Tijdschrift voor

COMPLIANCE

JAARGANG 22 - JUNI 2022 **3**

DEN HOLLANDER

Vingerwijzen, bijten zonder tanden en gebrek aan verantwoordelijkheidsgevoel: falend toezicht en regelgeving in een cryptowereld vol risico

P. Engering en L.J.H. Kort[1]

De adoptie van virtuele valuta (hierna aangeduid met crypto's) in de Nederlandse economie neemt toe. Naar schatting hebben momenteel 1.2 miljoen Nederlanders crypto's opgenomen in hun beleggingsportfolio.[2] Uit onderzoek onder jongeren van 18 tot en met 30 jaar uitgevoerd door het Nationaal Instituut voor Budgetvoorlichting (Nibud) en de Rabobank,[3] blijkt dat 25% van de respondenten belegt in crypto. Daarnaast blijkt uit berichtgeving van onder andere NOS[4] dat er een toename is van het aantal minderjarigen in handel in crypto. Ook bij het aantal bedrijven dat crypto's op de balans zet is een toename te zien. Bij een aantal grote buitenlandse bedrijven, zoals Tesla en MicroStrategy, is dit inmiddels bekend. Informatie over het aantal Nederlandse bedrijven en hun gemiddelde inleg lijkt momenteel relatief beperkt.

Crypto's worden met grote regelmaat omschreven als 'een anoniem online gebeuren' of vergeleken met piramidespelen of tulpenmanie[5]. Echter, de trendontwikkeling laat zien dat crypto 'here to stay' is. Het kan toegevoegde waarde leveren aan het huidige financiële stelsel en biedt tevens hulp bij humanitaire rampen. Op 26 februari jl. werd op het officiële Twitteraccount van Oekraïne een oproep[6] geplaatst voor het doneren van crypto's voor humanitaire doeleinden in hun oorlog tegen Rusland. Kort daarna werd bekend gemaakt dat het land uiteindelijk meer dan €55 miljoen heeft opgehaald. Het is echter belangrijk om niet alleen aandacht te hebben voor de kansen, maar vooral ook de risico's die crypto's met zich meebrengen, zoals witwassen, mogelijke omzeiling van sanctiewetgeving en cybercriminaliteit.

In het verleden hebben diverse instanties zoals De Nederlandsche Bank (DNB), Autoriteit Financiële Markten (AFM), de Financiële Inlichtingen- en Opsporingsdienst (FIOD), het Anti Money Laundering Centre (AMLC) en de Financial Action Task Force (FATF) gewaarschuwd voor de significante risico's van crypto's. De FIOD refereert in haar rapport in 2020 (niet publiek toegankelijk) over financial cybercrime aan een studie door Sean Foley, Jonathan R Karlsen en Talis J. Putnins[7] (mei 2019) dat een kwart van de Bitcoin-gebruikers en 46% van de Bitcoins betrokken zou zijn bij illegale activiteiten. Tegelijkertijd verschijnen meer rapporten waarin juist wordt geconcludeerd dat de risico's van crypto's minimaal zijn, zeker als we dit afzetten tegen het criminele gebruik van cash geld. Concludeerde Chainanalysis over 2020[8] nog dat het percentage criminele transacties met crypto's lag op 0,34% van alle transacties, in 2021[9] heeft zij dit percentage moeten corrigeren naar 0,62%. Feit is dat Chainalysis vaak wordt geciteerd, maar de vraag is hoe volledig zij kunnen zijn in hun analyses.

Het is onzeker in hoeverre de percentages volledig en betrouwbaar zijn en hoe deze cijfers uit genoemde onderzoeken tot stand zijn gekomen. Hier speelt tevens het in de criminologie bekende *'dark number of*

1. Peter Engering en Leon Kort hebben 14 respectievelijk 8 jaar consultancy ervaring op het gebied van Compliance Risk Management bij financiële instellingen. Samen zijn zij in februari 2022 Compliance Champs B.V. gestart met een focus op Know Your Customer (KYC) en Cryptocurrency Financial Crime Risk Management bij financiële instellingen en aanbieders van cryptodiensten. Zie voor meer informatie www.compliancechamps.com.
2. https://www.ipsos.com/nl-nl/12-miljoen-nederlanders-hebben-crypto-helft-investeert-minder-dan-eu500
3. https://www.nibud.nl/onderzoeksrapporten/rapport-jongvolwassenen-en-beleggen-2021-2/
4. https://nos.nl/artikel/2386328-ook-minderjarigen-in-cryptohandel-ik-dacht-snel-winst-te-kunnen-maken
5. https://www.riskcompliance.nl/news/crypto-en-tulpenmanie/
6. https://tinyurl.com/3s67va5d
7. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? | The Review of Financial Studies | Oxford Academic (oup.com)
8. https://go.chainalysis.com/2021-Crypto-Crime-Report.html
9. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

crime' een rol: *dat deel van de niet-geregistreerde criminaliteit dat op dit moment niet vanuit andere registraties of instrumenten bekend is of geschat kan worden*[10].

Criminelen zijn innovatief in het omzeilen van het toezicht door gebruik te maken van de nieuwste technologische ontwikkelingen zoals crypto's. Criminele activiteiten zoals witwassen vinden plaats met crypto's (virtueel geld) net zoals dat gebeurt met gewoon geld (fiduciair geld, zoals contant geld of digitale geldstromen). Maar hoe risicovol zijn die crypto's nu eigenlijk en hoe effectief is het toezicht? Dit artikel gaat in op de belangrijkste integriteitsrisico's rondom cryptotransacties en de belangrijkste problemen rondom het toezicht op crypto's. Hierbij wordt ook getracht om enkele mogelijke oplossingen voor deze problemen te beschrijven.

1. Belangrijkste integriteitsrisico's van crypto's

Hieronder worden verschillende integriteitsrisico's nader uitgewerkt.

1.1. Witwassen

Criminelen gebruiken verschillende methoden om hun identiteit en de herkomst van hun criminele gelden te verhullen. Het gebrek aan gedegen witwascontroles maakt de cryptomarkt aantrekkelijk voor criminelen. Een aantal indicatoren voor het witwassen van geld via crypto wordt hieronder uitgelicht. Zie voor meer indicatoren onder meer de publicaties van het AMLC[11] of de FATF.[12]

1.1.1. Transacties met of van internationale goksites

Het is strafbaar om te gokken bij buitenlandse aanbieders van online gokspelen. Dit is echter gemakkelijk te omzeilen met een VPN-verbinding, waarbij het IP-adres, en dus de fysieke locatie van de gebruiker, wordt versleuteld. Op meerdere Nederlandse cryptowebsites wordt aangeraden om bij alle cryptotransacties een VPN-verbinding te gebruiken om de identiteit te beschermen tegen bijvoorbeeld overheidsinstanties. Zoals op de site nl.cryptonews.com is vermeld: *'Het is een algemeen aanvaard feit dat privacy een fundamenteel mensenrecht is onder beschaafde mensen."*[13]. Dergelijke VPN-verbindingen zouden ook gebruikt kunnen worden bij transacties met goksites. Een artikel van Follow the Money[14] over illegale online casino's in Curaçao toont aan dat er een groot vermoeden is dat deze casino's worden gebruikt voor witwassen. Bij deze casino's kan met crypto betaald worden waardoor crypto bij witwaspraktijken betrokken zou kunnen worden. Dit in tegenstelling tot de gereguleerde Nederlandse casino's waar crypto niet als betaalmiddel geaccepteerd wordt. Internationale goksites vormen hierdoor een belangrijk witwasrisico.

1.1.2. Virtual Asset ATM's

Wereldwijd zijn er inmiddels ruim 30.000 zogeheten Virtual Asset ATM's.[15] Dit zijn geldautomaten waarmee contant geld kan worden omgewisseld in crypto. In Nederland zijn deze ook aanwezig en geregistreerd bij DNB. De toegevoegde waarde van deze geldautomaten is onduidelijk aangezien 10% marge wordt berekend terwijl via een online aanbieder dit veelal onder de 2% ligt. Onderzoek wijst uit dat deze automaten internationaal veelvuldig gebruikt worden voor fraude en het witwassen van criminele gelden.[16] Bijvoorbeeld via smurfen, waarbij de witwasser criminele gelden in het financiële systeem brengt door het geld in kleine sommen op te delen en op verschillende rekeningen te storten. Vanwege dergelijke risico's heeft de Financial Conduct Authority (FCA) de aanbieders van Virtual Asset ATMs in het Verenigd Koninkrijk recent gesommeerd hun activiteiten te stoppen. Daarnaast accepteert de Verenigde Bitcoinbedrijven Nederland (VBNL)[17] geen partijen als lid die handelen met contant geld en daardoor dus ook geen aanbieders van Virtual Asset ATM's.

1.1.3. Non-Fungible Tokens (NFTs)

NFTs zijn unieke digitale eigendomsbewijzen op de blockchain, bijvoorbeeld in relatie met digitale kunstwerken. Net als in de handel met traditionele kunst wordt de waarde bepaald door wat de koper er voor wil betalen. In de digitale wereld kan men zich hierbij verschuilen achter een walletadres[18]. Hierdoor kan een investeerder een digitale asset kopen en verkopen in een kort tijdsbestek onder dezelfde condities waardoor de prijs kunstmatig wordt opgedreven. Dit fenomeen wordt aangeduid met *wash*

10. Coleman, C., & Moynihan, J., 1996, Understanding crime data: haunted by the dark figure, Buckingham, Open University Press.
11. https://www.amlc.nl/indicatoren-voor-het-witwassen-van-geld-via-cryptocurrency/
12. https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html
13. https://nl.cryptonews.com/guides/moet-ik-vpn-gebruiken-voor-cryptocurrency-transacties.htm
14. https://www.ftm.nl/artikelen/casinos-op-curacao?share=67XvNTQAJoCHmb6b%2BXegPF9pOqf3R5LGcqlMPZSJNfGzpyVcEqY2oAEM8PuicPU%3D
15. https://coinatmradar.com/countries/
16. https://www.cnbc.com/2021/11/09/bitcoin-atms-criminals-target-cryptocurrency-transactions.html
17. Het doel van VBNL is het bewaken van de kwaliteit van de aangesloten Bitcoin bedrijven in Nederland door het bevorderen van zelfregulering en het voorkomen en bestrijden van Bitcoin gerelateerde fraude (www.verenigdebitcoinnederland.org) .
18. Een walletadres is een digitaal adres (in de vorm van een unieke identificatiecode) waar crypto's worden opgeslagen. Dit is vergelijkbaar met een bankrekeningnummer.

trading. Hiermee krijgt het bedrag een ogenschijnlijk legitieme herkomst. Dit zou mogelijk door middel van data-analyse wel opgespoord kunnen worden.[19]

1.1.4. Mixers

Een mixer, ook wel een *tumbler* genoemd, is een middel om de anonimiteit bij het gebruik van crypto's te vergroten. Er zijn twee hoofdtypen crypto mixers:

1. Gecentraliseerde mixers zoals BitLaundry;
2. Gedecentraliseerde mixers zoals Wasabi.

Cryptotransacties worden vastgelegd op de blockchain, waardoor de herkomst van crypto's te achterhalen is. Door een mixer te gebruiken is de transactiegeschiedenis (aard, omvang, wallets en partijen) niet te zien noch te reconstrueren. *Mixing services* opereren vaak vanuit landen met beperkte witwascontroles en lopen ter bevordering van de anonimiteit vaak via een Tor netwerk. Een Tor netwerk betreft een open netwerk voor anonieme communicatie gebaseerd op een techniek genaamd *onion routing*.[20] *Mixing services* hebben vaak weinig verhullende namen zoals, BitLaundry, waaruit impliciet blijkt voor welke activiteiten deze services voornamelijk worden gebruikt. Mixers zoals Wasabi worden echter ook gebruikt door idealistische gebruikers om hun privacy te beschermen.

1.2. Terrorismefinanciering

De prikkel voor terroristische organisaties om cryptocurrencies te gebruiken zit grotendeels in de anonimiteit en het gebrekkig toezicht. Criminelen kiezen vaak de weg van de minste weerstand. Waar in Europa de regelgeving voor strengere *Know Your Customer (KYC)* en transactiemonitoring vereisten heeft gezorgd, is dit niet overal ter wereld het geval. Uit een artikel van The Diplomat blijkt dat de vereisten in Azië ver achterblijven.[21] Dit zorgt ervoor dat criminele activiteiten, waaronder terrorismefinanciering, mogelijk naar deze landen verschuiven. Redenen voor het verminderen van het gebruik van crypto's voor financiers van terrorisme zijn de prijzen, de geleidelijke versterking van internationale organisaties en nationaal toezicht en de constante stroom aan cyberaanvallen. Daarnaast functioneren traditionele middelen voor het financieren van terrorisme nog steeds goed genoeg om fondsen op te halen voor terroristische organisaties. Daarom lijkt het gebruik van cryptocurrencies door terroristische organisaties nog beperkt.[22]

> Daarom lijkt het gebruik van cryptocurrencies door terroristische organisaties nog beperkt.

Dit wordt bevestigd in het Crypto Crime Report 2022 van Chainalysis[23] waarbij de kanttekening moet worden geplaatst hoe volledig zij kunnen zijn in hun analyses.

1.3. Omzeilen van sanctiewet- en regelgeving

Volgens persbureau Bloomberg[24] heeft de voorzitter van de Europese Centrale Bank (ECB), Christine Lagarde, financiële instellingen gewaarschuwd voor de omzeiling van sanctiewet- en regelgeving met crypto door Russische oligarchen. Dit wordt echter betwist door Jonathan Levin, co-founder van Chainalysis,[25] die aangeeft dat er onvoldoende bewijs is dat dit op systematische wijze gebeurt. Het is volgens hem wel mogelijk dat dit gebeurt, maar niet op de schaal die door Lagarde werd gesuggereerd. Omdat de cryptobedrijven ook moeten voldoen aan de Sanctiewet zullen zij deze transacties niet willen faciliteren. Zo kreeg het cryptobedrijf BitGo in 2020 een boete van ongeveer 100,000.00 dollar voor het faciliteren van transacties met een totale waarde van 9,127.79 dollar. De boete was ruim 10 keer zo hoog als de totale waarde van de transacties. Via peer-to-peer betalingen zoals LocalBitcoins.com, via VPN-verbindingen of via nieuwe accounts die nog niet gelinkt zijn aan een gesanctioneerd persoon, blijkt sanctieomzeiling echter nog steeds mogelijk.

> Via peer-to-peer betalingen zoals LocalBitcoins.com, via VPN-verbindingen of via nieuwe accounts die nog niet gelinkt zijn aan een gesanctioneerd persoon, blijkt sanctieomzeiling echter nog steeds mogelijk.

Gesanctioneerde personen kunnen kiezen voor crypto exchanges die zich minder houden aan de geldende wet- en regelgeving. Grote exchanges als Coinbase en Binance hebben aangegeven niet de accounts te willen blokkeren van alle klanten met de Russische nationaliteit.[26] Zij zijn van mening dat er niet op basis van nationaliteit gediscrimineerd kan worden en iedereen toegang zou moeten hebben tot financiële dienstverlening.

19. blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/
20. Onion routing is een techniek voor anonieme communicatie voor een computernetwerk. Berichten worden herhaaldelijk versleuteld en vervolgens verzonden via verschillende netwerknodes genaamd onion routers.
21. https://thediplomat.com/2022/02/cryptocurrency-and-terrorist-financing-in-asia/
22. https://academic.oup.com/policing/article/15/4/2329/6365869
23. https://go.chainalysis.com/2022-Crypto-Crime-Report.html
24. https://www.bloomberg.com/news/articles/2022-03-22/ecb-s-lagarde-says-cryptos-being-used-to-evade-russian-sanctions
25. https://www.bloomberg.com/news/articles/2022-03-17/crypto-experts-say-no-evidence-of-major-russia-sanctions-dodging
26. https://www.reuters.com/technology/coinbase-not-banning-russians-using-platform-ceo-says-2022-03-04/

1.4. Belastingontduiking

In Nederland bestaat de verplichting om crypto's aan te geven bij de belastingdienst[27]. Omdat crypto digitaal is, bestaat de mogelijkheid om deze overal ter wereld te verhandelen en op te slaan. Aangezien dit geld is dat voor de Belastingdienst moeilijk te traceren is, werkt dit het ontduiken van vermogensbelasting in de hand. Nederlandse aanbieders van cryptodiensten dienen in het kader van hun renseigneringsplicht het opgebouwde vermogen van hun klanten vrij te geven wanneer deze worden opgevraagd door de Nederlandse Belastingdienst.
Wetgeving met betrekking tot de internationale informatiedeling tussen exchanges is echter nog niet ingeregeld. De Organisatie voor Economische Samenwerking en Ontwikkeling (OECD) werkt momenteel aan een voorstel om een *Crypto-Asset Reporting Framework* (CARF) te creëren binnen de Europese Unie voor de automatische uitwisseling van informatie tussen landen van crypto-activa en aanpassingen te maken aan de *Common Reporting Standard* (CRS) om belastingontduiking tegen te gaan.[28] Om gerelateerde risico's te mitigeren kunnen financiële instellingen er voor kiezen om cryptotransacties alleen toe te staan bij aanbieders van cryptodiensten die voldoen aan de vereisten van de CRS. Deze mogelijke oplossing zal echter niet geliefd zijn onder fanatieke cryptoliefhebbers en zal zeer lastig zijn om te implementeren. Een vergelijkbaar voorbeeld komt uit de gokwereld. Met ingang van 1 oktober 2021 is de Wet Kansspelen[1] op afstand van kracht. Hierdoor is het voor Nederlanders mogelijk om in Nederland legaal online te gokken bij aanbieders van online kansspelen die een vergunning hebben bij de Kansspelautoriteit. Het is strafbaar (risico op een boete van 8.700 euro[1]) om te gokken bij een gokbedrijf zonder vergunning (lees: ook om te gokken bij buitenlandse aanbieders van online gokspelen).
Naast CARF zal ook de nieuwste richtlijn voor administratieve samenwerking op het gebied van belastingen, de *Directive for Administrative Cooperation 8* (DAC8), naar verwachting dit jaar worden ingevoerd.[29] De publieke consultatie is reeds gesloten in juni 2021. Deze richtlijn zal de aanbieders van cryptodiensten verplichten om de gegevens van haar klanten met de belastingautoriteiten te delen. Het probleem blijft overigens nog steeds dat partijen buiten de EU niet aan deze regels hoeven te voldoen en dat het gestalde vermogen bij bijvoorbeeld een Binance account buiten zicht blijft.

Deze richtlijn zal de aanbieders van cryptodiensten verplichten om de gegevens van haar klanten met de belastingautoriteiten te delen. Het probleem blijft overigens nog steeds dat partijen buiten de EU niet aan deze regels hoeven te voldoen

Belastingregels verschillen per land en zijn voornamelijk buiten de EU minder streng.

1.5. Cybercriminaliteit

De anonimiteit en snelheid van cryptotransacties, het wereldwijde en grensoverschrijdende karakter en het gebrek aan toezicht maken crypto's ook een interessant doelwit voor cybercriminelen. Hieronder worden enkele manier beschreven waarop cybercriminelen hun voordeel halen uit crypto's.

1.5.1. Ransomware (gijzelsoftware)

Bij een ransomware aanval stelen hackers intellectueel eigendom of persoonsgegevens. Veelal wordt door cybercriminelen crypto als losgeld gevraagd in ruil voor toegang tot de geïnfecteerde systemen. Dit is een snelle, effectieve en ogenschijnlijk anonieme manier om geld over te maken. Vaak wordt er na het ontvangen van de crypto gebruik gemaakt van een Bitcoin mixer waardoor de herkomst van het vermogen moeilijk traceerbaar is.

1.5.2. Hacks en diefstal

Ook (persoonlijke) wallets, platformen en exchanges zijn kwetsbaar voor cyberaanvallen. Door een hack kunnen onbevoegden toegang krijgen tot belangrijke (persoons) gegevens, zoals wachtwoorden of private keys, waardoor de crypto's van wallets of exchanges zijn te halen. Zo vond in maart 2022 bij *gaming-focused* blockchain platform Ronin Network[30] de een na grootste hack, ter waarde van 600 miljoen dollar, plaats. Interessant genoeg staan de crypto's nog op de wallet waar het na de hack naartoe is gestuurd en is dit adres aangemerkt als 'betrokken' bij de hack.[31]
Het Crypto Crime Report 2022 van Chainalysis[32] heeft aangegeven dat in 2021 voor 3.2 miljard dollar aan crypto's is gestolen. Dit is zes (!) keer zoveel als in 2020. In de cryptowereld bestaat de definitie van *'rug pull'*, wat letterlijk betekent: 'het vloerkleed onder je vandaan trekken.' Hierbij wordt een project of token gehypet (of de koers van een token opgedreven) voordat de eigena(a)r(en) er vandoor gaan met

27. https://www.belastingdienst.nl/wps/wcm/connect/nl/werk-en-inkomen/content/cryptovaluta
28. https://www.oecd.org/ctp/exchange-of-tax-information/oecd-seeks-input-on-new-tax-transparency-framework-for-crypto-assets-and-amendments-to-the-common-reporting-standard.htm
29. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Belastingfraude-en-ontwijking-aanscherping-van-de-regels-voor-administratieve-samenwerking-en-uitbreiding-van-de-uitwisseling-van-informatie_nl
30. https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/?sh=2e8f26452686
31. https://etherscan.io/address/0x098b716b8aaf21512996dc57eb0615e2383e2f96
32. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

het geld en zonder dat de investeerders hier geld aan overhouden. Een voorbeeld komt uit april 2021 waar de eigenaar van de Turkse exchange Thodex twee miljard dollar heeft gestolen van ongeveer 400.000 gebruikers en naar verluid is vertrokken naar Albanië.[33]

1.5.3. Cryptojacking

Cryptojacking, ook wel kwaadaardige cryptomining genoemd, is een opkomende online dreiging die zich op een computer of mobiel apparaat verbergt en de rekenkracht van het apparaat gebruikt om crypto's te 'delven'. Hiermee kunnen criminelen webbrowsers overnemen en allerlei apparaten binnendringen, van desktops en laptops tot smartphones en zelfs netwerkservers. In februari 2018 infiltreerden cybercriminelen enkele honderden Kubernetes-beheerconsoles van Tesla die toegankelijk waren zonder wachtwoordbeveiliging.

Omdat alle transacties altijd op de blockchain zichtbaar blijven, wordt het in de toekomst steeds lastiger voor criminelen om crypto's uit te laten keren vanuit een aanbieder van cryptodiensten. Dit komt mede doordat er steeds meer applicaties op de markt beschikbaar zijn die de transacties op de blockchain volgen.

> Zodra de wallet gegevens bekend zijn kunnen cryptotransacties worden gelinkt aan crimineel gedrag en specifieke personen. Er zijn een aantal mogelijkheden om dit te omzeilen

Zodra de wallet gegevens bekend zijn kunnen cryptotransacties worden gelinkt aan crimineel gedrag en specifieke personen. Er zijn een aantal mogelijkheden om dit te omzeilen:

1. De crypto in contanten verkopen. Particulieren hebben hierbij soms niet door dat dit een vorm van (digitale) heling is;
2. Via zogeheten peer-to-peer betalingen, zoals LocalBitcoins.com, waarbij twee individuen zonder tussenkomst van een derde partij crypto's kunnen omwisselen tegen fiat geld. Dit platform wordt ook veelvuldig gebruikt voor het witwassen van geld;
3. De crypto's online uitgeven bij bedrijven die deze betalingen accepteren;
4. Crypto's die worden uitgegeven middels een crypto creditcard waarbij gedurende de transactie crypto wordt omgezet in fiat geld.

33. https://www.bloomberg.com/news/articles/2021-04-22/turks-suspect-massive-crypto-losses-as-exchange-ceo-goes-missing

1.6. Private key verloren of vergeten

Een risico waar nog vaak aan voorbij wordt gegaan is het kwijtraken van crypto (in essentie de private key – de 'toegangsgegevens' voor de wallet) op het moment dat de crypto niet zijn opgeslagen bij een aanbieder van cryptodiensten. Percentages variëren per crypto maar voor bijvoorbeeld Bitcoin zijn percentages tot 20 % van alle beschikbare Bitcoin genoemd. Als deze gegevens kwijt zijn dan is het niet meer mogelijk om toegang te krijgen. Een bekend verhaal is dat van de Duitse programmeur Stefan Tomas die het wachtwoord kwijt is van zijn hardware wallet apparaat IronKey waar 7002 Bitcoin op staan (met een huidige waarde van 280 miljoen euro).[34]

1.7. Marktmisbruik

Het aantal voorbeelden waarbij sprake is van marktmisbruik (marktmanipulatie en/of handel met voorkennis, hetgeen bij beleggen bij wet verboden is[35]) neemt schrikbarend toe. Bijvoorbeeld middels een Initial Coin Offering (ICO's), het crypto equivalent van een Initial Public Offering (IPO) bij aandelen, waarbij geld wordt opgehaald als investering. Een mogelijkheid is via tokens. Een bekend voorbeeld is de Xpose token, waarbij allerlei 'finfluencers'[36] via sociale media de cryptomunt aanprezen zonder dat zij bewezen kennis hebben van het product of de cryptowereld. Van voormalig Ajax-directeur Marc Overmars tot aan Kroatisch international Ivan Rakitić en rapper Boef. Achteraf lijkt mogelijk sprake te zijn van oplichting. Deze reclamecampagnes zijn, zoals uit een aflevering van radar is gebleken, niet gebonden aan regelgeving.[37]

1.8. Gebrek aan kennis bij (jonge) beleggers en volatiliteit

Onderzoek van de FCA[38] heeft aangetoond dat in 2021 zo'n 38 % (tegenover 47 % in 2020) van de consumenten crypto koopt als een gok waarmee geld kan worden verdiend of verloren. Het rapport geeft ook indicaties dat steeds meer mensen crypto kopen zonder dat zij voldoende verstand hebben van crypto en de risico's die dit met zich meebrengen. Dit sluit aan bij de uitkomsten van het eerder in dit artikel genoemde rapport van de Nibud en Rabobank. In een recent artikel van het Financieel Dagblad wordt

34. https://vanguard-x.com/blockchain/lost-millions-in-bitcoin/
35. www.rijksoverheid.nl/onderwerpen/financiele-sector/gezonde-financiele-sector/verbod-op-marktmisbruik-en-handel-met-voorkennis
36. Finfluencers zijn influencers die zich op sociale media specifiek uitspreken over beleggen (www.afm.nl/nl-nl/nieuws/2021/december/verkenning-finfluencers)
37. radar.avrotros.nl/uitzendingen/gemist/item/deze-cryptomunt-maakt-jou-volgend-jaar-miljonair/
38. https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021

ook gewaarschuwd voor de verslavingsgevoeligheid onder jongeren waarbij het investeren wordt gezien als een spelletje ('*gamification*').[39] Vanwege het beperkte toezicht is het relatief eenvoudig om een rekening te openen bij een aanbieder van crypto's, zowel in Nederland als in het buitenland. Vervolgens is het eenvoudig is om bij partijen als Binance zeer risicovolle producten te kopen, zoals hefbomen,[40] of om crypto te lenen tegen een onderpand met rentepercentages boven de 20 %. De hoge volatiliteit is bij crypto's een groot risico. Een koersdaling of –stijging van meer dan 10% vindt geregeld plaats en het is dus van belang dat de (jonge) belegger op de hoogte is van de risico's tijdens het investeren.

2. Problemen in wet- en regelgeving en integriteitstoezicht op crypto's

De cryptowereld zit vol risico en vraagt hierdoor om gedegen toezicht. In de praktijk lijkt toezicht zeer beperkt aanwezig en wijzen de toezichthouders naar elkaar. Hieronder worden enkele actuele problemen geschetst.

2.1. Ontbreken van wettelijke verankering en toezicht

2.1.1. Onvoldoende toezicht op registratieplicht

Sinds 21 mei 2020 vallen bedrijven die diensten aanbieden voor het wisselen tussen crypto's en gewoon geld en bedrijven die cryptobewaarportemonnees aanbieden op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna: 'Wwft') onder het integriteitstoezicht van DNB. Aanbieders van cryptodiensten die in of vanuit Nederland actief willen worden, moeten een inschrijving in het openbaar register van DNB aanvragen. Hierbij gelden toelatingseisen die men normaal bij een vergunning zou verwachten, zoals een betrouwbaarheids- en geschiktheidstoets voor bestuurders, mede-beleidsbepalers, commissarissen en houders van een gekwalificeerde deelneming (aandelen >10%). Toezicht op de registratieplicht vindt echter niet altijd plaats. Een voorbeeld is Coinbase, een partij uit de Verenigde Staten zonder registratie in Nederland waarvan de Ideal-betalingen gewoon worden geaccepteerd. Tevens had Coinbase kort geleden nog een Nederlandse website[41]. De Nederlandse vertaling van de website is inmiddels verwijderd, mogelijk naar aanleiding van een melding van VBNL.

2.1.2. Ontbreken van wettelijke verankering

Daarnaast moeten deze bedrijven, net als financiële instellingen, voldoen aan de Wwft en de Sanctiewet 1977 (Hierna: 'Sanctiewet'). Hiermee wordt geïmpliceerd dat deze bedrijven als volwaardige poortwachters moeten worden gezien. Echter, er vindt geen prudentieel toezicht door DNB of (gedrags)toezicht door AFM plaats op deze bedrijven. Dit betekent dat er geen toezicht wordt gehouden op financiële bedrijfsrisico's en er geen sprake is van specifieke financiële consumentenbescherming, zoals dit bijvoorbeeld met het depositogarantiestelsel bij banken wel het geval is. Oorzaak hiervoor is het ontbreken van een wettelijke basis in de Wet op het financieel toezicht (Wft).

Om als product binnen het toepassingsbereik van de Wft te vallen, moeten crypto's gekwalificeerd zijn als financieel product (zoals een beleggingsobject, betaalrekening, elektronisch geld, financieel instrument en krediet) of geldmiddel (zoals chartaal geld, giraal geld en elektronisch geld)[42]. Crypto's zijn op dit moment niet te kwalificeren als financieel product of geldmiddel en vallen in beginsel dus niet onder toezicht. Hiermee is crypto in Nederland ook niet aangemerkt als wettig betaalmiddel. Niettemin kunnen activiteiten en diensten met betrekking tot crypto de aanbieder ervan onder voorwaarden toch binnen de reikwijdte van de Wft brengen. Voorbeelden van dergelijke activiteiten zijn:

1. Het handelen in cryptovaluta via een platform door middel van het optreden als tussenpersoon bij de aan- en verkoop van cryptovaluta;
2. Het verlenen van diensten met betrekking tot producten met cryptovaluta als onderliggende waarde; en
3. Het aanbieden van participaties van een fonds dat investeert in cryptovaluta.

Afhankelijk van de structuur en inhoud van de aangeboden activiteiten moet case-by-case worden bepaald of deze activiteiten onder toezicht vallen. Sommige producten die verband houden met crypto's kunnen bijvoorbeeld als financieel instrument gekwalificeerd worden waardoor bepaalde diensten binnen het toepassingsbereik van de Wft vallen. Ook structuren van bepaalde activiteiten die betrekking hebben op crypto's kunnen onder toezicht vallen, zoals het laten deelnemen van beleggers in een cryptofonds.

39. https://fd.nl/financiele-markten/1417938/beleggen-is-als-gamen-voor-de-jonge-roekeloze-beursgokker-lkd2ca9EqgMx
40. Met een hefboomproduct kan met een relatief geringe investering worden ingespeeld op een koersstijging of koersdaling. Door de hefboomwerking, die zelfs tot 100 kunnen gaan waarbij de positie dus 100 (!) keer zo groot is als de inleg, zijn dit type producten risicovoller dan een indirecte belegging in de onderliggende waarde.
41. https://www.coinbase.com/
42. https://www.barentskrans.nl/assets/uploads/2018/06/Cryptovaluta-wel-of-niet-onder-toezicht_VFP_2018-06.pdf

2.1.3. *De gevolgen*

Het ontbreken van een wettelijke basis leidt tot de vraag wat de exacte rol is van toezichthouders zoals DNB, AFM en de Autoriteit Consument en Markt (ACM).

Het ontbreken van een wettelijke basis leidt tot de vraag wat de exacte rol is van toezichthouders zoals DNB, AFM en de Autoriteit Consument en Markt (ACM)

AFM geeft aan nog niet formeel te kunnen optreden tegen misleidende video's, posts op social media en reclames ten aanzien van crypto[43], zoals ze dat wel kunnen bij foutieve informatie over beleggen.[44] Medewerkers van AFM gaan daarom de komende maanden voorlichting geven op scholen om leerlingen te waarschuwen voor de risico's van crypto. Daarnaast heeft de AFM slechts gewaarschuwd voor finfluencers.[45] Dit zorgt er echter niet voor dat het probleem wordt aangepakt bij de bron. Het programma Radar nam in een uitzending van 13 september 2021[46] ook terecht onder de loep hoe makkelijk het is om crypto's aan te maken en de gevaren van het ontbreken van toezicht door de AFM op deze malafide praktijken. Het is wachten op nadere wet- en regelgeving en op meer inzichten van de toezichthouders hoe financiële instellingen hiermee om zouden moeten gaan. Momenteel is wetgeving, zoals de Markets in Crypto Assets Regulation (MiCAR), in ontwikkeling. De invoering is inmiddels uitgesteld van 2024 naar op z'n vroegst 2025. Het is door dergelijke vertragingen een uitdaging om wet- en regelgeving aan te laten sluiten op de snelle technologische en decentrale ontwikkelingen in de markt. In de tussentijd wijst de AFM in een reactie op de uitzending van radar van maandag 11 april 2022[47] naar de Minister van Financiën, die weer wijst naar DNB en de AFM[48], en ondertussen blijven criminelen gebruik maken van de mankementen in het financiële systeem.

2.1.4. *Mogelijke oplossing*

Andere toezichthouders hebben inmiddels geen afwachtende houding. De Comisión Nacional del Mercado de Valores (CNMV) de Spaanse tegenhanger van de AFM, heeft in februari van dit jaar de verplichting opgenomen om cryptogerelateerde reclamecampagnes die gericht zijn op meer dan 100.000 mensen vooraf te controleren. Zij dienen hiervoor minimaal 10 dagen van tevoren over geïnformeerd te worden.[49] De Financial Conduct Authority (FCA), de Britse tegenhanger van de AFM, heeft daarnaast in januari 2022 al grote stappen gezet met een consultatiedocument[50] waar tot 23 maart jl. op gereageerd kon worden en deze zomer definitief moet zijn. Doel van dit document is consumenten te beschermen tegen onduidelijke, niet eerlijke en misleidende reclame bij investeringen die een hoog risico met zich meedragen (incl. crypto's). De Nederlandse toezichthouders lopen erg achter en zouden ook een vergelijkbaar consultatiedocument moeten voorleggen aan de belangrijke stakeholders in de industrie.

Daarnaast zou het onderzoekswaardig zijn om ICO's of de verkoop van tokens te scharen onder Wwft artikel 23b, eerste lid: *Een ieder die in of vanuit Nederland beroeps- of bedrijfsmatig diensten aanbiedt voor het wisselen tussen virtuele valuta en fiduciaire valuta registreert zich bij de Nederlandsche Bank,* en artikel 23c lid 3: *Een aanbieder als bedoeld in artikel 23b kan enkel diensten als bedoeld in dit hoofdstuk aanbieden indien hij geregistreerd is.* Hierdoor zou men voor het aanbieden van tokens (er is immers sprake van het wisselen tussen virtuele valuta en fiduciaire valuta) een registratie moeten hebben waar DNB toezicht op dient te houden. Een andere mogelijkheid is de verankering van crypto's als financieel instrument of geldmiddel waardoor crypto's onderdeel worden van de Wft.

2.2. Onduidelijkheid over de poortwachtersrol ten aanzien van crypto's

Financiële instellingen en crypto dienstverleners verlenen hun klanten toegang tot 'financiële' producten. Vanuit wet- en regelgeving wordt van hen verwacht dat ze actief zijn in het voorkomen van misbruik van het financiële systeem. Dit wordt ook wel aangeduid met de 'poortwachtersrol'.

2.2.1. *Poortwachtersrol en informatieasymmetrie*

Een belangrijk vraagstuk is hoe de poortwachtersrol van een financiële instelling, zoals een bank of betaaldienstverlener[51], zich verhoudt tot de poortwachtersrol van een aanbieder van cryptodiensten.

43. https://www.afm.nl/nl-nl/professionals/veelgestelde-vragen/innovationhub/cryptovaluta-onder-tz
44. https://amp.nos.nl/artikel/2423184-les-over-cryptomunten-moet-mbo-ers-wapenen-tegen-verleiding-snelle-geld.html
45. https://www.afm.nl/nl-nl/nieuws/2021/december/verkenning-finfluencers
46. https://radar.avrotros.nl/uitzendingen/gemist/item/pas-op-zo-simpel-is-het-om-een-cryptotoken-te-maken/
47. radar.avrotros.nl/uitzendingen/reacties/item/cryptoreclames-reactie-autoriteit-financiele-markten/
48. www.rijksoverheid.nl/documenten/kamerstukken/2021/11/02/antwoorden-op-kamervragen-over-het-toezicht-op-de-cryptosector
49. https://www.reuters.com/business/autos-transportation/spain-moves-rein-crypto-asset-advertising-2022-01-17/
50. https://www.fca.org.uk/publication/consultation/cp22-2.pdf
51. Betaaldienstverleners worden in het Engels aangeduid met Payment Service Providers (PSPs), zie voor meer informatie: www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/betaalinstellingen/vergunningaanvraag-betaaldiensten-overzichtspagina/definitie-betaaldienstverlener/

Zowel financiële instellingen, betaaldienstverleners als aanbieders van cryptodiensten dienen te voldoen aan de eisen van de Wwft en dus rijst de vraag: zijn deze partijen niet exact hetzelfde aan het controleren? De privacywetgeving beperkt de mogelijkheid tot data uitwisseling tussen aanbieders van crypto's.

> Het gebrek aan wet- en regelgeving en *guidance* van de toezichthouder laat daarmee financiële instellingen, betaaldienstverleners en aanbieders van cryptodiensten in het ongewisse bij hun rol als poortwachter van het financiële stelsel

Het gebrek aan wet- en regelgeving en *guidance* van de toezichthouder laat daarmee financiële instellingen, betaaldienstverleners en aanbieders van cryptodiensten in het ongewisse bij hun rol als poortwachter van het financiële stelsel.
Hierbij speelt ook informatieasymmetrie een grote rol. Enerzijds heeft een aanbieder van cryptodiensten geen inzicht in de banktransacties van een klant en anderzijds heeft een bank geen inzicht in de cryptotransacties van een klant wanneer eenmaal geld op de rekening van deze aanbieder is gestort, waarbij soms ook sprake is van een tussenkomst van een betaaldienstverlener. Hierdoor is het lastig om de plausibiliteit van transacties te achterhalen. Het is namelijk mogelijk dat een crypto munt 1000% in waarde stijgt wat men enkel kan achterhalen door de transacties te bekijken die voor een financiële instelling niet zichtbaar zijn.

2.2.2. Mogelijke oplossingen

Allereerst dient de DNB hulpmiddelen aan te bieden met betrekking tot de invulling van de poortwachtersrol. Bijvoorbeeld door het schrijven van een leidraad over hoe om te gaan met de informatieasymetrie en hoe crypto's gedurende CDD onderzoeken beoordeeld dienen te worden. Daarnaast kan door toezichthouders worden gekeken naar de mogelijkheid voor een *regulatory sandbox*. Dit is een 'zandbak' waar innovatieve ondernemingen in een gecontroleerde omgeving producten, diensten of verdienmodellen in de praktijk kunnen testen zonder dat zij aan alle wettelijke verplichtingen en beperkingen hoeven te voldoen. Het doel is om rechtsonzekerheid te minimaliseren en om innovatie te stimuleren door experimenteerruimte te bieden. In landen als het Verenigd Koninkrijk en Spanje[52] wordt op deze manier al uitgebreid geëxperimenteerd.

De AFM en DNB hebben een initiatief 'Maatwerk voor Innovatie' opgezet. [53]Op papier heeft dit kenmerken van een regulatory sandbox, maar in de praktijk wordt hier nog onvoldoende vervolg aan gegeven.

> De AFM en DNB hebben een initiatief 'Maatwerk voor Innovatie' opgezet. Op papier heeft dit kenmerken van een regulatory sandbox, maar in de praktijk wordt hier nog onvoldoende vervolg aan gegeven

In een dergelijke sandbox zou onderzocht kunnen worden of financiële instellingen kunnen leunen op de poortwachtersrol van de aanbieders van cryptodiensten, bijvoorbeeld middels '*whitelisting*'. Hierbij zouden transacties tussen financiële instellingen en aanbieders van cryptodiensten, die beide aantoonbaar voldoen aan de Wwft en de Sanctiewet, als betrouwbaar kunnen worden aangemerkt. Hierdoor hoeft niet tweemaal hetzelfde klantonderzoek plaats te vinden. Een mogelijkheid voor het uitwisselen van data ligt in de aansluiting van crypto dienstverleners bij Transaction Monitoring Nederland (TMNL),[54] waar verschillende banken eerder de handen ineen hebben geslagen om de samenhang van het zakelijke betalingsverkeer tussen de diverse banken te analyseren op mogelijk ongebruikelijke transacties.

2.3. Gebrek aan kennis over crypto bij financiële instellingen

2.3.1. Nieuw en complex fenomeen

Het onderwerp crypto is een vrij nieuw en complex fenomeen waar financiële instellingen nog onvoldoende aandacht aan besteden. Dit heeft mede te maken met het feit dat een duidelijk wettelijk kader ontbreekt, veel aandacht uitgaat naar achterstanden met betrekking tot Customer Due Diligence (CDD) en weinig trainingsmateriaal voorhanden is. Vanwege de toenemende adoptie van crypto zal mogelijk ook het crimineel gebruik in absolute getallen toenemen en is het van belang dat medewerkers van financiële instellingen, die toezien op de Wwft, in voldoende mate op de hoogte zijn van de risico's.

> Vanwege de toenemende adoptie van crypto zal mogelijk ook het crimineel gebruik in absolute getallen toenemen en is het van belang dat medewerkers van financiële instellingen, die toezien op de Wwft, in voldoende mate op de hoogte zijn van de risico's

2.3.2. Mogelijke oplossingen

Mogelijke oplossingen voor het vergroten van de kennis en awareness binnen de organisatie:

52. https://cointelegraph.com/news/regulatory-sandbox-and-defi-boom-how-spain-pushed-crypto-adoption-despite-the-pandemic
53. https://www.afm.nl/nl-nl/professionals/onderwerpen/innovationhub-maatwerk
54. https://tmnl.nl/

1. Bepaal een specifieke *integrity risk appetite*[55] ten aanzien van crypto's en neem deze op in de *Risk Appetite Statement*;
2. Definieer en beoordeel één of meerdere risico scenario's ten aanzien van crypto in de Systematische Integriteits Risico Analyse (SIRA);
3. Ontwikkel concreet beleid en werkinstructies voor medewerkers die in hun dagelijkse werk te maken hebben met het identificeren en beoordelen van risico's met betrekking tot crypto;
4. Train medewerkers zoals Compliance Officers en CDD-analisten door trainingsprogramma's te ontwikkelen en specifieke casuïstiek met elkaar te doorleven;
5. Laat de complexe casussen behandelen door (in crypto) gespecialiseerde afdelingen. Hiervoor zou een specifieke crypto desk kunnen worden ingericht.

2.4. Gebrek aan middelen bij financiële instellingen

2.4.1. Uitdagingen en effectiviteit van transactiemonitoring

Een belangrijk probleem voor financiële instellingen is hoe om te gaan met cryptotransacties en het voldoende inzicht verkrijgen in de herkomst van het vermogen. Te beginnen met het detecteren van transacties met aanbieders van crypto's. Van ruim 1000 aanbieders wereldwijd is bekend dat zij wel eens van bankrekening wisselen of gebruik maken van betaaldienstverleners. Dit maakt het voor de afdelingen die zich bezighouden met transactiemonitoring nagenoeg onmogelijk om hier hun business rules op aan te passen en actueel te houden.

Bij een partij als Ciphertrace is data van alle bankrekeningen in te kopen, maar wordt dit van een financiële instelling verwacht? Als men dan toch een transactie heeft gevonden waarbij een klant afwijkend gedrag vertoont, dient men op basis van de Wwft en de Wet financieel toezicht (Wft) risicogericht een onderzoek te doen. Een voorbeeld van een afwijkende transactie betreft een jong volwassene die ineens een half miljoen op zijn rekening gestort krijgt van een crypto dienstverlener. Deze onderzoeken om de herkomst van de gelden te achterhalen zijn zeer tijdsintensief, complex en leveren vaak niks op. Analisten moeten hiervoor bijvoorbeeld screenshots van wallets of de public key[56] opvragen bij de klant, of een analyse uitvoeren op de transacties op de blockchain om te onderzoeken of het verhaal van de klant plausibel is. Onder meer vanwege de angst voor boetes van DNB en het onduidelijke wettelijke kader wordt veel, tijdsintensief en dus kostbaar onderzoek gedaan naar veel transacties die na lang onderzoek plausibel blijken te zijn.

Onder meer vanwege de angst voor boetes van DNB en het onduidelijke wettelijke kader wordt veel, tijdsintensief en dus kostbaar onderzoek gedaan naar veel transacties die na lang onderzoek plausibel blijken te zijn

2.4.2. Mogelijke oplossing

Financiële instellingen kunnen gebruik maken van beschikbare blockchain analytics applicaties waarmee inzichtelijk kan worden gemaakt wat de herkomst van de gelden is en hoeveel crypto's een klant aanhoudt. Voorbeelden van dergelijke applicaties zijn van partijen als Chainalysis, Ciphertrace en Elliptic. Hoewel deze beschikbare applicaties in de markt vrij duur zijn, kan hiermee inzicht worden verschaft in de verschillende datapunten op de blockchain ter identificatie en beoordeling van risico's op onder andere witwassen, terrorismefinanciering en omzeiling van sanctieregelgeving. Om deze data beschikbaar te maken is het walletadres nodig van de klant, waardoor klantcontact altijd benodigd is.

3. Conclusie

Genoemde problemen laten zien dat het toezicht op crypto's op dit moment nog niet effectief is. Een duidelijk wettelijk kader ontbreekt nog en tevens is sprake van een gebrek aan voldoende kennis en (technologische) middelen bij financiële instellingen (dus niet de aanbieders van cryptodiensten) om risico's bij cryptotransacties te identificeren en te beoordelen. Tevens staat ter discussie waar de poortwachtersrol ten aanzien van cryptotransacties ligt: bij banken, betaaldienstverleners en/of crypto dienstverleners. Het is aan de toezichthouders om met de verschillende markpartijen in gesprek te gaan, gezamenlijk kennis en visie te ontwikkelen en verder richting te geven in de geschetste problematiek.

55. De *integrity risk appetite* ziet op de risicobereidheid van een organisatie ten aanzien van integriteitsrisico's. Hierbij wordt expliciet gemaakt welke risico's een organisatie wil accepteren, welke risico's moeten worden vermeden of worden verkleind door beheersmaatregelen te treffen.

56. Een public key is naast de private key één van de twee sleutels die gebruikt wordt voor het versleutelen van gegevens. De ene key dient voor het vercijferen en de ander voor het ontcijferen van informatie. De private key wordt gebruikt voor het wiskundig afleiden van de public key. In tegenstelling tot de private key, die volstrekt geheim moet blijven, is de public key bedoeld om uitgewisseld te worden met degene met wie men wil communiceren. Wanneer die persoon een public key heeft, kan hij daar crypto's naartoe zenden.

Genoemde problemen laten zien dat het toezicht op crypto's op dit moment nog niet effectief is

Een mogelijke oplossing ligt in een ketenbrede aanpak om crimineel gebruik tegen te gaan waarbij samenwerking en delen van data een grote rol speelt. Een goed voorbeeld hiervan is onder andere de samenwerking bij TMNL. Hiermee ontlasten financiële instellingen en aanbieders van cryptodiensten klanten die te goedertrouw zijn en wordt de pakkans voor criminelen vergroot.
Ondertussen wordt de technologie doorontwikkeld en zullen criminelen gebruik blijven maken van de zwakheden in het financiële systeem.