SBIR cyber security

Projecttitel:	**Crypto-valuta inlichtingen**
Bedrijf:	**Coblue Cybersecurity BV**
In samenwerking met:	**TNO**

Projectsamenvatting

Het gebruik van cryptovaluta – zoals bijvoorbeeld Bitcoin – is de laatste jaren sterk toegenomen. Dit gebruik is voor legitieme doeleinden, maar ook populaire in criminele activiteiten (witwaspraktijken, fraude, handel in illegale goederen en diensten, etc.). Om deze reden is er een toenemende behoefte aan inzicht in deze cryptovaluta-transacties.

Bitcoin is een pseudoniem netwerk: transacties zijn aan pseudoniemen te koppelen en geldstromen zijn te volgen. Bitcoin is zeker niet anoniem, zoals weleens beweerd wordt. Het is echter wel zo dat analyse van de gegevens van het gebruik van cryptovaluta's niet eenvoudig is. Om hier verandering in te brengen is het project *Crypto-valuta inlichtingen (CVI)* gedefinieerd.

Het primaire doel van CVI is het verschaffen van inzicht in cryptovaluta-transacties voor het ondersteunen van (forensisch) onderzoek naar criminele activiteiten waarin cryptovaluta een rol spelen. CVI speelt hiermee in op de vraag naar een inlichtingendienst voor cryptovaluta-transacties.

Om dit doel te bereiken is binnen het CVI project analyse-software ontwikkeld, die de eindgebruiker zelf in staat stelt om forensisich onderzoek naar Bitcointransacties en –gebruikers te doen.

De software, genaamd Cointel, ondersteunt forensisch onderzoek op verschillende manieren, waaronder:

- Clustering van transacties: hierin wordt de publiek toegankelijke transactiedata van Bitcoin (opgeslagen in de blockchain) geannalyseerd en gegroepeerd naar entiteiten. Een entiteit is een individu of organisatie die het beheer heeft over (een cluster van) bitcoinadres(sen).
- Patroonherkenning: hierin wordt verdere analyse gedaan naar specifieke transactiepatronen.
- Attributie ("de-pseudonimisatie"): met behulp van extra databronnen wordt persoon-identificeerende informatie gekoppeld aan bitcoinadressen en –clusters. In sommige gevallen kan zo de identiteit van een Bitcoingebruiker achterhaald worden.

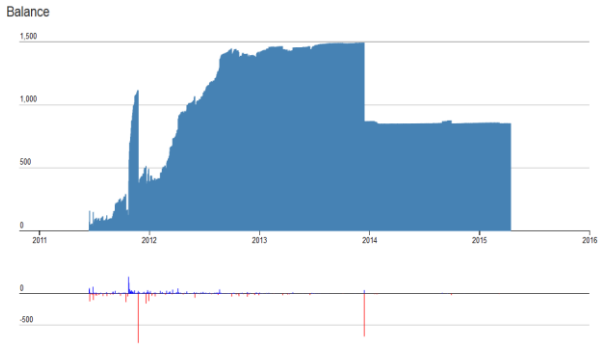
Middels een webbased interface kunnen gebruikers van Cointel antwoord krijgen op vragen als:

- Is er identificerende informatie beschikbaar over de entiteit die een bitcoinadres beheert? En zo ja, wat is deze informatie?
- Welke adressen behoren nog meer aan dezelfde entiteit? Adressen kunnen onderdeel zijn van een wallet. Welke adressen behoren nog meer in de wallet van dezelfde entiteit?
- Welke patronen zijn er te herkennen? Is informatie door een mixer gegaan? Welke transactieketens volgen hetzelfde patroon? Of volgen een specifiek type patroon?
- Wat is de omzet van een entiteit? Hoeveel omzet (in bitcoin of traditionele valuta) wordt omgezet door een entiteit? En wat is het verloopt van deze omzet?
- Welke (Geo)IP data is beschikbaar over een entiteit? Worden er nog meer wallets vanaf hetzelfde IP-adres beheerd?

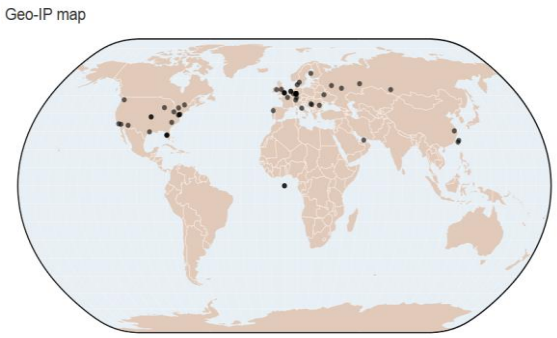
Onderstaand worden enkele rapportage-afbeeldingen van Cointel weergegeven.

Rapportage-afbeeldingen Cointel:

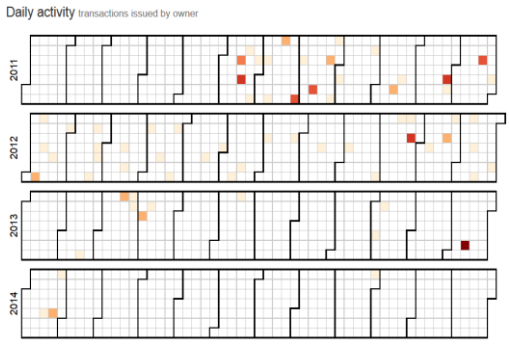
Outstanding balance over time



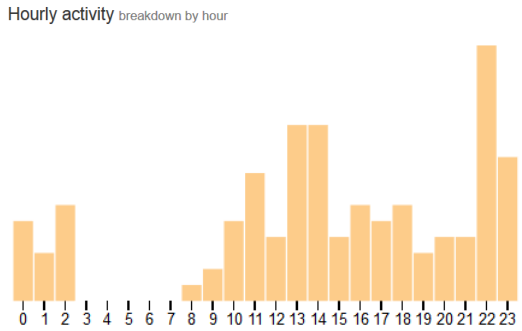
Geo-locations of transactions



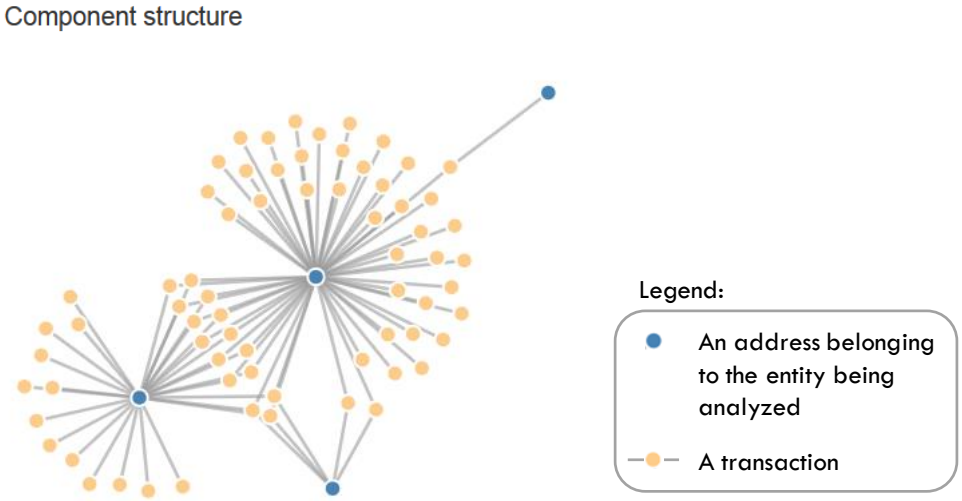
Daily transaction activity



Hourly transaction activity



Cluster of entity addresses



Deze aanbesteding volgt de Small Business Innovation Research (SBIR) methode. SBIR benut en ontwikkelt kennis, creativiteit en innovatiekracht van het bedrijfsleven voor innovaties die een passend antwoord geven op maatschappelijke opgaven.