De vermenging van ideologie en criminaliteit bij cryptovaluta

Thijmen Verburgh en Jocelyn van Rijs[*]

Cryptovaluta worden al zeker tien jaar voor een breed scala aan illegale doeleinden gebruikt. Vooral als betaalmiddel en als object van diefstal en oplichting. Een deel van de gemeenschap rondom het cryptovaluta-ecosysteem is aanhanger van het gedachtegoed waarin privacy als belangrijkste recht en financiële autonomie als het hoogste goed beschouwd worden. In sommige gevallen worden hierbij de verschillende vormen van crimineel misbruik van cryptovaluta voor lief genomen. De auteurs merken echter dat er naast deze ideologie vaak sprake is van een financiële drijfveer, die mogelijk meer invloed heeft dan genoemde ideologie, namelijk het runnen van een winstgevend bedrijfsmodel. Oftewel: de werkelijke drijfveren voor het gebruik van cryptovaluta zijn niet altijd duidelijk, en bij aansprakelijkheidsvraagstukken wordt vaak teruggevallen op ideologische uitgangspunten om gedrag te verantwoorden en aansprakelijkheid af te wenden. In dit artikel onderzoeken de auteurs de complexe relatie tussen ideologische motieven en financiële winst bij het gebruik van cryptovaluta.

Wat zijn cryptovaluta?

Cryptovaluta zijn digitale betalingssystemen gecreëerd en onderhouden door de toepassing van cryptografische technieken (Brown 2016).[1]

* Drs. T. Verburgh is senior technisch rechercheur bij de FIOD. Mr. J.E. van Rijs is onderzoeksleider financial cybercrime bij de FIOD.

1 Cryptografie vormt de basis voor privacy en beveiliging op internet. Veel informatie die via internet verstuurd wordt is versleuteld, bijvoorbeeld https-verkeer. Dit betekent dat de informatie niet te lezen of manipuleren is door derden. Alleen de verzendende en ontvangende partij hebben de sleutel waarmee ze de verstuurde informatie kunnen ontcijferen. Sleutels worden uitgewisseld met een wiskundig sleuteluitwisselingsprotocol. De identiteit van de persoon of website waarmee gecommuniceerd wordt, wordt gecontroleerd met een digitale handtekening. De cryptografische algoritmen die hiervoor gebruikt worden, zijn zo sterk dat de huidige computers ze niet kunnen kraken, bijvoorbeeld Elliptic Curve Cryptography en het RSA-algoritme. Deze algoritmen worden ook gebruikt door cryptovaluta, bijvoorbeeld om aan te tonen dat een transactie geldig is.

doi: 10.5553/JV/016758502024050002008

Het zogenoemde whitepaper uit 2008 waarin deze nieuwe vorm van een financieel systeem werd geïntroduceerd, was getiteld *Bitcoin: a peer-to-peer electronic cash system* (Nakamoto 2008). Satoshi Nakamoto introduceert hier het concept van de eerste vorm van 'cryptovaluta': een grootboek ('blockchain') waarin via een netwerk van nodes[2] alle transacties binnen het netwerk worden opgeslagen en via het internet inzichtelijk worden gemaakt.

Transacties worden gedaan na goedkeuring van (een deel van) de nodes van de blockchain. De manier van goedkeuring verschilt per blockchain. Wel is het altijd een proces dat door *computers* (de nodes) wordt uitgevoerd. Voor bitcoin koos Nakamoto de methode 'Proof of Work', waarbij de nodes moeilijke puzzels moeten oplossen die gegenereerd worden door een algoritme.[3]

Sinds 2008 hebben er veel ontwikkelingen plaatsgevonden binnen de cryptovalutawereld: er zijn bijvoorbeeld nieuwe blockchains ontwikkeld met nieuwe waardeonderdelen. Voorbeelden van blockchains zijn bitcoin en ethereum, met de bijbehorende 'coins', respectievelijk bitcoin en ether. Andere bekende cryptovaluta zijn USDT en USDC. Dit zijn zogenaamde stablecoins. Stablecoins zijn cryptovaluta waarbij de waarde van de 'coin' gekoppeld is aan de waarde van een fiatvaluta zoals de Amerikaanse dollar. Drie USDT is dan gelijk aan drie Amerikaanse dollars.

Hoewel de betalingssystemen vaak decentraal zijn, zijn er veel centraal functionerende entiteiten actief binnen het ecosysteem van de cryptovaluta. Zo blijkt uit onderzoek dat de hierboven beschreven 'nodes' soms in handen van slechts enkele partijen zijn (Xu e.a. 2023). Ook bestaan er exchanges: online 'geldwisselkantoren' tussen fiatvaluta en cryptovaluta, of tussen verschillende soorten cryptovaluta. Deze exchanges beheren vaak bedrijfsmatig het vermogen van anderen, waardoor een deel van de decentraliteit verloren gaat.

2 'Nodes' zijn computers die in een netwerk gegevens opslaan en verwerken. Het internet bestaat bijvoorbeeld uit servers die het internet in stand houden, dit zijn de nodes van het internet. In het geval van, bijvoorbeeld, het bitcoinnetwerk bestaat dit netwerk uit zogenaamde 'full nodes'. Deze nodes hebben een kopie van het hele bitcoinnetwerk opgeslagen en synchroniseren voortdurend zodat de laatste transacties worden opgeslagen. In essentie bevatten dus alle nodes een opslag van alle transacties van het bitcoinnetwerk. Het grootboek is dus altijd beschikbaar: als één node niet meer werkt, zijn er nog veel meer op het internet die het netwerk in stand houden en het grootboek inzichtelijk houden.

3 Verschillende blockchains werken op verschillende manieren. Andere blockchains kunnen dus andere methodieken toepassen.

doi: 10.5553/JV/016758502024050002008

De bekende quote 'not your keys, not your coins' verwijst dan ook naar het verlies van decentraliteit: als je het beheer van de cryptografische sleutels (de toegangscodes tot je cryptovaluta) uitbesteedt aan een derde partij, dan heb je ook niet de feitelijke macht over de cryptovaluta.

Ideologie en de gedachtegang achter cryptovaluta

Zonder een totaaloverzicht te geven van de sociale, politieke en financiële ontwikkelingen die eraan hebben bijgedragen,[4] wordt breed gedeeld dat cryptovaluta zijn ontstaan vanuit de behoefte een nieuw financieel systeem te bouwen waarbij de deelnemers aan dat systeem niet afhankelijk zijn van de klassieke financiële instituties: de macht over het eigen vermogen en wat daarmee gedaan wordt, moest terug naar de eigenaar van dat vermogen, zonder inmenging van een derde 'centrale' partij. De personen die hier veel interesse in hadden en naar een manier zochten om dit te bewerkstelligen, waren zeer geïnteresseerd in cryptografie en grote voorstanders van online privacy. Deze groep is bekend onder de naam *cypherpunks* (Assange e.a. 2012).
Hoewel het bij de introductie van de eerste cryptovaluta, bitcoin, niet de bedoeling lijkt te zijn geweest volledige anonimiteit te bieden (alle transacties op de blockchain waren immers te raadplegen via het internet), is de behoefte aan anonimiteit in de loop van de tijd wel degelijk een belangrijk onderdeel geworden van het verlangen om een alternatief financieel systeem te hebben. Anonimiteit, in de zin van het doen van financiële transacties die onzichtbaar zijn voor de statelijke autoriteiten, is tegenwoordig een belangrijke beweegreden in de cryptogemeenschap.
De afgelopen jaren heeft het fenomeen cryptovaluta sterk aan bekendheid gewonnen. Cryptovaluta werden op een bepaald moment meer mainstream en investeerders toonden interesse. Want zoals bij alle nieuwe producten of vormen van dienstverlening die uit ideologie zijn gestart, zijn er ook mensen die eraan meedoen om geld te verdienen. En omdat ze vrij toegankelijk zijn, begonnen cryptovaluta steeds meer een investeringsmogelijkheid voor de 'gewone man' te vormen, en werden ze meer dan alleen een decentraal alternatief voor 'cash'.

4 Hiervoor verwijzen we naar het boek *Cypherpunks. Freedom and the future of the internet* van onder anderen Julian Assange (2012).

doi: 10.5553/JV/016758502024050002008

Crimineel gebruik van cryptovaluta

Kenmerken

Het criminele gebruik van cryptovaluta gaat terug tot (in ieder geval) 2011, toen Ross Ulbricht een online marktplaats genaamd 'Silk Road' op het darkweb creëerde waarop illegale goederen, voornamelijk drugs, werden verhandeld. Hierbij gebruikte hij bitcoin als het betalingssysteem. In 2013 werd Silk Road ontmanteld door de Amerikaanse autoriteiten. Ross Ulbricht werd opgepakt en is op 25 mei 2015 veroordeeld tot een levenslange gevangenisstraf.[5]
Bepaalde kenmerken van cryptovaluta maken het voor criminelen aantrekkelijk om ze te integreren in hun businessmodel. Dit zijn decentraliteit, (pseudo)anonimiteit, snelheid en toegankelijkheid. Het behoeft geen verdere uitleg dat een systeem waarin geen derde partij acteert die transacties kan tegenhouden of criminele actoren kan herkennen in het voordeel werkt van iemand die criminele financiële transacties wil doen. Cryptovaluta zijn, net als cash, geschikt voor relatief anonieme waardeverplaatsing. Deze relatieve anonimiteit wordt bewerkstelligd door het *decentraal* opgezette netwerk. Op dat netwerk zijn de transacties weliswaar inzichtelijk via het internet, maar degenen die de transacties uitvoeren zijn in beginsel niet zichtbaar: cryptovaluta-adressen interacteren met andere cryptovaluta-adressen. Als niet bekend is welke persoon het cryptovaluta-adres beheert, dan blijft deze interactie anoniem. Maar omdat het met andere informatie soms mogelijk is de betrokkenheid van personen te achterhalen, spreekt men van *pseudoanonimiteit*. Toch kunnen criminelen, hoewel elke transactie publiekelijk inzichtelijk is, hun illegale transacties wel met verminderd risico uitvoeren. Dit verandert natuurlijk als er een koppeling gemaakt kan worden naar natuurlijke personen, bijvoorbeeld door middel van beslaglegging op administratie van een exchange die namen, (e-mail)adressen en andere identificerende gegevens van hun klanten kan koppelen aan transacties die deze klanten doen op hun platform. In dat geval kan er een totaalbeeld worden opgebouwd van het gebruik van deze adressen, waaronder transacties van meer dan tien jaar geleden.

5 Zie www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

doi: 10.5553/JV/016758502024050002008

De crimineel wil ook graag snel transacties doen, zodat de autoriteiten geen tijd krijgen om in te grijpen. Omdat (met name de georganiseerde) criminaliteit internationaal opereert, is deze snelheid ook bij transacties over landsgrenzen vereist. De snelheid van girale betalingen in Nederland ligt hoog, namelijk 5 seconden bij transacties tussen banken.[6] Deze snelheid neemt echter af als er internationale transacties uitgevoerd moeten worden. Een internationale transactie kan soms meerdere dagen in beslag nemen.[7],[8] De snelheid van cryptovalutatransacties ligt over het algemeen op minuten, zo worden er bij bitcoin elke 10 minuten transacties verwerkt. De uitvoeringssnelheid van wereldwijde transacties met behulp van cryptovaluta ligt dus soms aanzienlijk hoger dan bij het bancaire systeem. Ook zijn cryptovaluta heel *toegankelijk*: een stukje software en een internetverbinding zijn vaak al genoeg.[9] Hiermee kunnen vanaf elke plek transacties worden geïnitieerd.

Regulatie en wet- en regelgeving en internationaal speelveld

Een deel van de cryptovaluta-activiteiten staat of komt onder toezicht. Het toezicht ten aanzien van maatregelen tegen witwassen en terrorismefinanciering ligt bij De Nederlandsche Bank (DNB). Het toezicht ten aanzien van consumentbescherming en marktintegriteit ligt bij de Autoriteit Financiële Markten (AFM). Laatstgenoemd toezicht is nog niet in werking, dat zal in 2025 gebeuren. Beide toezichtregelingen vinden hun basis in Europese wetgeving.

AMLD 5

De Europese richtlijn die wordt aangeduid als de AMLD5 (Anti-Money Laundering Directive) verplicht de Europese lidstaten een registratieregime in te richten voor aanbieders van crypto-omwisseldiensten (van en naar fiatgeld) en cryptobewaarportemonnees. Ook verplicht deze richtlijn deze dienstverleners om klantonderzoek uit te voeren, transacties te monitoren, ongebruikelijke transacties te melden bij de

6 Zie www.betaalvereniging.nl/betalingsverkeer/giraal-betalingsverkeer/instant-payments.
7 Zie www.regiobank.nl/service/online-bankieren/overboeking-naar-het-buitenland.html#:~:text=Het%20duurt%20meestal%203%20tot,duurt%20het%20meestal%203%20werkdagen.
8 Zie www.forbes.com/advisor/in/money-transfer/best-ways-to-send-money/.
9 Er zijn hiernaast ook opties om offline transacties te initiëren. Deze moeten uiteindelijk wel worden gebroadcast naar het netwerk.

doi: 10.5553/JV/016758502024050002008

Nederlandse Financial Intelligence Unit en risicoanalyses te doen ten aanzien van witwassen en terrorismefinanciering. De verplichtingen uit de AMLD5 zijn omgezet in Nederlandse wetgeving (middels een aanpassing van de Wet ter voorkoming van witwassen en financieren van terrorisme – de Wwft).
In de toekomst wordt het toezicht breder en intensiever en meer direct gestuurd vanuit de Europese Unie via de zesde richtlijn, de AMLD6.[10]

FATF
De Financial Action Task Force (FATF) is een onafhankelijk intergouvernementeel orgaan dat beleid ontwikkelt en bevordert ter bescherming van het mondiale financiële systeem tegen het witwassen van geld, de financiering van terrorisme en de financiering van massavernietigingswapens. De FATF heeft zogenaamde aanbevelingen ontwikkeld, die worden erkend als internationale norm voor de bestrijding van witwassen en de financiering van terrorisme en proliferatie. De landen die lid zijn van de FATF worden op basis van deze aanbevelingen geëvalueerd. Ook ten aanzien van cryptovaluta heeft de FATF aanbevelingen gedaan.[11]
Het toepassen van wet- en regelgeving in een internationale, digitale wereld is lastig. Door het grote gemak waarmee mensen gebruik kunnen maken van cryptovaluta kunnen er ook met relatief weinig moeite online cryptovalutawisseldiensten worden aangeboden. Het komt voor dat zulke aanbieders zich actief lijken te onttrekken aan wet- en regelgeving.[12] Ze zoeken het meest gunstige vestigingsklimaat op (of geven zelfs aan dat ze nergens gevestigd zijn en volledig 'decentraal' opereren). Hun diensten worden echter wel wereldwijd aangeboden. Dit maakt het toepassen van regulering en toezicht een uitdaging voor overheden en zet de businesscase van wel meewerkende partijen onder druk. Zo geeft Litebit, een exchange die gestopt is wegens de gestegen compliancekosten als gevolg van een nieuwe wet, op 25 mei 2023 aan dat het frustrerend is dat partijen als Binance, OKX en

10 Een mooi overzicht wordt gegeven door Watsonlaw: https://watsonlaw.nl/en/anti-money-laundering-regulation-directive-6/.
11 Zie www.fatf-gafi.org/en/topics/virtual-assets.html.
12 Zie bijvoorbeeld www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf, p. 18.

doi: 10.5553/JV/016758502024050002008

Gate.io in Nederland klanten werven en bedienen zonder dat ze geregistreerd zijn bij DNB.[13]

Cryptovalutacriminaliteit

Er zijn verschillende manieren waarop cryptovaluta worden gebruikt bij het plegen van strafbare feiten. Hieronder bespreken we er een aantal. Daarbij wordt duidelijk dat er twee dominante vormen zijn van crimineel gebruik van cryptovaluta: als betaalmiddel en als object van het delict.

Cryptovaluta als betaalmiddel

Bij verschillende soorten criminaliteit wordt cryptovaluta gebruikt als betaalmiddel. Zo wordt bijvoorbeeld bij *dark(net) marktplaatsen* (of ondergrondse online marktplaatsen) al lange tijd betaald met bitcoin. Ook wordt soms de mogelijkheid gegeven om met een zogenaamde privacycoin zoals monero[14] te betalen. Men kan hiermee bijvoorbeeld drugs of wapens kopen. Volgens blockchainanalyse-bedrijven Chainalysis en TRM ging er in 2023 wereldwijd zo'n $ 1,5 tot 1,7 miljard om op dark(net) markets (TRM z.d.; Chainalysis 2024). Een oudere studie van Kruithof en collega's (2016) stelt dat 7,8% van de drugsverkopen op dark markets afkomstig zou zijn van Nederlandse verkopers. Huidige percentages zijn onbekend, maar aangenomen wordt dat Nederland nog steeds een significant aandeel heeft.
Cryptovaluta zoals bitcoin en monero worden ook gebruikt bij zogenaamde *ransomware-aanvallen*. Ransomware is een algemene benaming van software die, tegen de wil van de computergebruiker in, gegevens op een computer versleutelt of de computer ontoegankelijk maakt. De gebruiker van de computer wordt vervolgens gevraagd losgeld te betalen om de data op de computer weer toegankelijk te maken.[15] Het losgeld wordt altijd in cryptovaluta betaald. Volgens

13 Zie https://bitcoinmagazine.nl/nieuws/arthur-van-lier-litebit-er-komt-een-shake-out-van-cryptobedrijven-in-nederland-aan.

14 Privacycoins zoals monero zijn zo ontworpen en ontwikkeld dat ze (ten opzichte van andere cryptovaluta) meer anonimiteit en non-traceerbaarheid bieden.

15 Zie www.politie.nl/informatie/wat-is-ransomware-dan-zijn-uw-computerbestanden-ontoegankelijk-gemaakt.html#:~:text=Ransomware%20is%20een%20programma%20dat,cryptocurrency%2C%20zoals%20Bitcoin%20of%20Monero.

doi: 10.5553/JV/016758502024050002008

Chainalysis zou er in 2023 bij ransomware-aanvallen meer dan $ 1 miljard zijn buitgemaakt (Chainalysis 2024). In Nederland zijn in 2023 147 incidenten gemeld (Project Melissa 2024).[16]
Daarnaast kennen we gevallen waarin bij *gijzeling* een cryptovalutabetaling wordt geëist. De gijzelnemer in de Apple Store in Amsterdam in 2022 eiste bijvoorbeeld een bedrag van € 200 miljoen in cryptovaluta.[17] Ook bij de (ruil)handel van *kinderporno* wordt gebruik gemaakt van cryptovaluta als betaalmiddel (IOCTA 2021). Volgens Chainalysis (2024) zouden er tussen 2020 en 2023 meer dan 400 verkopers met cryptovalutawallets actief zijn geweest. En ook bij *terrorismefinanciering* zien we dat cryptovaluta gebruikt worden, bijvoorbeeld bij donaties aan terroristische organisaties.[18] Zo heeft de Israëlische overheid in juni 2023 $ 1,7 miljoen in beslag genomen van cryptovalutawallets die gelieerd waren aan onder andere Hezbollah.[19],[20] Volgens TRM (z.d.) zijn de meeste cryptovalutadonaties klein van aard: driekwart ervan kwam niet boven de $ 500.
Tot slot worden cryptovaluta gebruikt bij *ondergronds bankieren*,[21] voornamelijk vanwege het gemak en de snelheid die het systeem biedt. Grote hoeveelheden 'geld' kunnen immers relatief snel en anoniem internationaal worden verplaatst. Verder geeft Ludlow, senior witwasexpert bij de National Crime Agency (NCA) van Groot-Brittannië, aan dat '[d]ata gleaned from encrypted phone systems, used by high level criminals to communicate with each other, found "large movements of crypto being sent between South America and Europe" to pay for cocaine shipments to Europe'.[22]

Cryptovaluta als object van het delict

Soms worden cryptovaluta niet alleen als betaalmiddel ingezet, maar is het in de kern een onderdeel van de modus operandi of het strafbare feit. Hieronder volgen enkele voorbeelden.
In sommige gevallen van (online) *oplichting* worden mensen onder valse voorwendselen overgehaald te investeren in niet-bestaande

16 Zie www.ncsc.nl/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023.
17 Zie www.bbc.com/news/world-europe-60486726.
18 Zie https://crsreports.congress.gov/product/pdf/IF/IF12537/2.
19 Zie www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/.
20 Zie https://cointelegraph.com/news/israeli-authorities-seize-crypto-from-terror-organizations-credit-new-technology.
21 Zie www.amlc.nl/wp-content/uploads/2023/05/RIEC-AA-Ondergronds-bankieren.pdf.
22 Zie www.vice.com/en/article/pkax5k/money-laundering-organized-crime.

doi: 10.5553/JV/016758502024050002008

cryptovalutaprojecten. Het proces om mensen te overtuigen die investering te doen vereist veel contact tussen de oplichter en het slachtoffer. Bijvoorbeeld bij 'pig butchering' of 'romance scams' wordt er steeds om grotere investeringen gevraagd van het slachtoffer nadat er een romantische relatie is opgebouwd via chat- en/of telefooncontact. Deze vorm van oplichting is zeer lucratief: wereldwijd wordt er meer dan $ 1 miljard mee verdiend, aldus Chainalysis.[23] Vaak zijn er andere strafbare feiten gerelateerd aan deze vorm van oplichting, zoals witwassen. Chainalysis heeft in februari 2024 een goed overzicht gegeven van deze interactie en de omvang van 'pig butchering'.[24]

Een ander aan oplichting gerelateerd probleem is *verduistering* van cryptovaluta. Daarbij worden de cryptovaluta die iemand rechtmatig onder zich heeft niet teruggegeven aan de eigenlijk gerechtigde, terwijl dit wel wordt beloofd. In het cryptovaluta-ecosysteem worden veel projecten en initiatieven gestart met nieuwe technische componenten en toepassingen, maar niet elk project is wat het lijkt of doet wat het belooft. Zo heeft de rechtbank in Overijssel in 2022 een man veroordeeld tot vier jaar celstraf omdat hij onder andere de opnamefunctie van zijn cryptoplatform had dichtgezet, zodat klanten niet meer bij hun tegoeden konden.[25]

Daarnaast wordt er op blockchains dienstverlening aangeboden die het mogelijk maakt de traceerbaarheid van cryptovalutatransacties moeilijker te maken. Wanneer zo'n dienstverlening ook criminele geldstromen faciliteert, wordt er in witwastermen gesproken over een 'witwasfacilitator', die bijdraagt aan het verplaatsen en/of verhullen van de criminele herkomst of bestemming van cryptovaluta. Een voorbeeld is een zogenaamde 'mixer'. Dat is een onlinedienst die tegen betaling van een fee cryptovaluta mixt met cryptovaluta van andere gebruikers van de dienst. Wanneer de cryptovaluta weer uit de mixer gehaald worden, zijn instroom en uitstroom niet meer aan elkaar te koppelen, wat het witwassen van uit criminaliteit afkomstige cryptomunten makkelijker maakt. Zo'n mixer kan illegaal zijn als blijkt dat de dienst criminele transacties faciliteert. In een onderzoek van de FIOD tegen mixer Sinbad.io wordt door de FIOD aangegeven dat deze mixer

23 Zie www.chainalysis.com/blog/pig-butchering-human-trafficking/.
24 Zie www.chainalysis.com/blog/pig-butchering-human-trafficking/.
25 Rb. Overijssel 8 februari 2022, ECLI:NL:RBOVE:2022:348.

doi: 10.5553/JV/016758502024050002008

minstens € 178 miljoen aan cryptovaluta met een criminele herkomst zou hebben verhuld.[26]
Cryptovaluta worden ook gestolen. Bij deze vorm van *diefstal* wordt de toegang tot andermans cryptovaluta eerst verschaft en vervolgens worden de cryptovaluta weggenomen. Hierbij kan het bijvoorbeeld gaan om een kwetsbaarheid in een smart contract op de ethereumblockchain, waarbij die kwetsbaarheid gebruikt wordt om toegang tot cryptovaluta te krijgen. Een partij die veelvoudig cryptovalutadiefstallen pleegt, is Noord-Korea. Zij doen dit onder andere door zichzelf toegang te verschaffen tot een online casino of cryptovalutaleenplatform. Volgens de Amerikaanse overheid zouden deze cryptovalutadiefstallen een significante bijdrage leveren aan het Noord-Koreaanse raketprogramma.[27]

Observaties van de auteurs

Wanneer cryptovaluta het object van de criminele handeling zijn, zien we in verschillende onderzoeken enkele bijzonderheden die we in andere (cybercrime-)zaken eigenlijk niet tegenkomen.

Misbruik?

Social media triggeren mensen om cryptovaluta te bezitten, mee te doen in projecten of cryptovaluta te verhandelen. Sommigen doen dit vanuit de eerdergenoemde ideologie, anderen zien dit als een manier om (snel) geld te verdienen. Veel van deze mensen hebben niet de kennis in huis om de onderliggende (ICT-)techniek, wiskundige modellen en cryptografische elementen te begrijpen of te controleren. Hiervan wordt op dit moment veelvuldig misbruik gemaakt door criminelen.
We zien dat criminelen inspelen op de eagerness van potentiële slachtoffers om deel te nemen aan de cryptowereld en vervolgens moeilijk controleerbare ICT-technieken inzetten als modus operandi voor bijvoorbeeld het plegen van oplichting. De volgende twee voor-

26 Zie www.fiod.nl/fiod-haalt-grote-cryptovaluta-mixer-uit-de-lucht/.
27 Zie https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html.

doi: 10.5553/JV/016758502024050002008

beelden verduidelijken de hierboven genoemde modus operandi (cursivering door auteurs).

> In Groot-Brittannië zijn in 2023 twee personen veroordeeld wegens oplichting. Zij boden *niet-bestaande cryptovaluta* aan als investeringsmogelijkheid.[28] De Londense politie zegt daarover het volgende: 'It's easy for investors, and sadly victims in this case, to be sucked in to what they think is an *area of potential and growth for their hard earned cash* due to how new the area of crypto investment is. [Veroordeelde] and [veroordeelde] exploited this mindset and knowingly chose to simply take the victims' money for their own financial gain, with no intention whatsoever of providing a service that even resembled a credible investment.'

> In 2023 werden het in Singapore gevestigde bedrijf Terraform Labs PTE Ltd en zijn CEO door de Amerikaanse Securities and Exchange Commission (SEC) aangeklaagd wegens oplichting van investeerders. Terraform zou consumenten verkeerd hebben voorgelicht over hun Terraform-*ecosysteem* met bijbehorende blockchain Terra en Luna/TerraUSD-munt (een zogenaamde *algoritmische stablecoin*). Terraform bood een stablecoin aan die niet gedekt was door middel van traditioneel vermogen, maar door middel van hun eigen token, namelijk LUNA (ESMA 2023). Volgens de SEC was het ecosysteem *gedecentraliseerd* noch *financieel*, terwijl Terraform dit wel zo deed voorkomen.[29] De prijs werd volgens de SEC niet bepaald door een 'algoritmische stablecoin', maar door Terraform zelf.

Decentraliteit als argument voor niet-aansprakelijkheid?

Een interessante ontwikkeling die een meer juridische ondertoon heeft (en ook in strafrechtelijke context relevant is), is het gebruik van de eerdergenoemde behoefte aan *decentraliteit* als argument voor niet-aansprakelijkheid bij de cryptovalutagerelateerde activiteiten. Er wordt bijvoorbeeld een dienstverlening op een blockchain gebouwd (zoals het aanbieden van een munt of een mixer) en wanneer gebruikers vervolgens geld verliezen (bijvoorbeeld door diefstal), of wanneer er criminele activiteiten worden vastgesteld, claimen de bouwers en uitbaters van de dienstverlening dat ze niet aansprakelijk zijn voor het

28 Zie www.cityoflondon.police.uk/news/city-of-london/news/2023/july/the-hot-pursuit-of-justice-operation-curry-sees-investment-fraudsters-sentenced-to-six-years-for-500000-cryptocurrency-scam/.

29 Zie www.sec.gov/newsroom/press-releases/2023-32.

doi: 10.5553/JV/016758502024050002008

gebruik van de dienst omdat deze decentraal zou zijn opgezet, het staat immers op de blockchain. Dit probleem wordt ook door de European Securities and Markets Authority geconstateerd: '[T]here are serious risks to investor protection, due to (…) lack of a clearly identified responsible party' (ESMA 2023).

De vraag is echter of die decentraliteit altijd bestaat of van toepassing is. Net als de auteurs in het tijdschrift van de Bank for International Settlements (Aramonte e.a. 2021), die zelfs spreken van *decentralisation illusion*, hebben wij vanuit de praktijk ook de ervaring dat enkel het gebruik van blockchaintechniek niets zegt over (niet-)aansprakelijkheid. Als er verder wordt gekeken dan de technische infrastructuur van cryptovalutasystemen kan er in bepaalde gevallen vastgesteld worden dat er centrale entiteiten verantwoordelijk zijn voor het inrichten en uitbaten van een cryptovalutasysteem. Zo kan de doorontwikkeling van een 'decentraal' product bij een groep ontwikkelaars liggen die qua organisatie, verantwoordelijkheden en omvang vergelijkbaar is met, bijvoorbeeld, een klein bedrijf.

Om de (strafrechtelijke) aansprakelijkheid binnen decentrale cryptovalutasystemen goed te kunnen duiden is een brede mate van kennis noodzakelijk: enerzijds diepgaande technische kennis van eerdergenoemde ICT-infrastructuren, wiskundige modellen en cryptografische toepassingen en anderzijds kennis van onder andere organisatiestructuren en juridische aansprakelijkheidsvarianten. Een product of dienst is immers meer dan alleen de technische werking op een blockchain.

Een nieuw daderprofiel?

In verschillende zaken stellen wij vast dat de personen die betrokken zijn bij cryptovalutaprojecten en mogelijke criminele activiteiten niet binnen de daderprofielen passen die doorgaans in het strafrecht bekend zijn.[30] Hoewel er onderzoek is gedaan naar daders bij cybercriminaliteit lijkt juist het onderzoek naar drijfveren van daders beperkt: er is een vermoeden dat er financiële drijfveren zijn en dat prestige en erkenning binnen de gemeenschap belangrijk worden gevonden,[31] maar met name over de psychologische en politieke drijfveren is nog weinig bekend (Nederveen e.a. 2024).

30 Een mooi overzicht van de georganiseerde criminaliteit wordt gegeven in Van Koppen 2021.

31 Zie bijvoorbeeld Madari 2017.

doi: 10.5553/JV/016758502024050002008

Wij ervaren dat verschillende betrokkenen, dienstaanbieders of productontwikkelaars binnen het cryptovalutadomein, aangeven dat ze handelen uit ideologie (vaak financiële autonomie en financiële privacy), en dat zij vinden dat eventueel daarmee gepaard gaand strafrechtelijk handelen aan die ideologie ondergeschikt is.[32] Deze gedachte lijkt vaak voort te vloeien uit de eerdergenoemde basisopvatting van de cypherpunks, namelijk dat de bescherming van privacy als een van de belangrijkste mensenrechten moet worden gezien, met name in het digitale domein. Vanuit deze gedachtegang nemen ze crimineel gebruik van hun dienstverlening of product dus voor lief.
Het goed duiden van de mate waarin betrokkenen handelen vanuit een ideologie is complex. Het belang van de gedachtegang zoals hierboven beschreven kan gedurende de looptijd veranderen. Zo kan een product mogelijk vanuit die gedachtegang zijn ontstaan, maar zodra het aan populariteit wint een belangrijke inkomstenbron worden of investeerders aantrekken zodat er andere belangen gaan spelen. In verschillende opsporingsonderzoeken zien we daar indicaties van: opmerkingen van investeerders dat ze de inkomsten belangrijker vinden dan het weren van criminele gebruikers van een platform, cryptovalutadienstverleners die klanttegoeden gebruiken om persoonlijke uitgaven te doen, enzovoort. Natuurlijk komen deze situaties ook voor in de 'klassieke' criminaliteit. Echter, de combinatie met het hooghouden van ideologische intenties zien wij niet zo vaak.

Ideologie of winstbejag bij cryptovaluta?

Een deel van de bij het cryptovaluta-ecosysteem betrokken gemeenschap hangt het gedachtegoed aan waarin privacy als het belangrijkste recht en financiële autonomie als het hoogste goed worden beschouwd. Hierbij worden de verschillende vormen van crimineel misbruik van cryptovaluta, zoals hierboven beschreven, in sommige gevallen voor lief genomen. De auteurs merken echter dat er naast deze ideologie vaak ook een financiële drijfveer bestaat die mogelijk meer invloed heeft dan de ideologie, namelijk het runnen van een winstgevend bedrijfsmodel. Bij aansprakelijkheidsvraagstukken wordt echter vaak teruggevallen op ideologische uitgangspunten om gedrag

32 Deze ervaringen kunnen dus als anekdotisch worden aangemerkt.

doi: 10.5553/JV/016758502024050002008

te verantwoorden en aansprakelijkheid af te wenden. Het beter inzichtelijk krijgen van daderprofielen kan niet alleen de interventies vanuit de opsporing verbeteren, maar ook inzichten bieden voor beleidmakers als het gaat om cryptovalutagebruik: Hoe kun je daderschap voorkomen? Wat zijn de beste manieren om daders op te sporen? Hoe kun je het beste in gesprek gaan met verdachten? Door onderscheid te maken tussen mogelijke verschillende toepassingen en complexiteit van cryptovaluta in de modus operandi kan gerichter en efficiënter richting daders worden opgetreden. Drugsverkopers die cryptovaluta als betaalmiddel gebruiken via ondergronds bankieren vereisen wellicht een andere 'dadergerichte aanpak' dan personen die vanuit ideologie cryptovalutaprojecten starten en crimineel gebruik daarvan niet belangrijk vinden.

Literatuur

Aramonte e.a. 2021
S. Aramonte, W. Huang & A. Schrimpf, 'DeFi risks and the decentralisation illusion', *BIS Quarterly Review* 2021, p. 21-36.

Assange e.a. 2012
J. Assange, J. Appelbaum, A. Müller-Maguhn & J. Zimmermann, *Cypherpunks. Freedom and the future of the Internet*, New York/Londen: OR Books 2012.

Brown 2016
S.D. Brown, 'Cryptocurrency and criminality: the Bitcoin opportunity', *Police Journal: Theory, Practice and Principles* (89) 2016, afl. 4, p. 327-336.

Chainalysis 2024
Chainalysis, *The 2024 crypto crime report*, 2024.

ESMA 2023
ESMA (European Securities and Markets Authority), *Decentralised finance in the EU: developments and risks* (ESMA TRV Risk Analysis), 2023.

Europol 2021
Europol, *Internet Organized Crime Threat Assessment (IOCTA)*, Europol, 2021.

Van Koppen 2021
V. van Koppen, 'Daders van georganiseerde misdaad: wie zijn het en hoe raken ze betrokken?', *Justitiële verkenningen* (47) 2021, afl. 4, p. 23-36. DOI: 10.5553/JV/016758502021047004003.

doi: 10.5553/JV/016758502024050002008

Kruithof e.a. 2016
K.A.-H. Kruithof, J. Aldridge, D. Décary Hétu, M. Sim, E. Dujso & S. Hoorens, *Internet-facilitated drugs trade: an analysis of the size, scope and the role of the Netherlands*, RAND Europe 2016.

Madari 2017
R. Madari, 'Hackers' motivations: testing Schwartz's theory of motivational types of values in a sample of hackers', *International Journal of Cyber Criminology* (11) 2017, afl. 1, p. 78-97.

Nakamoto 2008
S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, Satoshi Nakamoto Institute 2008, https://nakamotoinstitute.org/library/bitcoin/.

Nederveen e.a. 2024
F. Nederveen, E. Silfversten, R. Slootweg & S. Hoorens, *Daderprofielen van cybercriminelen uit Oost-Europa en Rusland*, RAND Europe 2024.

Project Melissa 2024
Project Melissa, *Jaarbeeld ransomware 2023*, 2024.

TRM z.d.
TRM, *The illicit crypto economy: key trends from 2023*, z.d.

Xu e.a. 2023
G.Z. Xu, J. Gao, L. Zhu, F. Gao & J. Zhao, 'Statistical and clustering analysis of attributes of Bitcoin backbone nodes', *PLOS ONE* 8 november 2023, https://journals.plos.org/plosone/article/authors?id=10.1371/journal.pone.0292841.

doi: 10.5553/JV/016758502024050002008