

## FACTSHEET: De bitcoinmixer

15 mei 2020

Een bitcoinmixer ziet op onlinediensten die "mixing services" (ook wel "tumblers") worden genoemd. Tegen een betaling van een commissie aan de eigenaren van de mixer worden bitcoins (of andere crypto's) tegen andere bitcoins (of andere crypto's) gewisseld. De klant krijgt bitcoins in een andere samenstelling en betaalt hiervoor een commissie. Die commissie is een paar procent van de totale waarde aan bitcoins (denk aan 1% - 3%). Omdat bitcointransacties worden bijgehouden in een openbaar register (de Blockchain), is de herkomst van bitcoins te traceren. De bitcoinmixer zorgt ervoor dat het volgen van transacties wordt verhinderd. Mixing services hebben geen enkel ander doel dan het verhullen van de bron van herkomst van de bitcoins. Sommige van deze mixing diensten, zoals BitLaundry, vermelden dit ook expliciet: "Secure Launder renders your bitcoins completely untraceable, even to the most persistent forensic investigator."



Om het IP-adres van de dienstverlener en de klanten te verhullen zijn mixing services vaak via een Tor-netwerk bereikbaar. Voorts lijken mixing services vooral te opereren vanuit jurisdicties waarmee de justitiële samenwerking niet of nauwelijks plaatsvindt.<sup>2</sup> De mixer is zo ingericht dat de klant niet de eigen bitcoins terugkrijgt, ook niet als deze in verschillende porties door de mixer gaan. De bitcoins die de klanten terugkrijgen na het 'mischen', zijn bitcoins afkomstig van andere klanten die ook gebruikmaken van deze dienstverlening. Dit zijn bitcoins met een andere transactiegeschiedenis (herkomst). Door de mixer te gebruiken is de werkelijke transactiegeschiedenis (in aard, omvang, wallets en partijen) van de bitcoins van de klant na het mixen niet te zien noch te reconstrueren.<sup>3</sup> Aan de bitcoins die door een mixer zijn gegaan is het soms wel mogelijk om te zien dat gebruik is gemaakt van een mixer.<sup>4</sup> Van dit laatste wordt in de opsporingspraktijk veelvuldig gebruikgemaakt om een onderzoek naar de gebruiker te starten en het vormt een belangrijk onderdeel van de bewijsvoering.

Het gebruik van de bitcoinmixer is door FIU-NL aangemerkt als witwastypologie.<sup>5</sup>

De rechtbank Midden-Nederland overwoog ten aanzien van het gebruik van de bitcoinmixer het volgende: *'Daarbij komt dat sprake is van een aantal witwastypologieën. Niet alleen staan de transacties niet in verhouding tot de inkomsten van verdachte, maar er is ook geen legale economische verklaring voor de gewisselde valuta'soorten, er zijn grote geldbedragen contant opgenomen en zonder noodzaak voorhanden gehouden en er is gebruik gemaakt van bitcoinmixers. In het dossier wordt geconstateerd dat bitcoinmixers worden gebruikt om de herkomst van bitcoins te verbergen en er ook geen andere reden is om een dergelijke mixer te gebruiken.'*<sup>6</sup>

<sup>1</sup> <https://bitlaundry.com/laundry-bitcoin>.

<sup>2</sup> B.H.M. Custers, J.J. Oerlemans en R.L.D. Pool 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 2016 (2), 15 onder verwijzing naar: M. Möser, R. Böhme & D. Breuker, 'An inquiry into money laundering tools in the Bitcoin ecosystem', *eCrime Research Summit (eCRS)* 17-18 september 2013, p. 1-14. (<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6805780>).

<sup>3</sup> D. Moore en T. Rid, 'Cryptopolitik and the Darknet. Encryption policy is becoming a crucial test of the values of liberal democracy in the twenty-first century' *Survival*, 58 (1): Global Politics and Strategy 2016, p. 17.

<sup>4</sup> Voor uitgebreide informatie over de bitcoinmixer, zie R.S. van Wegberg, J.J. Oerlemans en M.O. van Deventer 'Bitcoin Money Laundering: Mixed Results? An explorative study on money laundering of cybercrime proceeds using Bitcoin', *Journal of Financial Crime* (2017, in press).

<sup>5</sup> <https://www.fiu-nederland.nl/nl/witwas-typologieen-0>

<sup>6</sup> ECLI:NL:RBMNE:2018:234