Nadere beschouwing over witwasrisico's bij gebruik van cryptovaluta en de impact van regulering

mr. A.B. Schoonbeek en mr. J.M. van Poelgeest*

Trefwoorden: witwasindicatoren, AML/CFT, cryptovaluta, registratieplicht, bitcoins, integere en beheerste bedrijfsvoering, crypto exchange, wallet, Wwft

* Annemarije Schoonbeek is advocaat te Amsterdam en tevens (hoofd)redacteur van het *Tijdschrift voor Compliance*. Jonneke van Poelgeest is advocaat te Amsterdam bij Trivvy Advocatuur.

1. Inleiding

Cryptovaluta heeft een vaste plek veroverd in onze economie. De reguliere poortwachters zoals banken, betaaldienstverleners en accountantsorganisaties, komen daarom in toenemende mate in aanraking met cryptovaluta. Tegelijkertijd spelen cryptovaluta nog steeds regelmatig een rol in witwasonderzoeken.[1] Gelet op de aan cryptovaluta verbonden risico's, levert dat de nodige compliance-uitdagingen op. Op grond van de vijfde anti-witwasrichtlijn worden aanbieders van diensten voor het wisselen tussen virtuele valuta en fiat valuta (zoals exchanges) en aanbieders van bewaarportemonnees (**crypto-instellingen**) aangemerkt als poortwachter. Vanaf implementatie in nationale regelgeving, vallen deze instellingen binnen het bereik van de Wet ter voorkoming van witwassen en financieren van terrorisme (**Wwft**).[2] Crypto-instellingen moeten op basis daarvan voldoen aan de kernverplichtingen uit de Wwft en tevens beschikken over een integere en beheerste bedrijfsvoering. Voor crypto-instellingen geldt een registratieverplichting bij De Nederlandsche Bank (**DNB**). Het wetsvoorstel tot implementatie van de vijfde anti-witwasrichtlijn is op dit moment nog steeds in behandeling bij de Eerste Kamer. Deze ontwikkelingen impliceren dat crypto-instellingen in toenemende mate deel gaan uitmaken van het reguliere financiële stelsel. De kans bestaat dat hieraan vertrouwen wordt ontleend door andere instellingen en consumenten. De vraag rijst welke impact de registratieplicht heeft op de kwetsbaarheden voor witwasrisico's van crypto-instellingen. In dit artikel gaan wij in op dit vraagstuk. Wij bespreken daartoe kort wat witwassen inhoudt en onder welke omstandigheden aan het gebruik van cryptovaluta witwasrisico's kleven (**paragraaf 2**). Vervolgens bespreken wij wat de gevolgen zijn van de registratie van crypto-instellingen (**paragraaf 3**). We sluiten af met een conclusie en vooruitblik (**paragraaf 4**). Wat cryptovaluta zijn en welke partijen precies onder de regelingen vallen, bespreken wij niet in dit artikel. Verwezen wordt naar eerdere publicaties hierover.[3]

1 Zie bijvoorbeeld de nieuwsberichten van het OM van 7 februari 2020 'Bitcoinhandelaar aangehouden in witwasonderzoek'.

2 Het wetsvoorstel Implementatiewet wijziging van de vierde anti-witwasrichtlijn (parlementair dossier 35.245) is op 10 december 2019 aangenomen door de Tweede Kamer. We gaan uit van de door de Tweede Kamer aangenomen tekst van het wetsvoorstel. Sinds oktober 2018 vallen cryptovaluta verder onder de FAFT-Recommendations. Dit betekent dat de FATF-landen op basis hiervan cryptovaluta binnen het bereik van het anti-witwasregelgeving en het toezicht daarop moeten brengen. De definitie van virtual asset service providers (VASP's) is ruimer is dan de crypto-instellingen als bedoeld in de vijfde anti-witwasrichtlijn. Nederland wacht nadere Europese regelgeving af ter implementatie van deze nieuwe standaard. Dit betekent dat er in de toekomst nadere regulering is te verwachten. Zie brief minister van Financiën van 26 juni 2019, kenmerk 2019-0000094167.

3 Zie bijvoorbeeld: A.A. Pasaribu, 'Enkele opmerkingen over virtuele valuta in de zin van de gewijzigde vierde anti-witwasrichtlijn', *Tijdschrift voor Sanctierecht en Onderneming* 2019, p. 234-240 en J.M. van Poelgeest en A.B. Schoonbeek, 'Poortwachters in onrustig vaarwater; enkele actuele ontwikkelingen op het gebied van witwasbestrijding', *Tijdschrift voor sanctierecht en onderneming* 2018, p. 79-86. Niet alle activiteiten met betrekking tot cryptovaluta worden gereguleerd op grond van de vijfde anti-witwasrichtlijn. Partijen die bijvoorbeeld crypto naar crypto diensten aanbieden (zonder aanbieder van een bewaarportemonnee te zijn) vallen niet onder

2. Op welke manier kunnen virtuele valuta worden misbruikt voor witwasdoeleinden

2.1 Back to basics: witwassen

Verschillende autoriteiten hebben erop gewezen dat cryptovaluta kwetsbaar zijn voor witwasrisico's.[4] Deze risico's houden met name verband met de mogelijkheid van anonimiteit en het feit dat transacties in cryptovaluta niet aan landsgrenzen zijn gebonden. Om de vraag te beantwoorden hoe kwetsbaar cryptovaluta nu precies zijn voor witwasrisico's, is van belang wanneer sprake is van witwassen.[5] Witwassen kan worden omschreven als het (doen) verrichten van handelingen, waardoor een voor de wet verzwegen vermogensaanwas ogenschijnlijk een legale oorsprong krijgt. Witwassen is strafbaar gesteld in art. 420bis (opzetwitwassen), art. 420ter (gewoontewitwassen), art. 420quater (schuldwitwassen) en art. 420quater1 (eenvoudig witwassen) Wetboek van Strafrecht (Sr). Art. 420bis lid 1, onderdelen a en b Sr omschrijft opzetwitwassen als (1) van een voorwerp de werkelijke aard, de herkomst, de vindplaats, de vervreemding of de verplaatsing verhullen (2) het verbergen of verhullen wie de rechthebbende op een voorwerp is of het voorhanden heeft (3) een voorwerp verwerven, voorhanden hebben, overdragen of omzetten of gebruik maken van een voorwerp, terwijl men weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf. Voor opzettelijk witwassen is vereist dat de verdachte de witwashandeling(en) verricht, terwijl hij wist of bewust de aanmerkelijke kans heeft aanvaard dat het voorwerp uit misdrijf afkomstig is. Voor het aannemen van schuldwitwassen is slechts vereist dat redelijkerwijs moet worden vermoed, bijvoorbeeld door de aanwezigheid van witwasindicatoren, dat het voorwerp uit misdrijf afkomstig is.[6]

2.2 Ook zonder concreet gronddelict kan sprake zijn van witwassen

Een belangrijk bestanddeel van het witwasdelict, is dus dat het moet gaan om voordelen 'afkomstig uit enig misdrijf' (gronddelict). Deze voordelen kunnen zowel cryptovaluta als giraal of contant geld (dat wordt omgezet in cryptovaluta) betreffen. Gronddelicten kunnen verder alle soorten misdrijven zijn: van drugshandel tot fraude zoals belastingontduiking en cybercrime. Voor het bewijs van witwassen is de aanwezigheid van een concreet bewezen gronddelict niet vereist.[7] Ook bij afwezigheid daarvan kan sprake zijn witwassen. In de rechtspraak[8] is het volgende toetsingskader ('6-stappenplan') ontwikkeld (zie figuur bovenaan p. 95).

het toepassingsbereik van de richtlijn. Ook bijvoorbeeld de cryptocurrency software aanbieders (waarmee via een API trades kunnen worden geïnitieerd) vallen buiten het bereik van de regelgeving.

4 De witwas- en terrorismefinancieringsrisico's (inherent risk exposure) worden in de zogeheten supranationale risicoanalyse (SRNA) van de Europese Commissie aangeduid als significant/very significant, zie annex bij COM(2019) 370 final, p. 103/104 (SWD(2019) 650 final). Zie voor een beschrijving van de risico's ook the Financial Action Task Force (FATF), 'Virtual Currencies Key Definitions and Potential AML/CFT Risks', juni 2014, http://www.fatf-gafi.org/.

5 We gaan uit van het Nederlands normenkader.

6 Illustratief is de strafrechtelijke transactie ex art. 74 Sr die door ING is gesloten met het Openbaar Ministerie (OM). Deze had ook betrekking op schuldwitwassen (naast overtreding van de Wwft). Dit wordt als volgt onderbouwd: *'ING NL had redelijkerwijs moeten vermoeden dat bepaalde geldstromen die via de bankrekeningen van haar cliënten liepen afkomstig waren uit enig misdrijf. (...) ING NL* [heeft] *diverse signalen ontvangen over specifieke cliënten die een vermoeden van witwassen op hadden moeten leveren. (...) ING NL heeft (...) vaker witwassignalen gemist. (...). Deze omstandigheden leiden er toe dat ING NL door het OM schuldwitwassen verweten wordt.'* (toevoeging, JMvP en ABS). Zie persbericht OM van 4 september 2018 'ING betaalt 775 miljoen vanwege ernstige nalatigheden bij voorkomen witwassen'.

7 Zie o.a. HR 28 september 2004, ECLI:NL:HR:2004:AP2124.

8 Ontleend aan Gerechtshof Amsterdam 11 januari 2013, ECLI:NL:GHAMS:2013:BY8481. Dit toetsingskader is – zij het niet door de zes stappen expliciet te noemen – ook bevestigd door de Hoge Raad (HR 18 december 2018, ECLI:NL:HR:2018:2352, rechtsoverwegingen 2.3.2 en 2.3.3). In de uitspraken van onder meer Rechtbank Rotterdam van 19 december 2017, ECLI:NL:RBROT:2017:10225 en Gerechtshof Den Haag 26 juni 2019, ECLI:NL:GHDHA:2019:1725 wordt dit toetsingskader ook toegepast met betrekking tot virtuele valuta (bitcoins).

Stap 1	Is er direct bewijs voor één of meer gronddelicten?
Stap 2	Zo nee, zijn de aangedragen feiten van dien aard dat sprake is van een concreet witwasvermoeden? Dit witwasvermoeden kan worden ontleend aan witwasindicatoren, zoals feiten van algemene bekendheid en vastgestelde witwastypologieën.
Stap 3	Zo ja, dan mag van de verdachte verwacht worden dat hij een verklaring geeft over de herkomst van het voorwerp danwel de voorwerpen.
Stap 4	Het moet daarbij gaan om een concrete, min of meer verifieerbare en niet op voorhand hoogst onwaarschijnlijke verklaring voor de herkomst van het voorwerp c.q. de voorwerpen.
Stap 5	Indien deze verklaring is gegeven, ligt het op de weg van het openbaar ministerie om nader onderzoek te doen naar de uit de verklaringen van de verdachte blijkende alternatieve herkomst van de voorwerpen.
Stap 6	Uit de resultaten van dit onderzoek zal vervolgens moeten blijken of met voldoende mate van zekerheid kan worden uitgesloten dat de voorwerpen een criminele herkomst hebben.

2.3 Witwassen kan onder omstandigheden worden gebaseerd op witwasindicatoren

Een vermoeden van witwassen kan worden gebaseerd op witwasindicatoren. Als er dan geen concrete en verifieerbare verklaring wordt gegeven om witwassen uit te sluiten, kan witwassen op basis daarvan bewezen worden verklaard. Er bestaan drie categorieën witwasindicatoren[9]: (1) door het FATF en de FIU-Nederland (**FIU**) vastgestelde witwastypologieën[10] (2) feiten van algemene bekendheid die duiden op witwassen[11] en (3) overige indicatoren. De witwastypologieën worden in Nederland vastgesteld door de FIU.[12] Deze typologieën omvatten onder meer:

- het ontbreken van een legale economische verklaring voor het wisselen van grote geldbedragen;
- de transacties staan niet in verhouding tot de inkomsten;
- het feit dat er een beloning werd verkregen voor de door verdachte uitgevoerde wisseltransacties; en
- geldbedragen van behoorlijke omvang (...) die niet terug zijn te vinden in (officiële) boeken van en evenmin kunnen worden verantwoord met stukken van reguliere handelsactiviteiten;

Met betrekking tot virtuele valuta zijn in 2017 de volgende witwastypologieën vastgesteld.

1. *Het meermalen binnen een relatief korte periode vanaf bankrekening(en) opnemen van aanzienlijke contante bedragen, geheel of in delen, zonder een kennelijke economische noodzaak en in combinatie met het meermalen giraal ontvangen van bedragen (waarbij die bedragen in geval van de handelaar in virtuele betaalmiddelen kennelijk afkomstig zijn uit de verkoop van virtuele betaalmiddelen).*
2. *De aankoop van virtuele betaalmiddelen waarbij aan ten minste twee van de volgende kenmerken is voldaan:*
   a) *de koper biedt zijn diensten aan via internet middels vraag- en aanbodsites;*
   b) *de koper stelt geen identiteit van de verkoper vast;*
   c) *de koper schermt de eigen identiteit af;*
   d) *de koper rekent in contanten af;*
   e) *de koper brengt een ongewoon hoog percentage wisselcommissie in rekening;*
   f) *de transactie vindt plaats in een (openbare) omgeving waar veel publiek aanwezig is waardoor het veiligheidsrisico voor de koper vermindert;*

[9] Brochure witwasindicatoren van het Anti-Money Laundering Centre (AMLC), zie https://www.amlc.nl/witwasindicatoren/.

[10] Dit betekent overigens niet dat het aan de verdachte is om aannemelijk te maken dat het voorwerp niet van misdrijf afkomstig is (HR 18 december 2018, ECLI:NL:HR:2018:2352). De werking van de onschuldpresumptie behandelen wij niet in dit artikel.

[11] Zie art. 339 lid 2 Wetboek van Stafvordering. Feiten van algemene bekendheid hoeven niet te worden bewezen.

[12] Zie https://www.fiu-nederland.nl/nl/witwas-typologieen-0. Op internationaal niveau worden typologieën vastgesteld door de FATF. Zie http://www.fatf-gafi.org.

g) een legale economische verklaring voor de wijze van omwisseling is niet aannemelijk;
h) de omvang van de aangekochte virtuele betaalmiddelen is niet aannemelijk in relatie tot gemiddeld particulier gebruik;
i) de koper is niet bij de Kamer van Koophandel en niet bij de Belastingdienst bekend voor het zijn van wisselinstelling.

3. *De koper en/of verkoper maakt/maken bij de verkoop van virtuele betaalmiddelen gebruik van een zogenaamde mixer.*[13]

Het in juni 2019 verschenen OESO Handboek voor medewerkers van de Belastingdienst 'Indicatoren van witwassen en terrorismefinanciering'[14] bevat ook indicatoren met betrekking tot cryptovaluta, bijvoorbeeld het accepteren, handelen in of beschikbaar hebben van 'coins' met een historie op het '*dark web*'. Deze hebben niet de status typologie, maar kunnen worden beschouwd als witwasindicatoren. De witwasindicatoren zijn ook relevant voor de verplichting om ongebruikelijke transacties te melden, nu reeds bij een vermoeden van witwassen een dergelijke melding moet worden gedaan (zie paragraaf 3.4, hierna).

2.4 Witwassen met behulp van cryptovaluta in de rechtspraak

De betekenis van witwasindicatoren is voor de beoordeling van de risico's bij de dienstverlening door en/of aan crypto-instellingen in het bijzonder van belang nu in de regel geen concrete gronddelicten met betrekking tot transacties zullen kunnen worden aangewezen. Dit beeld wordt bevestigd in de beschikbare rechtspraak over witwassen met behulp van bitcoins. Daarin is meermaals, ook zonder concreet gronddelict, witwassen bewezen verklaard met behulp van witwasindicatoren. Het gaat in een aantal gevallen om inkoop van bitcoins van partijen die anoniem wensten te blijven tegen betaling in contanten onder afslag van een relatief hoge provisie.[15] In een enkel geval gaat het om witwassen door een bankrekening ter beschikking te stellen voor ontvangst en vervolgens contant opnemen van gelden die afkomstig zijn van transacties met bitcoins (geldezels).[16] Onder meer aan de volgende feiten en omstandigheden wordt in de rechtspraak een witwasvermoeden ontleend:

- Transacties staan niet in verhouding tot de inkomsten van de verdachte.
- Geen verklaring voor de gewisselde valutasoorten.
- Het smurfen (het overboeken van kleine bedragen) van de girale ontvangsten uit verkoop bitcoins.
- Bitcoins afkomstig van bitcoinclusters die direct of indirect afkomstig waren van het *dark web*.
- Dat met betrekking tot één cliënt kon worden vastgesteld dat deze zich bezighield met drugshandel.

Hierbij geldt dat de strafrechter meestal uit meerdere witwasindicatoren in onderlinge samenhang het witwasvermoeden afleidt.
In een uitspraak van rechtbank Rotterdam wordt overwogen dat het een feit van algemene bekendheid is dat bitcoins dikwijls worden gebruikt in het criminele circuit zoals drugshandel.[17] Door een andere rechter is daarentegen juist overwogen dat het enkel voorhanden hebben van een kleine hoeveelheid bitcoins juist niet een vermoeden van witwassen rechtvaardigt.[18]

[13] Door het FATF als volgt gedefinieerd: *'Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A-mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction.'* Zie The Financial Action Task Force (FATF), 'Virtual Currencies Key Definitions and Potential AML/CFT Risks', juni 2014, p. 6

[14] Zie http://www.oecd.org/tax/crime/Indicatoren-van-witwassen-en-terrorismefinanciering-Handboek-voor-medewerkers-van-de-Belastingdienst.pdf. Zie met name p. 59 en 89. Zie hierover ook: https://www.amlc.nl/nieuwe-versie-oeso-handboek-witwasindicatoren/.

[15] Dit was onder meer aan de orde in de volgende uitspraken: Rechtbank Overijssel 22 oktober 2019, ECLI:NL:RBOVE:2019:3787, Gerechtshof Den Haag 26 juni 2019, ECLI:NL:GHDHA:2019:1725, Gerechtshof Amsterdam 27 februari 2019, ECLI:NL:GHAMS:2019:585 (*Lancashire*, zie overwegingen met betrekking tot bitcoincluster #4), Rechtbank Rotterdam 4 april 2018, ECLI:NL:RBROT:2018:5197, Rechtbank Rotterdam 30 mei 2018, ECLI:NL:RBROT:2018:4269 (onderzoek 'IJsberg', zie met name rov. 4.2.4.3), Rechtbank Midden-Nederland 3 april 2018, ECLI:NL:RBMNE:2018:1180 en Rechtbank Midden-Nederland 14 november 2017, ECLI:NL:RBMNE:2017:5713.

[16] Zie bijvoorbeeld Rechtbank Rotterdam 13 maart 2019, ECLI:NL:RBROT:2019:2408, ECLI:NL:RBMNE:2017:5713.

[17] Rechtbank Rotterdam 13 maart 2019, ECLI:NL:RBROT:2019:2408.

[18] Zie een uitspraak van de Rechtbank Amsterdam van 13 maart 2018, ECLI:NL:RBAMS:2018:1738, zoals in hoger beroep bevestigd: Gerechtshof Amsterdam 4 april 2019, ECLI:NL:GHAMS:2019:1152).

In andere uitspraken wordt meer specifiek (als feit van algemene bekendheid) aangenomen dat transacties via marktplaatsen zoals het *dark web* in overwegende mate drugs- en andere illegale transacties betreffen. Deze omstandigheid wordt gezien als een sterke aanwijzing dat de betreffende bitcoins uit misdrijf afkomstig zijn.[19] Relevant in dat kader is dat zogeheten vermenging[20] kan plaatsvinden. In rechtspraak is aangenomen dat als door vermenging van *dark web* markets afkomstige bitcoins worden vermengd met bitcoins met mogelijk wel legale herkomst het voor al deze bitcoins tezamen verkregen bedrag als geheel of ten dele uit misdrijf afkomstig moet worden aangemerkt.[21] Het vermogensbestanddeel met een criminele herkomst laat zich daardoor niet meer individualiseren. Overigens komt in de rechtspraak, niet alleen de criminele herkomst van cryptovaluta aan bod, maar ook witwassen door voordelen uit (eigen) misdrijf (geldbedragen) om te zetten in bitcoins. Daarbij is geoordeeld dat een dergelijke omzetting (onder omstandigheden) wordt beschouwd als op verhulling te zijn gericht, omdat daarmee de geldbedragen niet traceerbaar kunnen worden gemaakt.[22]

2.5 Resumerend

Rechtspraak bevestigt het beeld dat cryptovaluta (bitcoins) en de daarbij betrokken dienstverleners kwetsbaar zijn voor witwasrisico's. Ook zonder concreet gronddelict kan witwassen worden bewezen. Ook transacties, waarmee een instelling of consument niet rechtstreeks in aanraking komt (verder weg in de keten), kunnen maken dat cryptovaluta of de opbrengsten uit misdrijf afkomstig kunnen zijn. Uit de aanwezigheid van witwasindicatoren moet een vermoeden van witwassen worden afgeleid. Daarbij moet worden meegewogen dat aan transacties in bitcoins, gelet op de specifieke kenmerken, een inherent risico op witwassen kleeft. Om witwasrisico's te kunnen identificeren, is het aldus van belang om goed van de witwasindicatoren op te hoogte te zijn. De rechtspraak is nog volop in ontwikkeling. De lijn daarin lijkt momenteel te zijn dat bij bitcoins die afkomstig zijn van het *dark web* moet worden aangenomen dat deze een criminele herkomst hebben en dat, indien dat niet het geval is, weliswaar bij transacties met bitcoins sprake is van een hoog inherent risico op witwassen, maar dat het van de overige feiten en omstandigheden afhangt of witwassen kan worden bewezen. Het enkel voorhanden hebben van (een beperkt aantal) bitcoins lijkt daarvoor niet voldoende. Bij bedragen die zijn verkregen uit transacties met zowel bitcoins die afkomstig zijn van het *dark web* en andere bitcoins, geldt dat het gehele bedrag als geheel of ten dele afkomstig uit misdrijf moet worden beschouwd.

3. Regulering van crypto-instellingen

3.1 Registratie van crypto-instellingen

Zoals in de inleiding vermeld heeft de implementatie van de vijfde anti-witwasrichtlijn tot gevolg dat crypto-instellingen binnen het bereik van de Wwft vallen. Dat betekent dat naast de kernverplichtingen uit de Wwft, zoals het verrichten van een (integriteits) risicoanalyse, het inrichten van risicomanagement[23], het risicogebaseerd verrichten

[19] Zie onder meer de uitspraken van Rechtbank Midden-Nederland van 14 november 2017, ECLI:NL:RBMNE:2017:5713, Rechtbank Rotterdam 19 december 2017, ECLI:NL:RBROT:2017:10225, Rechtbank Rotterdam 5 april 2018, ECLI:NL:RBROT:2018:5197 en Rechtbank Rotterdam 30 mei 2018, ECLI:NL:RBROT:2018:4269.

[20] Dit betekent dat indien van misdrijf afkomstige vermogensbestanddelen zijn vermengd met vermogensbestanddelen die zijn verkregen door middel van legale activiteiten, het aldus vermengde vermogen kan worden aangemerkt als mede of deels uit misdrijf afkomstig.

[21] Dit kwam in het bijzonder aan de orde in Rechtbank Midden-Nederland 14 november 2017, ECLI:NL:RBMNE:2017:5713. Voor zover wij hebben kunnen nagaan wordt evenwel in één uitspraak (Rechtbank Rotterdam 30 mei 2018, ECLI:NL:RBROT:2018:4269), overwogen dat ontvangsten uit *wallets* die voor slechts 4%, 1% en 8% zijn besmet met ontvangen bitcoins afkomstig van het *dark web* zonder nadere toelichting onvoldoende is om bij te dragen aan een vermoeden van witwassen.

[22] Hof Den Bosch 11 maart 2019, ECLI:NL:GHSHE:2019:965. Tegen de uitspraak is cassatie ingesteld. In de conclusie van 18 februari 2020, ECLI:NL:PHR:2020:148, wordt verwezen naar de gelijksoortige oordelen van Rechtbank Rotterdam 17 december 2018, ECLI:NL:RBROT:2018:10879 en Rechtbank Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814.

[23] Zie § 1.2 van de Wwft (art. 1f tot en met 2f van de Wwft). Dit betekent dat een beleidsbepaler moet worden aangewezen voor de naleving van de Wwft, voor zover passend bij de aard en omvang van de instelling, de instelling beschikt over een compliance officer en de instelling er zorg voor draagt dat op onafhankelijke wijze een

van cliëntenonderzoek, monitoren van zakelijke relaties en transacties en de verplichting om ongebruikelijke transacties te melden bij het FIU voor deze instellingen ook gaat gelden dat zij moeten beschikken over een integere en beheerste bedrijfsvoering. Het in te richten risicomanagement op grond van de Wwft betekent dat een beleidsbepaler moet worden aangewezen voor de naleving van de Wwft. Daarnaast zal, voor zover passend bij de aard en omvang van de instelling, de instelling over een compliance officer dienen te beschikken en de instelling dient er dan zorg voor te dragen dat er op onafhankelijke wijze een auditfunctie wordt uitgoefend.[24] De auditfunctie controleert de naleving door een instelling van de bij of krachtens de Wwft gestelde regels en de uitoefening van de compliancefunctie.

Er geldt daarnaast een registratieplicht bij DNB.[25] In eerste instantie is een vergunningplicht voorgesteld[26], maar dit is na kritiek gewijzigd in een registratieplicht.[27] Hiervoor gelden zodanige eisen dat *de facto* sprake is van een vergunning. De eisen zijn vergaand en lijken soms feitelijk niet haalbaar voor crypto-instellingen. In deze paragraaf gaan we hierop nader in, met een focus op:

- de integriteitsrisicoanalyse (SIRA) (paragraaf 3.2);
- het risico acceptatiebeleid (vastleggen van *de risk appetite*) (paragraaf 3.3);
- het cliëntenonderzoek en de monitoring van zakelijke relaties en transacties (paragraaf 3.4);
- compliance-uitdagingen in relatie tot *wallets* en toepassing van de *travel rule* (paragraaf 3.5).

3.2 Integriteitsrisicoanalyse (SIRA)

Een crypto-instelling dient een integriteitsrisicoanalyse op te stellen en actueel te houden (een SIRA).[28] Daarnaast geldt dat de instelling een adequaat beleid dient te voeren dat de integere en beheerste bedrijfsvoering waarborgt. Dit betekent dat daarin de naleving van de Wwft is gewaarborgd. Daarnaast zullen belangenverstrengeling, strafbare feiten of andere wetsovertredingen en relaties met cliënten of derden die het vertrouwen in de crypto-instelling kunnen schaden moeten worden tegengegaan.[29]

Voor de instelling is van belang om de relevante risico's in kaart te brengen, zodat de instelling in staat is daarop toegespitste maatregelen te treffen om de risico's adequaat te beheersen. Uit de SIRA dient te blijken of, en zo ja, welke integriteitsrisico's binnen de *risk appetite* vallen en/of beheersmaatregelen nodig zijn om de risico's te mitigeren. Het is vervolgens van belang dat de SIRA goed wordt (door)vertaald binnen de organisatie. De norm van de integere en beheerste bedrijfsvoering is afkomstig uit de Wet op het financieel toezicht (Wft) voor financiële instellingen. De door DNB ontwikkelde *guidance* voor het opstellen van een integriteitsrisicoanalyse voor financiële instellingen kan worden gebruikt door crypto-instellingen. DNB verwijst daarnaar in haar *guidance* voor crypto-instellingen. In de SIRA moeten de risico's in kaart worden gebracht waarbij rekening moet worden gehouden met risicofactoren die verband houden met het type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden. Bij het maken van de SIRA zal de crypto-instelling rekening moeten houden met de supranationale en nationale risicoanalyse op het gebied van witwassen, maar ook met overige bronnen waaruit kwetsbaarheden van cryptovaluta en crypto-instellingen voor integriteitsrisico's zijn af te leiden. De SIRA moet resulteren in een (periodieke) analyse van de (eventueel gewijzigde) risico's, in (aangepaste) risicobeheersingsmaatregelen en vervolgens in monitoring en het eventueel herzien van de risicoanalyse. De SIRA dient op verzoek beschikbaar te worden gesteld aan de bevoegde toezichthouder(s). Op basis van de SIRA moeten op de eigen organisatie toegespitste interne procedures en maatregelen worden vastgesteld. De SIRA kan als volgt schematisch worden weergegeven (zie figuur bovenaan p. 99).[30]

auditfunctie wordt uitgeoefend (zie art. 2d Wwft). Daarnaast geldt overigens dat de instelling op grond van de vereiste IBB dient te beschikken over op betrouwbaarheid en geschiktheid getoetste (mede) beleidsbepalers.

[24] Zie art. 2d Wwft. Daarnaast geldt overigens dat de instelling dient te beschikken over op betrouwbaarheid en geschiktheid getoetste (mede) beleidsbepalers.

[25] Zie bijvoorbeeld https://www.toezicht.dnb.nl/2/50-237963.jsp.

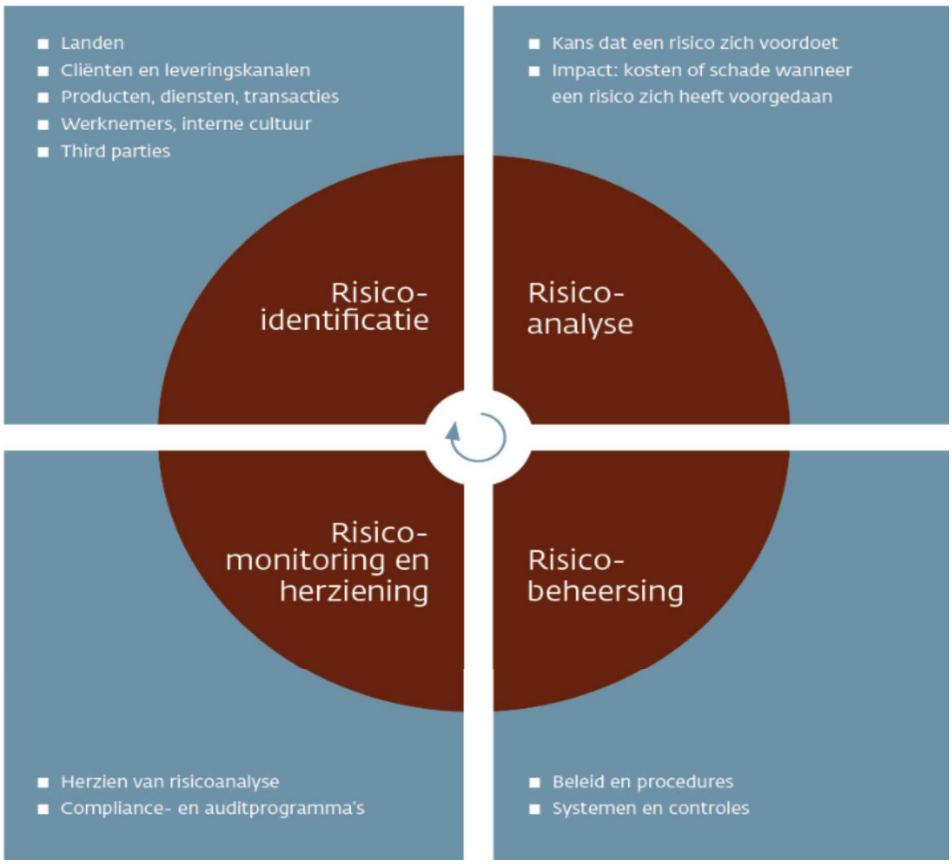
[26] Zie https://www.internetconsultatie.nl/wijzigingamld4.

[27] Art. 23b Wwft (nieuw).

[28] Art. 2b Wwft. https://www.toezicht.dnb.nl/2/50-238029.jsp. In dit verband kan rekening worden gehouden met de guidance van DNB op dit gebied voor andere partijen, zie https://www.toezicht.dnb.nl/binaries/50-234068.pdf.

[29] Art. 23j Wwft (nieuw).

[30] Dit overzicht komt uit het DNB document 'de integriteitsrisicoanalyse': https://www.toezicht.dnb.nl/binaries/50-234068.pdf.



Een belangrijk onderdeel van de SIRA is het formuleren van op de eigen organisatie toegespitste risico's (risico scenario's). Het is daarbij van belang het bedrijfsmodel in beeld te hebben en informatie te verzamelen over de cliënten(portefeuille), diensten en producten. Door de producten (cryptovaluta), de wijze van dienstverlening (online) en de veelal ruime geografische activiteiten, zal de SIRA risicoscenario's bevatten waaruit hoge inherente bruto risico's op witwassen volgen.

Voorbeelden van risicoscenario's die door crypto-instellingen worden geïdentificeerd zijn onder meer:
- Vervalsing van kopie identiteitsbewijs of het aanleveren van een kopie van een gestolen identiteitsdocument;
- Het omwisselen of verhandelen van cryptovaluta, waarbij de cryptovaluta die worden aangeboden aan of verhandeld worden via de betreffende crypto-instelling geheel of ten dele uit misdrijf afkomstig zijn (zie ook hiervoor); en
- Omzetten van uit misdrijf afkomstig giraal of contant geld in cryptovaluta.

Hierbij moet worden beoordeeld of deze risico's kunnen worden beheerst en/of deze (al dan niet middels het toepassen van additionele maatregelen) binnen de *risk appetite* van de crypto instelling vallen.

3.3 Risico acceptatiebeleid en risk appetite

Een crypto-instelling dient te beschikken over een risico-acceptatiebeleid (*risk appetite*)[31] waaruit blijkt welke risico's zij wel en niet wenst te accepteren. Het duidelijk vastleggen van het risico-acceptatiebeleid is van belang in het kader van de anti-witwasregelingen, de integere en beheerste bedrijfsvoering en naleving van de sanctieregelgeving. Het acceptatiebeleid moet zo worden ingericht dat de instelling in staat is om de risico's die zij in het kader van haar bedrijfsvoering accepteert kan beheersen.

Doelgroep en geografische activiteiten
In het kader van (risico)acceptatie moet bijvoorbeeld worden bepaald wat de doelgroep is: consumenten of (ook) bedrijven.

[31] Hier zal de crypto-instelling rekening kunnen houden met de DNB brochure Good practice Integrity Risk Appetite, te raadplegen via: https://www.toezicht.dnb.nl/binaries/50-236706.pdf.

Witwasrisico's kunnen bijvoorbeeld ontstaan bij ondoorzichtige (bedrijfs)structuren en verborgen (uiteindelijk) belanghebbenden of bedrijven die illegale inkomstenbronnen verkrijgen. Witwasrisico's kunnen (deels) worden beheerst door het beperken van de geografische gebieden waar de activiteiten worden aangeboden, bijvoorbeeld door cliënten uit zogeheten (derde-)hoog risicolanden uit te sluiten van de diensten (in de interne procedures, op de website, de voorwaarden met de cliënt en het inschrijvingsproces). In dit verband is de woonplaats van consumenten van belang en voor bedrijven de vestigingsplaats. Voor wat betreft bedrijven geldt dat ook zal moeten worden bepaald hoe wordt omgegaan met complexe (internationale) structuren, uiteindelijk belanghebbenden in hoog risicolanden en/of politiek prominente personen, waar een hoger risico aan verbonden is.

Productbeleid
In het kader van (risico)acceptatie beleid zal de crypto-instelling moeten bepalen welke producten worden aangeboden, geaccepteerd en/of verhandeld. Hoe meer een cryptovaluta bijvoorbeeld de focus op privacy heeft, hoe lastiger het is voor de crypto-instelling om na te gaan wat de herkomst is van de cryptovaluta. De *privacy coins* kunnen naar verwachting niet meer worden verhandeld via de bij DNB geregistreerde partijen.

3.4 Eisen cliëntenonderzoek en monitoring en beheersing van (witwas)risico's

De *risk appetite* werkt door in het cliëntenacceptatiebeleid (bij aanvang en doorlopend). De uitkomsten van de SIRA, inclusief de *risk appetite*, moeten verder worden vertaald naar risico's en beheersmaatregelen in relatie tot individuele cliënten.[32] Crypto-instellingen dienen namelijk, net als andere instellingen, cliëntenonderzoek te verrichten, waarbij de mate en diepgang is afgestemd op het risicoprofiel van de cliënt. Het cliëntenonderzoek stelt de instelling in staat tot:
- Identificatie en verificatie identiteit van de cliënt;
- Identificatie en verificatie van de identiteit van de vertegenwoordiger (indien van toepassing);
- Identificatie en verificatie van de uiteindelijk belanghebbende (**UBO**);
- Bij cliënten die rechtspersoon zijn: inzicht in de eigendoms- en zeggenschapsstructuur;
- Het doel en de beoogde aard van de zakelijke relatie vaststellen;
- Zonodig een onderzoek naar de bron van de middelen;
- Opstellen van een risicoprofiel; en
- Een voortdurende controle van de zakelijke relatie en verrichte transacties en actueel houden van gegevens.

De eisen die worden gesteld aan crypto-instellingen lijken zwaarder dan voor bestaande instellingen. Het uitgangspunt van de toezichthouder is op dit moment namelijk dat cliënten van crypto-instellingen (altijd) als hoog risico dienen te worden beschouwd. Dit is onder meer gebaseerd op de (wijze van) dienstverlening en de aard van de producten (cryptovaluta).[33] Dit betekent dat de crypto-instellingen standaard een verscherpt cliëntenonderzoek (en monitoring) moeten uitvoeren.[34]

Voor wat betreft identificatie en verificatie van de identiteit van de cliënt, geldt dat dit kan worden uitgevoerd middels het opvragen van een kopie identiteitsbewijs in combinatie met een overboeking van een klein bedrag, maar dat daarnaast wel aanvullende (verificatie)maatregelen vereist zijn. Daarbij geldt dat voor verificatie vereist is dat dit gebeurt op basis van gegevens uit betrouwbare en onafhankelijke bron.[35] Daarbij is van belang dat de crypto-instelling gegevens controleert op echtheid. Hier dient de crypto-instelling zelf risicogebaseerd

[32] Bij andere instellingen is dit een belangrijk aandachtspunt gebleken, zie bijvoorbeeld: https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-trustkantoren/nieuwsbrief-trustkantoren-augustus-2019/index.jsp.

[33] Zie bijvoorbeeld Leidraad Wwft, Wwft BES en Sanctiewet van de AFM, p. 20. Zie ook een nieuwsbericht AFM d.d. 25 juli 2018 'Toepasbaarheid Wwft op (beheerders van) beleggingsinstellingen in crypto's'.

[34] Hierbij is ook belangrijk dat op dit moment is gesteld dat de crypto-instellingen binnen Europa aan de nationale wet- en regelgeving in de lidstaten moeten voldoen. Zo wordt nu aangenomen dat crypto-instellingen die zijn gevestigd in andere lidstaten met een registratie in de betreffende staat ook een registratie nodig hebben bij DNB om in Nederland diensten te kunnen verlenen. Aangezien de meeste crypto-instellingen in diverse landen actief zijn, levert dat een behoorlijk intensieve klus op, temeer nu de verschillende landen andere eisen stellen.

[35] Indien de cliënt een bedrijf is geldt ook voor identificatie en verificatie van de UBO. In verband met de verificatiemogelijkheden wordt ook verwezen naar de opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, 23 January 2018: https://eba.europa.eu/esas-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process.

invulling aan te geven. Het standpunt op dit moment is dat de bij andere financiële partijen toegepaste standaard methodes (bij een cliënt met een gemiddeld risico), zoals een kopie identiteitsbewijs met een overboeking van een klein bedrag, niet voldoende zal zijn.[36] De uitdagingen voor crypto-instellingen op dit gebied hebben deels te maken met de karaktereigenschappen van *wallets* (zie paragraaf 3.5).

Gelet op het hoge risicoprofiel van haar cliënten, dient een crypto-instelling daarnaast onderzoek te verrichten naar de bron van de middelen die bij de zakelijke relatie of de transactie worden gebruikt. Dit onderzoek moet zien op de plausibiliteit van de legale herkomst van de middelen. De bron van de middelen kan worden opgevraagd middels een formulier waarbij de cliënt moet aangeven wat de bron is en (afhankelijk van het risicoprofiel) bewijs moet aanleveren over die bron (bijvoorbeeld erfenis, loondienst, ondernemer etc.).[37] Crypto-instellingen dienen (in dat kader) vast te stellen wat de herkomst is van de cryptovaluta (en bijvoorbeeld of deze uit het *dark web* afkomstig zijn door de chain te volgen).[38] Zij kunnen gebruik maken van partijen die een blockchainanalyse van transacties verrichten (bijvoorbeeld Chainalysis) zodat bijvoorbeeld vastgesteld kan worden dat er mogelijk iets 'mis' is met de herkomst.[39] Als een dergelijke conclusie volgt uit de chain, dient de instelling daar passende gevolgen aan te verbinden (door bijvoorbeeld de aangeboden cryptovaluta niet te accepteren en de transactie niet uit te voeren). Echter, voor de cryptovaluta met kenmerken van anonimiteit (de *privacy coins*) geldt dat het feitelijk onmogelijk is om de herkomst is van de cryptovaluta vast te stellen. Dit heeft waarschijnlijk tot gevolg dat deze cryptovaluta niet meer via de geregistreerde partijen kunnen worden verhandeld.

Monitoring en melden ongebruikelijke transacties

Naast het verrichten van het cliëntenonderzoek, zal de crypto instelling de zakelijke relatie en de transacties risicogebaseerd moeten monitoren. Het transactiemonitoringproces moet herleidbaar zijn tot de SIRA. DNB verwacht dat crypto-instellingen per cliënt een transactieprofiel opstellen. Bij afwijkingen daarvan en/of indien het economisch gezien of anderszins niet logisch of passend is dat een bepaalde cliënt een transactie wil doen, moet de crypto-instelling nader onderzoek instellen. Beoordeeld moet worden of dit een signaal is van een mogelijke ongebruikelijke transactie (alert). De monitoring moet de instelling in staat stellen om onverwijld ongebruikelijke transacties te melden bij FIU. Of een transactie ongebruikelijk is, wordt vastgesteld aan de hand van indicatoren. Uit het voorgestelde implementatiebesluit wijziging vierde anti-witwasrichtlijn[40] volgt dat voor crypto-instellingen de volgende indicatoren gelden (1) transacties van een bedrag van € 15.000, - of meer (2) of een transactie van € 10.000, - of meer waarbij een omwisseling plaatsvindt tussen virtuele valuta in contante fiduciaire valuta (gewoon geld) en (3) de instelling heeft aanleiding om te veronderstellen dat een transactie verband kan houden met witwassen of financieren van terrorisme. Voor wat betreft de laatste indicator is een vermoeden voldoende. Zoals hiervoor toegelicht is een witwasvermoeden in beginsel reeds aan de orde, indien witwasindicatoren van toepassing zijn. Crypto-instellingen zullen dan ook, naast de objectieve indicatoren en intern ontwikkelde risico-indicatoren, relevante witwasindicatoren moeten inbedden in de transactiemonitoring om te voorkomen dat signalen van witwassen ten onrechte worden gemist.

3.5 Wallets en risicobeheersing

De karaktereigenschappen van *wallets* leiden tot de nodige uitdagingen bij de naleving van de Wwft en de sanctieregelgeving. In tegenstelling tot bijvoorbeeld bankrekeningen zijn *wallets* (en de cryptovaluta op die *wallet*) namelijk weliswaar van iemand of van een bedrijf, maar deze persoon of bedrijf is (bewijstechnisch) niet

[36] Hierover ook: https://www.toezicht.dnb.nl/2/50-237935.jsp.

[37] DNB merkt in de Leidraad Wwft en Sw, versie december 2019, op dat het voor hoogrisico cliënten ook nodig is om inzicht te hebben in de vermogenspositie.

[38] Zo ook de AFM in haar nieuwsbericht 'Toepasbaarheid Wwft op (beheerders van) beleggingsinstellingen in crypto's' van 25 juli 2018. Voor de integere en beheerste bedrijfsvoering is het daarnaast van belang dat strafrechtelijke delicten worden voorkomen zodat het ook vanuit perspectief relevant kan zijn om vast te stellen wat de herkomst is. Daarnaast geldt overigens nog dat voor de sanctieregelingen van belang kan zijn tussen welke personen/partijen een transactie plaatsvindt (zodat aan de sanctielijsten kan worden getoetst).

[39] Dit kan zijn omdat er een mixer is gebruikt bij de (voorgaande) transacties, omdat de cryptovaluta afkomstig zijn van een *wallet* die op een 'black list' is opgenomen (bijvoorbeeld omdat die *wallet* eerder in verband is gebracht met criminele activiteiten) of omdat de cryptovaluta (direct of indirect) een link hebben met de *dark web*.

[40] Zie https://www.internetconsultatie.nl/besluitwijzigingamld4.

eenvoudig te koppelen aan een *wallet*. Bovendien kan bijvoorbeeld een ledger (een hardware wallet) fysiek worden doorgegeven aan een ander (door deze te overhandigen en de code te verstrekken). Van de crypto-instellingen wordt evenwel verwacht dat inzichtelijk wordt gemaakt van wie een wallet is die betrokken is bij een transactie. Als cryptovaluta worden overgemaakt van de ene wallet naar de andere wallet, is het de bedoeling dat de crypto-instelling van beide *wallets* vaststelt van wie de *wallet* is (en de betreffende relevante personen moet screenen ter uitvoering van de sanctieregelingen). Dit is een belangrijke maar ook uitdagende eis voor crypto-instellingen gelet op het ontbreken van een koppeling tussen een persoon/bedrijf en een *wallet*. Degene die toegang heeft tot de *wallet*, heeft ook de beschikking over de cryptovaluta. Kwaadwillende criminelen zullen door deze karaktereigenschap van *wallets* echter onzichtbaar kunnen blijven. In ieder geval zal de crypto-instelling om dit risico te beheersen maatregelen moeten nemen. Een instelling die koopt en verkoopt (in eigen naam) zal kunnen eisen dat de *wallet* en cryptovaluta van de betreffende persoon (cliënt) zijn. Dit kan worden verklaard door de betreffende persoon. Daarnaast kan de toegang tot de *wallet* worden aangetoond door bijvoorbeeld een transactie uit te voeren. Transacties naar derde partijen kunnen in dat geval worden uitgesloten (hoewel dat praktisch wellicht niet sluitend kan worden vastgesteld). De instelling maakt dan alleen cryptovaluta over naar de – bij de instelling bekende – *wallet* van de cliënt. Voor exchanges is het complexer om vorm te geven aan deze eis. De andere *wallet* kan immers worden aangehouden bij bijvoorbeeld een andere exchange (mogelijk een exchange in een derde land die niet onder soortgelijke anti-witwasregelingen valt).

De uitdagingen op dit vlak voor crypto-instellingen vloeien mede voort uit Aanbevelingen van de FATF.[41] Aanbeveling 15 luidt als volgt. *'To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations'*. Paragraaf 7(b) van de Interpretative Note (IRN) bij deze aanbeveling luidt als volgt[42]: '*Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to beneficiary VASPs and counterparts (if any), and make it available on request to appropriate authorities. It is not necessary for this information to be attached directly to virtual asset transfers. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities.*' De minister heeft hierover het volgende opgemerkt: '*VASP's [virtual asset service providers] moeten elkaar op de hoogte stellen van wie de verzendende en ontvangende partijen in de transactie zijn. Dit is cruciaal om daadwerkelijk in staat te zijn om verdachte transacties te kunnen identificeren en om te voorkomen dat illegale transacties plaatsvinden. Hierbij gaat het om beperkte informatie, namelijk de naam van verzender en begunstigde, het cryptoadres van verzender en begunstigde, en informatie om de verzender te identificeren. Deze verplichting is alleen van toepassing op transacties waarbij er zowel aan de verzendende als ontvangende kant VASP's zijn betrokken, en de benodigde informatie mag alleen worden gedeeld tussen de VASP's in de desbetreffende transactie.*'[43]

De cryptovalutamarkt is echter nog niet volgroeid en een onderling werkend systeem van informatiedeling is voor zover ons bekend op dit moment nog niet aanwezig. Het blockchain-systeem en cryptovaluta en *wallets* zijn in ieder geval op dit moment niet zo opgezet dat aan deze *travel rule* wordt voldaan (in beginsel wordt er juist geen data meegestuurd met een transactie). Om te voldoen zullen de crypto-instellingen dan onderling samen moeten werken en (vrijwillig) informatie moeten uitwisselen met andere exchanges. In deze fase lijkt dit lastig om te realiseren. Verschillende crypto instellingen in diverse staten zijn onderworpen aan verschillende implementaties van de anti-witwasrichtlijn. Daar komt bij dat er enkele grote exchanges zijn en daarnaast diverse kleinere partijen, waarbij de grote partijen wellicht zelf (kunnen) bepalen aan wie zij wel of niet de benodigde informatie ter beschikking stellen.[44] Mogelijk dat in de toekomst een centrale instelling een oplossing kan bieden, waar gegevens van *wallets* en de bijbehorende personen kunnen worden geregistreerd. De Aanbevelingen van de FATF en de IRN moeten nog worden omgezet naar regelgeving op Europees niveau. Het zou wenselijk zijn als (bij die gelegenheid) het voorgaande nader

[41] Zie http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[42] Zie hierover https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.

[43] Brief Minister van Financiën met kenmerk: 2019-0000094167.

[44] De zoektocht naar een oplossing lijkt vooral gelegd te worden bij de betreffende crypto-instellingen. Al zijn er wel partijen die claimen dat er een travel rule compliant systeem is.

wordt geregeld zodat crypto-instellingen in de toekomst beter in staat zijn om aan de vereisten op dit vlak te voldoen.[45]

4. Conclusie en vooruitblik

Cryptovaluta zijn en blijven gevoelig voor witwassen door de aard en kenmerken van cryptovaluta en *wallets*. De voorgestelde registratieplicht voor crypto-instellingen heeft tot gevolg dat crypto-instellingen moeten voldoen aan alle kernverplichtingen van de Wwft en daarnaast moeten beschikken over een integere en beheerste bedrijfsvoering. Dit zijn zware eisen, maar desondanks kunnen witwasrisico's niet geheel worden uitgesloten. Gelet op de karaktereigenschappen die zijn verbonden aan cryptovaluta en *wallets*, is het voor veel crypto-instellingen verder een uitdaging om aan alle Wwft-eisen te voldoen. Het kan voor criminelen, mede door de aard van de dienstverlening en de aard van cryptovaluta, interessant blijven om de crypto-instellingen te misbruiken voor witwasdoeleinden. Aan de andere kant zou de registratie ook een bepaalde verschuiving van de criminele/hoog risico cliënten en producten tot gevolg kunnen hebben naar niet geregistreerde partijen.

Voor andere instellingen, zoals banken, trustkantoren en accountantsorganisaties, geldt dat door de zware wettelijke eisen (transacties via) een geregistreerde crypto-instelling mogelijk een lager risicoprofiel zal kunnen hebben dan (transacties via) een niet geregistreerde crypto-instelling. Deze instellingen hebben echter een eigen verantwoordelijkheid om te waarborgen dat zij de Wwft en sanctieregelgeving naleven met betrekking tot de crypto-instellingen, om de daaraan verbonden integriteitsrisico's adequaat te kunnen beheersen en tevens om eigen betrokkenheid bij witwassen te voorkomen.[46] Zij zullen onder meer een eigen risicobeoordeling moeten maken en bepalen of zakelijke relaties met geregistreerde crypto-instellingen en/of cliënten die transacties via een geregistreerde crypto-instelling doen, passen binnen de eigen *risk appetite*. Daarbij zal de instelling met de kwetsbaarheden die thans nog aan de orde zijn rekening moeten houden.[47] Daarbij geldt dat thans bij een transactie door een geregistreerde instelling het regelmatig zal voorkomen dat in de keten niet geregistreerde instellingen betrokken zijn, onder meer omdat de vijfde anti-witwasrichtlijn nog niet overal is geïmplementeerd en transacties ook van buiten Europa kunnen komen en niet alle partijen onder het toepassingsbereik vallen.

Voor zover het gaat om een zakelijke relatie met een crypto-instelling kan voor de beoordeling informatie worden betrokken over procedures en maatregelen op het gebied van de Wwft en de sanctieregelgeving en de integere en beheerste bedrijfsvoering van de crypto-instelling, waarbij in de toekomst ook informatie over de werking van de procedures en maatregelen om naleving van de Wwft te waarborgen zal kunnen worden betrokken nu een auditverplichting wordt ingevoerd.

Door onder meer ervaringen in de sector, de auditverplichting en het doorlopend toezicht op crypto-instellingen, zal in de toekomst meer informatie beschikbaar zijn over de naleving van de Wwft en beheersing van witwasrisico's door crypto-instellingen. Dit artikel geeft dus nog maar een beginstand weer. Eerst is de Eerste Kamer aan zet om het wetsvoorstel ter implementatie van de vijfde anti-witwasrichtlijn wel of niet aan te nemen. We zijn nieuwsgierig naar wat de toekomst gaat brengen! ■

[45] Zie ook art. 65 lid 1 vijfde anti-witwasrichtlijn. Het verslag over de toepassing van deze richtlijn – uiterlijk op 11 januari 2022 – zal zo nodig vergezeld gaan van wetgevingsvoorstellen over een toegankelijke centrale database waarin de identiteit van portemonneeadressen van gebruikers worden geregistreerd, als ook zelfverklaringsformulieren ten behoeve van de gebruikers van virtuele valuta.

[46] Zij lopen immers het risico op strafrechtelijke aansprakelijkheid voor (faciliteren van) witwassen. Zie hierover ook: A.B. Schoonbeek, W.M. Shreki en M.T. van der Wulp, 'Bitcoins, witwassen & integriteitsrisico's', *TvCo* 2017, nr. 2, p. 88-95.

[47] Dit artikel bevat geen volledige beschrijving van potentiële kwetsbaarheden.