

# Cryptoonopticon, of een korte geschiedenis van cryptoactiva en het strafrecht

mr. B.W. Newitt<sup>1</sup>

Cryptoactiva zijn ondanks de pas relatief recente popularisatie slecht meer weg te denken uit onze maatschappij. Meer dan 10% van de Nederlanders bezit naar schatting inmiddels enige vorm van cryptoactiva.<sup>2</sup> Nu de eerste daadwerkelijke transactie middels cryptoactiva dit jaar 15 jaar geleden op de zogenaamde 'Bitcoin Pizza Day' plaatsvond,<sup>3</sup> lijkt het een mooi moment voor een overzicht van de geschiedenis en de huidige stand van zaken. Dit artikel zal een kort historisch overzicht proberen te schetsen van de het ontstaan van cryptoactiva, welke juridische stappen zijn genomen om cryptoactiva in Nederland te reguleren, en welke ontwikkelingen aanleiding gaven tot die stappen. Daarbij zal ik voor de overzichtelijkheid geen gebruik maken van eerder vigerende begrippen als cryptovaluta of virtuele valuta, maar steeds de relatief nieuwe term 'cryptoactiva' gebruiken zoals geïntroduceerd door de recent geïmplementeerde Europese *Markets in Crypto Asset Regulation*.<sup>4</sup> Die term cryptoactiva bestrijkt kort gezegd alle digitale weergaven van waarde of rechten die middels een 'distributed ledger technologie' of vergelijkbare technologie worden geadministreerd.

## 1. Een korte ontstaansgeschiedenis van cryptoactiva

Ook omdat ik verwacht dat in andere artikelen in dit blad reeds de nodige aandacht uit zal gaan naar Satoshi Nakamoto, wil ik in deze bijdrage de geschiedenis wat verder terug in de tijd, maar wat dichterbij huis laten beginnen. Te weten, bij het Centrum voor Wiskunde en Informatica (nader: CWI) destijds wat verlaten gelegen in een uithoek van de Amsterdamse Watergraafsmeer waar inmiddels het bruisende *Science Park* staat.<sup>5</sup>

### 1.1. David Chaum en eCash

Het CWI kreeg in 1988 de eerste trans-Atlantische internetverbinding van Europa, en verzorgde enige tijd voor heel Europa de toegang tot het Amerikaanse internet.<sup>6</sup> Het CWI trok mede daarom veel getalenteerde programmeurs aan. Een aantal van die programmeurs van het CWI werd door David Chaum, een beroemde Amerikaanse hoogleraar en privacy-

voorvechter, destijds verbonden aan de UVA, in 1989 betrokken bij het intekenen op de tender voor rekeningrijden van het Ministerie van Verkeer en Waterstaat.<sup>7</sup> Hoewel het rekeningrijden uiteindelijk nooit is ingevoerd, leidde de samenwerking van Chaum met de programmeurs van het CWI tot de oprichting van de onderneming DigiCash BV te Amsterdam. Deze BV had ten doel internetbetalingen te faciliteren met behoud van privacy, net als mogelijk was met het toen nog alom aanwezige contante geld.<sup>8</sup> Chaum, van wie een deel van zijn joodse familie was vermoord in de tweede Wereldoorlog, was om begrijpelijke redenen geen voorstander van volstrekte openbaarheid van het (economische) gedrag van mensen op het internet. De gedachte binnen DigiCash luidde dat, nu mensen met min of meer onherleidbaar contant geld een brood, krant of toeweg konden betalen, digitaal geld ook dergelijke kleinere onherleidbare transacties moest kunnen faciliteren.<sup>9</sup> De kern van de techniek van DigiCash betrof de door Chaum reeds in 1983 ontwikkelde 'blind signature'.<sup>10</sup> Dit is een cryptografische vorm van een handtekening waarbij de inhoud van een bericht

1. Brendan Newitt is werkzaam als advocaat bij De Roos & Pen te Amsterdam.  
2. *Kamerstukken II*, 2024-25, 27879, nr. 111 (Kamerbrief Minister van Financiën 3 juli 2025).  
3. Op welke dag op 22 mei 2010 door Laszlo Hanyecz voor 10.000 Bitcoin, naar toenmalige waarde zo een 40 Amerikaanse dollar, en naar huidige waarde zo een miljard euro, twee pizza's werden aangeschaft, zie [https://en.wikipedia.org/wiki/History\\_of\\_bitcoinaatstelijk\\_geraadpleegd\\_26\\_augustus\\_2025](https://en.wikipedia.org/wiki/History_of_bitcoinaatstelijk_geraadpleegd_26_augustus_2025).  
4. Verordening (EU) 2023/1114 betreffende cryptoactiva-markten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937, PbEU 2023, L 150.  
5. Eric Smit, *Betalen met crypto's is 30 jaar geleden in Amsterdam bedacht*, Follow The Money, 27 mei 2024, <https://www.ftm.nl/artikelen/digital-currency-bestaat>

-vandaag-30-jaar laatstelijk geraadpleegd 26 augustus 2025.  
6. Destijds nog het NSFNet, zie <https://www.cwi.nl/en/n-ews/centrum-wiskunde-informatica-viert-30-jaar-open-internet-in-europa/> laatstelijk geraadpleegd 30 augustus 2025.  
7. Eric Smit, *Betalen met crypto's is 30 jaar geleden in Amsterdam bedacht*, Follow The Money, 27 mei 2024.  
8. Julia Kagan, eCash: Overview Rise and Fall, 31 maart 2021, <https://www.investopedia.com/terms/e/ecash.asp> laatstelijk geraadpleegd 26 augustus 2025.  
9. Eric Smit, *Betalen met crypto's is 30 jaar geleden in Amsterdam bedacht*, Follow The Money, 27 mei 2024.  
10. David Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology, Springer, Boston, MA, 1983; doi.org/10.1007/978-1-4757-0602-4\_18.

wordt gemaskeerd voordat het cryptografisch wordt ondertekend.<sup>11</sup> Hoewel pilots liepen bij Deutsche Bank, Credit Suisse en Citibank<sup>12</sup> was de eerste bank die DigiCash daadwerkelijk implementeerde de kleinere Mark Twain Bank in Amerika.<sup>13</sup> Het betaalsysteem werkte als volgt. Met een aangemaakte digitale portemonnee zette je via de bank dollars om in eCash, als digitaal equivalent van contant geld op zak hebben. Je kon daarmee betalen voor goederen, informatie of diensten aan een andere partij (die ook een digitale portemonnee van DigiCash moest hebben) middels een mail of online transactie.<sup>14</sup> De ontvanger kon daarna de eCash weer inleveren bij de eigen bank en ontving daarvoor een bijschrijving op zijn eigen rekening. Door het systeem van *blind signatures* kon de bank niet zien van wie de verzender van de betaling was, maar wel dat de betaling echt was.<sup>15</sup> Voor Chaum en DigiCash BV was betoogbaar evengoed sprake van een ideologische onderneming als van een businessmodel. Chaum vreesde reeds in de vroege jaren 90 al voor de nachtmerrie van het digitaal panopticon<sup>16</sup> dat het leven in cyberspace zou kunnen worden. In zijn eigen woorden: *‘in one direction lies unprecedented scrutiny and control of people’s lives; in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.’*<sup>17</sup>

ECash werd nooit erg breed uitgerold, en DigiCash zag, mede door de (te) principiële eisen die het stelde aan de aangeboden samenwerkingen met bijvoorbeeld Microsoft, een brede implementatie aan zich voorbijgaan. Mede daardoor verloor het al snel de concurrentieslag om internetbetalingen van de creditcard en ging het in 1998 failliet.<sup>18</sup> Desondanks wordt Chaum door velen toch gezien als een van de belangrijkste de grondleggers van de huidige cryptoactivawereld. Een echt cryptoactiva kan eCash, naar de huidige maatstaven gemeten, echter nog niet genoemd worden, nu bij eCash nog sprake was

van een centrale *trusted party* (DigiCash BV) en het overmaken van fiatgeld, met een bijbehorend voorde-riingsrecht in fiatvaluta op een gereguleerde bank. Mede in reactie op de introductie van eCash en andere digitale internetbetaalmiddelen werden wel de FATF-aanbevelingen aangevuld met bepalingen voor E-money, en werd in EU verband de E-money richtlijn<sup>19</sup> ontwikkeld.<sup>20</sup>

## 1.2. Blockchain, Hashcash en de Cypherpunks

Gedurende het bestaan van eCash vonden ook andere belangrijke ontwikkelingen plaats die in het bijzonder bijdroegen aan de huidige cryptoactivawereld, waarbij vaker wel dan niet betrokkenen bij de Cypherpunk-mailinglijst van grote invloed waren. De Cypherpunkbeweging ontstond eind jaren 80 en kreeg toegenomen importantie met de oprichting van de elektronische mailinglijst ‘*Cypherpunks*’ in 1992. Daar besprak een informele groep van activisten, technologen en cryptografen strategieën om de privacy van individuen te verbeteren en zich te verzetten tegen surveillance door de overheid of bedrijven.<sup>21</sup> In 1991 legden twee deelnemers aan de mailinglijst<sup>22</sup> genaamd Stuart Haber en W. Scott Stornetta de basis voor wat later de Blockchain zou worden.<sup>23</sup> Hun paper beschrijft hoe een document nagenoeg onvervalsbaar gevalideerd kan worden met een timestampserver middels een chronologische ketting van gehashte data. In 1991 richtten zij ook het bedrijf *Surety* op dat gebruik maakte van deze technologie.<sup>24</sup>

In 1997, een jaar voor het faillissement van DigiCash, lanceerde Adam Back het idee van HashCash, ook aanvankelijk in een e-mail binnen de Cypherpunk-mailinglijst.<sup>25</sup> Hoewel ook behept met de naam *cash* was niet zozeer sprake van een betaalmiddel maar

11. <https://en.wikipedia.org/wiki/DigiCash> laatstelijk geraadpleegd 26 augustus 2025.  
 12. Eric Smit, Betalen met crypto’s is 30 jaar geleden in Amsterdam bedacht, Follow The Money, 27 mei 2024.  
 13. <https://en.wikipedia.org/wiki/DigiCash>, laatstelijk geraadpleegd 26 augustus 2025.  
 14. Eric Smit, Betalen met crypto’s is 30 jaar geleden in Amsterdam bedacht, Follow The Money, 27 mei 2024.  
 15. Stephen Levy, *E-money, that’s what I want*, Wired Magazine, 1 december 1994, <https://www.wired.com/1994/12/emoney/> laatstelijk geraadpleegd 26 augustus 2025.  
 16. Een panopticon, of panopticum, is een oorspronkelijk uit de architectuurfilosofie begrip ontleend aan het oudgriekse woord voor alziend. Het oorspronkelijke door Jeremy Bentham in de 18e eeuw bedachte concept betrof een ronde koepelgevangenis waarbij alle gevangenen van een instelling door één centrale bewaker konden worden geobserveerd, maar nooit zeker wisten wanneer zij geobserveerd werden. In Nederland waren de koepelgevangenissen van Breda, Arnhem en Haarlem mede op dit principe geïnspireerd.  
 17. Ibid.  
 18. Eric Smit, Betalen met crypto’s is 30 jaar geleden in Amsterdam bedacht, Follow The Money, 27 mei 2024.  
 19. Richtlijn 2000/46/EG van het Europees Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomisch toezicht op de werkzaamheden van instellingen voor elek-

tronisch geld inmiddels vervangen door Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (Voor de EER relevante tekst).  
 20. M. Krueger, *Offshore E-money issuers and monetary policy*, First Monday 12 mei 2005, oorspronkelijk uitgegeven in oktober 2001, <https://firstmonday.org/ojs/index.php/fm/article/view/1513> laatstelijk geraadpleegd 26 augustus 2025.  
 21. Zie ook: <https://en.wikipedia.org/wiki/Cypherpunk> laatstelijk geraadpleegd 1 september 2025.  
 22. <https://cointelegraph.com/news/blockchain-co-inventor-offers-his-view-into-satoshi-nakamotos-background> en <https://medium.com/coin-story/coin-perspective-11-stuart-haber-d1445257dc98>  
 23. S. Haber, en W.S. Stornetta, *How to time-stamp a digital document*. Journal of Cryptology 3, 1991, p. 99–111. <https://doi.org/10.1007/BF00196791>.  
 24. <https://www.vice.com/en/article/what-was-the-first-blockchain/> laatstelijk geraadpleegd op 26 augustus 2025.  
 25. <http://www.hashcash.org/papers/announce.txt> en later meer formeel uitgewerkt in zijn artikel *Hashcash- A Denial of Service Counter-Measure*, van 1 augustus 2002.

van een soort digitaal postzegelsysteem om verzending van spammail economisch onhaalbaar te maken. Zijn systeem zou gebruikt zou kunnen worden totdat, naar de verwachting van Adam Back zelf, eCash van DigiCash zodanig breed zou zijn geïmplementeerd dat hiermee ook een digitale postzegeconomie van de grond zou komen (dan wel in het geval DigiCash zou falen, of, zelfs erger nog volgens Adam Back, DigiCash verplicht zou worden de identiteit van gebruikers aan transacties te koppelen.) Meer nauwkeurig gezegd betrof HashCash een cryptografisch hash-gebaseerd proof-of-work-algoritme dat een bepaalde hoeveelheid werk vereist om te berekenen, maar waarvan de uitkomst achteraf eenvoudig worden kan geverifieerd.<sup>26</sup> De bedoeling van HashCash was om spam-mails tegen te gaan door te vereisen dat een bepaalde hoeveelheid rekenkracht van een computer werd gebruikt voordat een e-mail werd bezorgd. Een normale e-mailgebruiker zou hiervan geen merkbaar nadeel ervaren, maar spam-mailzenders, wiens businessmodel gebaseerd is op het verzenden van gigantische hoeveelheden mail voor nagenoeg geen kosten, zouden hierdoor op den duur niet langer een winstgevend businessmodel hebben.

In 1998 deelden Nick Szabo en Wei Dai, opnieuw beiden deelnemers aan de Cypherpunks- mailinglijst separaat maar haast gelijktijdig hun gelijksoortige ideeën voor een cryptoactivabetaalstelsel met de wereld.<sup>27</sup> De voornaamste bijdrage van Wei Dai en Nick Szabo in hun respectievelijke voorstellen van B-money en BitGold kan gezien worden als 1) hun idee om de boekhouding van de transacties middels de blockchain niet aan een centrale partij over te laten, maar in een gedeelde boekhouding verspreid onder gebruikers, en 2) hun voorstel om de waarde van de valuta (mede) afhankelijk te laten zijn van cryptografisch proof-of-work (geïnspireerd door HashCash). Szabo suggereerde daarnaast al de vergelijking tussen proof-of-work generatie van nieuwe cryptografische munten en het mijnen van goud. Beide projecten zijn echter blijven steken in de theorie.

### 1.3. BitCoin

Zoals bij de lezer van deze uitgave bekend mag worden verondersteld, was het uiteindelijk Satoshi Na-

kamoto<sup>28</sup> die op 31 oktober 2008 niet enkel diens whitepaper 'Bitcoin: A Peer-to-Peer Electronic Cash System' publiceerde, maar ook kort daarna overging tot het daadwerkelijk in de praktijk uitrollen van het Bitcoin-systeem. Op 12 januari 2009, drie dagen na het lanceren van de eerste BitCoin-software, maakte Satoshi Nakamoto 50 Bitcoin over,<sup>29</sup> waarvan de eerste 10 naar opnieuw een lid van de Cypherpunk mailinglijst, Hal Finney, die belangrijk werk had verricht binnen de sfeer van *reusable proof-of-work*.<sup>30</sup> De whitepaper van Satoshi Nakamoto is een parel van eenvoud, waarin hij met minimale wiskundige intermezzo's zijn Bitcoin-systeem voor de lezer uiteenzet. Hoewel hij, zoals hierboven beschreven, in zekere zin voortbouwde op illustere voorgangers dient zijn bijdrage, waarin hij de gedachten van zijn voorgangers in één elegant en functionerend geheel verwerkt, allerminst geminimaliseerd te worden.

Het concept is tamelijk briljant in zijn eenvoud. Een Bitcoin-munt wordt door Satoshi Nakamoto gedefinieerd als een ketting van digitale handtekeningen. Elke eigenaar draagt de munt over aan de volgende eigenaar door digitaal een *hash*<sup>31</sup> van de vorige transactie en de publieke sleutel van de volgende eigenaar te signeren, en deze aan het einde van de munt toe te voegen. Een begunstigde kan de ketting van handtekeningen verifiëren om de keten van eigendom te verifiëren.<sup>32</sup> Deze werkwijze is niet onvergelykbaar met de werking van het kadaster of met het oude endossementsysteem bij rechten aan order.<sup>33</sup>

Om te voorkomen dat een onbetrouwbare gebruiker dezelfde digitale munt meermalen kan uitgeven, moeten in het algemeen gezegd bij minimaal één partij alle transacties en hun volgorde bekend zijn. Waar dat in het reguliere betaalsysteem gecontroleerd werd door een centrale *trusted party* zoals een bank, stelt Nakamoto voor om in het Bitcoin systeem iedere transactie publiek te maken voor iedereen, en een systeem te implementeren waardoor alle deelnemers het eens zijn over de volgorde van die transacties. Voor die volgorde wordt een timestamp systeem gebruikt zoals eerder ontwikkeld door Stornetta en Haber.<sup>34</sup> Om die op een *peer to peer* basis te laten draaien wordt een proof-of-work systeem gebruikt gelijkend op het HashCash systeem van Back.<sup>35</sup> De proof-of-work die het systeem draaiend houdt, genereert daarnaast bij elke nieuw block

26. <https://en.wikipedia.org/wiki/Hashcash> laatstelijk geraadpleegd op 26 augustus 2025.  
 27. <http://www.weidai.com/bmoney.txt> en [https://en.wikipedia.org/wiki/Nick\\_Szabo](https://en.wikipedia.org/wiki/Nick_Szabo), laatstelijk geraadpleegd op 26 augustus 2025.  
 28. Er wordt overigens aangenomen dat dit slechts een pseudoniem is voor de persoon of groep personen die Bitcoin heeft ontwikkeld.  
 29. <https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/> via [https://en.wikipedia.org/wiki/History\\_of\\_bitcoin](https://en.wikipedia.org/wiki/History_of_bitcoin) laatstelijk geraadpleegd op 26 augustus 2025.  
 30. [https://en.wikipedia.org/wiki/Hal\\_Finney\\_\(computer\\_scientist\)](https://en.wikipedia.org/wiki/Hal_Finney_(computer_scientist)) en <https://www.guinnessworldrecords.com/world-records/696243-first-bitcoin-transaction> laatstelijk geraadpleegd op 26 augustus 2025.

31. 'Een hashfunctie of hashalgoritme is in de informatica een algoritme dat invoer uit een breed domein van waarden omzet in een meestal kleiner bereik, meestal een deelverzameling van de gehele getallen. De uitvoer van een hashalgoritme wordt de hash, hashcode of digest van de invoer genoemd; Vgl. <https://nl.wikipedia.org/wiki/Hashfunctie>, laatstelijk geraadpleegd op 26 augustus 2025.  
 32. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* p. 2, te downloaden via [www.bitcoin.org](http://www.bitcoin.org), laatstelijk geraadpleegd op 26 augustus 2025.  
 33. Vgl. artikel 3:93, 3:238 en 3:236 BW.  
 34. Overigens werd in de aangehaalde stukken noch door Stornetta en Haber noch door Satoshi Nakamoto het woord *blockchain* gebruikt.  
 35. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* p. 5 en 6.

een Bitcoin die ten goede komt aan de aanmaker van het block. Die beloning werkt als een prikkel voor eerlijke deelnemers aan het systeem, en zorgt daarnaast voor de nodige toestroom van Bitcoins voor het digitale monetaire netwerk. Net als Szabo maakt Nakamoto hier de vergelijking met het mijnen van goud.<sup>36</sup>

Hoewel reeds in theorie geopperd door Szabo en Dai, was het ook in praktijk geheel publiek maken van alle transacties binnen een betaalsysteem, om zo zonder een centrale *trusted party* te kunnen werken, een bijkans revolutionaire paradigmaverschuiving. De enige oplossing voor de hiermee gepaard gaande privacyproblematiek was volgens Nakamoto dan ook het introduceren ook een nieuw model van privacy. Waar in de reguliere betaalsystemen de privacy beschermd werd door de informatie over de transactie niet verder te verspreiden dan de deelnemers aan de transactie en de betrokken bank (of andere *trusted party*), zou binnen Bitcoin de privacy beschermd worden door juist de *identiteit* van de personen achter de transacties af te schermen. Hoewel eenieder alle transacties in zou kunnen zien in wat wij inmiddels de *'public ledger'*<sup>37</sup> zijn gaan noemen, zou, indien de gebruikers van het Bitcoin-netwerk de nodige voorzorgen namen, niemand individuen kunnen koppelen aan die transacties. Het is deze vorm van privacy middels pseudonimisering (waarbij de *public key* en/of het *walletadres* het pseudoniem van de gebruiker zijn) waarop de strijd tussen veiligheid en de bescherming van de persoonlijke levenssfeer zich vooral zal manifesteren in het betugelen door de overheid van (de uitwassen van) cryptoactiva.

Een verdere belangrijke stap in het tot wasdom komen van cryptoactiva was de eerdergenoemde "Bitcoin Pizza Day" op 22 mei 2010. Hoe onbeduidend een transactie bestaande uit een aanschaf van twee pizza's met Bitcoin ook mag lijken, was dat de dag waarop gestaafd werd dat deze digitale valuta zonder centrale *trusted party* of connectie met een nationale fiatvaluta, toch als fiduciaire valuta – dat wil zeggen: een valuta wiens waarde ontleend wordt aan het vertrouwen dat er goederen en diensten mee gekocht kunnen worden- kon worden gebruikt.

Hoewel het nog enige tijd duurde voordat nadere cryptoactiva werden ontwikkeld (LiteCoin stamt uit 2011 en Ethereum uit 2015) zijn inmiddels talloze duizenden cryptoactivamunten, tokens en netwerken actief, hoewel het overgrote merendeel daarvan geen serieuze economische waarde of tractie heeft gekregen.<sup>38</sup>

## 2. De eerste uitwassen en de eerste handhaving

'*Bitcoin A Peer-to-Peer Electronic Cash System*', en ook eerder eCash, gaven (mede qua naam) aan dat het systeem bedoeld was als digitaal alternatief voor 'cash' oftewel contanten,<sup>39</sup> een geldvorm die ook onder criminelen om verschillende redenen de voorkeur heeft. Toch kregen cryptoactiva, mede door de oorspronkelijk zeer geringe waarde daarvan aanvankelijk weinig aandacht van de opsporingsdiensten als een crimineel betaalmiddel.

### 2.1. Silk Road, de eerste darknetmarkt

De eerste uitwas waarop redelijkerwijs wel gehandhaafd moest worden kwam in 2011, toen Ross Ulbricht onder het pseudoniem *Dread Pirate Roberts* de digitale marktplaats 'Silk Road' oprichtte. Deze marktplaats was enkel toegankelijk middels het TOR-netwerk, vaak door mensen aangeduid als het darknet.<sup>40</sup> Al snel werden op Silk Road wereldwijd illegale zaken verhandeld, voornamelijk drugs, en de koopprijs werd altijd in Bitcoin voldaan ten behoeve van de anonimiteit.<sup>41</sup>

In oktober 2013 werd Silk Road met enige hulp van onder meer Nederland<sup>42</sup> door de Amerikaanse FBI opgedoekt en Ross Ulbricht gearresteerd, wat in 2015 leidde tot een levenslange gevangenisstraf. In januari van dit jaar werd hij echter door de Amerikaanse president Trump gratie verleend.<sup>43</sup> Binnen het onderzoek werden meer dan 144.000 Bitcoin in beslag genomen, en cryptoactiva kregen voor het eerst serieuze aandacht van opsporingsdiensten, zowel in Amerika als daarbuiten.

### 2.2. Het eerste Nederlandse beslag op cryptoactiva

Door het grote marktaandeel van Silk Road in de internationale online drugshandel en de Nederlandse ondernemersgeest (en voorname rol in de wereldwijde XTC-productie), hoeft het geen verbazing te wekken dat het eerste beslag op cryptoactiva in Nederland ook verband hield met Silk Road. Bij de zogenaamde *'Bende van Sinterklaas'*, een groep die op Silk Road XTC tabletten verkocht en naar de afnemers verzond in DVD-doesjes met opdruk van kerkmuziek, werd in april 2013 het eerste Nederlands beslag op cryptoactiva gelegd. Over de tap had de politie de verdachten al horen spreken over 'Bitcoins'

36. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* p. 4.

37. Net als het begrip blockchain komt ook het begrip *public ledger* niet voor in het whitepaper van Nakamoto.

38. [https://en.wikipedia.org/wiki/List\\_of\\_cryptocurrencies](https://en.wikipedia.org/wiki/List_of_cryptocurrencies) laatstelijk geraadpleegd op 26 augustus 2025.

39. In die zin is de veelgebruikte aanprijzing van Bitcoin als het *'digitale goud'* onder de cryptoactiva dus minder treffend.

40. Zie: [https://nl.wikipedia.org/wiki/Tor\\_\(netwerk\\_laatste\\_lijk\\_geraadpleegd\\_op\\_26\\_augustus\\_2025\)](https://nl.wikipedia.org/wiki/Tor_(netwerk_laatste_lijk_geraadpleegd_op_26_augustus_2025)).

41. <https://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace> laatstelijk geraadpleegd op 26 augustus 2025.

42. *Aanhangsel Handelingen II*, 2013–14, nr. 1326 (beantwoording Kamervragen).

43. <https://www.theguardian.com/us-news/2025/jan/21/ross-ulbricht-silk-road-trump-pardon>

en een geïnteresseerde diender besloot op het internet eens uit te zoeken wat dat nou voor dingen waren. Nadat hij de materie enigszins begreep en er een USB-stick met een wallet met 147 Bitcoin in beslag was genomen, besloot hij een financieel en digitaal expert erbij te halen, met wie de politie zelf een wallet aanmaakte waarop zij de Bitcoins tijdelijk plaatsten. Het duurde uiteindelijk nog enige maanden tot het Openbaar Ministerie zover was dat het zelf ook een wallet had aangemaakt, waarna op 1 januari 2014 de Bitcoins, destijds nog onder de regeling voor beslag op buitenlandse valuta, werden verzilverd en het beslag vervolgens werd gelegd op de wisselwaarde in Euro's.<sup>44</sup> In 2014 is daarna ook het in beslag nemen van cryptoactiva vastgelegd door het OM in de Handleiding Inbeslagname Bitcoins,<sup>45</sup> waarin onder meer werd voorgeschreven dat inbeslaggenomen cryptoactiva zo snel mogelijk dienen te worden omgezet in fiatvaluta,<sup>46</sup> onder meer op grondslag van artikel 117 Sv.<sup>47</sup> Deze wijze van werken van het beslag heeft helaas tevens ten gevolge dat een eventuele last tot teruggave van strafrechtelijk beslag op cryptoactiva zich in beginsel beperkt tot de waarde ten tijde van de vervreemding (volgens beleid van het OM uiterlijk vijf dagen na de inbeslagneming), en niet de waarde die de cryptoactiva op het moment van de last tot teruggave vertegenwoordigt.<sup>48</sup>

### 2.3. De eerste stappen naar cryptoactivatracing

In Europa leidde de Silk Road kwestie onder meer tot de oprichting in Nederland van het project ITOM (*Illegal Trade on Online Marketplaces*) waarbij door de Nederlandse autoriteiten internationale samenwerking werd gezocht, en voor het eerst in serieuze mate werk leek te worden gemaakt van het feit dat de *public ledger* (nagenoeg) alle cryptoactivatransacties publiekelijk volgbaar maakt, wat kansen biedt voor de opsporing.<sup>49</sup>

Het eerste bekende grotere onderzoek van de Nederlandse politie waarbij *cryptoactivatracing* bijdroeg aan het vinden van verdachten, vond in 2014 plaats in een onderzoek naar factuurfraude. In deze zaak liet de politie een analyse los op de cryptoactiva die een katvanger van de factuurfraude had moeten laten omzetten in cryptoactiva bij een bepaalde cryptoactivabeurs. De recherchekundige maakte daaruit

op dat 85% van de aangekochte cryptoactiva middels een web van transacties uiteindelijk bij één bepaald walletadres terecht kwam. Door middel van ingezette 'reguliere' bijzondere opsporingsbevoegdheden vond de politie vervolgens de personalia van de houder van dat walletadres, en de eerste verdachte via cryptoactivatracing was gevonden.<sup>50</sup> Elena Muller, van het witwasteam van de FIOD, gaf naar aanleiding van een gelijksoortige zaak in dezelfde periode aan dat, hoewel er in het begin de kennis ontbrak om met Bitcoin om te gaan, Nederlandse opsporingsdiensten inmiddels de nodige expertise in huis hadden. Hoewel die stelling in 2014 wellicht nog wat voorbarig was, zijn de Nederlandse opsporingsdiensten in 2025 erg behendig geworden in cryptoactivatracing, waarbij zij voor de echt complexe tracing de hulp inschakelen van gespecialiseerde bedrijven zoals Chainalysis.<sup>51</sup>

### 2.4. Cryptolocker en de eerste ransomware

2014 was ook het jaar dat Cryptolocker werd ontmanteld, een van de eerste grote ransomware trojans.<sup>52</sup> Ransomware is kwaadaardige software die bestanden of systemen versleutelt, waarna losgeld wordt geëist om toegang te herstellen. Cryptolocker versleutelde alle bestanden van geïnfecteerde gegevensdragers, en verzorgde de ontsleuteling enkel na betaling van een losgeldbedrag in Bitcoin (0,8 BTC in de eerste 3 dagen of 10 Bitcoin op een later moment).<sup>53</sup> Hoewel het onderzoek naar Cryptolocker werd geleid door het Amerikaanse Department of Justice speelde het Nederlandse bedrijf Fox IT een belangrijke rol bij het uitvogelen van de sleutels waarmee partijen hun data weer konden vrijkrijgen zonder betaling van losgeld. Het feit dat betaling in Bitcoin werd gevraagd, terwijl de cryptoactivamunt verder nog weinig courant was, droeg opnieuw niet bij aan een goede reputatie van cryptoactiva.

### 2.5. De val van Mt Gox

Een laatste ontwikkeling uit 2014 die vermeldenswaard kan worden geacht, is de val van de Bitcoin handelsbeurs Mt Gox. Deze Japanse bitcoinbeurs verwerkte begin 2014 nog meer dan 70% van alle wereldwijde bitcointransacties maar later in 2014

44. Alles: Bijlage bij *Kamerstukken II*, 2014-15, 34200 V1, nr. 1 (Jaarverslag politie 2014), p. 37.

45. Deze handleiding is overigens kennelijk nog niet openbaar gemaakt.

46. Fiatvaluta zijn kort gezegd valuta die door de bevoegde autoriteiten van een staat zijn uitgegeven en/of door die bevoegde autoriteiten zijn aangemerkt als wettig betaalmiddel. Binnen Nederland is de Euro de fiatvaluta (zie Artikel 128 (1) VWEU en Artikel 11 van Verordening (EG) Nr. 974/98).

47. Jansens, Soetart en De Vos, *'Beslag en Beheer van Cryptovaluta: de Bitcoin'* Panopticon 2017, no 38, p. 44.

48. Vgl Gerechtshof Den Haag 24 oktober 2018, ECLI:NL:GHDHA:2018:2821 icm Hoge Raad 12 mei 2020, ECLI:NL:HR:2020:845 en Gerechtshof Den Haag 1 april 2025, ECLI:NL:GHDHA:2025:623.

49. *Kamerstukken II*, 2014-15, 29911, nr. 114 p. 27 (Verantwoording aanpak georganiseerde criminaliteit 2014). Er was overigens reeds daarvoor al enige (beperkte) aandacht voor cryptoactiva in de criminele sfeer, zie *Aanhangsel Handelingen II*, 2012-13, nrs. 2162 en 2508 (Beantwoording van Kamervragen).

50. *Kamerstukken II*, 2014-15, 29911, nr. 129, Bijlage 780961 p. 27 (Rapportage aanpak georganiseerde ondermijnende criminaliteit 2015).

51. Zie <https://en.wikipedia.org/wiki/Chainalysis> laatstelijk geraadpleegd 26 augustus 2025.

52. Een trojan is een type kwaadaardige malware dat zich voordoet als een legitieme software. Zie ook [https://en.wikipedia.org/wiki/Trojan\\_horse\\_computing](https://en.wikipedia.org/wiki/Trojan_horse_computing).

53. <https://en.wikipedia.org/wiki/CryptoLocker> laatstelijk geraadpleegd 26 augustus 2025.

stortte de beurs in toen een zeer groot deel van de daar aangehouden Bitcoins (ongeveer 650.000) verdwenen bleken. Later bleek dat deze Bitcoins stapsgewijs weggenomen waren uit de wallet van Mt Gox gedurende een langere periode. Het zegt veel over de sterk stijgende waarde van Bitcoin dat de resterende Bitcoin al snel voldoende waard bleken om de gedupeerde houders alsnog schadeloos te stellen in fiatvaluta.<sup>54</sup> Dit financiële debacle zorgde er echter wel voor Japan versneld een uitgebreid wettelijk reguleringsregime opzette voor bepaalde cryptoactiva-dienstverlening zoals cryptoactiva beurzen.<sup>55</sup>

## 2.6. Langzame stappen richting een regulerend kader

Ook in de rest van de wereld zaten de autoriteiten niet stil. Er werd zowel op nationaal niveau als binnen internationale gremia, zoals de De Financial Action Task Force (nader: FATF)<sup>56</sup> en de Europese Unie, druk overlegd over wat de correcte wijze zou zijn om de cryptoactiva en de onderliggende (blockchain-)technologie op de juiste wijze tegemoet te treden, en uitwassen te bestrijden. Het Amerikaanse *Financial Crimes Enforcement Network* (nader: FinCen) van het Amerikaanse *Department of the Treasury* leek als eerste een werkbaar plan van aanpak te hebben gevonden. FinCen kwam reeds in maart 2013 met een *interpretative guidance* van bancaire regelgeving waarin het aangaf dat het bepaalde Amerikaanse bancaire regelgeving<sup>57</sup> zo zou interpreteren dat partijen die fiatgeld omwisselen van en naar cryptoactiva door FinCen als *Money Service Bureau* zou worden aangemerkt. Daarmee zouden die partijen komen te vallen onder reeds geldende *Anti Money Laundering* (nader: AML) verplichtingen voor bepaalde financiële instellingen. De toepassing van die regelgeving op deze zogenaamde op- en afritten van de cryptoactivawereld, hield onder meer in dat dergelijke partijen zich bij de overheid dienden te registreren, en verplicht werden tot cliëntenonderzoek en transactiemonitoring.<sup>58</sup> Het duurde echter nog tot 2015 dat FinCen de eerste grote boete op zou leggen voor overtreding van die regels.<sup>59</sup>

In 2014 bracht het FATF diens eerste rapport uit over de potentiële (witwas)risico's van cryptoactiva.<sup>60</sup> Ook de European Banking Authority kwam in 2014 met een rapport, waarin het adviseerde om, gezien de complexe en internationale problematiek die rijst bij het reguleren van cryptoactiva, in ieder geval de dienstverleners die de op- en afrit tot de cryptoactivawereld verleenden, AML-verplichtingen op te leggen via Europese regelgeving.<sup>61</sup> Concreet zou dat betekenen dat ook in Europa de partijen die het omwisselen van fiatvaluta naar cryptoactiva (en andersom) verzorgden, zouden worden verplicht tot registratie, cliëntonderzoek en transactiemonitoring.

Ook in de EU kwam reeds in 2016 een concept antiwitwasrichtlijn met betrekking tot de problematiek gereed.<sup>62</sup> waarbij, zoals in Amerika reeds tot uitvoering gebracht, en door de European Banking Authority voorgesteld, de op- en afritten van de cryptoactivawereld zouden worden gereguleerd. Het zou echter het nog geruime tijd duren voordat dat regelgevend kader daadwerkelijk van kracht zou worden.

## 3. Cryptoactiva-criminaliteit wordt vanaf 2016 meer gemeengoed

Na de eerste zaken waarin cryptoactiva een voorname faciliterende rol speelden, volgden nadere strafbare feiten waarin cryptoactiva een rol speelde elkaar snel op. Vooral vanaf 2016 is in veel cijfers een sterke jaarlijkse toename te zien,<sup>63</sup> vermoedelijk mede veroorzaakt door de toegenomen populariteit van cryptoactiva en de toegenomen waarde daarvan. Ik zal hieronder een aantal van de meest voorkomende vormen van dergelijke criminaliteit bespreken.

Het is bij cijfers over de toename van cryptoactiva-criminaliteit overigens wel nuttig om in gedachten te houden dat, ook door de steeds verdergaande popularisering van cryptoactiva, het percentage van de waarde van cryptoactiva dat in verband kan worden gebracht met criminaliteit ieder jaar juist afneemt. Daarnaast mag worden opgemerkt dat de waarde van cryptoactiva die in verband kan worden gebracht met criminaliteit nog steeds zeer beperkt

54. <https://tweakers.net/nieuws/222442/failliete-bitcoinbeurs-mt-gox-begint-proces-terugbetaling-bitcoin-crediteuren.html> Opgemerkt mag daarbij worden dat de daadwerkelijke terugbetaling schijnbaar nog gaande is.

55. <https://www.japantimes.co.jp/business/2024/10/21/markets/karpeles-japan-return/> en Takato Fukui, Keisuke Hatano, Takeshi Nagese, Huan Lee Tan, 'Blockchain, Legal 500 Country Comparative Guides 2024', 2025 Legalease Ltd, p. 1.

56. De Financial Action Task Force (on Money Laundering) is een intergouvernementele organisatie die in 1989 op initiatief van de G7 werd opgericht om beleid te ontwikkelen ter bestrijding van het witwassen van geld. De FATF stelt normen vast en bevordert de implementatie van wettelijke, regelgevende en operationele maatregelen bij de lidstaten. Het kan echter zelf geen bindende regelgeving uitbrengen.

57. Dit betreft voornamelijk onderdelen van de *Bank Secrecy Act* van 1970, 12 U.S.C. 1829b, 12 U.S.C. 1951-1960, 31 U.S.C.

5311-5314, 5316-5336 (zoals geamendeerd door ondermeer de *Money Laundering Control Act* van 1986, 36).

58. FinCen Guidance of 18 March 2013, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN 2013-G001.

59. Dit betrof een boete van 700.000 aan Ripple labs voor het ongeregistreerd aanbieden van cryptoactiva (XRP) tegen betaling van fiatgeld en het niet bezitten van adequaat AML-beleid, zie <https://web.archive.org/web/20150512222302/http://>

60. *Virtual Currencies Key Definitions and Potential AML/CTF Risks*, FATF Report June 2014.

61. EBA Opinion on 'virtual currencies', EBA/Op/2014/08, European Banking Authority 4 July 2014.

62. Proposal for a Directive Of The European Parliament And Of The Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, Straatsburg, 5 juli 2016.

63. Vgl. bijvoorbeeld <https://cryptohead.io/research/crypto-crime/> laatstelijk geraadpleegd op 26 augustus 2025.

is vergeleken met de waarde van contant geld dat in verband kan worden gebracht met criminaliteit.<sup>64</sup>

#### 4. Enkele veelvoorkomende en vormen van cryptoactivacriminaliteit

##### 4.1. 'Hacken' van cryptoactiva

Hacken van cryptoactiva betreft het wederrechtelijk binnendringen in de digitale infrastructuur van cryptobeurzen, wallets of blockchain-gerelateerde systemen, met als doel toegang te verkrijgen tot cryptoactiva. Deze vorm van criminaliteit maakt vaak gebruik van technische kwetsbaarheden in software of fouten van beheerders of gebruikers. In augustus 2021 werd bijvoorbeeld door een hacker misbruik gemaakt van een kwetsbaarheid in de software van *Poly Network* en werd meer dan USD 600 miljoen aan cryptoactiva weggenomen. De hacker gaf kort daarna aan dat hij enkel wilde aantonen dat de software onveilig was, en gaf uiteindelijk al de gestolen cryptoactiva terug.<sup>65</sup>

##### 4.2. Ransomware-aanvallen met cryptoactivabetaaling

Na de eerder besproken Cryptolocker trojan heeft ransomware een periode een aanzienlijke toename gekend. Ransomware is zoals eerder besproken kwaadaardige software die bestanden of systemen versleutelt, waarna losgeld vaak in cryptoactiva wordt geëist om toegang te herstellen. Dergelijke aanvallen richten zich op zowel individuen, ondernemingen als kritieke infrastructuur en worden vaak uitgevoerd door georganiseerde criminele groeperingen. De WannaCry-aanval in 2017 gebruikte een onbekende<sup>66</sup> *zero day* kwetsbaarheid in Windows-systemen om wereldwijd meer dan 300.000 computers te versleutelen, waarbij de daders losgeld vroegen in Bitcoin.<sup>67</sup>

##### 4.3. Phishing in relatie tot cryptoactiva

Phishing betreft het misleiden van slachtoffers, doorgaans via e-mails of valse websites, om vertrouwelijke informatie zoals privésleutels, *seed phrases*<sup>68</sup> of inloggegevens van cryptowallets of beurzen prijs te geven, vaak door het slachtoffer te misleiden tot

het inloggen op een nagebootste inlogpagina. De aanvallen zijn overwegend zeer professioneel opgezet en bootsen vaak haast naadloos officiële communicatie van bekende platforms na. In maart 2022 werd bijvoorbeeld het Ronin Network, verbonden aan het populaire blockchain-spel *Axie Infinity*, slachtoffer. Criminelen wisten via een phishingaanval *validator nodes* over te nemen en zo USD 620 miljoen dollar aan Ethereum en USDCoin<sup>69</sup> te stelen.

##### 4.4. Cryptojacking (illegaal minen van cryptoactiva)

Cryptojacking houdt in dat criminelen, zonder toestemming van de eigenaar, de rekenkracht van een computer, smartphone of server gebruiken om cryptoactiva te minen. Dit gebeurt via geïnfecteerde software of webscripts, vaak zonder dat het slachtoffer zich hiervan bewust is, maar met nadelige gevolgen voor apparaatprestaties en energierekening. Coinhive, een programma dat oorspronkelijk leek te zijn ontwikkeld als alternatief voor het tonen van reclames op websites<sup>70</sup> werd tot het opdoeken daarvan in 2019 al snel de meest gebruikte software voor cryptojacking.<sup>71</sup>

##### 4.5. Oplichting via rug pulls

Bij *rug-pulls* zetten criminelen schijnbaar legitieme cryptoprojecten op, inclusief websites en whitepapers, om investeerders te overtuigen die cryptoactiva te kopen. Nadat voldoende geld is opgehaald, verdwijnen de oprichters met de opgehaalde fondsen. In 2021 werd bijvoorbeeld de Squid Game Token gelanceerd, gebaseerd op de populaire Netflix-serie. De ontwikkelaars blokkeerden verkoopmogelijkheden en verdwenen met circa 3 miljoen USD aan investeerdersgeld.<sup>72</sup> De *One Coin* oprichters maakten het nog bonter, en verkochten miljarden aan pre-sale tokens alvorens te verdwijnen zonder dat ooit één coin was gemint.<sup>73</sup> De *hard rugpull* lijkt de laatste jaren plaats te maken voor de *soft* of *slow rugpull*, waar niet langer in een keer gecashd wordt, maar waarbij de oplichters een project geleidelijk laten afsterven met meenamen van de geïnvesteerde fondsen in plaats van dit in een plotselinge "*rug pull*" te doen.

64. Europol Spotlight, Cryptocurrencies: Tracing The Evolution Of Criminal Finances 2022, ISBN 978-92-95220-37-9.

65. [https://en.wikipedia.org/wiki/Poly\\_Network\\_exploit](https://en.wikipedia.org/wiki/Poly_Network_exploit) laatstelijk geraadpleegd op 26 augustus 2025.

66. De kwetsbaarheid was overigens wel bekend bij de NSA, en die kennis werd buitgemaakt door hackergroep de Shadow Brokers, die de onbekende kwetsbaarheid ongeveer een maand voor de WannaCry aanval lekte op het internet.

67. [https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) laatstelijk geraadpleegd op 26 augustus 2025.

68. Dit betreft een verzameling woorden die gebruik kan worden om een cryptoactivawallet te herstellen.

69. [https://en.wikipedia.org/wiki/USDC\\_\(cryptocurrency\)](https://en.wikipedia.org/wiki/USDC_(cryptocurrency)) laatstelijk geraadpleegd op 26 augustus 2025.

70. <https://www.coindesk.com/markets/2018/02/13/salon-offers-readers-choice-between-ads-and-mining-monero> laatstelijk geraadpleegd op 30 augustus 2025.

71. <https://en.wikipedia.org/wiki/Cryptojacking> laatstelijk geraadpleegd op 30-08-2025.

72. [https://en.wikipedia.org/wiki/2021\\_Squid\\_Game\\_cryptocurrency\\_scam](https://en.wikipedia.org/wiki/2021_Squid_Game_cryptocurrency_scam) laatstelijk geraadpleegd op 26 augustus 2025.

73. <https://blockchain.news/flashnews/crypto-trading-alert-extraction-targets-reached-as-slow-rug-pull-signals-merge-what-traders-need-to-know> en <https://en.wikipedia.org/wiki/OneCoin> laatstelijk geraadpleegd op 26 augustus 2025.

#### 4.6. Valse cryptoactivabeleggingsplatforms

Er zijn op het internet verschillende oplichtingsstructuren actief die zich voordoen als cryptoactivabeleggingsplatform, maar eigenlijk een oplichtingsvorm betreffen waarbij geen van de gelden belegd worden in cryptoactiva, en de belegger zijn geld nooit meer terugziet.<sup>74</sup> Om slachtoffers naar dat valse platform te lokken, wordt vaak gebruik gemaakt van een aantal specifieke oplichtingstrucs.

##### 4.6.1. 'Pig butchering'

*Pig Butchering* is een vorm van een datingfraude waarbij slachtoffers via langdurig online contact – vaak via datingapps, chatapps of social media – na het eerst opbouwen van een emotionele band, door hun vermeende geliefde misleid worden overtuigd om geld in fictieve beleggingsplatformen te investeren. De oplichters nemen ruim de tijd om vertrouwen te winnen en presenteren zich vaak als knap uitzijnde personen. Steeds meer slachtoffers raken hun spaargeld kwijt aan zogenaamde cryptobeleggingsplatforms die hen werden gepresenteerd door vermeende online geliefden. Slachtoffers kunnen in het algemeen hun geld eenvoudig "investeren", maar nooit meer opnemen.<sup>75</sup> In Kansas in de Verenigde Staten is zelfs een bank ten onder gegaan in een Pig Butchering scam, omdat de CEO daarvan maar liefst 47 miljoen dollar in een fictief cryptoplatform had gestoken op aangeven van een persoon die hij enkel kende via het internet.<sup>76</sup>

##### 4.6.2. Valse BN-er nieuwsberichten

In Nederland zijn in het verleden veel nepadvertenties met Jort Kelder, John de Mol, Chantal Janzen en andere bekende Nederlanders gebruikt om mensen te misleiden tot het beleggen in valse cryptoactivaplatforms.<sup>77</sup> Deze advertenties presenteerden vaak zich als een nieuwsbericht van een betrouwbare krant, waaruit zou blijken dat de betreffende bekende Nederlander zogenaamd zeer veel geld verdiende met beleggen in cryptoactiva, en bevatten een doorverwijzing naar het valse beleggingsplatform dat de bekende Nederlander daarvoor zou gebruiken. De advertenties werden online verspreid via een heel scala trucs om zowel de online adver-

tentieplatforms als het publiek te misleiden, wat tot grote schade leidde voor de slachtoffers die uiteindelijk hun geld kwijt waren aan niet bestaande cryptoactivabeleggingen.<sup>78</sup>

#### 4.7. Pump & dump fraude

*Pump & dump*-constructies zijn gecoördineerde fraudestructuren die zijn overgewaaid van de wereld van de *penny-stocks* naar de wereld van de cryptoactiva, waarbij oplichters misleidende of verzonden informatie gebruiken om de prijs van een bepaald cryptoactiva op te drijven. Eerst zorgen de fraudeurs dat zij de grootste positie hebben in de beoogde, verder vaak waardeloze cryptoactiva. Nadat zij de cryptoactiva voor een lage prijs hebben aangeschaft, verspreiden zij valse berichten, vaak via agressieve marketingcampagnes en met gebruik van sociale media, om nieuwe investeerders aan te trekken. De fraudeurs gebruiken daarnaast vaak ook 'wash trading' om de prijs op te drijven. Dit is het heimelijk met betrokken partijen over en weer handelen met gebruik van verschillende wallets, waardoor de openbare markt cijfers lijken aan te geven dat de vraag naar, en prijs van, een bepaalde cryptoactiva snel toeneemt.<sup>79</sup>

Nadat de fraudeurs de prijs van de betreffende cryptoactiva voldoende hebben opgeschroefd, dumpen ze al hun cryptoactiva waardoor de prijs weer keldert. Door deze plotselinge uitverkoop blijven nietsvermoedende beleggers<sup>80</sup> zitten met sterk gedevalueerde en vaak waardeloze cryptoactiva. Waar bij de eerdergenoemde valse cryptoactivaplatforms vaak valse advertenties met bekende Nederlanders worden gebruikt, lijkt bij pump & dump daarentegen vaak sprake van werkelijke betrokkenheid van (internet)beroemdheden waarbij die beroemdheden vaak ook worden misleid om reclame te maken voor de cryptoactiva die kort daarna gedumpt zullen worden.<sup>81</sup>

#### 4.8. Darknetmarkets

Cryptoactiva worden nog steeds gebruikt bij illegale transacties op darknetmarkets, hoewel de vorm van betaling lijkt te zijn verschoven van Bitcoin

74. De grens tussen een rug-pull, een vals cryptoproject en pump & dump fraude is overigens niet telkens helder, en er bestaat veel overlap.

75. Met uitzondering van soms een kleine opname in het begin, om het slachtoffer verder te overtuigen van de legitimiteit van het valse platform, en hem te overtuigen nog meer geld te investeren.

76. <https://eu.cjonline.com/story/news/crime/2024/05/28/kansas-bank-ceo-embezzled-millions-in-crypto-scheme-that-killed-bank/73843999007/> laatstelijk geraadpleegd op 26 augustus 2025.

77. <https://opgelicht.avrotros.nl/hulp/vraag-antwoord/artikel/cybercriminelen-misbruiken-bn-ers-voor-valse-bitcoin-advertenties-ik-werd-echt-in-het-verhaal-meegetrokken/> en [https://www.occrp.org/en/project/scam-empire-celebrities-voice-anger-and-frustration-over-online-](https://www.occrp.org/en/project/scam-empire-celebrities-voice-anger-and-frustration-over-online-scam-ads-that-target-fans)

[scam-ads-that-target-fans](https://www.rtl.nl/nieuws/economie/artikel/5257164/bitcoin-nepadvertenties-nederlandse-rechter-cfd-beleggen) laatstelijk geraadpleegd op 26 augustus 2025.

78. <https://www.rtl.nl/nieuws/economie/artikel/5257164/bitcoin-nepadvertenties-nederlandse-rechter-cfd-beleggen>, laatstelijk geraadpleegd op 26 augustus 2025.

79. Vgl. [https://en.wikipedia.org/wiki/Wash\\_trade](https://en.wikipedia.org/wiki/Wash_trade) laatstelijk geraadpleegd op 30 augustus 2025.

80. Een meer cynische cryptoactivadeskundige zou daarbij mogelijk opmerken dat een aanzienlijk deel van deze cryptoactivabeleggers het 'pumpen' zal vermoeden en gecalculereerd hopen daar nog voor de 'dump' uit te stappen.

81. <https://www.bnr.nl/nieuws/financieel/10507645/influencers-aangepakt-na-illegale-cryptoreclames> en <https://www.metronieuws.nl/televisie/2022/04/cryptoreclames-cryptovaluta-influencers-regelgeving/> laatstelijk geraadpleegd op 26 augustus 2025.

naar privacycoins<sup>82</sup> zoals Monero.<sup>83</sup> Naast de eerder beschreven marktplaats Silk Road, waren bekende darknetmarkets Alphabay en Hansa. Deze werden met een niet geringe inbreng van de Nederlandse autoriteiten door een internationaal samenwerkingsverband van opsporingsdiensten opgerold.<sup>84</sup> De populariteit van de ouderwetse markts die gehost werden op het darkweb lijkt momenteel echter af te nemen door het in toenemende mate populaire alternatief van openbare illegale handelschats en handelskanalen op Telegram.<sup>85</sup>

#### 4.9. Waardeoverdracht in het criminele milieu

Ook buiten criminele marktplaatsen op het darkweb worden cryptoactiva vanwege het pseudonieme karakter inmiddels gebruikt als betaalmiddel voor zaken die het daglicht niet kunnen verdragen zoals handelshoeveelheden drugs,<sup>86</sup> grootschalige wapenhandel,<sup>87</sup> financiering van terrorisme<sup>88</sup> en kinderpornografie.<sup>89</sup> De FIOD ziet een grote toename van digitale criminele geldstromen,<sup>90</sup> en volgens onze Minister is inmiddels zelfs sprake van een ‘financieel ondergronds stelsel’ waar partijen op grote schaal crimineel vermogen verplaatsen door cash- en cryptotransacties.<sup>91</sup>

#### 4.10. Witwassen

In de lagere rechtspraak werd in lijn met de Runcap-jurisprudentie<sup>92</sup> al relatief snel aangenomen

dat Bitcoin (en daarmee vermoedelijk ook alle andere cryptoactiva) een voorwerp was in de zin van artikel 420bis en 420quater Sr.<sup>93</sup> De Hoge Raad heeft dat standpunt echter pas in 2024 uitdrukkelijk bevestigd.<sup>94</sup> Door de zeer ruime delictomschrijving van artikel 420bis t/m 420quater kan bij alle in dit hoofdstuk genoemde gedragingen, alsook bij andere misdrijven waarbij cryptoactiva betrokken is, vaak al snel tevens sprake zijn van witwassen.<sup>95</sup>

Als we kijken naar witwassen in enge zin, dus witwassen waarbij het daadwerkelijke doel is de illegale oorsprong van voorwerpen te verhullen,<sup>96</sup> valt op dat binnen cryptoactivawereld verschillende professionele partijen actief zijn die het witwassen van crimineel vermogen middels cryptoactiva als dienst aanbieden. Vaak wordt daarbij gebruik gemaakt van tumblers, mixers, ongereguleerde Over the Counter (nader : OTC) diensten en ongereguleerde cryptoactivabeurzen, waarop ik straks nog kort zal ingaan in het kader van de (on)toereikendheid van de eerste Nederlandse strafrechtelijke regelgeving.

### 5. De eerste Nederlandse strafrechtelijke regulerende kaders

Hoewel de E-Money richtlijn mede zijn aanleiding vond in e-Cash en diens tijdgenoten, bood deze richtlijn weinig soelaas voor handhaving van cryptoactiva. Dit, nu deze richtlijn in feite enkel zag op nieuwe digitale transactievormen van fiatvaluta, waar nog steeds een vorderingsrecht op een regu-

82. Dit betreffen coins waarvan Monero en Zcash twee van de bekendste zijn, zie <https://en.wikipedia.org/wiki/Monero> en <https://en.wikipedia.org/wiki/Zcash> laatstelijk geraadpleegd op 1 september 2025.

83. K. Bahamazava en R.Nanda, *The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence*, Forensic Science International: Digital Investigation, nr. 40, 2022, ISSN 2666-2817.

84. [https://en.wikipedia.org/wiki/Operation\\_Bayonet\\_\(dark\\_net\)](https://en.wikipedia.org/wiki/Operation_Bayonet_(dark_net)) laatstelijk geraadpleegd op 26 augustus 2025.

85. <https://www.newsweek.com/telegram-darknet-researchers-analyzed-1950811> en <https://www.wired.com/story/the-internets-biggest-ever-black-market-shuts-down-after-a-telegram-purge/> laatstelijk geraadpleegd op 26-08-2025. Telegram is een versleutelde *instant messaging service* die onder meer zeer grote en openbaar toegankelijke groepsgesprekken ondersteunt, in welke gesprekken de deelnemers onder onherleidbaar pseudoniem kunnen communiceren.

86. <https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/> laatstelijk geraadpleegd op 26 augustus 2025.

87. <https://www.wsj.com/finance/currencies/crypto-fuels-russian-shadow-trade-for-weapons-parts-1bfdc1a1> laatstelijk geraadpleegd op 01-09-2025.

88. <https://www.fiod.nl/aanhouding-vanwege-terrorismedinanciering-met-bitcoins/> laatstelijk geraadpleegd op 26 augustus 2025.

89. <https://humantraffickingfront.org/cryptocurrency-use-in-the-online-sexual-exploitation-of-children/> laatstelijk geraadpleegd op 26 augustus 2025.

90. Bijlage bij *Kamerstukken II*, 32715, nr. 5 (Jaarverslag FIOD 2024), p. 3.

91. <https://www.rijksoverheid.nl/actueel/nieuws/2025/06/10/minister-van-weel-blijft-volop-inzetten-op-doorbreken-criminele-verdienmodellen> laatstelijk geraadpleegd op 26 augustus 2025.

92. Hoge Raad 31 januari 2012, ECLI:NL:HR:2012:BQ9251. In deze zaak oordeelde de Hoge Raad dat digitale gegevens onder omstandigheden als een ‘goed’ (in de zin van artikel 310 Sr) konden aangemerkt. Daarbij achtte de Hoge Raad onder meer relevant of de gegevens waarde hebben voor de betrokken partijen, en of de beschikkingsmacht over de gegevens over kan gaan van de ene partij op de andere.

93. Rechtbank Noord-Holland 10 maart 2017, ECLI:NL:RBNHO:2017:1937 is de oudste zaak die ik hierover op [rechtspraak.nl](https://rechtspraak.nl) aantrof.

94. Hoge Raad 25 juni 2024, ECLI:NL:HR:2024:887, r.o. 3.7.

95. Geheel terzijde valt zelfs de vraag te stellen of de ruime opzet van de strafbaar stelling van witwassen inmiddels niet de een van de voornaamste drijvende factoren is in de toenemende verwevenheid tussen boven en onderwereld, waaronder in de wereld van de cryptoactiva. Door de huidige strafbaarstelling van witwassen (en de brede onderzoeksplichten van veel marktpartijen genoemd in de WWFT) is een crimineel, meer dan hij anders zou zijn, betoogbaar haast genoodzaakt om een legale herkomst te fingeren voor diens criminele inkomsten, waarvoor het opzetten van legale ondernemingen of participeren in legale ondernemingen van anderen de eenvoudigste weg lijkt.

96. <https://www.eurojust.europa.eu/news/criminals-operating-illegal-financial-service-launder-millions-euros-but-not-enough-to-arrest> en <https://www.europol.europa.eu/media-press/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case> laatstelijk geraadpleegd op 27 augustus 2025.

liere financiële dienstverlener tegenover stond.<sup>97</sup> Zo een vorderingsrecht bestond, als een van de centrale uitgangspunten, bij gedecentraliseerde cryptoactiva nu juist niet. Hoewel er in 2013 reeds Kamervragen over werden gesteld, vond de wetgever het nog lang niet nodig aparte (WWFT-)regelgeving in te voeren voor cryptoactiva.<sup>98</sup>

Mede omdat zulke regelgeving volgens de wetgever beter op Europees niveau geregeld kon worden diende nog lang gewacht te worden op de AMLD 5,<sup>99</sup> die pas in afgeronde vorm werd gepubliceerd op 19 juni 2018, met uiterste implementatiedatum 10 januari 2020.<sup>100</sup> Vergelijkbaar met de Amerikaanse regelgeving die al in 2013 was aangepast, schreef die richtlijn zoals eerder aangegeven onder meer voor dat aanbieders van diensten die wisselen tussen cryptoactiva<sup>101</sup> en fiduciaire valuta (en aanbieders van wallet-diensten)<sup>102</sup> onder het toepassingsgebied van de witwasrichtlijn dienden te worden gebracht als meldplichtige entiteiten, waarmee in zekere zin een controle werd gebouwd op de op- en afrit van de cryptoactivawereld.<sup>103</sup> Omdat alle navolgende transacties binnen de cryptoactivawereld in beginsel openbaar en volgbaar zijn in de public ledger van de blockchain, beoogde deze controle een breder toezicht mogelijk te maken op de cryptoactivawereld.

De implementatiewet welke volgde op deze richtlijn, werd uiteindelijk pas op 21 mei 2020 van kracht.<sup>104</sup> Deze implementatiewet bracht voornamelijk wijzigingen aan in de WWFT en de WED. In de WWFT werden middels aanpassingen in artikel 1a aanbieders voor diensten voor het wisselen tussen cryptoactiva (destijds onder de noemer virtuele valuta) en fiduciaire valuta (en aanbieders van wallet-diensten) aangemerkt als instelling voor de WWFT.<sup>105</sup> Deze aanpassing bracht met zich dat deze partijen gehouden waren aan clientonderzoek te doen alvorens tot enige dienstverlening over gaan,<sup>106</sup> transacties te monitoren en ongebruikelijke transacties te melden bij de Financial Intelligence Unit.<sup>107</sup> Daarnaast bracht de implementatiewet middels aanvul-

ling van de WWFT met artikel 23b-23j (oud) een registratieplicht mee bij DNB.<sup>108</sup> Die registratieplicht bij DNB bracht op zijn beurt tevens verschillende verplichtingen met zich in het kader van een integere bedrijfsvoering. Artikel 23g WWFT (oud) verbood tot slot partijen vanuit het buitenland beroeps of bedrijfsmatig diensten wisseldiensten of wallet-diensten aan te bieden, behalve voor zover de aanbieder reeds onder gelijkwaardig toezicht stond in een door de Minister aangewezen land. Tegen overtreding van de regels was veelal zowel bestuursrechtelijke handhaving mogelijk als strafrechtelijke sanctionering middels de WED.<sup>109</sup>

## 5.1. Beperkingen van dit regulerend kader

Deze regelgeving zou, indien wereldwijd consistent geïmplementeerd, waarschijnlijk een zekere mate van succes tegen crimineel misbruik van cryptoactiva hebben kunnen behalen. Echter is nog onvoldoende uitgekristalliseerd in hoeverre dit Europese regelgevend kader in de per definitie internationale en gedecentraliseerde wereld van cryptoactiva niet voornamelijk de administratieve kosten voor welwillende partijen verhoogden, en voor kwaadwillende partijen weinig verschil maakten. Hetzelfde valt overigens in zekere mate in te zeggen voor de later nog te bespreken recente MiCAR en TFR-regelgeving.

Naast deze problematiek met betrekking tot jurisdictie en decentralisatie, namelijk dat er in beginsel weinig tegen te doen is wanneer een Nederlandse consument een aanbieder van wisseldiensten of wallet-diensten van buiten de EU wil gebruiken, bestaan er verschillende andere diensten die het controleren van de op- en afritten van de cryptoactivawereld minder effectief maken. Een aantal van die diensten zal ik hieronder beschrijven.

- 
97. Vgl. artikel 2 lid 2 van E-money Directive 2009/110/EC en implementatie van de definitie elektronisch geld in artikel 1:1 WFT.
98. *Aanhangsel Handelingen II*, 2013-14, nr. 830 (Beantwoording Kamervragen).
99. Richtlijn (EU) 2018/843 Van Het Europees Parlement En De Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU.
100. Richtlijn Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, PB L 156 van 19 juni 2018, artikel 4.
101. Aldaar nog genaamd 'virtuele valuta' maar ziende grotendeels op dezelfde materie als het huidige 'cryptoactiva'.
102. Dat wil zeggen, een (rechts-)persoon die diensten aanbiedt om namens haar cliënten cryptografische privé-sleutels te beveiligen om virtuele valuta aan te houden, op te slaan en over te dragen.
103. Richtlijn (EU) 2018/843 artikel 1 jo Richtlijn (EU) 2015/849 artikel 2 lid 3.
104. Stbl. 2020, 148.
105. Wet van 22 april 2020 tot wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en de Wet toezicht trustkantoren 2018 in verband met de implementatie van richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156) (Implementatiewet wijziging vierde anti-witwasrichtlijn), Stbl. 2020, 146, art 1.
106. Vgl. art. 4 lid 1 WWFT.
107. Vgl. art. 16 WWFT.
108. Implementatiewet wijziging vierde anti-witwasrichtlijn, onderdeel P.
109. Implementatiewet wijziging vierde anti-witwasrichtlijn, Implementatiewet artikel IVA en paragraaf 4.2 WWFT (oud).

## 6. Bemoeilijking van volgen van crypto-activatransactiestromen

### 6.1. Tumblers, mixers en chainhoppers

Hoewel de pseudonimiteit van cryptoactiva zoals gezegd een bepaalde mate van complexiteit van herleidbaarheid tot een gebruiker met zich brengt, maakt het openbare karakter van de public ledger van de blockchain de stromen van cryptoactiva zelf in beginsel zeer eenvoudig volgbaar, wat de privacy allerminst ten goede komt. Er zijn verschillende strategieën bedacht om die volgbaarheid van cryptoactiva te bemoeilijken, waarvan de twee meest voorkomende zijn:

- Mixing services of tumblers: diensten die verschillende cryptotransacties of cryptoactiva op enige wijze samenvoegen en/of mengen, en daarmee de link tussen verzender en ontvanger verhullen;
- Chain hopping: het snel opeenvolgend wisselen tussen verschillende soorten cryptoactiva om cryptoactivatracing te bemoeilijken.

Indien een aanbieder van een privacy tool zoals een mixer, tumbler of chainhopper beseft of zou moeten beseffen dat de cryptoactiva een criminele herkomst heeft, is het handelen zoals eerder opgemerkt strafbaar als witwassen.<sup>110</sup> De moeilijkheid is echter dat, het publieke karakter van de *public ledger* inachtig, tumblers en mixers voor veel cryptoactiva-gebruikers in een reële privacybehoefte voorzien. Indien immers op enig moment de houder van een bepaalde wallet bekend wordt, is het mogelijk om alle transacties van die persoon in het verleden en de toekomst in kaart te brengen. Mede in het licht van de recente golf van ontvoeringen van cryptoactivamiljonairs en hun familieleden,<sup>111</sup> kan een zeker legitiem nut van dergelijke *privacy tools* slecht ontkend worden. Een algeheel verbod op tumblers, mixers en chainhoppers is dan ook niet aan de orde, hoewel uit de jurisprudentie blijkt dat Nederlandse rechters al snel, en betoogbaar soms te snel, bereid zijn een *mens rea* aan te nemen bij de aanbieders van dergelijke privacy tools. In 2024 is bijvoorbeeld een betrokkene bij ‘Tornado-cash’ in Nederland veroordeeld voor ge-

woontewitwassen, nadat een deel van de gebruikers van Tornado Cash crimineel bleek.<sup>112</sup> Tornado-cash was echter een van de meest gebruikte privacy-tools van het Ethereum-netwerk, en leek grotendeels legitieme gebruikers te hebben.

### 6.2. Ongereguleerde beurzen en OTC-diensten

In de EU dienen alle cryptoactivabeurzen en OTC-handelaren onder vergunning te werken en dienen zij zich aan de toepasselijke WWFT-regels te houden omtrent bijvoorbeeld cliëntidentificatie.<sup>113</sup> In verschillende buitenlandse zijn (*peer to peer*) cryptoactivabeurzen en OTC-diensten echter nog ongereguleerd.<sup>114</sup> Indien een beurs of OTC-handelaar<sup>115</sup> geen administratie bijhoudt van de aankopende en verkopende partijen, gaat de kennis van eigendom van cryptoactiva die eerder bij de inrit verkregen was verloren, en wordt de kennis over de afrit niet vastgelegd.<sup>116</sup> Door het internationale karakter van cryptoactiva kan zo steeds meer kennis van de op- en afrit verloren gaan, hetgeen toezicht op enkel de op- en afrit van de cryptoactivawereld steeds minder toereikend maakt om zicht te hebben op de betrokkenen bij cryptoactivastromen.

## 7. Het nieuwe alomvattende EU regelgevend kader van MiCAR en TFR

Hoewel bij de totstandkoming van de Digital Services Act<sup>117</sup> (nader: DSA) als opvolger van de Richtlijn inzake Elektronische Handel oorspronkelijk overwogen werd om verschillende diensten met betrekking tot cryptoactiva en *distributed ledgers* meer uitdrukkelijk onder het bereik van de DSA (en daarmee, waar van toepassing, ook de onder het bereik van de Safe Harbour bepalingen) te brengen,<sup>118</sup> is zulks in de uiteindelijke tekst van de DSA niet gebeurd.

In plaats daarvan heeft de EU besloten een uitgebreid afzonderlijk regelgevend kader te ontwikkelen voor diensten van de informatiemaatschappij die betrekking hebben op cryptoactiva, voornamelijk mid-

110. Daarnaast zal een in de EU gevestigde partij die mixing, tumbling of chain hopping services aanbiedt zich in beginsel moeten houden aan de regels van de Markets in Crypto Asset Regulation en de Transfer of Funds Regulation, op welke regelingen ik later in zal gaan.

111. <https://www.nbcnews.com/tech/crypto/crypto-kidnap-ping-bitcoin-price-crime-rcna215047> laatstelijk geraadpleegd op 1 september 2025.

112. Rechtbank Oost-Brabant 14 mei 2024, ECLI:NL:RBOBR:2024:2069.

113. Er zijn naar mijn weten overigens geen OTC-dienstverleners in Nederland met een vergunning actief.

114. <https://koinly.io/nl/blog/top-no-kyc-crypto-exchanges/> laatstelijk geraadpleegd op 25 augustus 2025.

115. Gelijk aan zoals door de Hoge Raad uitdrukkelijk is overwogen met betrekking tot Hawala-bankieren, lijken ongereguleerde beurzen of OTC-diensten overigens niet enkel door criminele partijen te worden gebruikt, maar worden deze OTC-diensten ook gebruikt als een manier voor handelaren om legale inkomsten uit handel of ar-

beid terug te sturen naar landen met een gebrekkige bancaire sector, of restrictieve currency controls zoals Venezuela of China.

116. Hierbij past overigens de voetnoot dat veel ongereguleerde OTC-diensten en cryptoactivabeurzen in landen met een ontoereikend regelgevend kader, ondanks het gebrek aan toepasselijke regelgeving, desondanks uit eigen beweging aan klantidentificatie en administratie doen.

117. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

118. Vgl. European Parliamentary research Service, *DSA Value Added Assessment*, PE 654.180, October 2020, p. 1, 84, 85 en 229 en Anja Hoffmann & Alessandro Gasparotti, *Liability for illegal content online Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a “Digital Services Act”*, cepStudy, March 2020 p. 32.

dels de Markets in Crypto Asset Regulation<sup>119</sup> (nader: MiCAR,) en de Transfer of Funds Regulation (Nader: TFR).<sup>120</sup> Ik zal daarvan hieronder een kort beeld schetsen.

## 7.1. MiCAR

De MiCAR creëert een uitgebreid regelgevend kader waarin voor verschillende soorten cryptoactiva en cryptoactivadienstverlening verschillende verplichtingen en vergunningen worden geïntroduceerd, en regels worden gesteld met betrekking tot handel met voorwetenschap en marktmanipulatie.<sup>121</sup>

### 7.1.1. Soorten cryptoactiva

Waar de Europese en Nederlandse regelgeving eerder sprak over ‘virtuele valuta’ en daarbinnen geen relevant onderscheid werd aangebracht, brengt de MiCAR niet enkel een hernaaming mee tot ‘cryptoactiva’ (‘crypto-assets’) maar brengt deze tevens een onderscheid aan tussen drie verschillende soorten cryptoactiva, die onder verschillende regulerende kaders worden geplaatst (voor zover die niet al onder andere financiële regelgeving vallen).

Deze drie typen cryptoactiva zijn:<sup>122</sup>

- E-money tokens (EMT’s): dit zijn cryptoactiva die beogen hun waarde te stabiliseren door te verwijzen naar een fiatvaluta.<sup>123</sup> Deze cryptoactiva beogen een elektronisch vervangmiddel voor munten en bankbiljetten te zijn en worden waarschijnlijk gebruikt om betalingen te doen. Hieronder vallen bijvoorbeeld stablecoins zoals Tether, wiens waarde één op één aan de Amerikaanse dollar gekoppeld is.
- Activagerelateerde tokens (*asset referenced tokens of ART’s*): dit zijn cryptoactiva die beogen hun waarde te stabiliseren door te verwijzen naar een andere waarde of recht, of een combinatie daarvan, waaronder een combinatie van fiatvaluta’s. Deze brede categorie is bedoeld om omzeiling te voorkomen en de verordening toekomstbestendig te maken. Hieronder vallen bijvoorbeeld Pax

Gold, een cryptoactiva die aan de goudprijs gekoppeld is, en het (inmiddels ter ziele gegane) Libra-coin project van Facebook, wiens waarde gekoppeld zou zijn aan een gewogen mandje van verschillende fiatvaluta.

- Andere cryptoactiva: hieronder vallen alle cryptoactiva die geen activagerelateerde tokens of e-money tokens zijn. Dit is de grootste groep met de grootste verscheidenheid en onder deze groep worden mede ook alle *utility-tokens* verstaan. Onder deze groep vallen bijvoorbeeld Bitcoin, Ethereum, Litecoin en alle andere cryptoactiva met een enkel fiduciaire waarde, alsmede alle tokens die dat alleen bedoeld zijn om toegang te verlenen tot een dienst die door de uitgever ervan wordt aangeboden.<sup>124</sup> Bij die laatste kan je bijvoorbeeld denken aan Filecoin, die gebruikt wordt om te betalen voor decentrale gegevensopslag binnen het Filecoin netwerk.

De zogenaamde non-fungible tokens (NFT’s) vooral bekend van de op de blockchain geregistreerde en verhandelbare digitale kunstwerken,<sup>125</sup> vallen in beginsel niet onder de MiCAR, nu deze niet als met elkaar inwisselbaar worden beschouwd. Wel merkt de preambule op dat wanneer NFT’s in een grote serie of verzameling worden uitgegeven, dat moet worden beschouwd als een indicator dat ze mogelijk wél als inwisselbaar moeten worden gezien. Het louter toekennen van een unieke identificatiecode aan een NFT is volgens de preambule op zichzelf niet voldoende om deze als uniek en niet-vervangbaar te classificeren. Of dit betekent dat populaire NFT’s zoals de Bored Apes<sup>126</sup> of de Cryptopunks,<sup>127</sup> (die beiden in een grote oplage zijn gemaakt die vaak slechts in details verschillen) nu wel of niet de definitie van cryptoactiva onder de MiCAR zullen vallen, lijkt een zaak die later door de rechter zal moeten worden uitgemaakt.

De MiCAR is daarnaast niet van toepassing op cryptoactiva die tevens vallen onder de definitie van elders reeds in EU recht gereguleerde financiële instrumenten, deposito’s, geldmiddelen en verzekeringen.<sup>128</sup> De European Securities and Markets Authority (nader: ESMA) heeft richtlijnen uitgebracht over

119. Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactiva-markten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937.

120. Voorstel voor een Verordening van het Europees Parlement en de Raad tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering, 20 juli 2021, 2021/0239 (COD).

121. In MiCAR titel VI.

122. MiCAR preambule sub 18.

123. Niet zijnde elektronisch geld zoals gedefinieerd in Richtlijn 2009/110/EG.

124. MiCAR art. 3 ahf en sub 9.

125. Zoals het digitale kunstwerk *Everdays: the first 5000 days* van de kunstenaar Beeple, waarvan de NFT door veilinghuis Christie’s in 2021 voor bijna USD 70 MLN werd geveild.

126. [https://en.wikipedia.org/wiki/Bored\\_Ape](https://en.wikipedia.org/wiki/Bored_Ape) laatstelijk geraadpleegd op 27 augustus 2025.

127. <https://en.wikipedia.org/wiki/CryptoPunks> laatstelijk geraadpleegd op 27 augustus 2025.

128. Meer specifiek stelt de preambule van MiCAR daarover onder 9: ‘Bijgevolg sluit deze verordening uitdrukkelijk cryptoactiva van haar toepassingsgebied uit die als financiële instrumenten in de zin van Richtlijn 2014/65/EU kunnen worden aangemerkt, cryptoactiva die kunnen worden aangemerkt als deposito’s in de zin van Richtlijn 2014/49/EU van het Europees Parlement en de Raad (7), met inbegrip van gestructureerde deposito’s in de zin van Richtlijn 2014/65/EU, cryptoactiva die kunnen worden aangemerkt als geldmiddelen in de zin van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad (8), behalve indien zij kunnen worden aangemerkt als elektronischgeldtokens (“e-moneytokens”), cryptoactiva die kunnen worden aangemerkt als securitisatieposities in de zin van Verordening (EU) 2017/2402 van het Europees Parlement en de Raad (9), en cryptoactiva die als schade- of levensverzekeringscontracten, pensioenproducten of -regelingen en socialezekerheidsregelingen kunnen worden aangemerkt.’

wanneer een cryptoactiva als zo een financieel instrument moet worden aangemerkt.<sup>129</sup> Dergelijke cryptoactiva zullen in beginsel onder dat andere regelgevend kader blijven vallen. De richtlijnen van de ESMA benadrukken onder meer dat inhoud boven vorm voorrang heeft, en dat een cryptoactivum als financieel instrument dient te worden aangemerkt indien het onder de definitie van een effect valt in de zin van MiFID II. In dat geval dienen cryptoactiva onderworpen te zijn aan dezelfde regels als traditionele financiële instrumenten, in overeenstemming met het beginsel van technologische neutraliteit.<sup>130</sup> De uitgifte en toelating tot de handel<sup>131</sup> van nieuwe cryptoactiva binnen de EU is met de komst van de MiCAR aan strenge regels gebonden, in ieder geval vergeleken met de eerdere leemte in regelgeving hieromtrent. Kort gezegd moet de uitgever van alle soorten cryptoactiva een (mede) in de EU gevestigde rechtspersoon zijn.<sup>132</sup> Bij alle soorten cryptoactiva dient tevens een whitepaper opgesteld te worden met informatie over de uitgever, het project, de rechten en plichten verbonden aan de cryptoactiva, de onderliggende technologie en de risico's.<sup>133</sup> De uitgever is aansprakelijk voor onvolledige of incorrecte informatie in het whitepaper, welke aansprakelijkheid niet contractueel kan worden uitgesloten.<sup>134</sup> De reclame die voor het cryptoactivum gemaakt wordt, moet in lijn zijn met het whitepaper en mag niet misleidend zijn.<sup>135</sup>

Uitgevers van e-money tokens moeten daarnaast beschikken over een vergunning als kredietinstelling<sup>136</sup> of als elektronisch geldinstelling.<sup>137</sup> De uitgever van e-money tokens moet verder op verzoek van de houder de e-money tokens tegen nominale waarde terugbetalen in de valuta waarop het token betrekking heeft<sup>138</sup>. Dit gaat uiteraard gepaard met verschillende dekkingsverplichtingen.

Activagerelateerde tokens mogen slechts worden uitgegeven door kredietinstellingen of rechtspersonen die over een vergunning beschikken krachtens MiCAR,<sup>139</sup> verleend door de bevoegde autoriteit van een lidstaat. Voor de vergunning worden onder meer eisen gesteld aan het governancekader en het beheer van de activa reserves.<sup>140</sup> Voor 'significant activagerelateerde tokens' (kort gezegd: tokens met meer dan tien miljoen houders of een kapitalisatie van meer dan 5 miljard euro) gelden aanvullende eisen opgelegd door de Europese Bankautoriteit waaronder

extra kapitaalvereisten, toezicht en stresstests.<sup>141</sup>

De Nederlandse Bank is in Nederland primair verantwoordelijk voor het toezicht op de uitgifte van activagerelateerde tokens en e-money tokens, en de Autoriteit Financiële Markten is primair verantwoordelijk voor het toezicht op uitgevers van andere soorten cryptoactiva, alsmede het toezicht op aanbieders van cryptoactivadiensten, en het voorkomen van marktmisbruik.<sup>142</sup>

### 7.1.2. Vergunningsplicht voor CASP's

Met de introductie van MiCAR wordt een zeer brede en uiteenlopende groep cryptoactivadiensverleners, in de literatuur veelal aangeduid met CASP's (cryptoasset service providers), verplicht om over een vergunning van de AFM te beschikken om binnen de Europese markt te kunnen opereren.<sup>143</sup> Het betreft de volgende diensten:<sup>144</sup>

- a. bewaren en beheren van cryptoactiva namens cliënten;
- b. exploiteren van een cryptoactivahandelsplatform;
- c. omwisselen van cryptoactiva voor geldmiddelen;
- d. omwisselen van cryptoactiva voor andere cryptoactiva;
- e. uitvoeren van cryptoactivaorders namens cliënten;
- f. plaatsen van cryptoactiva;
- g. ontvangen en doorgeven van cryptoactivaorders namens cliënten;
- h. verlenen van advies over cryptoactiva;
- i. verzorgen van portefeuillebeheer voor cryptoactiva;
- j. verlenen van cryptoactivaoverdrachtdiensten namens cliënten.

Aan al deze diensten worden verschillende algemene en dienstspecifieke eisen gesteld met betrekking tot de vergunningsverlening.<sup>145</sup> De vergunning is in beginsel in de gehele EU geldig, met enkel een meldingsplicht indien men diensten wil verlenen in een andere lidstaat dan de lidstaat waarin de vergunning verkregen is.<sup>146</sup> Die vergunningsvereisten kunnen zien op kapitaalvereisten, eisen aan de bekwaamheid en integriteit van invloedrijke personen binnen de dienstverlener, interne controles, bedrijfsvoering

129. ESMA Richtsnoeren betreffende de voorwaarden en criteria voor de kwalificatie van cryptoactiva als financiële instrumenten van 19 maart 2025, zie <https://www.esma.europa.eu/document/guidelines-conditions-and-criteria-qualification-crypto-assets-financial-instruments>.

130. ESMA Richtsnoeren betreffende de voorwaarden en criteria voor de kwalificatie van cryptoactiva als financiële instrumenten van 19 maart 2025, paragraaf 14 en 15.

131. Ter vereenvoudiging van dit artikel zal ik enkel spreken over de uitgifte, de toelating tot de handel is aan min of meer gelijke regels gebonden.

132. MiCAR art 4 lid 1 sub a.

133. MiCAR art 6, 19 en 51.

134. MiCAR Art.15, 26, en 52.

135. MiCAR art. 7, 29 en 53.

136. Overeenkomstig Richtlijn 2009/110/EG, zie MiCAR preamble onder 66.

137. Overeenkomstig Richtlijn 2013/36/EU, zie MiCAR preamble onder 66.

138. MiCAR art 49.

139. MiCAR art 16 lid 1.

140. MiCAR art. 18.

141. MiCAR art. 43-45.

142. Kamerstukken II, 2023-25, 36 527, nr. 3 en <https://www.afm.nl/nl-nl/sector/cryptopartijen/toezicht>

143. Behalve als de CASP al beschikt over een vergunning als kredietinstelling en voldoet aan de vereisten van artikel 60 MiCAR.

144. MiCAR artikel 3 sub 16.

145. MiCAR Titel 5.

146. MiCAR artikel 59 lid 7 en 65.

en de financiële integriteit. De eisen gaan soms heel ver, zoals de eis dat een aanbieder van een cryptoactivahandelsplatform geen cryptoactiva op het platform mag laten verhandelen met een ingebouwde privacyfunctie, zoals de populaire privacycoins Monero of Zcash.<sup>147</sup> In het algemeen kan verder vastgesteld worden dat de MiCAR een zeer ruime definitie geeft van ‘cryptoactiva diensten’, waarmee niet eenvoudig dienstverlening op het vlak van cryptoactiva valt te bedenken die daar niet onder valt. Dit is tevens van belang in het kader van de gelijktijdig ingevoerde *Transfer of Funds Regulation* waar ik later over zal komen te spreken.

### 7.1.3. Voorkomen van marktmisbruik

In Titel VI geeft de MiCAR verschillende regels omtrent marktmisbruik, omdat cryptoactiva in algemene zin niet vallen onder de Market Abuse Regulation 596/2014 (nader: MAR). Dit, omdat cryptoactiva veelal niet zijn aan te merken als financieel instrument. De cryptoactivawereld biedt daarentegen echter dezelfde, en betoogbaar meer, mogelijkheden om marktmisbruik te plegen.<sup>148</sup> Om dergelijk misbruik tegen te gaan worden in MiCAR gelijksoortige regels omtrent marktmisbruik ingevoerd als in de MAR. Ten eerste dient informatie die als voorwetenschap kan worden aangemerkt (zijnde kort gezegd: concrete niet openbaar gemaakte informatie die van invloed kan zijn op de toekomstige koers van cryptoactiva) in beginsel zo snel mogelijk openbaar te worden gemaakt door de verantwoordelijke partijen.<sup>149</sup> Ten tweede wordt handel met voorwetenschap verboden, alsook de onrechtmatige openbaarmaking van dergelijke voorwetenschap.<sup>150</sup> Tot slot wordt marktmanipulatie verboden. Marktmanipulatie is kort gezegd een zeer breed scala van illegitiem gedrag dat de vraag, het aanbod, of de koers van een cryptoactivum bedoelt te manipuleren, tot aan het verspreiden van geruchten toe.<sup>151</sup> De meer cynische cryptoactivabeleggers zullen zich mogelijk afvragen wat er nog van de altcoinmarkt overblijft wanneer illegitiem gedrag om de vraag naar een cryptoactiva te manipuleren verboden wordt. In hoeverre de MiCAR het einde betekent voor Europese crypto-influencers, en of het nog toegestaan is om te tweeten dat

een bepaald cryptoactiva ‘to the moon’ zal gaan, zal de tijd moeten uitwijzen.

## 7.2. Transfer of Funds Regulation

### 7.2.1. Informatievastlegging en verificatieverplichtingen

In de Transfer of Funds Regulation<sup>152</sup> (nader: TFR) worden zeer ruime informatievastleggingsverplichtingen opgelegd aan verleners van cryptoactivadiensten. Bij iedere overdracht van cryptoactiva die wordt uitgevoerd door een aanbieder van cryptoactivadiensten dient in beginsel de volgende informatie te worden gevoegd:<sup>153</sup>

- De naam van de initiator<sup>154</sup> en de begunstigde van de transactie;<sup>155</sup>
- Het *distributed ledger* adres van de initiator en de begunstigde en/of hun cryptoactivarekeningnummers;
- Het adres van de initiator met inbegrip van het land en het nummer van diens officiële ID kaart of diens cliëntidentificatienummer, dan wel diens geboortedatum en plaats;
- Indien mogelijk en van toepassing: de identificatiecode voor juridische entiteiten (ofwel LEI: *legal entity identifier*).<sup>156</sup>

De betreffende informatie dient in beginsel vijf jaar bewaard te worden. Een overdracht van cryptoactiva door een aanbieder van cryptoactivadiensten mag daarenboven niet plaatsvinden voordat de dienstverlener de juistheid van deze informatie heeft geverifieerd op basis van gegevens, documenten of informatie uit betrouwbare en onafhankelijke bron.<sup>157</sup>

Het valt op dat, waar bij overmaken van fiatgelden door reguliere (niet-crypto) betaaldienstverleners<sup>158</sup> nog een grensbedrag van € 1000,- bestaat, de TFR zo een grensbedrag niet heeft opgenomen voor aanbieders van cryptoactivadiensten. Bij overmakingen onder dat grensbedrag hoeft een reguliere betaaldienstverlener in beginsel enkel de naam en het rekeningnummer van de betaler en de begunstigde te

147. MiCAR art 79 lid 3. Een uitzondering wordt gemaakt als het handelsplatform de houders en de transactiesgeschiedenis van de van die ‘privacycoins’ identificeert, hetgeen zowel technisch als praktisch niet goed mogelijk is.

148. Omdat veel cryptoactiva (nog) geen breed gedragen *use-case* bezitten is de waarde daarvan betoogbaar in grotere mate afhankelijk van (beïnvloedbaar) marktsentiment dan dat bij financiële instrumenten met een concretere onderliggende waarde het geval is. Zie ook: Aysan, Caporin en Cepni, ‘Not all words are equal: Sentiment and jumps in the cryptocurrency market’ *Journal of International Financial Markets, Institutions and Money* nr. 91, maart 2024, Elsevier 101920.

149. MiCAR art 88.

150. MiCAR art 89 en 90.

151. MiCAR art 91.

152. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accom-

panying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (TFR).

153. TFR art 14.

154. De initiator is de persoon die houder is van een cryptoactivarekening of vergelijkbaar product, en een overdracht van cryptoactiva toestaat of opdracht geeft of het initiatief neemt tot overdracht van cryptoactiva, zie TFR art 3 aanhef en sub 21.

155. De begunstigde is de persoon die de beoogde ontvanger van de overdracht van cryptoactiva is, zie TFR art 3 aanhef en sub 21.

156. Zie voor meer informatie [https://nl.wikipedia.org/wiki/Legal\\_Entity\\_Identifier](https://nl.wikipedia.org/wiki/Legal_Entity_Identifier) laatstelijk geraadpleegd op 27 augustus 2025.

157. TFR art 14 lid 6 en art 17.

158. Zijnde partijen zoals bedoeld in artikel 1, lid 1, van Richtlijn (EU) 2015/2366, natuurlijke of rechtspersonen die op grond van artikel 32 van die richtlijn een ontheffing genieten en rechtspersonen die een ontheffing op grond van artikel 9 van Richtlijn 2009/110/EG genieten.

voegen bij een transactie. Die informatie hoeft verder onder dat grensbedrag in beginsel niet te worden geverifieerd door de betaaldienstverlener alvorens de betaling uit te voeren.<sup>159</sup> Een dergelijke uitzondering is ook overwogen voor aanbieders van cryptoactivadiensten, maar is uiteindelijk niet doorgevoerd in de verordening. De preambule meldt als rechtvaardiging van dit verschil dat overdrachten van cryptoactiva, in vergelijking met geldovermakingen, vanwege hun mondiale bereik en technologische kenmerken op grotere schaal en sneller door meerdere rechtsgebieden heen kunnen bewegen, en het eenvoudiger is om grote cryptoactivaoverdrachten op te breken in veel kleine overdrachten.<sup>160</sup>

Hoewel voor deze rechtvaardiging wel iets te zeggen is, acht ik het ook om andere redenen niet erg waarschijnlijk dat na invoering van de MiCAR en de TFR een meer dan verwaarloosbaar deel van de criminelen voor illegitieme betalingen nog gebruik zullen maken van aanbieders van cryptoactivadiensten in de EU. Ik acht het waarschijnlijker dat zulke criminelen overdrachten zullen doen vanuit (en naar) zelfgehoste wallets dan wel dat zij gebruik zullen maken van minder streng gereguleerde aanbieders van cryptoactivadiensten van buiten de EU. In die zin zou deze onbegrensde informatievergarings- en verificatieverplicht voor de aanbieders van cryptoactivadiensten in de EU vooral aangemerkt kunnen worden als een overmatig bezwarende administratieve last.

### 7.2.2. Alle MiCAR-aanbieders van cryptoactivadiensten worden WWFT-instelling

Daarnaast bracht de TFR een wijziging aan in de Anti-Money Laundering Directive EU 2015/849. Met die wijziging werden alle aanbieders van cryptoactivadiensten in de zin van de MiCAR als ‘*financiële instelling*’ aangemerkt in de zin van die witwasrichtlijn.<sup>161</sup> Dit werkt middels implementatie door in de Nederlandse WWFT, waar alle aanbieders van cryptoactivadiensten in de zin van de MiCAR inmiddels gelden als WWFT-instelling,<sup>162</sup> met de bijbehorende verplichtingen van cliëntidentificatie, transactiemonitoring en het melden van ongebruikelijke transacties. Art 18 TFR merkt in dat licht nog op dat ontbrekende of onvolledige informatie die ex artikel

art 14 TFR bij iedere cryptoactivaoverdracht dient te worden gevoegd, moet worden meegenomen in afweging of sprake is verdachte en meldenswaardige transactie.

### 7.3. Het toekomstige kader van DAC8

Hoewel ik fiscale en monetaire kwesties in het algemeen buiten beschouwing heb gelaten voor dit artikel, meen ik dat het toekomstige kader van DAC8 toch kort het vermelden waard is. Naar verwachting zal op 1 januari 2026 de Wet implementatie EU-richtlijn gegevensuitwisseling cryptoactiva ingaan. Onder deze implementatie van de fiscale Richtlijn DAC8 (Directive 2023/2226 amending Directive 2011/16/EU on administrative cooperation in the field of taxation)<sup>163</sup> zijn alle aanbieders van cryptoactivadiensten kort gezegd verplicht om gegevens over de mogelijke belastbare cryptobezittingen en overdrachten van hun gebruikers te verzamelen en te rapporteren aan bevoegde autoriteit van de betreffende lidstaat ten behoeve van belastingheffing. De lidstaten zijn op hun beurt verplicht de gegevens en inlichtingen over elkaars ingezetenen automatisch uit te wisselen.<sup>164</sup>

### 7.4. De stappen van de Verenigde Staten

Ook de Verenigde Staten zijn bezig een meeromvattende regelgevend kader omtrent cryptoactiva vorm te geven. De recent van kracht geworden GENIUS-Act,<sup>165</sup> welke in de Verenigde Staten stablecoins reguleert, lijkt op het eerste gezicht niet op heel andere gedachten te stoelen dan de stablecoinregelgeving het MiCAR kader in de EU, hoewel de Amerikaanse wetgeving iets flexibelere mogelijkheden lijkt te bieden voor cryptoactivaondernemers<sup>166</sup> en die wetgeving kennelijk vanuit monetair gezichtspunt tevens beoogt de rol van de dollar als wereldwijde reserve-munt te verstevigen.<sup>167</sup> Het Amerikaanse CLARITY-wetsvoorstel<sup>168</sup> dat kort gezegd andere vormen van cryptoactiva reguleert, lijkt op het eerste gezicht ook niet onvergelijkbaar met de regelgeving van de MiCAR, hoewel deze eerste opnieuw iets meer flexibiliteit lijkt te bieden voor ondernemers.<sup>169</sup> Daarnaast heeft de regering van President Trump, welke

159. TFR art 5 en 6. Verificatie is wel voorgeschreven indien de betaaldienstverlener de gelden contant of als anoniem elektronische geld heeft ontvangen, of redenen heeft te vermoeden dat de overboeking verband houdt met witwassen of het financieren van terrorisme.

160. TFR preambule sub 29 en 30. De voorbeelden die gegeven worden van hoe zulke betalingen in kleine deeltjes worden opgesplitst lijken overigens niet direct de soort transacties te zijn waarvoor een cryptoactivadienstverlener zou worden gebruikt, maar eerder de soort transacties die door een technisch onderlegde crimineel zelf zou vormgeven.

161. TFR art. 38.

162. Via artikel 1a lid 1 en lid 3 ahf en sub k jo artikel 1 lid 1 WWFT.

163. Richtlijn (EU) 2023/2226 Van De Raad van 17 oktober 2023 tot wijziging van Richtlijn 2011/16/EU betreffende

de administratieve samenwerking op het gebied van de belastingen.

164. *Kamerstukken II, 2024-25 36 782 nr. 3, p.4.*

165. Guiding and Establishing National Innovation for U.S. Stablecoins Act, S.1582.

166. <https://www.pelagiaslaw.com/post/mica-vs-genius-act-a-comparative-analysis-of-emerging-stablecoin-frameworks> laatstelijk geraadpleegd op 27 augustus 2025.

167. Zie en <https://fd.nl/financieel-markten/1567003/opmars-digitale-dollar-dreigt-euro-in-het-nauw-te-brengen> en <https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/> laatstelijk geraadpleegd op 1 september 2025.

168. Digital Asset Market Clarity Act of 2025, H.R.3633

169. <https://brightnode.io/blog/articles/blockchain-web3-insights/mica-vs-clarity-act-launching-a-token-in-the-eu-vs-us> laatstelijk geraadpleegd op 27 augustus 2025.

president overigens middels de \$TRUMP-coin<sup>170</sup> en World Liberty Financial<sup>171</sup> niet onaanzienlijke belangen heeft in cryptoactiva, meermalen zijn steun uitgesproken voor de cryptoactivasector, en aangegeven de Verenigde Staten het wereldcentrum van cryptoactiva te willen maken.<sup>172</sup> De regering Trump heeft verder middels verschillende *executive orders* beleid afgekondigd met betrekking tot versimpelde regulering van de cryptoactivasector of een eenvoudigere vervlechting van de cryptoactivasector met de reguliere financiële sector.<sup>173</sup> De *executive orders* van de regering Trump hebben inmiddels al geleid tot het opheffen van het National Cryptocurrency Enforcement Team<sup>174</sup> van het Department of Justice, dat gericht was op vervolgingen van crimineel misbruik van cryptoactiva, met name door cryptoactivabeurzen, mix- en tumblingdiensten en witwassers.<sup>175</sup> Tevens is een nieuw beleid van het Department of Justice tot stand gekomen om niet langer te focussen op de strafrechtelijke vervolging van aanbieders van cryptoactivadiensten voor handelingen van hun eindgebruikers of het onopzettelijke overtreden van regelgeving. In plaats daarvan dient volgens het nieuwe beleid gefocust te worden op personen die middels cryptoactiva investeerders financiële schade toebrengen of cryptoactiva gebruiken voor crimineel handelen met betrekking tot drugs, mensenhandel of terrorisme.<sup>176</sup>

## 8. Enige kritische aantekeningen bij MiCAR en TFR

Hoewel de MiCAR en de TFR een zeer uitgebreid en goed doordacht kader bieden waarbinnen theoretisch een groot deel van het misbruik van cryptoactiva zou kunnen voorkomen, moet opgemerkt worden dat ook hier het gedecentraliseerde en internationale karakter van cryptoactiva de beoogde uitwerking mogelijk belemmert.

De MiCAR verbiedt EU-ingezetenen immers niet om gebruik te maken van diensten van aanbieders van cryptoactivadiensten van buiten de EU. Hoewel het aanbieders van cryptoactivadiensten elders in de wereld niet toegestaan is zonder een EU-vergunning actief cliënten in de EU te benaderen of in de EU actief reclame te maken voor hun diensten, mogen zij die diensten wel verlenen indien dat gebeurt op ini-

tatief van een EU-ingezetene.<sup>177</sup> Dat een deel van de EU-ingezetenen van die niet EU-diensten gebruik zal gaan maken acht ik niet onwaarschijnlijk. Ten eerste vrees ik dat de criminele Europese cryptoactivagebruikers hun cryptoactiva vermoedelijk al ver voor de intreding van de MiCAR en de TFR hebben verplaatst naar zelfgehoste wallets of aanbieders van cryptoactivadiensten gevestigd in minder streng gereguleerde staten, om zo aan het verscherpte toezicht onder de MiCAR en de TFR te ontsnappen. Daarnaast zullen ook de meer principiële cryptoactivagebruikers van het eerste uur het vermoedelijk geen prettig idee vinden dat hun cryptoactivatransacties en cryptovermogen in de EU constant gemonitord worden, op een nog strengere wijze dan dat bij transacties met fiatvaluta gebeurt.

Daarnaast zullen de kosten van niet EU-aanbieders van cryptoactivadiensten vermoedelijk steeds verder uiteenlopen met de kosten van de EU-dienstverleners. Zulks, in verband met kosten van de administratie- en monitoringsverplichtingen die de MiCAR en TFR (en straks DAC8) met zich brengen. De Europese Commissie nam aan dat het vertrouwen dat de consument en investeerders met dank aan MiCAR in de Europese cryptoactivamarkt mag stellen, zal compenseren voor de toenemende kosten, onder meer door een toegenomen waarde van toegelaten cryptoactiva.<sup>178</sup> Dat is een redelijk plausible gedachte met betrekking tot partijen die een nieuwe cryptoactiva op de EU markt brengen, maar of die compenserende omstandigheid evenzeer opgeld zal doen voor andere aanbieders van cryptoactivadiensten zoals de Commissie verwacht, acht ik onzeker. De kosten van de compliance-verplichtingen onder de TFR lijken mij bijvoorbeeld slecht te compenseren middels toegenomen vertrouwen, wanneer de dienst het verzorgen van kleine cryptoactivatransacties betreft.

Daarbij mag worden opgemerkt dat door het internationale karakter van cryptoactiva, en het feit dat cryptoactiva momenteel nog niet gebruikt pleegt te worden voor betalingen van huur, verzekeringen of hypotheek, noch voor de ontvangst van het salaris, het vermoedelijk minder dan bij een bankrekening voor de hand ligt dat iemand graag een cryptoactivarekening wil aanhouden bij een aanbieder die in het eigen land gevestigd is. Ook omdat relatief

170. [https://en.wikipedia.org/wiki/\protect\TU\textdollarrTrump](https://en.wikipedia.org/wiki/\protect\TU\textdollarrTrump laatstelijk geraadpleegd op 27-08-2025) laatstelijk geraadpleegd op 27-08-2025.

171. [https://en.wikipedia.org/wiki/World\\_Liberty\\_Financial](https://en.wikipedia.org/wiki/World_Liberty_Financial laatstelijk geraadpleegd op 27 augustus 2025) laatstelijk geraadpleegd op 27 augustus 2025.

172. [https://www.cnn.com/2024/08/29/trump-crypto-plan-coming-election-harris.html](https://www.cnn.com/2024/08/29/trump-crypto-plan-coming-election-harris.html laatstelijk geraadpleegd op 27-08-2025) laatstelijk geraadpleegd op 27-08-2025.

173. Zie <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>, <https://www.whitehouse.gov/fact-sheets/2025/08/fact-sheet-president-donald-j-trump-democratizes-access-to-alternative-assets-for-401k-investors/> en <https://www.whitehouse.gov/presidential-actions/2025/03/establishment-of-the-strategic-bitcoin-reserve-and-united-states-digital-asset-stockpile/> laatstelijk geraadpleegd op 27 augustus 2025.

174. US DOJ Memorandum of the Deputy Attorney General, van 7 April 2025, 'Ending Regulation By Prosecution', [https://www.justice.gov/dag/media/1395781/dl?inline](https://www.justice.gov/dag/media/1395781/dl?inline laatstelijk geraadpleegd op 27 augustus 2025) laatstelijk geraadpleegd op 27 augustus 2025.

175. [https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team](https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team laatstelijk geraadpleegd 28 augustus 2025) laatstelijk geraadpleegd 28 augustus 2025.

176. US DOJ Memorandum of the Deputy Attorney General, van 7 April 2025, 'Ending Regulation By Prosecution', [https://www.justice.gov/dag/media/1395781/dl?inline](https://www.justice.gov/dag/media/1395781/dl?inline laatstelijk geraadpleegd op 27 augustus 2025) laatstelijk geraadpleegd op 27 augustus 2025.

177. MiCAR artikel 61 en preambule onder 75.

178. Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, p. 84 en 85.

veel informatie over de diensten die bepaalde aanbieders van cryptoactivadiensten leveren door gebruikers daarvan zonder veel aandacht voor nationale grenzen via het internet onderling met elkaar wordt gedeeld,<sup>179</sup> zal het verbod op actieve acquisitie of actieve reclame binnen de EU mogelijk minder van belang zal bij voor een keuze van sommige consumenten voor een aanbieder van cryptoactivadiensten.

## 9. Ten uitgeleide

Cryptoactiva en hun voorgangers hebben sinds hun ontstaan zelden veel rustige momenten gekend. Van een toepassing ontwikkeld door privacyvoorvechters die een digitaal equivalent voor anonieme contante betalingen wilden maken, naar een wereldwijde markt met een kapitalisatie van meerdere triljoenen,<sup>180</sup> met vele hoge bergen en diepe dalen daartussenin.

Met de invoering van de MiCAR en de TFR (en het aankomende DAC8), kan zonder veel omhaal gesproken worden van een nadere stap naar het digitaal panopticon waarvoor Chaum vreesde, en welke de grondleggers van cryptoactiva juist wilden voorkomen. Enkel de betaling met zelf-geminede cryptoactiva tussen twee personen die gebruik maken van

zelfgehoste cryptoactivawallets lijkt in Nederland aan de argusogen van de EU-regelgeving te ontsnappen. Alle overige wijzen van gebruik van cryptoactiva lijken, vooral via de brede definitie van het begrip cryptoactivadiensten, te moeten worden vastgelegd, bewaard, en potentieel gedeeld met de overheid. De regelgeving is zelfs strenger dan bij reguliere betalingsdiensten, waar nog een grensbedrag is opgenomen voor kleine bedragen waaronder de vastleggingsverplichting minder strikt is. Als David Chaum en veel van de Cypherpunks niet nog gewoon in leven waren, zouden zij zich vermoedelijk omdraaien in hun graf. Cryptoactiva in de EU zijn met het nieuwe regelgevend kader betoogbaar geen alternatief meer voor een betaalsysteem buiten financiële instellingen om, nu veel van de bij de cryptoactivawereld betrokken partijen met het huidige regelgevende kader ofwel wel een de-facto financiële instellingen moeten worden, ofwel zichzelf op moeten heffen.

Enkel de toekomst zal ons leren in hoeverre de MiCAR en TFR zullen bijdragen aan een veilige en innovatieve Europese en wereldwijde cryptoactivasfeer, en in hoeverre de rest van de wereld gelijksoortige regels zal aannemen. De ontwikkeling van cryptoactiva hebben zich tot nog toe nooit goed laten voorstellen, behalve dan met de stelling “*never a dull moment in crypto*”.

179. Zoals de bijvoorbeeld verschillende cryptocurrency *Subreddits*, die miljoenen gebruikers kennen.

180. <https://www.reuters.com/business/crypto-sector-breaches-4-trillion-market-value-during-pivotal-week-2025-07-18/> laatstelijk geraadpleegd op 27 augustus 2025.