

Witwassen 2.0: van sporttas naar smartphone – de jacht op cryptogeld

20-6-2025 | Witwassen2.0

Mr. drs. E.E.G. Engwirda

Witwassen is niet meer wat het was. De sporttas vol contanten heeft plaatsgemaakt voor digitale wallets. Door anonieme wisseldiensten en mixers lijkt cryptovermogen lastig te traceren, maar de FIOD doet actief onderzoek naar deze digitale geldstromen. Wij zien veel van deze zaken voorbij komen in onze fiscale en strafrechtpraktijk.

Voor wie wordt verdacht van crypto-witwassen is het speelveld radicaal veranderd, merken wij. Niet alleen zijn de technische middelen van de opsporing sterk verbeterd, ook juridisch is sprake van een nieuwe werkelijkheid. In dit blog bespreek ik die realiteit – zoals geschetst in het FIOD Jaarverslag 2024 – én wat dat betekent voor de verdediging.

Van blockchain naar bewijsmateriaal

In het jaarverslag over 2024 krijgt digitale financiële criminaliteit expliciete aandacht naast btw-fraude, waarover [collega Thijs Droog deze blog schreef](#)¹. De FIOD noemt cryptovaluta een 'structureel onderdeel van het crimineel financieel ecosysteem'. Mixers, privacycoins (moeilijk traceerbare coins zoals Monero) en decentrale wisseldiensten spelen daarbij een centrale rol.

De FIOD profileert zich als technisch specialist. Medewerkers worden opgeleid in blockchainanalyse, AI-tools worden

ingezet om inbeslaggenomen data te analyseren en de FIOD werkt samen met internationale opsporingsdiensten en binnen Nederland onder andere met het Team High Tech Crime (THTC) van de politie. Zo werden in 2024 bijvoorbeeld twee grote [cryptovaluta-wisseldiensten Cryptex en pm2btc](#)² offline gehaald. Om beslag te kunnen leggen op de crypto werkte de FIOD samen met Chainalysis en Tether.io. De boodschap is duidelijk: cryptovaluta zijn niet langer onvindbaar. Beslaglegging leidt ertoe dat de valuta op zijn minst jaren niet beschikbaar zijn, vaak ook worden zij onmiddellijk verkocht en in het ergste geval worden ze afgepakt. Het is goed om hierop bedacht te zijn en maatregelen te nemen voor het te laat is.

Internationale dimensie

Crypto stopt niet bij de grens, en de opsporing ook niet (meer). In 2024 behandelde de FIOD **272 buitenlandse rechtshulpverzoeken** met crypto als rode draad. Regelmatig zien wij dat cliënten te maken krijgen met een buitenlandse bevrozing van hun wallet of beslag op digitale vermogensbestanddelen, zonder dat daar Nederlandse verdenkingen aan voorafgaan.

Internationaal bewijs roept kritische rechtsvragen op: hoe is het verkregen? Is het recht op een eerlijk proces gewaarborgd, zeker als dat plaatsvond in

‘Opvallend is dat de FIOD niet alleen de klassieke verdachte in het vizier heeft, maar ook zogeheten *facilitators*’

bijvoorbeeld China of Rusland? Iedere verdachte heeft er namelijk recht op om zijn zaak te laten beoordelen door een onafhankelijke en onpartijdige rechter, binnen een redelijke termijn, en om de kans te krijgen om zich te verdedigen.

Van verdachte naar ‘facilitator’

Opvallend is dat de FIOD niet alleen de klassieke verdachte in het vizier heeft, maar ook zogeheten *facilitators*. Denk aan:

- ondernemers die cryptobetalingen accepteren zonder (voldoende) KYC;
- jonge ‘geldeuzels’ die hun wallet ‘even uitlenen’;
- programmeurs die smart contracts schrijven waarmee anderen anoniem kunnen storten en opnemen.

Die brede benadering maakt dat ook goedwillende maar onvoorzichtige mensen en bedrijven in het strafrechtelijk vizier terecht kunnen komen. Zeker in een digitale context, waar transacties anoniem en grensoverschrijdend verlopen, ligt het risico op juridische betrokkenheid op de loer.

Drie uitdagingen voor de verdediging

1 | Digitale bewijslast is complex – en feilbaar

Blockchainanalyse lijkt objectief, maar daar is behoorlijk wat op af te dingen. Veel analyses zijn gebaseerd op software van commerciële partijen zoals Chainalysis. De achterliggende algoritmes zijn niet transparant en de ‘wallet labels’ (bijvoorbeeld: afkomstig van darknet) waarop justitie vertrouwt, zijn niet verifieerbaar. Dat roept ook vragen op over of er wel sprake is van een eerlijk proces.

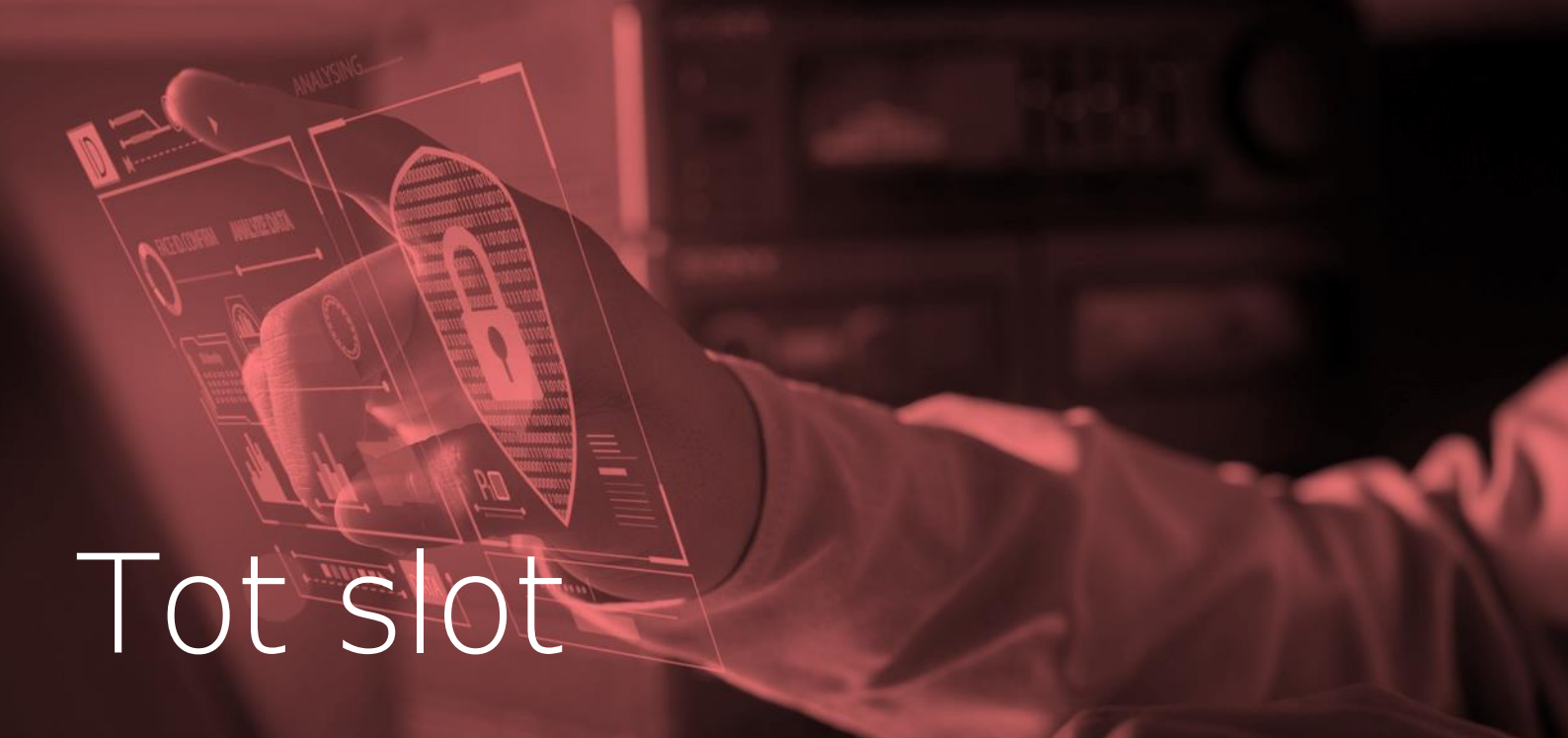
De verdediging doet er verstandig aan altijd de ruwe data, methode en context van de analyse kritisch te toetsen. In de zaak **ECLI:NL:RBROT:2023:10720** oordeelde rechtbank Rotterdam dat een Chainalysis-rapport onvoldoende zelfstandig bewijs opleverde zonder nadere verificatie.

Ook de vraag wanneer een transactie op de blockchain toerekenbaar is aan een specifieke persoon heeft veel ingewikkelde aspecten. Het walletadres is een sleutel, maar zonder aanvullende bewijzen zoals het IP-adres, toegang tot de seed-phrase etc. is niet zeker of iemand daadwerkelijk eigenaar is van een wallet.

2 | Actieve betrokkenheid van facilitators
Strafrechtelijk onderzoek richt zich ook op facilitators. Wanneer wordt het faciliteren van bijvoorbeeld mixers en privacycoins of het gebruik van een cryptoplatform zonder voldoende KYC-procedures als strafrechtelijk verwijtbaar gezien? Recent werd de [oprichter van Tornado Cash nog veroordeeld tot ruim vijf jaar gevangenisstraf](#)². Omdat de mixer was ontwikkeld zonder functionaliteiten die identificatie, controle of opsporing mogelijk maken. Volgens de rechtbank was het de mixer Tornado Cash die de link tussen een storting en een opname verbrak en daarmee de oorspronkelijke herkomst verhulde; witwassen dus. Het argument dat de gebruiker zelf koos voor het gebruik (en eventueel witwassen) en dat de leverancier van de mixer niet verantwoordelijk was, werd van tafel geveegd.

Er is sprake van een spanningsveld: zijn betrokkenen die platforms aanbieden, interfaces bouwen etc. slechts onderdeel van een (crypto)infrastructuur en in die zin neutraal, of is betrokkenheid bij een crypto infrastructuur die door criminelen wordt gebruikt strafrechtelijk verwijtbaar? Dan moet er namelijk wel sprake zijn van opzet of op zijn minst van het willens en wetens accepteren van het risico dat een ander jouw code of infrastructuur gebruikt voor witwassen.

3 | Feitelijke omkering van de bewijslast
Een cruciaal aandachtspunt is de wijze waarop het OM in witwaszaken de herkomstverklaring naar de verdachte schuift.



Tot slot

Bronnen

- 1 | <https://www.jaeger.nl/btw-fraude-in-2025-nog-steeds-in-de-schijnwerpers/>
- 2 | <https://www.fiod.nl/beslag-op-7-miljoen-euro-cryptos-en-2-cryptovaluta-wisseldiensten-offline/>
- 3 | <https://uitspraken.rechtspraak.nl/detail?id=ECLI:NL:RBOBR:2024:2069>
- 4 | <https://www.jaeger.nl/expertise/cryptocurrency/>

In lijn met vaste jurisprudentie van de Hoge Raad (HR 13 juli 2010, ECLI:NL:HR:2010:BM0787, **het witwas stappenplan**) kan van de verdachte worden verlangd dat hij bij een gerechtvaardigd vermoeden van witwassen een concrete en verifieerbare verklaring geeft over de legale herkomst van zijn vermogen. Gebeurt dat niet of onvoldoende, dan kan dit worden meegewogen als belastend.

Bij crypto is dat extra problematisch. Veel early adopters beschikken niet over een sluitende administratie en sommige wallets zijn (bewust of niet) niet herleidbaar. Toch wordt het ontbreken van een verklaring steeds vaker door het OM opgevoerd als bewijsindicatie voor witwassen. In feite leidt dat tot een **omkering van de bewijslast** – iets dat haaks staat op het uitgangspunt van het strafproces. Het uitgangspunt is immers dat iedere verdachte onschuldig is tot het tegendeel bewezen is.

Tot slot: digitale opsporing vraagt digitale verdediging

De FIOD lijkt klaar voor de digitale toekomst. Dat is terecht – maar van de verdediging mag dan ook worden verlangd dat zij die toekomst begrijpt en daar tegenwicht aan biedt. Het strafproces digitaliseert. Daarmee wordt het complexer – én kwetsbaarder. Dat vergt een verdediging die technisch onderlegd is, kritisch blijft op ‘objectieve’ analyses en juridische grenzen bewaakt. Ons kantoor heeft die expertise in huis. Waar opsporing steeds meer vertrouwt op technologie, blijft de rechtsbescherming mensenwerk.

Vragen over een strafrechtelijke verdenking? Neem dan contact op met een van [onze specialisten bij Jaeger Advocaten](#)⁴ voor een vrijblijvend gesprek.

Meer informatie of advies?

Kijk op www.jaeger.nl/kennisbank voor meer informatie over diverse onderwerpen en thema's. Als u vragen heeft, advies nodig heeft of een probleem wilt oplossen, kunt u contact opnemen met ons. Wij staan voor u klaar. U kunt ons bereiken op 020 - 676 04 81 of mail ons op info@jaeger.nl