

Artikel

Handen wassen en witwassen in tijden van Covid-19

Mr. N. (Nosh) van der Voort en mr. W.M. (Willemijn) Warnaars*

1. Inleiding

286

Waar menig individu de afgelopen periode zijn handen stuk wast door het coronavirus, zijn criminelen druk bezig met het herorganiseren van handelsstructuren om geldbedragen wit te wassen. Zo berichtte *Het Financieele Dagblad (FD)* op 12 mei jl. dat het cashtransport is belemmerd door alle grenssluitingen en ook internationale verrekeningen van bijvoorbeeld drugstransporten stokken. Om deze redenen kunnen de grote hoeveelheden zwart geld minder makkelijk verplaatst worden, waardoor het zich op bepaalde plekken zal gaan ophopen. Zo vond de politie begin mei van dit jaar in een woning in Eindhoven bijna € 13 miljoen. Een van de grootste vondsten van contant geld ooit in Nederland, aldus de politie.¹ Nu de coronacrisis grote financiële gevolgen heeft en risico's kent voor criminelen, is de vraag hoe zij nu hun illegaal verdiende geld zullen verplaatsen.²

De verwachting van het *Anti Money Laundering Centre (AMLC)* is dat witwassen met een digitale omweg via *cryptocurrency*, zoals bijvoorbeeld bitcoins, zal plaatsvin-

den.³ Geen gekke gedachte nu het 'oude vertrouwde' handelspatroon flink verstoord is geraakt. Georganiseerde misdaadgroepen hebben immers de neiging om veel energie te steken in het diversifiëren van witwasmethodes, van primitieve tot zeer complexe structuren. In veel gevallen geven criminelen er de voorkeur aan om winst te genereren in contanten, omdat het gebruik hiervan het gemakkelijkst de illegale herkomst van de winst verhult. Op deze manier voorzien criminelen (deels) in hun levensonderhoud met cash afkomstig uit illegale bron. Dat is momenteel ingewikkelder, omdat veel bedrijven geen cash aannemen of tijdelijk gesloten zijn (of waren) en daarom een significante omzetsdaling (zouden moeten) kennen. Denk aan de traditionele dekmantels in de vorm van een nagelstudio, zonnestudio, café, kapsalon of sportschool. Veel scenario's voor het doorstaan van deze 'zwar(t)e financiële crisis' van criminelen zijn denkbaar, maar een daarvan zal door het anonieme en digitale karakter voor de slimme crimineel het aantrekkelijkste zijn: het witwassen van zwart geld door middel van *cryptocurrencies*, zoals bijvoorbeeld bitcoins.

In deze bijdrage stellen wij het witwassen van bitcoins (in tijden van de pandemie) centraal. Wij gaan kort in op de werking van bitcoins (par. 2), hoe het witwassen van bitcoins in de praktijk gebeurt (par. 3 en 4), welke risico's er – op het eerste gezicht – aan het witwassen van bitcoins kleven (par. 5) en ronden af met een blik op de toekomst.

* Nosh van der Voort is advocaat bij Simmons & Simmons op de afdeling Crime, Fraud & Investigations. Willemijn Warnaars is advocaat bij Simmons & Simmons op de afdeling Crime, Fraud & Investigations.

1. 'Politie vindt € 12,5 miljoen in verborgen ruimte woning Eindhoven', NOS 6 mei 2020.

2. Het is immers een feit van algemene bekendheid dat het voorhanden hebben van zoveel contant geld in woning of auto grote risico's meebrengt en bovendien hoogst ongebruikelijk is in het geval dat geld op legale wijze is verkregen. Zie hof Leeuwarden 26 augustus 2011, ECLI:NL:GHLEE:2011:BR5801.

3. 'Het effect van Corona op de witwasbestrijding', website *Anti Money Laundering Centre* 12 mei 2020.

2. Bitcoins in een notendop

Een beschrijving van wat een bitcoin precies is en hoe de onderliggende *blockchain technologie* werkt, valt buiten het bestek van deze bijdrage.⁴ Echter, om te begrijpen hoe het witwassen van bitcoins in zijn werk gaat, beschrijven wij in deze paragraaf kort de functionaliteit van bitcoins.

Bitcoins zijn een vorm van elektronisch, virtueel geld dat inwisselbaar is en decentraal wordt beheerd. Het is de eerste implementatie van een concept genaamd *cryptocurrency*. Een van de doelstellingen van bitcoins is om betalingen mogelijk te maken zonder tussenkomst van een bank.⁵ Het gedecentraliseerde karakter van bitcoins maakt dat er daardoor, in tegenstelling tot muntenheden als de euro en de dollar, geen centrale autoriteit of financiële instelling betrokken is die bitcoins uitgeeft, en – vooral – beheert of controleert.⁶ De kracht van bitcoins ligt in het snel verzenden van geld.⁷ Bitcoins kunnen namelijk binnen enkele seconden worden verzonden naar ieder andere bitcoingebruiker ter wereld. Voor het overboeken van bitcoins is enkel het bitcoin-adres van de ontvanger nodig.⁸ Doordat de namen van verzender en ontvanger niet worden vermeld bij iedere transactie, genieten partijen meer anonimiteit dan bij een reguliere banktransactie.⁹ Deze anonimiteit maakt dat bitcoins veel worden gebruikt in het criminele circuit. Europol signaleerde al een verschuiving van het gebruik van meer traditionele betaalmethoden naar digitale betaalmethoden, zoals bitcoin. De reden hiervoor is waarschijnlijk dat criminelen ervan uitgaan dat crypto's meer anonimiteit bieden.¹⁰ Volgens Europol is bitcoin de meest gebruikte cryptovaluta door criminelen.¹¹ Een schatting is dat bitcoins betrokken zijn bij ongeveer \$ 76 miljard aan illegale activiteiten per jaar, dat is 46% van alle bitcointransacties.¹² De mogelijkheid om wereldwijd anoniem betalingen te verrichten zonder tussenkomst van een bank of andere centrale autoriteit, heeft als bewezen keerzijde dat dergelijke betalingen ook kunnen worden verricht teneinde de criminele herkomst van de

bitcoins te verhullen. Met andere woorden: om geld via bitcoins wit te wassen.

3. Witwassen in de zin van artikel 420bis Sr

In de kern is witwassen het versluieren van de band tussen een voorwerp en het misdrijf waaruit dit voorwerp afkomstig is, waarmee de schijn wordt gewekt dat dit voorwerp een legale oorsprong kent.¹³ Met andere woorden: men weet (opzetwitwassen), of had redelijkerwijs moeten weten (schuldwitwassen), dat het voorwerp afkomstig is uit enig misdrijf. Het handelen van de witwasser is er steeds op gericht zijn criminele opbrengsten te verbergen voor justitie.¹⁴ Om de integriteit van het financiële en economische verkeer te beschermen, is sinds 2001 het verrichten van zogenoemde *verhullingshandelingen*¹⁵ en *plaatsingshandelingen*¹⁶ apart strafbaar gesteld in artikel 420bis lid 1 Sr. Gewoontewitwassen (artikel 420ter Sr) en schuldwitwassen (artikel 420quater Sr) zijn hiervan afgeleide delicten. Tevens kent de wet sinds 1 januari 2017 de strafbaarstelling van eenvoudig witwassen (artikel 420bis.1 Sr) en eenvoudig schuldwitwassen (artikel 420quater.1 Sr).

Klassieke witwasconstructies

Om de door het AMLC voorspelde toevlucht van criminelen tot crypto's zoals bitcoins beter te kunnen begrijpen, zullen hieronder kort de meest voorkomende klassieke witwasmethoden worden aangestipt.¹⁷

De meest voorkomende en gemakkelijkste klassieke methode is het verplaatsen van chartaal (contant) geld

4. Zie voor een volledige uitwerking het handboek: W.M. Warnars, *Witwassen van Bitcoins. De Omgekeerde bewijslast bij het witwassen van bitcoins in het licht van de onschuldpresumptie*, Celsus Juridische uitgeverij: Weert 2018.
5. S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 2008, te raadplegen via de link: <https://bitcoin.org/bitcoin.pdf>, p. 1.
6. A.P. Engelfriet, 'Ontwikkeling en Recht: waar gaat het heen met bitcoin?', *Tijdschrift voor Internetrecht* 2014, afl. 5, p. 149.
7. S. Visser, 'Nieuwe witwastypologieën in de strijd tegen witwassen met virtuele betaalmiddelen', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, afl. 7, p. 219. Door het ontbreken van een centrale autoriteit of financiële instelling zijn ook de transactiekosten een stuk lager.
8. B.H.M. Custers, J.J. Oerlemans & R.L.D. Pool, 'Ransomware, crypto-ware en het witwassen van losgeld in bitcoins', *Strafbblad* 2016, afl. 2, p. 91.
9. Visser 2017, p. 219.
10. Europol, *the Internet Organised Crime Threat Assessment*, 2019. Zie ook Europol, *the Internet Organised Crime Threat Assessment*, 2016.
11. Europol, *the Internet Organised Crime Threat Assessment*, 2019, p. 54.
12. Sean Foley e.a., 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', *The Review of Financial Studies*, Volume 32, Issue 5, May 2019, p. 1798-1853.

13. F. Diepenmaat, *De Nederlandse strafbaarstelling van witwassen: een onderzoek naar de reikwijdte en de toepassing van artikel 420bis Sr*, Deventer: Wolters Kluwer 2016, p. 64; F. Deruyck & G.C. Haverkate, *Witwassen in Nederland en België*, Nijmegen: Wolf Legal Publishers 2008, p. 5-6.
14. *Kamerstukken II 1999/2000*, 27159, nr. 3, p. 2 (MvT).
15. Verhullingshandelingen hebben, zoals de naam het al aangeeft, betrekking op het verbergen of verhullen van de werkelijke aard, herkomst, vindplaats, vervreemding, verplaatsing, rechten of op de eigendom van voorwerpen, wetende dat deze voorwerpen van misdrijf afkomstig zijn. Deze handelingen impliceren een zekere doelgerichtheid en beslissing voor de strafbaarheid zijn de aard en het effect van het handelen. Dit wil zeggen dat het handelen van de witwasser erop gericht moet zijn om het zicht op een bepaald voorwerp, of het zicht op de zeggenschap ten aanzien van dat voorwerp, te bemoeilijken en daarbij moet het handelen eveneens geschikt zijn om dat doel te bereiken.
16. Plaatsingshandelingen omvatten het verwerven, bezitten, overdragen, omzetten en gebruikmaken van voorwerpen waarvan men weet dat deze van misdrijf afkomstig zijn. In tegenstelling tot de verhullingshandelingen volstaat bij dit type handelingen een feitelijke vaststelling ten aanzien van het bewijs. Dit houdt in dat simpelweg moet worden vastgesteld dat de verdachte de genoemde handeling heeft verricht ten aanzien van het voorwerp waarvan hij weet dat het van misdrijf afkomstig is.
17. Dit overzicht is echter niet uitputtend. Zie voor een uitgebreid overzicht het Landelijk Informatie en Expertise Centrum, 'Landelijk beeld ondermijnende criminaliteit', Den Haag 2019 en 'Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware', *Wetenschappelijk onderzoek- en Documentatiecentrum* (WODC) 2016.

met als uiteindelijke doel de criminele herkomst te verhullen voor politie en justitiële autoriteiten. Het verplaatsen van geld vindt doorgaans op twee verschillende manieren plaats: enerzijds door middel van fysieke verplaatsing (via vliegtuigen of vrachtverkeer) naar een ander land, waar het geld vervolgens wordt geïnvesteerd in onroerend goed of andere zaken, anderzijds door een girale verplaatsing door middel van bijvoorbeeld een money-transfer of door het geld om te zetten in een andere valuta (of, zoals we later zullen zien, in bitcoins) waardoor op die manier het geld wordt witgewassen.

Een tweede klassieke witwasmethode is het afgeschermd consumeren. Afgeschermd consumptie kan zowel in Nederland als in het buitenland plaatsvinden. Bij deze witwasmethode wordt vaak gebruik gemaakt van katvangers, bijvoorbeeld door aankopen te doen via de rekening van iemand anders, dan wel door een registergoed zoals een auto, op de naam van die katvanger te laten registreren.

Daarnaast maken criminelen gebruik van *loan back-constructies*. De crimineel leent hier het eigen verdiende zwarte geld aan zichzelf door gebruikt te maken van valse identiteiten en rekeningen (veelal in het buitenland) van katvangers. Op deze manier worden er schijnleningsovereenkomsten gesloten door 'onafhankelijke' partijen. In werkelijkheid is het een en dezelfde criminele organisatie waar het geld van de buitenlandse rekening en Nederlandse rekening heen en weer wordt geschoven.

288

Ten slotte is er nog het creëren van een 'gefingeerde omzet'. In deze methode wordt de omzet van een legale onderneming gemanipuleerd. Dit gebeurt door cash zwart geld op te voeren als omzet en de inkomsten van legale werkzaamheden te mengen met zwart geld. Een variant op deze omzetmanipulatie is de zogenoemde *Trade Based Money Laundering* (TBML)-methode. Het geld wordt dan daadwerkelijk in het bedrijf gehouden, waarbij het zwarte geld gebruikt wordt om legale internationale transacties te verrichten: in het ene land worden goederen gekocht en vervolgens in een ander land verkocht. Op deze manier is er een verplaatsing van het geld geweest op een voor de buitenwereld legitieme wijze, echter wordt er bij de TBML-methode veelal gebruik gemaakt van valse facturen.

In al deze bovengenoemde klassieke witwasmethodes speelt contant geld een grote rol en in elk van deze witwasprocessen maken criminelen (noodzakelijk) gebruik van contant geld. Nu de hele wereld in meerdere of mindere mate te kampen heeft gehad met een *lockdown*, is het gebruikelijke betalings- en dus witwassysteem echter ontregeld. Bedrijven met veel contante omzet, en om die reden gewild als witwasmachine, waren bijvoorbeeld gesloten en kenden een significante omzetsdaling. Criminelen zullen de winsten willen en moeten blijven witwassen voordat zij deze kunnen uitgeven. Wanneer de winst immers niet wordt witgewassen, kan de oorsprong ervan gemakkelijk worden opgespoord en leidt dat tot ophoping van grote hoeveelheden contant geld.

De Autoriteit Financiële Markten (AFM) en de Europese Bankautoriteit (EBA) waarschuwden op 1 april jl. al dat financiële ondernemingen extra alert moeten zijn op witwassen.¹⁸ Volgens de EBA bewijst het verleden dat criminelen in tijden van crisis hun criminele activiteiten regelmatig opvoeren en nieuwe technieken ontwikkelen voor onder meer witwassen: 'As most economies are facing a downturn, financial flows are likely to diminish. However, experience from past crises suggests that in many cases, illicit finance will continue to flow. (...) new techniques and channels of laundering money are likely to emerge.'¹⁹ De EBA roept om deze reden financiële ondernemingen op de geldende procedures en maatregelen in de strijd tegen witwassen en terrorismefinanciering scherp in acht te houden en effectief te handhaven. Bovendien riep de AFM ondernemingen op specifiek te letten op nieuwe vormen van witwassen en financieren van terrorisme: 'Waar nodig dienen ondernemingen hun systematische integriteitsrisicoanalyses te bezien in het licht van de recente ontwikkelingen, in het bijzonder ten aanzien van sectoren die hard geraakt worden door de neergang van de economie.'²⁰ Banken zijn dus gewaarschuwd en zullen extra kritisch moeten zijn bij transacties die zij onder ogen krijgen. De op 8 juli 2020 opgerichte Transactie Monitoring Nederland, waarbij Rabobank, ABN AMRO, ING, Triodos en de Volksbank hun krachten bundelen in de strijd tegen witwassen, zal een extra stimulans zijn in deze strijd.²¹ Door het combineren van de betaaldata in één netwerk en de daaropvolgende analyse van deze 'bulkdata' op verdachte patronen, hopen de banken criminele geldstromen beter in beeld te krijgen en criminelen die op dit moment onder de radar blijven in het zicht te krijgen.

De € 16 miljard aan crimineel geld dat jaarlijks in Nederland wordt witgewassen²² zullen criminelen toch op een manier willen circuleren. Hoe blijft een crimineel onder de radar en verplaatst deze in tijden van corona en verscherpt toezicht nog wél zijn geld? Via de handel in cryptocurrencies zoals bitcoins. Het toezicht op deze digitale valuta is immers niet optimaal, de pakkans is niet groot en wegens het virtuele karakter heeft een *lock-down* wegens de pandemie geen belemmerend effect.

18. 'EBA: financiële ondernemingen moeten extra alert zijn op witwassen', website *Autoriteit Financiële Markten* 1 april 2020.

19. 'EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic', *European Banking Authority* 31 maart 2020, raadpleegbaar via: https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20provides%20additional%20clarity%20on%20measures%20to%20mitigate%20the%20impact%20of%20COVID-19%20on%20the%20EU%20banking%20sector/Statement%20on%20actions%20to%20mitigate%20financial%20crime%20risks%20in%20the%20COVID-19%20pandemic.pdf.

20. 'EBA: financiële ondernemingen moeten extra alert zijn op witwassen', website *Autoriteit Financiële Markten* 1 april 2020.

21. 'Transactie Monitoring Nederland unieke stap in strijd tegen witwassen en terrorismefinanciering', website *Nederlandse Vereniging van Banken* 8 juli 2020.

22. 'Aard en omvang van criminele bestedingen', *WODC* 2018, p. 13.

4. Witwassen van en via bitcoins

Blijkens de jurisprudentie kan er onderscheid worden gemaakt tussen het witwassen *van* bitcoins en het witwassen van geld *via* bitcoins. Er is sprake van witwassen van bitcoins, indien bitcoins afkomstig uit enig misdrijf worden omgezet in giraal of contant geld. Het hoeft hierbij niet duidelijk te zijn door wie, wanneer en waar dit misdrijf concreet is begaan.²³ Ter illustratie kan worden gewezen op een vonnis van de rechtbank Midden-Nederland.²⁴ In deze zaak gaat het om een verdachte die in drugs handelde via het dark web. Voor de drugs werd betaald in bitcoins. De verdachte was te koppelen aan negen bankrekeningen en uit informatie van Bitonic²⁵ bleek dat er op die rekeningen voor ruim € 500.000 aan bitcoins was verzilverd tegen giraal geld. Door het verzilveren van de bitcoins had de verdachte de criminele herkomst van deze bitcoins verhuuld.

Men spreekt van witwassen van geld *via* bitcoins, indien er met enig misdrijf geld is verdiend en dit criminele geld vervolgens met behulp van bitcoins wordt omgezet naar giraal of contant geld.²⁶ Het onderscheid tussen beide vormen zal voornamelijk een rol spelen bij het opstellen van de tenlastelegging bij een vervolging door het Openbaar Ministerie. Indien sprake is van witwassen *van* bitcoins zal veelal sprake zijn van het 'voorhanden hebben' van bitcoins verkregen uit *eigen* misdrijf. De crimineel verkreeg immers de bitcoins als betaling voor zijn eigen drugshandel. Wanneer sprake is van witwassen van geld *via* bitcoins zal de omzetting van zwart geld in bitcoins aan te merken zijn als een 'omzettingshandeling'.²⁷ Hoewel het aantal uitspraken waarin deze vorm zich voordoet gering is, blijft de manier waarop kan worden witgewassen bij beide vormen nagenoeg hetzelfde. Echter vindt bij het witwassen van geld *via* bitcoins een extra handeling plaats, namelijk dat het criminele geld eerst wordt omgezet in bitcoins, waarnaar deze bitcoins vervolgens op diverse manieren, die in onderstaande paragraaf worden beschreven, kunnen worden witgewassen.²⁸

Vormen van witwassen van bitcoins

Om een duidelijker beeld te krijgen van de werkwijze van criminelen beschrijft deze paragraaf verschillende vormen van witwassen van bitcoins.

- *Het omwisselen van bitcoins via reguliere wisselkantoren en exchanges*

De eerste en meest eenvoudige manier waarop het witwassen van bitcoins plaatsvindt is door de bitcoins via een regulier wisselkantoor, zoals Bitonic, of exchange te verzilveren tegen giraal geld.²⁹ De bitcoins worden door de klant overgemaakt naar het bitcoinadres van het wisselkantoor of exchange. Tegen betaling van een commissie wordt de tegenwaarde bijgeschreven op een door de klant gekozen bankrekening. Omzetten in chartaal geld is niet mogelijk.³⁰ Hierin schuilt al meteen het grootste gevaar. Bitcoins zijn in beginsel anoniem en het gebruik ervan kan het de opsporingsinstanties bemoeilijken om criminelen te identificeren, behoudens de gevallen waarin een koppeling tussen een bitcoinadres en een bankrekening kan worden gemaakt. Bitcoins zijn namelijk gebaseerd op de zogenoemde *blockchain*-technologie, waarbij gebruik wordt gemaakt van een openbaar grootboek waarin elke transactie wordt bijgehouden en ingezien kan worden. Het gevolg is dat alle transacties uit een en dezelfde bitcoin *wallet*, aan elkaar gekoppeld kunnen worden. Om deze reden zullen criminelen het anonieme karakter trachten te behouden door gebuikt te maken van verschillende *wallets* met andere namen, waardoor de koppeling tussen verschillende transacties wordt bemoeilijkt. Door gebruik te maken van analysesoftware, waarvan Chainalysis de bekendste is, is het voor opsporingsinstanties mogelijk om bepaalde *wallets*, van een en dezelfde crimineel, toch aan elkaar te koppelen.³¹ Door het koppelen van de verschillende *wallets* naar een gebruiker, hoevnd de opsporingsinstanties alleen nog de identiteit achter de gebruikte pseudoniemen te achterhalen (hetgeen veelal mogelijk is via openbare bronnen).

Sinds de implementatie van de vijfde antiwitwasrichtlijn (AMLD5) in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) op 21 mei jl. worden wisselkantoren en aanbieders van *wallets*³² zelfs aangemerkt als financiële instellingen. Dit impliceert onder meer dat zij zich moeten registreren bij De Nederlandse Bank, die vervolgens toezicht op hen houdt, en dat deze aanbieders gehouden zijn om aan de hand van een zogenaamd Know Your Customer (KYC)-beleid verscheidene maatregelen te treffen om onder meer de

23. HR 17 december 2013, ECLI:NL:HR:2013:2001, r.o. 2.3, NJ 2014/75.

24. Rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234.

25. Bitonic is een van de bekendste bitcoin-wisselkantoren in Nederland, waar een ieder in ruil voor een klein percentage van het transactiebedrag bitcoins kan kopen en/of verkopen.

26. Zie bijvoorbeeld rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814.

27. Het 'voorhanden hebben' en het 'omzetten' zijn beide plaatsingshandelingen zoals bedoeld in art. 420bis lid 1 onder b Sr. Het verschil tussen witwassen van bitcoins en witwassen van geld *via* bitcoins speelt dus vooral een rol bij het opstellen van de tenlastelegging; voor de kwalificatie heeft het geen consequenties.

28. Het omzetten van zwart geld naar bitcoins is blijkens het recent verschenen arrest van de Hoge Raad (HR 30 juni 2020, ECLI:NL:HR:2020:1171) op zichzelf al een verhuulingshandeling, waardoor al sprake is van witwassen.

29. Om van witwassen ex art. 420bis sr te spreken dienen de bitcoins die worden verzilverd afkomstig te zijn uit enig misdrijf. Het omwisselen van 'schone' bitcoins in giraal geld is immers toegestaan.

30. 'Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware', WODC 2016, p. 87.

31. Zie o.a. rb. Rotterdam 19 december 2017, ECLI:NL:RBROT:2017:10225.

32. In de Wwft wordt voor de term *wallets* de Nederlandse vertaling 'bewaarportemonnee' gebruikt.

identiteit van de verkoper vast te stellen.³³ Zo is het aanmaken van een account verplicht en dient iedere klant zich te identificeren, door het uploaden van een kopie van een paspoort of rijbewijs.³⁴ Het spreekt voor zich dat een malafide bitcoingebruiker anoniem wenst te blijven.

• *De bitcoinhandelaar*

Het gebrek aan anonimiteit bij de verkoop van bitcoins via reguliere wisselkantoren of exchanges creëerde een markt voor tussenpersonen die de verkoop voor hun rekening nemen: de zogenoemde bitcoinhandelaren.³⁵ Dit zijn personen die bedrijfsmatig, voor eigen rekening en risico, bitcoins aan- en/of verkopen tegen contant geld.³⁶ Via advertenties op het internet (www.localbitcoins.com) of het dark web komen een verkoper van bitcoins en een bitcoinhandelaar met elkaar in contact, waarna zij elkaar doorgaans ontmoeten op openbare plaatsen. Ter plaatse worden de bitcoins overgeboekt naar de *wallet* van de bitcoinhandelaar en in ruil daarvoor ontvangt de verkoper direct de afgesproken tegenwaarde in contant geld.³⁷ De aangekochte bitcoins worden vervolgens door de bitcoinhandelaar via wisselkantoren of exchanges verzilverd tegen giraal geld. Door dit ontvangen geldbedrag in contanten op te nemen is het voor de bitcoinhandelaar mogelijk om – wederom tegen contant geld – bitcoins aan te kopen.³⁸ Op eenzelfde wijze verkoopt een bitcoinhandelaar bitcoins tegen contanten.³⁹ Een bitcoinhandelaar hanteert een commissiepercentage voor zijn diensten. Dit percentage is echter beduidend hoger dan dat van reguliere wisselkantoren, exchanges of bankinstellingen: waar dergelijke dienstverleners namelijk een percentage rekenen tussen de 0,25–0,30% van de transactiewaarde, ligt dit percentage bij een bitcoinhandelaar rond de 7 en 15%.⁴⁰

De reden om desondanks deze aanzienlijke vergoeding te betalen en gebruik te maken van de diensten van een bitcoinhandelaar ligt in de geboden anonimiteit, alsmede de criminele herkomst van de bitcoins.⁴¹ In tegenstelling tot reguliere wisselkantoren, exchanges en bankinstellingen, treft een bitcoinhandelaar geen maatregelen om de

identiteit van de verkoper vast te stellen, noch houdt hij een administratie van zijn klanten bij. Met andere woorden: hij kent zijn klanten niet. Deze (gegarandeerde) anonimiteit maakt dat een verkoper buiten het zicht blijft van opsporingsinstanties, en dat is wegens de criminele herkomst van de bitcoins juist net wat een malafide klant wil.

Het gevaar bij deze witwasvorm zit evenwel in het char-tale geld. Waar laat je immers al die grote hoeveelheden contant geld? Het is een feit van algemene bekendheid dat het fysiek vervoeren van grote bedragen in contanten een aanzienlijk veiligheidsrisico met zich meebrengt.⁴² Dit impliceert dat een crimineel bij het witwassen van bitcoins op den duur tegen dezelfde problemen aanloopt als bij het witwassen van ‘normale’ voorwerpen. Op grond van het bovenstaande kan tevens worden vastgesteld dat de bitcoinhandelaar als belangrijke schakel fungeert in het witwasproces van criminelen, waardoor hij zich eveneens schuldig maakt aan witwassen. Hij aanvaardt immers bewust de aanmerkelijke kans dat de bitcoins die hij van zijn klanten krijgt afkomstig zijn uit enig misdrijf. Door de bitcoins vervolgens om te zetten in contanten op de manier zoals hiervoor beschreven heeft hij de criminele herkomst hiervan verhuuld.⁴³

• *De bitcoinmixer*

Een derde manier waarop het witwassen van bitcoins plaatsvindt is door gebruik te maken van een zogenoemde bitcoinmixer.⁴⁴ Iedere bitcointransactie wordt automatisch opgeslagen in de blockchain, hetgeen maakt dat de herkomst van de bitcoins voor justitie traceerbaar is. Om te voorkomen dat de daadwerkelijke (criminele) herkomst van de bitcoins te achterhalen is, kan worden gebruikgemaakt van een ‘bitcoinmixer’.⁴⁵ Tegen betaling van een commissie boeken talloze deelnemers (een deel van) hun bitcoins over naar de *wallet* van de online-dienstverlening.⁴⁶ De verzamelde bitcoins worden vervolgens ‘gemixt’ en in delen verdeeld over de *bitcoinwallets* van de deelnemers. De bitcoinmixer is daarbij zo ingericht dat een deelnemer nooit zijn eigen bitcoins terugkrijgt.⁴⁷ De teruggegeven bitcoins zijn veelal vermengd met de bitcoins van andere deelnemers,

33. Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (AMLD5). Per 21 mei 2020 is deze vijfde antiwitwasrichtlijn geïmplementeerd in de Wwft.

34. Vóór de implementatie van de AMLD5 werd door het merendeel van de Nederlandse wisselkantoren al een KYC-beleid gevoerd.

35. Visser 2017, p. 219.

36. ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, *Anti Money Laundering Centre* augustus 2017, De Bilt, p. 9, te raadplegen via de link: www.amlc.nl/wp-content/uploads/2018/05/notitie-de-bitcoinhandelaar-amlc-2017v2.pdf.

37. Visser 2017, p. 220.

38. ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, *Anti Money Laundering Centre* augustus 2017, De Bilt, p. 13.

39. Vgl. rb. Rotterdam 30 mei 2018, ECLI:NL:RBROT:2018:4267.

40. ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, *Anti Money Laundering Centre* augustus 2017, De Bilt, p. 13.

41. Visser 2017, p. 220.

42. Hof Den Bosch 25 maart 2015, ECLI:NL:GHSHE:2015:1181. Zie bijvoorbeeld ook rb. Rotterdam 5 april 2018, ECLI:NL:RBROT:2018:5197.

43. In augustus 2017 heeft de Nederlandse Financial Intelligence Unit (FIU-Nederland) duidelijkheid gegeven over wanneer handel in cryptocurrencies een vermoeden van witwassen oplevert. Ten aanzien van (malafide) bitcoinhandelaren zijn ook negen kenmerken opgenomen, waarvan aan twee daarvan moet zijn voldaan, wil sprake kunnen zijn van een gerechtvaardigd vermoeden van witwassen.

44. In de geraadpleegde literatuur wordt met de term ‘bitcoinmixer’ zowel verwezen naar de onlinedienstverlening als naar het programma dat wordt gebruikt voor het mixen van de bitcoins.

45. R.J. de Jong, ‘Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht’, *Tijdschrift voor Bijzonder Strafrecht & Handhaving* maart 2017, afl. 1, p. 12.

46. Visser 2017, p. 221.

47. ‘De bitcoinhandelaar, een faciliterende rol bij de cash-out van criminele verdiensten’, *Anti Money Laundering Centre* augustus 2017, De Bilt, p. 7.

maar kunnen ook door de bitcoinmixer geheel nieuw aangemaakte bitcoins zijn.⁴⁸ Het vorenstaande heeft als resultaat dat het digitale spoor van transacties in de blockchain is verbroken. Het is enkel de bitcoinmixer die nog wetenschap heeft van de daadwerkelijke herkomst van de oorspronkelijke bitcoins.⁴⁹ Een bitcoinmixer heeft om die reden geen enkel ander doel dan het verhullen van de herkomst van de bitcoins.

De vraag of het gebruik van een dergelijke mixer is aan te merken als een handeling gericht op het verhullen of verbergen van de herkomst van de bitcoins werd voor het eerst bevestigend beantwoord door de rechtbank Midden-Nederland.⁵⁰ Om de anonimiteit van de bitcoinmixer en zijn klanten te waarborgen, is deze dienstverlening alleen te bereiken via een zogeheten TOR-netwerk.⁵¹ Hoewel het aldus onmogelijk zal zijn om de daadwerkelijke herkomst te achterhalen, is het inmiddels wel mogelijk om vast te stellen of gebruikgemaakt is van een dergelijke mixer.⁵²

Het witwassen van bitcoins is een een ideaal speelveld voor de slimme crimineel, zou men denken. De werkelijkheid is echter genuanceerder. De ontwikkelingen van de aangescherpte Wwft-regelgeving en de regulering van de digitale munt, zullen criminelen – zo nemen wij aan – met argusogen bekijken.

5. (Illusoire) risico's van witwassen door middel van bitcoins

Zoals eerder aangestipt zijn Nederlandse aanbieders van *wallets* en *exchanges* sinds mei 2020 verplicht om een Wwft-beleid te voeren, in die zin dat zij een cliëntenonderzoek dienen te verrichten, risico's moeten beoordelen en onderzoek moeten uitvoeren naar ongebruikelijke transacties. Indien zij menen dat sprake is van een ongebruikelijke transactie moet deze zelfs verplicht gemeld worden bij FIU-Nederland.

Het toezicht op bitcoins lijkt zodoende te zijn gereguleerd. Het pseudo-anonieme karakter, dé reden waarom criminelen zich in 2008 massaal tot deze cryptocurrency wendden, is hiermee op het eerste gezicht ver-

dwenen; voor het doen van een (witwas)transactie is immers een (niet-gereguleerde) *wallet* nodig. Wat echter vanuit de ogen van justitie en politie problematisch is, is dat er twee verschillende soorten aanbieders van *wallets* bestaan die niet allebei onder de reikwijdte van de Wwft vallen.⁵³

Blijkens artikel 1 lid 1 Wwft wordt met een aanbieder van een bewaarportemonnee een entiteit bedoeld die diensten aanbiedt om namens haar cliënten cryptografische privésleutels⁵⁴ te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen. Onder bovenstaande definitie vallen volgens de memorie van toelichting slechts zogenaamde *custodial wallet providers*.⁵⁵ *Custodial wallet providers* zijn aanbieders die (namens de bitcoin gebruiker) de *private key* onder zich houden en op die manier een bepaalde mate van controle hebben over de bitcoins die aangehouden worden in de *wallet*: zij houden de bitcoins aan en kunnen deze opslaan en zelfs overdragen.⁵⁶

Het tweede type aanbieder is de zogenoemde *software wallet provider* (een *non-custodial wallet provider*). In tegenstelling tot *custodial wallet providers* zijn *software wallet providers* niet in staat om zelfstandig te beschikken over de *private key* en hebben zij geen toegang tot de bitcoins. Zij bieden slechts applicaties of fysieke apparaten aan voor gebruikers om toegang te krijgen tot hun bitcoins en deze op te slaan. Die applicatie geeft gebruikers enkel inzicht in de balans van hun bitcoins; de *private key* blijft in handen van de bitcoin-gebruiker zelf.

Het spreekt voor zich dat criminelen op geen enkele manier verbonden willen zijn aan wildvreemden, laat staan dat zij een 'financiële instelling' grip willen laten hebben op hun (criminele) bitcoins. Zij zullen dus naar onze mening altijd kiezen voor een *non-custodial wallet provider*, en laat dit type aanbieder nou nét niet onder reikwijdte van de Wwft te zijn gebracht.⁵⁷

48. Custers, Oerlemans & Pool 2016, p. 92.

49. De Jong 2017, p. 15.

50. Zie rb. Midden-Nederland 14 november 2017, ECLI:NL:RBMNE:2017:5713; ECLI:NL:RBMNE:2017:5716. Zie ook rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234.

51. TOR staat voor 'The Onion Router' en is een gratis software voor anonieme communicatie waar de IP-adressen van computergebruikers worden verduisterd en de netwerkcommunicatie wordt versleuteld. Zie voor meer informatie 'Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware', WODC 2016, p. 86.

52. Visser 2017, p. 222. Ook het gebruik van een bitcoinmixer is sinds augustus 2017 een van drie witwastypologieën in het kader van de aan- en verkoop van cryptocurrency.

53. Om volledig te zijn, kan er ook nog onderscheid gemaakt worden tussen soorten *wallets*, te weten software, hardware, online en paper *wallets*.

54. Vanuit een bitcoinwallet kunnen bitcoins worden verzonden en ontvangen. Een bitcointransactie vindt (simpel gezegd) plaats door het invullen van het transactiebedrag, het bitcoinadres van zowel de verzender als de ontvanger en de digitale handtekening van de verzender. Deze digitale handtekening bestaat uit een cryptografisch onlosmakelijk met elkaar verbonden geheime sleutel (*private key*) en een openbare sleutel (*public key*). De *private key* wordt eveneens opgeslagen in de *wallet* en is van essentieel belang bij het ondertekenen van de bitcointransactie. Zonder de *private key* kan men niets met de bitcoins. De *private key* kan niet worden gewijzigd. Hiermee wordt onder meer gewaarborgd dat bitcoins alleen kunnen worden uitgegeven door de persoon die de bitcoins onder zich houdt. De *public key* daarentegen is voor het gehele netwerk zichtbaar en dient onder meer ter verificatie van de digitale handtekening.

55. *Kamerstukken II* 2018/19, 34245, nr. 3, p. 3-4 (MvT).

56. Eigenlijk worden bitcoins niet zelf opgeslagen in de bitcoinwallet, maar bevat de bitcoinwallet slechts de *private key*, die nodig is om toegang te krijgen tot het bitcoinadres en dus ook tot de eigen bitcoins.

57. Dit komt omdat zij niet (zelfstandig) beschikken over de *private key* en dus op geen enkele manier toegang hebben tot de bitcoins. Hierdoor zijn zij niet of nauwelijks in staat om te voldoen aan de verplichtingen van de vierde antiwitwasrichtlijn, zoals het monitoren van transacties.

Zodoende is het nog maar de vraag of de Nederlandse implementatie van AMLD5 een voldoende afschrikkend effect heeft op criminelen, zoals door menigeen vooraf werd gehoopt.⁵⁸

6. Afsluitende beschouwingen

Cash is king, maar ten tijde van de coronacrisis lijkt dat toch anders te liggen. Vanwege besmettingsgevaar worden mogelijkheden tot betaling in chartaal geld aanzienlijk beperkt en nu de hele wereld in meerdere of mindere mate te kampen heeft (gehad) met een *lockdown*, heeft ook de offline (internationale) handel stil gelegen.⁵⁹ De coronacrisis heeft derhalve grote financiële gevolgen, ook voor criminelen. Het witwassen van geld wordt een grotere uitdaging voor criminelen. Het geld wordt normaliter op grofweg twee manieren verplaatst: enerzijds door middel van fysieke verplaatsing (vliegtuigen, vrachtverkeer) en anderzijds door zwart geld om te zetten in andere waardes, denk aan de aanschaf van goederen of crypto's, zoals bitcoins. Doordat de wereld enkele maanden in *lockdown* was – en het fysiek vervoeren van geld in beginsel onmogelijk was – werd door het AMLC voorspeld dat criminelen cryptocurrencies, zoals bitcoins, weer massaal zouden gaan gebruiken voor hun witwasactiviteiten.

Covid-19 zal de komende maanden de gemoederen bezig blijven houden. Het verleden leert ons dat criminelen een crisistijd misbruiken door de criminele activiteiten op te voeren en op een creatieve manier trachten te profiteren van de ontstane disruptie. (Financiële) ondernemingen dienen om die reden de geldende procedures en maatregelen in de strijd tegen witwassen en terrorismefinanciering scherp in acht te nemen. Criminelen doen er immers alles aan om de herkomst van hun criminele geld te verhullen. Daarvoor misbruiken zij vaak meerdere banken. Een effectieve handhaving is dus noodzakelijk. De opgerichte Transactie Monitoring Nederland is in dit verband een welkome samenwerking om de verdachte patronen op te sporen en criminele geldstromen beter in beeld te krijgen.

Criminelen zullen namelijk tijdens deze pandemie blijven reageren dan wel anticiperen op de telkens veranderende omstandigheden en hun witwasprocessen blijven aanpassen. Ze zullen ontwikkelingen in de gaten houden en de mazen in wet- en regelgeving opzoeken om te allen tijde onder de radar van politie en justitie te blijven.

Het digitaliseren van de stappen in het witwasproces door middel van (omzetting in) bitcoins zoals door het

AMLC is voorspeld, is een logische ontwikkeling door het relatief anonieme karakter en de waardeinstijging die het de laatste tijd kenmerkt.⁶⁰ Echter, de handel in crypto's, onder andere bitcoins, ligt met de implementatie van de AMLD5 in de Wwft meer onder een vergrootglas. Tellen we de strenge eisen die de rechtspraak stelt aan het ontzenuwen van het bewijsvermoeden dat sprake is van witwassen van of via cryptovaluta daarbij op, dan wordt de pakkans wel groter. Weerhoudt dit criminelen ervan om zwart geld wit te wassen via deze cryptocurrency? Vooralsnog niet. Op het eerste gezicht lijkt het toezicht op bitcoins te zijn gereguleerd en het pseudo-anonieme karakter te zijn verdwenen. Echter, als de verschillende *wallet providers* meer in detail worden bekeken, blijven er methoden over waarbij het witwassen via crypto's niet geheel onmogelijk wordt gemaakt. Exemplarisch is de *non-custodial wallet provider* die niet onder het nieuwe Wwft-regime valt. Zodoende is de Nederlandse implementatie van AMLD5 op papier een effectieve oplossing, maar is het in de praktijk nog maar de vraag of dit een voldoende afschrikkend effect zal hebben op criminelen.

Eén ding staat vast en dat is het feit dat de coronacrisis vraagt om meer alertheid voor witwassen. De pandemie en de *lockdowns* hebben invloed op de globale economie én op de witwaspraktijken van criminelen. En ook als de *non-custodial wallet provider* eenmaal onder het bereik van de antiwitwasregelgeving zal worden gebracht, zal het wachten zijn op een nieuwe methode waarmee criminelen hun zwarte geld (via virtuele valuta) kunnen witwassen.

58. Zie o.a. Bijlage 1 bij *Kamerstukken I 2017/18*, 34775, nr. W.

59. Dit in tegenstelling tot de online handel waar bijvoorbeeld Ahold de omzet zag stijgen in het eerste kwartaal van 2020 met 14,7% tot € 18,2 miljard en de nettowinst nam zelfs met 48% toe tot € 645 miljoen, zie 'Ahold profiteert fors van corona: winst stijgt bijna met de helft', *RTL Nieuws* 7 mei 2020.

60. 'Bitcoin kort boven de \$10.000', *FD* 26 juli 2020.