om geld om te wisselen in 80 verschillende valuta.	Ongeverifieerde online accounts: drempel $ 1000 per dag, limiet van $ 500 per transactie en niet meer dan 2 transacties per dag. Geverifieerde accounts: drempel $ 5000 per 3 dagen.
Banken	NL	Ter plekke	Cash	-

Bijlage 5 Overige resultaten kwantitatief onderzoek

In paragraaf 5.2 zijn de kenmerken van de money mule gepresenteerd zoals die zijn verkregen uit de gegevensset die de vier grootste banken van Nederland ter beschikking hebben gesteld. Deze bijlage geeft verdere achtergrondinformatie over het tot stand komen van deze resultaten en presenteert daarnaast enkele nieuwe resultaten die, hoewel gerelateerd, niet direct betrekking hebben op de onderzoeksvragen zoals deze zijn gepresenteerd in paragraaf 1.2.

De gegevens

Binnen het ETCF-samenwerkingsverband hebben de ABN-AMRO, ING, Rabobank en SNS bank alle phishing en malware transacties over de periode 2012 t/m 2015 ter beschikking gesteld, hetgeen een uitbreiding betreft van drie jaar ten opzichte van Mauritz (2014). Deze vier gegevenssets bestaan voor elke bank uit zowel de frauduleuze transacties die door de slachtoffers zijn gerapporteerd als de transacties die de software van de bank om fraude te voorkomen heeft gedetecteerd als phishing of malware transacties.[268] Elke gegevensset bestaat uit een verzameling van gebeurtenissen en elke gebeurtenis kan één of meerdere verschillende transacties bevatten.

Om dit verder toe te lichten wordt een fictief voorbeeld gebruikt van een gebeurtenis waar via malware wordt geprobeerd om een rekening te beroven waar € 2.652,12 op staat. Tijdens deze gebeurtenis wordt tweemaal € 1.000 overgemaakt naar de bankrekeningen van twee verschillende money mules, en de overige € 652,12 wordt op de rekening van een derde money mule gestort. De fraudedetectiesoftware van de bank vindt de twee transacties van € 1.000,00 verdacht en blokkeert deze, maar de transactie van € 652,12 wordt niet door de detectiesoftware opgemerkt. In totaal bestaat deze gebeurtenis dus uit drie transacties waarvan er twee zijn gedetecteerd en de derde is gerapporteerd door het slachtoffer. Voor het onderzoek van gegevens is ervoor gekozen om elke transactie (ongeacht of deze succesvol was of niet) te gebruiken als basiseenheid voor de analyse.

Elke transactie heeft een set met attributen, tabel B5.1 geeft een overzicht van de belangrijkste. Hierbij moet worden opgemerkt dat de banken niet altijd alle gevraagde attributen konden leveren en dat daarom niet alle attributen altijd bekend waren voor alle transacties. Bijvoorbeeld, indien een transactie naar het buitenland plaatsvond, ontbreken (nagenoeg altijd) alle overige

268 Het kan worden niet uitgesloten dat de gegevenssets ook frauduleuze transacties bevatten die niet met phishing of malware van doen hebben.

attributen en voor transacties naar een zakelijke rekening ontbreken uiteraard de persoonskenmerken (buiten de naam van de onderneming).

Om een volledig beeld te krijgen van de frauduleuze transacties is besloten om de individuele datasets samen te voegen. Hierdoor moesten voor sommige attributen keuzes worden gemaakt hoe ze het best gepresenteerd konden worden. Bijvoorbeeld, voor het attribuut 'plaats begunstigde' komt het voor sommige steden voor dat er meerdere namen/schrijfwijzen bestaan, denk hierbij bijvoorbeeld aan Den Haag/'s-Gravenhage maar ook Zwijndrecht/Zwyndrecht of Capelle aan den IJssel/Capelle ad IJssel. Uiteindelijk is besloten om het bestand 'Kerncijfers wijken en buurten 2009-2012,[269] een gegevensset die tijdens de analyse ook een belangrijke rol heeft gespeeld, te koppelen via de postcode en als 'plaats begunstigde' de respectievelijke gemeente te nemen. De resulterende gegevensset bestaat uit een totaal van 18.557 gebeurtenissen die uit 23.320 transacties bestaan die betrekking hadden op banking malware of phishing.

Tabel B5.1 Overzicht van de belangrijkste attributen die zijn gebruikt voor dit onderzoek van de gegevenssets van de grootbanken over malware- en phishing-activiteiten

Attribuut
Gebeurtenis*
Gestolen bedrag (€ 0 bij blokkade)*
Indicatie of rekeningnummer van *slachtoffer* zakelijk of particulier is**
Rekeningnummer begunstigde*
Indicatie of rekeningnummer van *begunstigde* zakelijk of particulier is**
Land van rekeningnummer begunstigde***
Naam begunstigde**
Geboortedatum begunstigde***
Plaats begunstigde***
Postcode begunstigde***
Geslacht begunstigde***
Nationaliteit begunstigde**
Bank*

* Deze attributen zijn altijd in alle gegevenssets aanwezig.

** Deze attributen ontbreken volledig in de gegevenssets van één of meerdere banken.

*** Deze attributen zijn in alle gegevenssets aanwezig, maar niet altijd gevuld.

Voor het bepalen van de kenmerken van de money mules die zijn gepresenteerd in paragraaf 5.2 is gekozen om alleen de particuliere rekeningen mee te nemen. Hoewel dit betekent dat bedrijven die een bankrekening beschikbaar stelden aan criminelen zijn uitgesloten van de analyses, levert dit geen problemen op voor de interpretatie. Dit komt voornamelijk omdat buiten de naam van het bedrijf verdere kenmerken ontbreken waardoor ze geen ver-

269 Centraal Bureau voor de Statistiek, te verkrijgen via http://statline.cbs.nl (laatst geraadpleegd in februari 2016).

dere rol konden spelen in de analyses. Daarnaast ontbreekt voor de meerderheid van de transacties naar het buitenland informatie over de rekeninghouder en is besloten om alle transacties naar het buitenland ook uit te sluiten voor verdere analyse. Tot slot is er nog een kleine fractie van transacties, zelfs binnen Nederland, waarvoor geen verdere informatie beschikbaar was buiten een bankrekeningnummer en het gestolen bedrag. Ook deze transacties zijn niet verder meegenomen in de verdere analyses. Dit betekent dat in totaal de gegevensset voor deze paragraaf bestaat uit 11.654 transacties (50% van de totale gegevensset) en dat de resultaten in paragraaf 5.2 alleen betrekking hebben op money mules in Nederland.

Kenmerken van de geldstromen

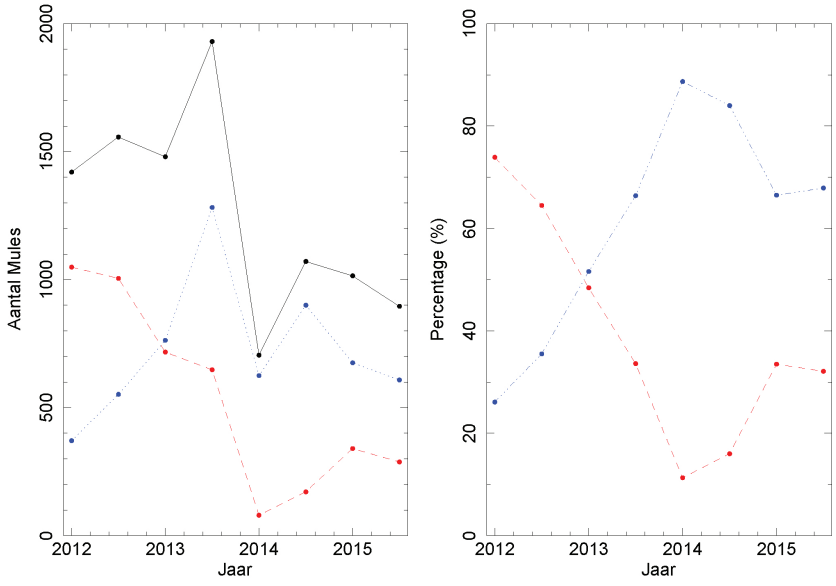
In paragraaf 4.1 zijn de twee modus operandi besproken voor het witwassen van het geld verkregen uit malware. In het eerste model wordt het frauduleus verkregen geld in de eerste fase witgewassen via money mules. In het tweede model komt naar voren dat criminelen voor het witwassen van de frauduleus verkregen gelden ook gebruikmaken van online betalingsdienstverleners (zoals iDeal) die op hun beurt betalingen naar webwinkels, Bitcoin exchangediensten en voucherdiensten faciliteren. Tevens worden soms vanuit de geïnfecteerde computer van het slachtoffer direct aankopen voor luxegoederen gedaan.

De rest van deze paragraaf laat zien dat het hierboven beschreven beeld ook wordt bevestigd door de gegevensset van de banken. Echter, deze gegevensset bevat naast de malware- ook de phishingtransacties, het is niet mogelijk om beide vormen te onderscheiden. Hoewel phishing geen deel uitmaakt van de onderzoeksvragen zoals deze zijn geformuleerd in paragraaf 1.2, is het verwant aan malware. Hierom is besloten om de onderstaande resultaten als bijlage op te nemen in het rapport.

Figuur B5.1

Aantal transacties ten gevolge van malware of phishing (vaste lijn) uitgesplitst naar geblokkeerde (gestippelde lijn) en geslaagde transacties (gestreepte lijn)

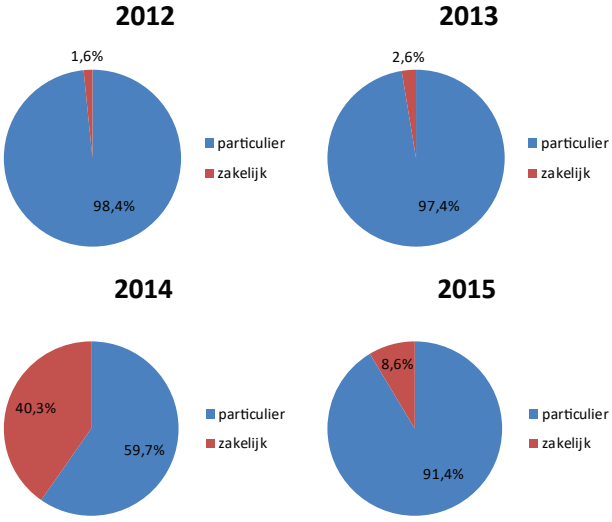
Percentage van transacties ten gevolge van malware of phishing dat is geblokkeerd (gestippelde lijn) of geslaagd (gestreepte lijn)



Tabel B5.1[270] heeft al laten zien dat er sinds 2012, de periode die samenvalt met de gegevensset, een sterke afname is in het totale bedrag dat door fraude met internetbankieren is verkregen. Volgens respondenten komt deze afname voornamelijk door een verbetering in het detecteren en blokkeren van malware transacties door de banken (zie paragraaf 2.2). Figuur B5.1 toont hoe het aantal transacties zich heeft ontwikkeld in deze periode. In het linkerpaneel wordt zowel het totale aantal (vaste lijn) als uitgesplitst naar geblokkeerde (gestippelde lijn) en geslaagde transacties (gestreepte lijn) over de tijd getoond. Duidelijk is dat het aantal transacties piekt in de tweede helft van 2013, waarna een daling wordt waargenomen. Het rechterpaneel van figuur B5.1 toont het percentage van geslaagde en geblokkeerde transacties over tijd. Hier is een sterke stijging te zien in het percentage gedetecteerde frauduleuze transacties in de periode 2012-2014. Vanaf de tweede helft van 2014 de verslechtert de detectie, maar wordt bijna 70% van de frauduleuze transacties nog steeds geblokkeerd.

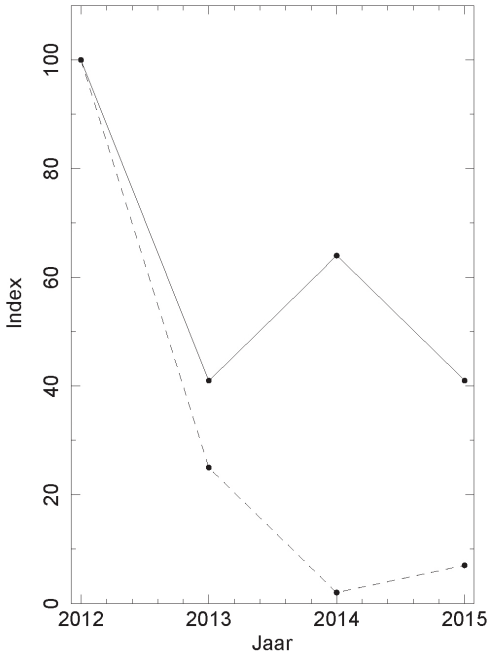
270 Zie bijvoorbeeld www.betaalvereniging.nl/nieuws/daling-fraude-met-internetbankieren-zet-door voor een overzicht van de economische schadecijfers door internetbankieren (geraadpleegd april 2016).

Figuur B5.2 Uitsplitsing van de transacties per jaar naar type bankrekening (zakelijk of particulier) van het slachtoffer



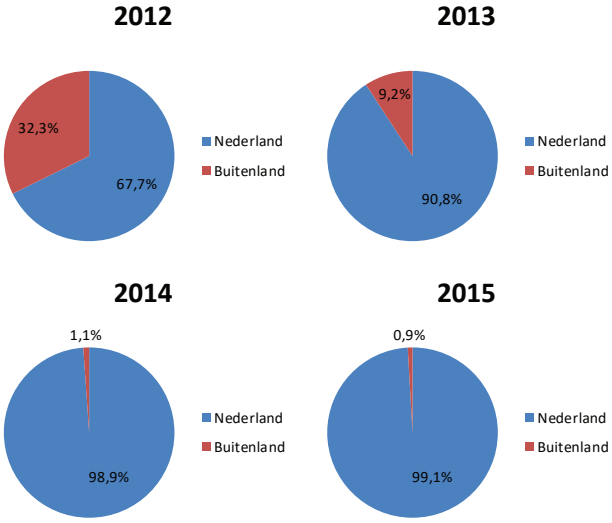
Naast de daling merkten respondenten in paragraaf 2.2 ook op dat er een verschuiving plaatsvindt van fraude met particuliere rekeningen naar die van het midden- en kleinbedrijf (MKB). In figuur B5.2 wordt deze bewering gestaafd, door per jaar de transacties uit te splitsen naar type bankrekening van het slachtoffer. Niet alle gegevenssets van de banken lieten toe om de uitsplitsing naar particuliere of zakelijke rekening te maken en daarom is ervoor gekozen om alleen percentages te tonen om herleiding naar individuele banken te voorkomen. In 2014 lijkt er een sterke toename te zijn in het aantal zakelijke rekeningen dat slachtoffer is geworden van financiële fraude, maar zoals figuur B5.3 toont, is dit relatief. Hier wordt de relatieve afname getoond van zowel de fraude met zakelijke (vaste lijn) als met particuliere (gestreepte lijn) rekeningen over de tijd. Het wordt duidelijk dat ook de fraude met zakelijke rekeningen is afgenomen, maar niet zo sterk als die met particuliere rekeningen. Hoewel uit de gegevensset niet kan worden bepaald waarom deze afname bij zakelijke rekeningen minder sterk is, lijkt het erop dat detectie van frauduleuze transacties bij zakelijke rekeningen lastiger is. Een reden zou kunnen zijn dat zakelijke rekeningen vaker te maken hebben met overboekingen van relatief grote hoeveelheden geld dan particuliere rekeningen, waardoor verdachte transacties minder opvallen.

Figuur B5.3 Relatieve afname van de zakelijke (vaste lijn) en particuliere rekeningen (gestreepte lijn) over tijd, waarbij 2012 is geïndexeerd op 100



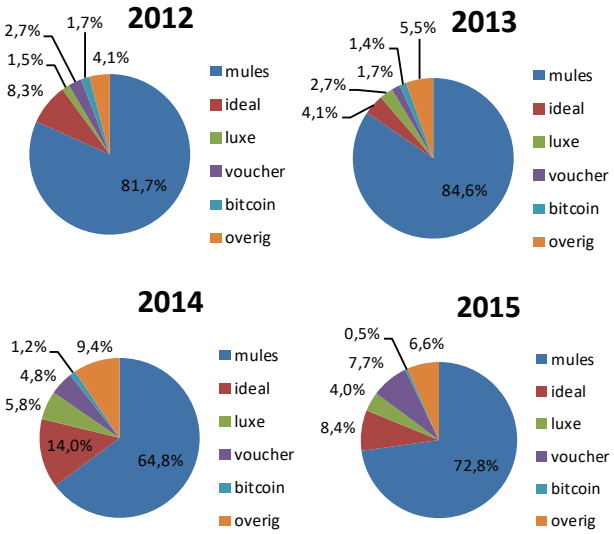
Een derde uitsplitsing die kan worden gemaakt, is naar nationale en internationale transacties. Dit wordt getoond in figuur B5.4. Ook hier is ervoor gekozen om alleen percentages te tonen, omdat niet voor alle transacties kon worden bepaald in welk land het rekeningnummer van de begunstigde zich bevond en absolute nummers hierdoor niet representatief zouden zijn. Figuur B5.4 laat zien dat procentueel het aantal transacties naar het buitenland al sinds 2012 aan het afnemen is en in 2015 minder dan 1% van het totaal uitmaakt.

Figuur B5.4 Uitsplitsing van de transacties per jaar naar binnenlandse of buitenlandse bestemming



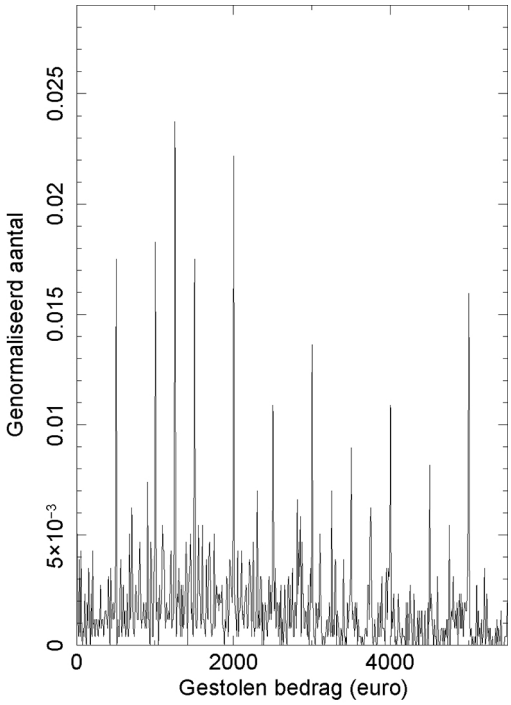
Uit de gegevensset komt naar voren dat hoofdzakelijk vijf verschillende stromen kunnen worden geïdentificeerd, namelijk het witwassen via (1) money mules, (2) webwinkels, (3) luxeproducten, (4) vouchers en (5) Bitcoins. Figuur B5.5 toont het relatieve gewicht van elke geldstroom. Dit figuur laat zien dat een grote meerderheid van de verdiensten uit banking malware en phishing nog steeds via money mules worden witgewassen. Hoewel door de jaren een daling met frauduleuze transacties via money mules is waar te nemen, is duidelijk dat money mules nog steeds een disproportioneel belangrijke plaats innemen binnen het witwasproces van banking malware en phishing.

Figuur B5.5 Overzicht van betalingsmethoden die gebruikt worden bij frauduleuze transacties uit banking malware en phishing



Figuur B5.5 is als volgt tot stand gekomen. Allereerst is het attribuut 'Indicatie of rekeningnummer van begunstigde zakelijk of particulier is' gebruikt om de uitsplitsing te maken naar witwassen via money mules (alle particuliere rekeningen) en producten (alle zakelijke rekeningen). Uit de namen die bij de zakelijke rekeningen behoren, konden de bekende Bitcoin exchanges en online betalingsdiensten (iDeal-betalingen) worden gefilterd. Er is gekozen om aankopen bij zowel de grote internet-winkels (zoals Bol.com en Coolblue) als internetwinkels van bekende bedrijven (zoals BCC en Mediamarkt) onder iDeal-betalingen te laten vallen in plaats van ze als een aparte groep te classificeren. De groep vouchers bestaat voornamelijk uit beltegoeden of cadeaukaarten die webwinkels aanbieden. Uiteraard bestaat bij de grote webwinkels ook de mogelijkheid tot aanschaf van een voucher, maar deze winkels zijn toch voornamelijk bekend voor hun producten en zijn dus onder iDeal-betalingen geschaard. Voor de luxeproducten hebben we alle bedrijven geselecteerd die de termen 'autodealer', 'juwelier', 'goud' en synoniemen daarop bevatten. De overige zakelijke rekeningen hebben we onder de groep 'overig' geschaard. Uit een visuele inspectie van de namen lijkt het dat deze groep voornamelijk uit kleine zelfstandigen bestaat.

Figuur B5.6 Verdeling van de bedragen die worden overgeboekt na een geslaagde transactie naar een money mule



Tot slot toont figuur B5.6 verdeling van het typische bedrag dat wordt overgemaakt naar een money mule in Nederland indien de transactie slaagt.

Hoewel er gemiddeld € 2.571 wordt overgemaakt, is het opvallend dat de transacties sterke pieken vertonen bij veelvouden van € 500 (namelijk € 500, € 1000, € 1500, etc.). Daarnaast is er nog één piek, de sterkste, rond € 1250, een bedrag dat precies overeenkomt met de weeklimiet van de Rabobank.[271] De overige banken hebben daglimieten van € 1000 (ING), € 500 (ABN) en € 1000 (SNS) wat overeenkomt met € 500 of een veelvoud daarvan.

271 Zie www.rabobank.nl/particulieren/service/betalen-en-opnemen/pas-en-cardlimieten-geldopname, voor de opnamelimieten van de Rabobank (laatst geraadpleegd in februari 2016).