# FinCrime & technologie in de toekomst

Financieel Economische Criminaliteit (afgekort FEC) kent veel verschillende vormen; van het witwassen van cash en het financieren van terrorisme tot het handelen in illegale middelen en het ontduiken van belasting met behulp van cryptocurrency. Wij interviewden meerdere financial crime-, cybercrime-, cryptocurrency- en OSINT- experts om een zo volledig mogelijk beeld te krijgen van de huidige en toekomstige trends in financieel economische criminaliteit. Zo bespraken we de verscheidenheid van criminele activiteiten, de hedendaagse uitdagingen van analisten en onderzoekers en hoe technologie kan ondersteunen in de strijd tegen FEC nu en in de toekomst. De uitwerking van deze interviews leest u in deze whitepaper.

DataExpert

## Wat zijn de ontwikkelingen rondom FEC?

Enkele jaren geleden zijn een paar grote witwaszaken en schandalen aan het licht gekomen bij verschillende Nederlandse grootbanken. Destijds zijn door De Nederlandsche Bank (DNB) significante boetes uitgedeeld aan de betreffende banken. Sindsdien houdt de DNB strikt in de gaten of deze banken wel voldoen aan hun poortwachtersfunctie, waarbij het de bedoeling is dat klanten op de juiste manier gescreend worden bij toelating. Dit fenomeen staat bekend als het Know Your Customer-principe (KYC). Daarnaast wordt gecontroleerd of transacties wel actief worden gemonitord op mogelijke witwaspraktijken en corruptie. Deze werkzaamheden vallen onder de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft). Bijgevolg hebben de grootbanken in de afgelopen jaren duizenden analisten aangenomen die zich dagelijks bezighouden met KYC en transactiemonitoring.

Naast overheden en banken die scherper toezicht zijn gaan houden op financieel economische criminaliteit, is ook de bevolking bewuster geworden van dit fenomeen. Dit komt onder meer door het uitlekken van de Panama en Paradise papers, maar ook andere bekende zaken zoals de miljardenfraude bij Wirecard, hebben de publieke interesse gewekt. De publieke druk om witwassen, fraude en corruptie tegen te gaan is daardoor aanzienlijk toegenomen.

Het strengere toezicht vanuit de banken en de maatschappij, en strikte wet- en regelgeving heeft het voor criminelen noodzakelijk gemaakt om op zoek te gaan naar andere, creatieve en meer anonieme vormen van criminaliteit om geld te verdienen. Gesteld kan worden dat ze deze ook hebben gevonden. Hieronder lichten we enkele huidige vormen van FEC toe die tijdens de interviews met de experts aan bod zijn gekomen.


**Figuur 1**: Voorbeeld fraudezaak Wirecard

### *Cybercrime*

De afgelopen jaren heeft cybercrime een vogelvlucht genomen. Het is niet langer een scholier die op zolder iemand hackt, maar het zijn volledig georganiseerde bedrijven die criminele praktijken uitvoeren. Cybercrime biedt aan criminelen niet alleen de mogelijkheid om financiële instellingen op te lichten of grote bedrijven aan te vallen, maar er is bijvoorbeeld ook een sterke toename van slachtofferschap onder MKB-bedrijven. Deze bedrijven hebben vaak niet genoeg middelen om zichzelf optimaal te beschermen tegen bijvoorbeeld Malware of Ransomware. Ook is de consument een geliefd doelwit. Met behulp van Social Engineering technieken worden ze eenvoudig opgelicht. Denk bijvoorbeeld aan datingfraude (recent voorbeeld; de Tinder Swindler), identiteitsfraude en Phishing.

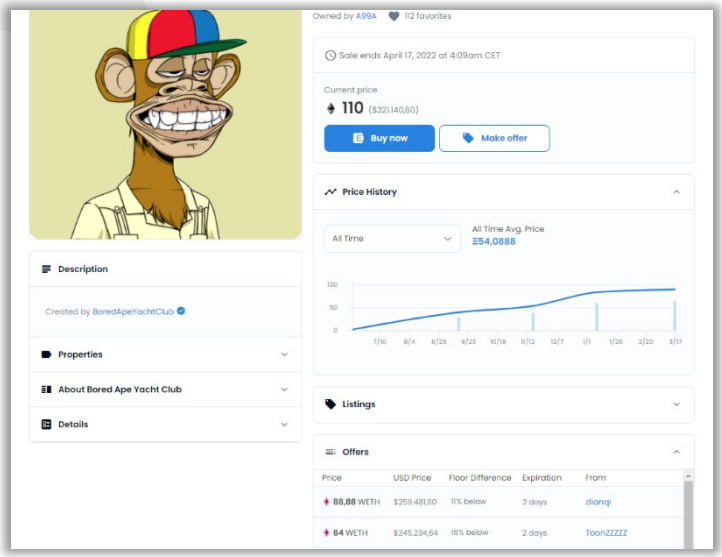

**Figuur 2**: Darkweb advertenties

Naast het direct aanvallen van bedrijven en consumenten, is ook de handel in PayPal accounts, bankrekeningnummers, creditcardgegevens of gevoelige data op het darkweb een vorm van cybercriminaliteit die plaatsvindt.

### *Cryptocurrency*

Cryptocurrency en de blockchain bieden interessante mogelijkheden voor het drijven van handel en het uitvoeren van betalingen. Naast het traden via crypto wallets en het gebruikmaken van Decentralized Finance diensten, zijn er tegenwoordig ook Bitcoin ATM's en bijvoorbeeld cryptocreditcards die veel financiële voordelen met zich meebrengen. Cryptocurrency hebben hun populariteit onder meer te danken aan hun anonieme karakter. Via decentrale platformen kunnen personen, zonder zich te hoeven identificeren, direct toegang krijgen tot verschillende financiële diensten. Het anonieme karakter maakt de wereld van cryptocurrency uitermate interessant voor criminelen. Criminelen zetten cryptocurrency regelmatig in om geld wit te wassen, losgeld te eisen en belasting te ontduiken.

Voorbeeld belastingontduiking met NFT's (Non Fungible Tokens):
*Persoon A beschikt over een Bored Ape NFT zoals te zien in de onderstaande afbeelding. Deze aap met regenboog pet is 110 Ethereum waard. De NFT staat geregistreerd bij Binance, een gecentraliseerde exchange. Doordat gecentraliseerde exchanges een verificatie van de identiteit van gebruikers vragen (inclusief ID-kaart/paspoort), is het vermogen van personen op deze exchange traceerbaar voor de Belastingdienst. Om belasting te ontduiken kan Persoon A de aap "verkopen" aan een eigen gedecentraliseerde wallet zoals MetaMask voor slechts een schijntje van de daadwerkelijk waarde, als voorbeeld nemen we 0,2 Ethereum. De Belastingdienst kan vervolgens alleen de 0,2 Ethereum zien als vermogen en kan niet controleren aan wie de NFT met een daadwerkelijke waarde van 110 Ethereum is verkocht.*




**Figuur 3**: Bored Ape NFT (bron: opensea.io)

### *Oplichting via FinTechs*

FinTechs hebben een groeiende rol in de financiële sector. FinTech is een samenstelling van twee woorden: financial en technology. FinTech bedrijven combineren financiële diensten en producten met innovatieve technologie. Voorbeelden van succesvolle Nederlandse FinTechs zijn bijvoorbeeld Knab & Bunq (FinTech banken) en Adyen & Mollie (Payment Service Providers).

Doordat de DNB graag voldoende ruimte geeft aan innovatie in de financiële markt (bron: dnb.nl) houden ze minder strikt toezicht op bijvoorbeeld de onboarding processen en transactiemonitoring maatregelen bij beginnende FinTechs. Daarnaast is het niet makkelijk voor de DNB om de regelgeving tijdig aan te passen aan de snelle technologische ontwikkelingen in de financiële markt. Hierdoor kunnen criminelen vrij eenvoudig gebruikmaken van de financiële diensten van de FinTechs. Vaak hoeven ze enkel een foto te maken, een ID-kaart te scannen en enkele contactgegevens in te vullen. Eenmaal akkoord bevonden kunnen ze niet alleen gebruikmaken van de dienstverlening van de

FinTech, maar bijvoorbeeld ook aan de hand van afgeleide identificatie bij andere financiële dienstverleners creditcards opvragen voor malafide praktijken.

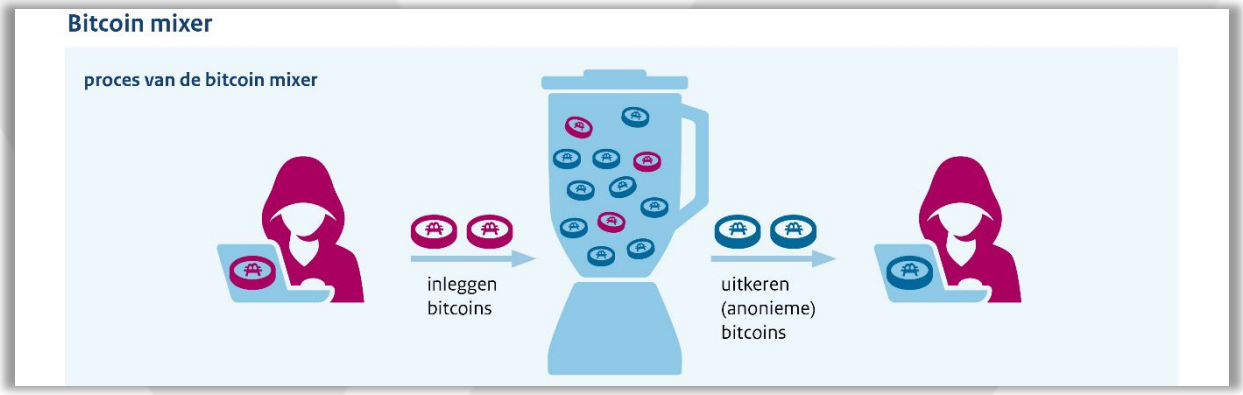
### *Trade-based money laundering*

Naast de financieel economische criminaliteit in de digitale wereld wordt fraude ook nog altijd gepleegd in de fysieke wereld. Een van deze vormen van fraude is trade-based money laundering (TBML). Bij deze vorm van criminaliteit zetten criminelen handelsstructuren op om geld wit te wassen. Het gaat hier dan vaak om goed georganiseerde constructies. Een mooi voorbeeld van TBML is het witwassen van geld door middel van export van aardappelen. Hierbij investeren de criminelen contant geld in grondstoffen die vervolgens worden geëxporteerd naar en verkocht worden in het buitenland. Het identificeren van TMBL vindt nu nog vaak per toeval plaats, maar geschat wordt dat er miljoenen worden witgewassen (bron: AMLC.nl)

## Wat zijn de te verwachte nieuwe vormen van FEC?

Welke vormen van financieel economische criminaliteit zich in de toekomst voor gaan doen naast de hiervoor genoemde voorbeelden, valt volgens alle geïnterviewde experts niet te voorspellen. (Cyber)criminelen blijven inventief en veranderen regelmatig hun ***modus operandi***. Wellicht switchen de criminelen wel terug naar de traditionele betaalmethoden waarbij ze weer gebruik gaan maken van papieren formulieren om geld over te boeken en cash geld, terwijl de opsporing voornamelijk digitaal plaatsvindt.

Wat wel naar voren kwam bij de interviews is de verwachting dat het traceren van criminaliteit steeds complexer zal worden. Zo wordt er in de cryptocurrency wereld nu al volop gewerkt aan het bouwen van zogenoemde mixers voor verschillende blockchain technologieën. Een mixer is een soort blender die meerdere overgemaakte digitale valuta's in stukjes versnippert en vervolgens verspreidt over meerdere transacties. Met deze ontwikkeling zou het zomaar kunnen dat het Follow the Money principe onmogelijk wordt gemaakt met betrekking tot opsporing van witwassen in de cryptocurrency wereld. Onderstaande afbeelding van de Belastingdienst beeldt het mixer principe goed uit.




**Figuur 4:** Bitcoin mixer (bron: FIOD)

## Welke uitdagingen komen kijken bij het opsporen van FEC?

*Kennis up-to-date houden, internationale samenwerking intensiveren en grote hoeveelheden complexe data in combinatie met te weinig tijd.*

### *Kennis up-to-date houden*

Eén van de grootste uitdagingen volgens de geïnterviewde experts is het op peil en up-to-date houden van de kennis van de onderzoekers en analisten. Enkel door zicht te hebben op welke

stappen criminelen doorlopen en door over veel domeinkennis te beschikken, kan criminaliteit succesvol worden opgespoord. Criminelen blijven namelijk continu hun werkwijze verfijnen en hun modus operandi aanpassen op basis van nieuwe technologieën en wet- en regelgeving.

### *Internationale samenwerking*

Doordat er veel verschillende betaalmiddelen zijn en verschillende vormen van criminaliteit, is het volgens de respondenten van het interview noodzakelijk dat er op internationaal en nationaal niveau, maar ook binnen een bedrijf, wordt samengewerkt. Zo zou bijvoorbeeld één centrale organisatie die het onboarden van klanten voor banken voor zijn rekening neemt wenselijk zijn. Hierdoor hoeft niet iedere bank elke keer een klant zelf te onboarden wat veel tijd en middelen zou besparen. Helaas is samenwerken makkelijker gezegd dan gedaan. De wet- en regelgeving, waaronder AVG (Algemene Verordening Gegevensbescherming), maakt dit erg lastig en in veel gevallen onmogelijk.

### *Te veel complexe data en te weinig tijd*

Een andere uitdaging die in elk gesprek naar voren kwam, is de grote hoeveelheid data die bij onderzoeken komt kijken. Onderzoekers en analisten hebben te maken met veel verschillende databronnen en dataformaten: open bronnen, transactiegeschiedenissen, aangeleverde documenten door klanten, et cetera. Vaak is deze data ook nog eens verspreid over tientallen systemen. Ondanks het feit dat er technologie beschikbaar is, vergt het nog altijd veel handmatig werk en een enorme hoeveelheid aan mankracht, en dus geld, om door al deze data heen te spitten en tijdig de relevante informatie te identificeren. De brede variatie aan casuïstiek maakt het tevens lastig om processen te standaardiseren.

### *Up-to-date houden van risico indicatoren*

Momenteel wordt er veel gebruik gemaakt van standaard lijsten en indicatoren binnen financiële instellingen en in de opsporingswereld. Maar wat als een nieuw verschijnsel zich voordoet? Valt deze dan wel op? Ook kijkt men nu vaak naar uitschieters (anomalieën), echter bij vormen van criminaliteit zoals Trade-based money laundering is er geen sprake van dergelijke uitschieters. Het is dan ook belangrijk dat de gehanteerde risico indicatoren continu worden bijgewerkt.

## Welke technologieën kunnen analisten en onderzoekers ondersteunen in de strijd tegen FEC en waarom?

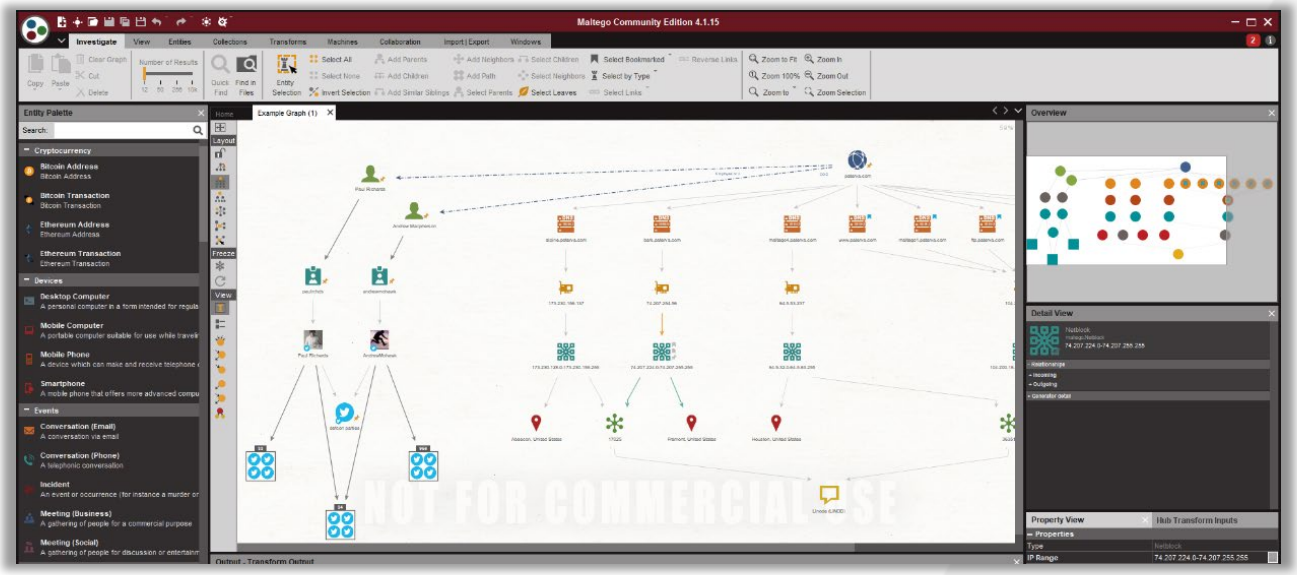
De basis voorsuccesvolle criminaliteitsbestrijding is kennis en ervaring van analisten. Technologie kan onderzoekers en analisten daarentegen wel zeer goed ondersteunen bij het verkennen van data, data begrijpen, data analyseren en vervolgens data omzetten naar inzetbare intelligentie. Hieronder lichten wij verschillende technologieën uit het DataExpert portfolio toe die de strijd tegen financieel economische criminaliteit kunnen vereenvoudigen.

### *Het verzamelen van data uit open bronnen*

Data uit open bronnen kan uw eigen data verreiken en kan helpen bij het onboarden van klanten (KYC) en het in kaart brengen van netwerken. Er zijn in de markt veel verschillende platformen, producten en plug-ins die kunnen helpen met data uit open bronnen te zoeken, te verzamelen, te monitoren, te analyseren en te rapporteren.

Eén zeer populaire open source intelligence (OSINT) tool binnen de opsporingswereld is **Maltego**. Met **Maltego** kunnen onderzoekers en analisten informatie uit open bronnen zoals het darkweb, fora en Reddit verzamelen en verbinden. De software beschikt over een grafische link analyse interface en

vele transforms die het mogelijk maken om andere tooling door middel van API toegang te integreren met het platform.




**Figuur 5:** Maltego software

Daarnaast zijn er ook Web Intelligence platformen zoals **Cobwebs** die gerichte intelligence uit grote hoeveelheden data extraheren met behulp van machine learning algoritmes. Zo ondersteunt Cobwebs onderzoekers en analisten bij het (real time) monitoren van online activiteiten en het verzamelen en analyseren van data uit digitale open bronnen, social media en het deep- en darkweb.

### *Het extraheren & analyseren van ongestructureerde data*

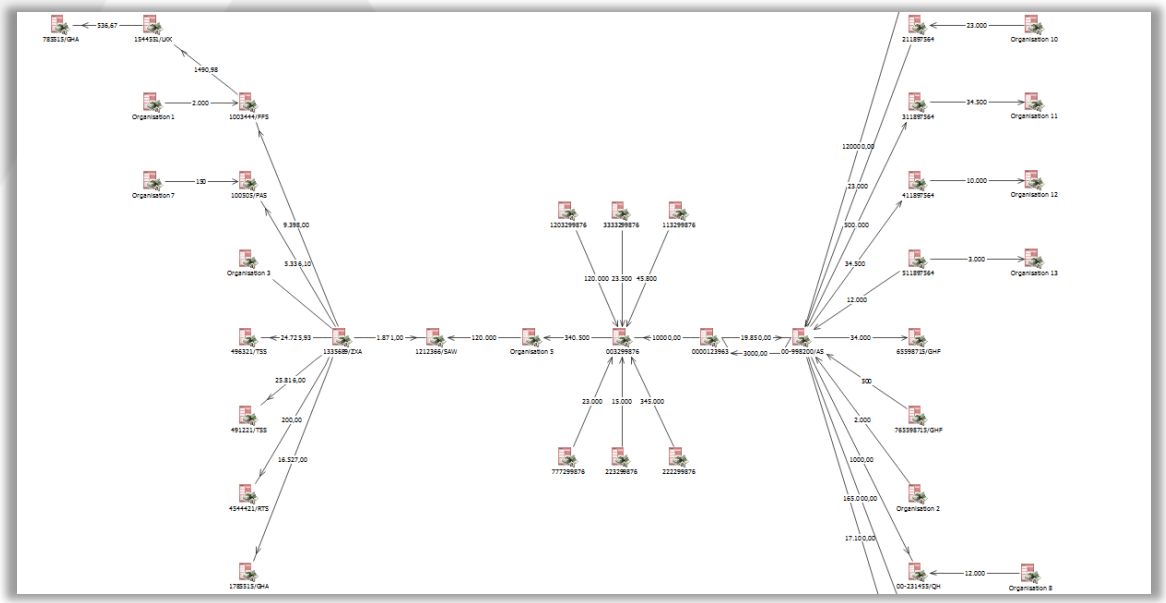
Steeds meer data die ten behoeve van criminaliteitsbestrijding wordt gebruikt is ongestructureerd, denk bijvoorbeeld aan inhoud van nieuwsberichten of social media posts. Het gebrek aan één standaard structuur, het volume van de beschikbare data (big data) en de vele formaten bemoeilijkt het analyseproces. Met de software oplossing **i2 TextChart** kunnen analisten en onderzoekers uit vele duizenden e-mails, openbare bronnen en/of financiële documenten, locaties en andere entiteiten en relaties extraheren voor verdere visualisatie en analyse. i2 TextChart verrijkt de visualisatie en netwerkanalyse van gestructureerde data met geautomatiseerde extracties van meer dan 36 verschillende type entiteiten, 200+ relaties en (geografische) locaties.


**Figuur 6:** i2 TextChart

### *Financial Crime Analysis*

Software zoals **i2 Analyst's Notebook (Premium)** helpen onderzoekers en analisten met het inzichtelijk maken van data door zoek- en linkanalysefunctionaliteiten. Diverse soorten

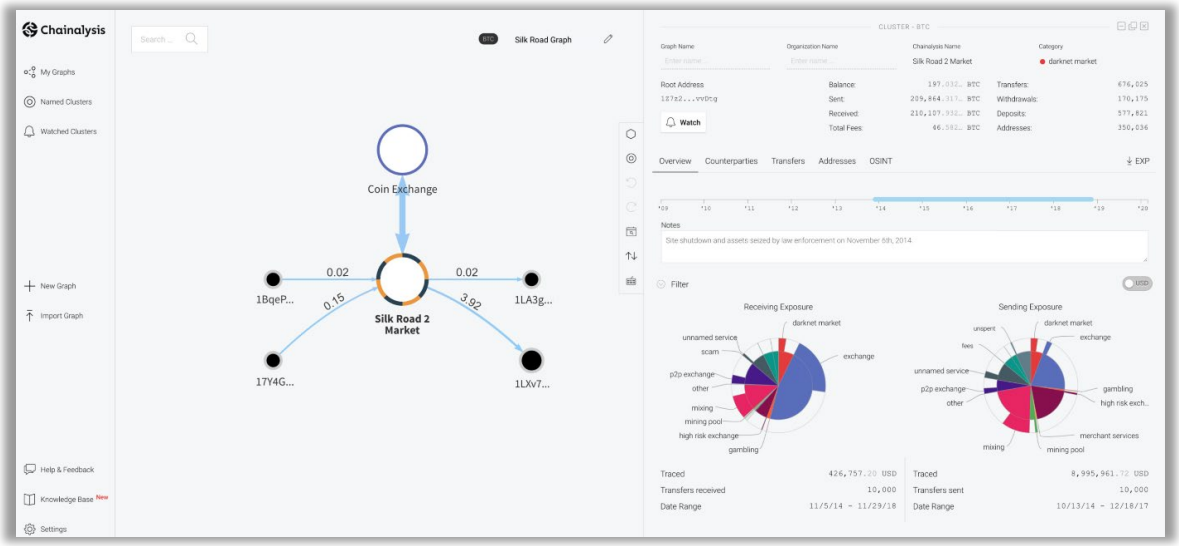
gestructureerde gegevens (telefoongesprekken, transacties, IP-adressen etc.) worden over elkaar gelegd en gevisualiseerd door middel van heatmaps, relaties, histo- en diagrammen etc. Relationele netwerken, tijdlijnen en geografische weergaves worden zo in één oogopslag duidelijk. Met de visualisatie functionaliteiten kunnen onderzoekers en analisten vervolgens de modus operandi van criminelen in beeld brengen.



**Figuur 7:** i2 Analyst's Notebook

### *Het analyseren van cryptocurrency transacties*

Zoals eerder beschreven is cryptocurrency een geliefd betaalmiddel van criminelen. En hoewel ze het onderzoekers en analisten knap lastig maken om hun transacties te monitoren, is het niet onmogelijk. Cryptocurrency transacties worden nu eenmaal opgeslagen in een openbaar grootboek. Met behulp van geavanceerde technologie kunnen cryptocurrency transacties in de blockchain worden gemonitord, gecollecteerd en geanalyseerd om zo met de juiste inzichten te kunnen acteren op witwaspraktijken en terrorismefinanciering. **Chainalysis** biedt verschillende oplossingen voor het uitvoeren van cryptocurrency onderzoeken.




**Figuur 8:** Chainalysis

## Hoe ziet de technologie van de toekomst eruit?

Zoals hierboven omschreven zijn er veel verschillende tools in de markt die analisten en onderzoekers kunnen ondersteunen bij hun onderzoek. Ondanks het nu al brede aanbod, waren we ook benieuwd wat nog beter kan in de toekomst op het gebied van technologie. De respondenten van het interview kwamen met één duidelijke wens: **een platform waarin alle databronnen tegelijk kunnen worden doorzocht op een Google-achtige manier.** Waarbij het idealiter ook een schaalbare oplossing betreft en niet dure hardware kosten met zich meebrengt.

Ook gaven de experts aan te verwachten dat AI/Machine Learning in de toekomst analisten en onderzoekers zal ontlasten door automatisch enorme datasets te scannen, patronen en afwijkingen te identificeren, verbanden te leggen en de resultaten samen te vatten. De eerste stappen zijn hier overigens al in gezet. Zo maakt de hiervoor omschreven tool Cobwebs al gebruik van AI.

## Conclusie

Eén ding is ons na alle gesprekken duidelijk geworden: **stilzitten is geen optie!** Om de ontwikkelingen binnen financieel economische criminaliteit bij te kunnen houden, is het van belang dat onderzoekers en analisten (blijven) beschikken over de juiste skills en expertise. Kortom: trainen, trainen, trainen en kennisdelen.

Ook de juiste technologie kan financiële instellingen en opsporingsinstanties helpen met het inzichtelijk maken van de complexe modus operandi van criminelen. Door efficiënt data te vergaren, samen te voegen en te analyseren kunnen netwerken in kaart worden gebracht, tijdlijnen inzichtelijk worden gemaakt en afwijkingen eruit worden gefilterd.

## DataExpert denkt graag met u mee

Welke werkwijze en hulpmiddelen in de strijd tegen financiële criminaliteit binnen een organisatie passen, verschilt per organisatie. Dit wordt beïnvloed door het type databronnen waarmee gewerkt wordt, de capaciteit, de gewenste onderzoeken, het budget etc. De experts van DataExpert denken graag met u mee om de juiste werkwijze in kaart te brengen.

Ook kunnen wij u en uw collega's opleiden in het analyseren van (cryptocurrency) data met en zonder tools, het uitvoeren van OSINT-onderzoeken en het inzichtelijk maken van cybercrime.


**T:** +31 (0)318 543173
**E:** info@dataexpert.nl
**W:** www.dataexpert.nl
**A:** Vendelier 65, 3905 PD Veenendaal