

# New money laundering typologies in the fight against money laundering by means of virtual currencies

mr. S. Visser\*

## 1. Introduction

Since 2013 the Financial Intelligence Unit (FIU)<sup>1</sup> has seen a variety of reports from banks of unusual transactions with more or less the same commentary: 'Not normal account behaviour: the client receives large amounts of money originating from bitcoin exchanges. The client then withdraws those amounts immediately. There is no apparent economic necessity for doing so. The account shows a number of bitcoin sales but no purchases.' Three investigation teams from the FIOD (Fiscal Intelligence and Investigation Service) and the police investigated this behaviour.<sup>2</sup> Their conclusion: all of these persons are bitcoin traders<sup>3</sup> helping criminals to launder money. The investigation teams also observed another phenomenon: the bitcoin mixer. Both the trading of virtual currencies such as bitcoin and the use of a mixer of virtual currencies have since been validated as money laundering typology. This article examines the phenomena of 'bitcoin trader' and 'bitcoin mixer' and how they relate to money laundering. It concludes with new money laundering typologies for the purchase and sale of virtual currencies.

## 2. General remarks about bitcoin

For a better understanding of the activities of the bitcoin trader and the bitcoin mixer we must first describe some of the general background to bitcoin, how payments are made with bitcoin, how bitcoins are acquired and the extent to which bitcoin involves a risk of money laundering.

### 2.1 What is bitcoin and how are payments made with bitcoin?

Bitcoin is an independent payment system with its own virtual coin, whereby users are able to conduct transactions with one another directly through the internet without any intermediation by other parties such as banks. A bitcoin consists of a piece of encrypted computer code to which a value is assigned in Euros, or some other legal means of payment, by the market of supply and demand.<sup>4</sup> The value of bitcoin fluctuates considerably.<sup>5</sup> Bitcoin is not regarded as money in the Netherlands but as a means of exchange.<sup>6</sup> In order to pay with bitcoins or to receive bitcoins you need a bitcoin address. The bitcoin address is the public component of a key pair and it can be shared with a trading partner. The bitcoin address is comparable to a bank account number. A bitcoin address has a minimum of 27 and a maximum of 34 characters. The private component (private key) of the key pair cannot be shared and must be carefully saved. In practice the transfer of bitcoins is a matter of filling in the bitcoin address of the recipient (the payee) and the number of bitcoins (the transaction

---

\* mr. S. Visser is account manager and project leader anti-money laundering at the Anti Money Laundering Centre (AMLC) in De Bilt. This article was published in *Tijdschrift voor Bijzonder Strafrecht & Handhaving* December 2017.

<sup>1</sup> Institutions subject to the Money Laundering and Terrorist Financing (Prevention) Act (the Wwft) must report any unusual transactions to the Financial Information Unit (pursuant to Wwft Section 16).

<sup>2</sup> See for example <https://www.om.nl/vaste-onderdelen/zoeken/@92718/10-aanhoudingen/> (consulted on 31 July 2017).

<sup>3</sup> In this article the term 'bitcoin trader' refers to bitcoin traders who match the profile set out in paragraph 4.1.

<sup>4</sup> Much has already been written about bitcoin. For a detailed account of (the background of) bitcoin I refer the reader to J. Baukema, 'Bitcoin: een (ongereguleerd) betaalmiddel van de toekomst?', *Tijdschrift voor Financieel Recht*, December 2013, no. 12 and R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H* March 2017, no. 1.

<sup>5</sup> <http://www.spectator.co.uk/2016/03/is-bitcoin-a-safe-haven-against-mainstream-money-mayhem/> (consulted on 31 July 2017). For the conversion to Euros the 'Historical Exchange Rates' can be used, see for example <https://www.investing.com/currencies/btc-usd-historical-data> (consulted on 15 August 2017). The volatility of the bitcoin is frequently referred to by the media, see for example M. Stravens, 'Bitcoin on the rise again after period of big swings', *Het Financieel Dagblad*, 8 February 2017.

<sup>6</sup> For a detailed account of the legal and tax qualification of bitcoin see R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H* March 2017, no. 1. Regarding bitcoins as a means of exchange rather than money has consequences for the supervision exercised by the state. In this regard see J. Baukema, 'Virtuele valuta: (toezichtrechtelijke) stand van zaken', *Tijdschrift voor Financieel Recht*, September 2014, no. 9.

amount) and then clicking on 'Send'.<sup>7</sup> Your bitcoins are kept in your bitcoin wallet. You can download a wallet from [www.bitcoin.org](http://www.bitcoin.org). Inside the wallet you can generate one or more bitcoin addresses. Bitcoin addresses and bitcoin wallets are not linked to an identity or name. You can use bitcoins in various ways, just like other currencies. First of all you can make (consumer) purchases with bitcoins. This can be done both online through webshops that accept bitcoins as a means of payment and in ordinary shops that accept bitcoins. Payment is made by scanning a QR-code or holding your telephone next to a sales register with NFC.<sup>8</sup> You can also invest or speculate in bitcoins.

## 2.2 How do you acquire bitcoins?

You can acquire bitcoins in several ways:

- *Bitcoins are earned by 'mining'*

Bitcoin has to be virtually 'mined'. Every day the bitcoin system releases a certain number of bitcoins to people mining bitcoins. New bitcoins are tied up in algorithms which are extremely difficult to crack. They can only be cracked by deploying computer power. Anyone can mine bitcoins by purchasing the necessary hardware and appropriate software.

- *Bitcoins are bought from money changers, market places (exchanges) and traders*

The first way to buy bitcoins is through a bitcoin exchange office. Bitcoin exchange offices buy and sell bitcoins for their own account and risk. They issue purchase and sale prices against which bitcoin can be bought or sold from them. Examples of bitcoin exchange offices are Bitonic and BTCdirect. The costs of exchange at Bitonic vary from 0.1% to 1.5% of the transaction amount. Apart from bitcoin exchange offices there are also bitcoin marketplaces. These are trading exchanges where parties can buy and sell bitcoins to and from one another. A marketplace (exchange) is an intermediary which brings together supply and demand, makes possible a market with transactions and price-setting, and keeps records of the credit balances of money and bitcoins held by the clients. Examples of popular bitcoin exchanges are *Kraken* and *BitStamp*. For all transactions from bitcoin to Euros and vice versa which are facilitated by the exchange, *Kraken* charges a fee of 0.26% and Bitstamp a fee of 0.1 to 0.25% depending on the size of the transaction. On BL3P, the market place of Bitonic, a fee of 0.25% is charged. Third party costs (processing payments) are charged on to the client separately.<sup>9</sup> Using so-called bitcoin machines it is possible to purchase bitcoins with cash. You can insert Euro notes into the bitcoin machine, whereupon the equivalent value in bitcoins is deposited in your digital wallet. There are several of these machines in the Netherlands.<sup>10</sup> It is also possible to purchase bitcoins in person (face to face) for cash. Traders offer to buy bitcoins for cash through LocalBitcoins.com.<sup>11</sup> The person concerned thereby specifies the price and the limits (minimum and maximum transaction size) applicable to his (cash) purchases and sales. These traders are further discussed in paragraph 4.1.

- *Someone pays you in bitcoins for delivered goods or services*

You can also acquire bitcoins by accepting payment in bitcoins for the delivery of goods or services in the daily course of business. The equivalent value in bitcoin of the goods and services delivered by you is then transferred directly to your wallet. Those goods and services may also be illegal.<sup>12</sup>

---

<sup>7</sup> For more detailed information in this regard see B.H.M. Custers, J.J. Oerlemans and R.L.D. Pool, 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 2016, no. 2, part 15.

<sup>8</sup> NFC (Near Field Communication) is a contactless method of communication. NFC is used, for example, for the contactless payments made with bank cards.

<sup>9</sup> There is also a (limited) number of platforms that do not work with orders but operate primarily as an intermediary or marketplace which brings together supply and demand. A well-known example of this is LocalBitcoins.com.

<sup>10</sup> Some of these machines allow you to exchange bitcoins for Euros, see D. van Vliet, 'Dringen bij pinmachine voor bitcoin', *AD* 17 August 2017, <http://www.ad.nl/rotterdam/dringen-bij-pinmachine-voor-bitcoin~a58ade43/>.

<sup>11</sup> There is a similar platform for the virtual currency Monero, see R.R. O'Leary, 'Monero Is Getting Its Own Version of LocalBitcoins', 30 August 2017, <https://www.coindesk.com/monero-getting-version-localbitcoins/>.

<sup>12</sup> If you offer goods or services through a webshop that accepts bitcoins as an online currency then the payment will be settled through a Payment Service Provider (PSP). Examples of a PSP are Bitpay, Qantani Payments and Mollie.

### 2.3 Money laundering risks with bitcoin

A bitcoin address and a bitcoin wallet are not linked to an identity or name. Such anonymity makes bitcoin attractive for criminal activities.<sup>13</sup> Bitcoins offer an opportunity to launder illegally acquired money in a relatively anonymous way.<sup>14</sup> A lot of trade on darknet markets (such as AgoraMarket and AlphaBay) can only be paid for with bitcoins.<sup>15</sup> The majority of the goods offered on a dark-web marketplace are illegal.<sup>16</sup> They include such things as drugs, weapons and child pornography, stolen credit-card data, and services related to cyber criminality. The use of bitcoins is also common among criminals in the field of cybercrime and the financing of terrorism.<sup>17</sup> For a long time cash has been the preferred option when it comes to illegal activities. The problem with cash is the logistics (storage, transport, bulk) but it also has the advantages of anonymity and the absence of a paper trail. The strength of bitcoin is the speed at which money can be sent. Payments can be made anywhere in the world in just a few seconds. The names of the sender and receiver are not specified with the payment so that the parties enjoy greater anonymity than is the case with regular bank transactions. Europol estimates that 40% of intra-criminal payment transactions were conducted in bitcoins in 2015.<sup>18</sup> Even though bitcoin is a legal system and bitcoins are legal currency, there are still money laundering risks associated with the use and exchange of bitcoins.<sup>19</sup>

### 3. The anonymity of bitcoin

During bitcoin transactions you use a wallet and one or more bitcoin addresses. Wallets and addresses are not linked to a name. To that extent you remain anonymous.<sup>20</sup> All bitcoin transactions are visible however and in theory traceable. Every transaction that takes place in the bitcoin network is stored in the so-called Blockchain. The moment of the transaction, the bitcoin addresses and the amount involved in the transaction are all recorded in this public ledger. You can enter a bitcoin address<sup>21</sup> in the search screen of the online Blockchain. You then receive an overview of all the transactions conducted using that address. Through the Blockchain bitcoins can (in theory) be traced back to the moment they first came into existence. Through the website <http://walletexplorer.com> you can see all the transactions that have been conducted with a particular wallet.<sup>22</sup> In other words by using these tools, all available through the internet, you can find out which transactions have been conducted with which particular bitcoin address. You can also find out which bitcoin addresses belong with which particular wallet.

A bank account is needed in order to purchase and sell bitcoins through bitcoin exchange offices or bitcoin exchanges. Funds are transferred to the exchange office or the exchange from that account, in exchange for bitcoins. When bitcoins are sold the equivalent value is transferred to the bank account by the exchange office or exchange. The identity of the account holder is known to the bank, as are all (other) financial transactions.

---

<sup>13</sup> See also R. Betlem, 'Meer controle op bitcoin-transacties', *Het Financieele Dagblad* 3 August 2016.

<sup>14</sup> This was already confirmed by FBI in 2012. See: FBI, 'Bitcoin virtual currency. Unique features present distinct challenges for deterring illicit activity', *Wired* 5 September 2012, [www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf) (consulted 14 August 2017).

<sup>15</sup> See also R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H March* 2017, no. 1, p. 1 and R.S. van Wegberg, J.J. Oerlemans and 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, p. 4.

<sup>16</sup> D. Moore and T. Rid, 'Cryptopolitik and the Darknet. Encryption policy is becoming a crucial test of the values of liberal democracy in the twentyfirst century', *Survival* February-March 2016, issue 58, no. 1, p. 15-22.

<sup>17</sup> Report Europol 2015, 'The Internet Organised Crime Threat Assessment', p. 11, available for consultation via <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015> (consulted 15 August 2017) and Report FATF 2014, 'Virtual Currencies, key definitions and potential AML/CFT risks', p. 5, available for consultation via <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (consulted on 21 August 2017).

<sup>18</sup> Report Europol 2015, *The Internet Organised Crime Threat Assessment*, p. 46.

<sup>19</sup> De Jong says on this subject: 'The technology behind bitcoin makes it possible to transfer funds anonymously. This increases the risk of money laundering.' See R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H March* 2017, no. 1, p. 5. See also A.B. Schoonbeek, W.M. Shreki and M.T. van der Wulp, 'Bitcoins, witwassen & integriteitsrisico's', *Tijdschrift voor Compliance* April 2017, p. 95 and *Nieuwsbrief banken* June 2014, 'DNB warns banks and payment institutions of integrity risks with virtual currencies', 3 June 2014, <http://nieuwsbrief.dnb.nl/edition/nieuwsbrief/-nieuwsbrief-2014/152> (consulted 31 July 2017).

<sup>20</sup> De Jong: 'The technology behind bitcoin makes it possible to transfer funds anonymously. The risk of money laundering is thereby increased.' See R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H March* 2017, no. 1, p. 5. See also A.B. Schoonbeek, W.M. Shreki and M.T. van der Wulp, 'Bitcoins, witwassen & integriteitsrisico's', *Tijdschrift voor Compliance* April 2017, p. 95 and *Nieuwsbrief banken* June 2014, 'DNB warns banks and payment institutions of integrity risks with virtual currencies', 3 June 2014, <http://nieuwsbrief.dnb.nl/edition/nieuwsbrief/-nieuwsbrief-2014/152> (consulted 31 July 2017).

<sup>21</sup> <http://blockchain.info> (consulted 31 July 2017).

<sup>22</sup> You can enter a bitcoin address in the search field on this website. A message then appears telling you that this bitcoin address is part of a particular wallet. After that you see all the transactions conducted with the wallet. When you press the 'show wallet addresses' button, all the bitcoin addresses belonging to the wallet are displayed.

By combining the bitcoin transactions and the financial data of the bank account, a clear picture emerges of the duration and scale of the trading by the person concerned. The bank has a duty to report unusual transactions so that this information can also become known outside the bank.<sup>23</sup> This lack of anonymity during the cash-out of bitcoins creates a market for middlemen, the bitcoin traders, who accept the cash-out for their own account.

## 4. The bitcoin trader

### 4.1 The profile of the bitcoin trader

A bitcoin trader is a person who purchases and/or sells bitcoins for cash, on a commercial basis, for his own account and risk. A bitcoin trader is recognisable by the high frequency of bitcoin transactions, the large number of bitcoins in his possession, the large number of bitcoins exchanged at an exchange or exchange office, and the large amounts transferred to his bank account from an exchange or exchange office, even though there are no business activities visibly paid for by means of bitcoins.<sup>24</sup> The seller of bitcoins and the bitcoin trader come into contact through advertisements placed on the 'surface' web by the bitcoin trader, on localbitcoins.com for example or through forums on the dark web or on a bitcoin platform. The seller of bitcoins and the bitcoin trader then meet up in the physical world, after which the bitcoin transaction takes place on the spot through the internet. The seller transfers bitcoins directly to the wallet of the trader, after which the trader gives the agreed equivalent value to the seller in cash. The transaction is then complete. On localbitcoins.com traders offer to buy bitcoins for cash at set rates (exchange rates) and within set limits (size of the transaction). Traders sell bitcoins for cash in the same way.<sup>25</sup> Criminal investigations show<sup>26</sup> that the cost of using a bitcoin trader is considerably higher than it is for an exchange office or an exchange. It is not unusual for a trader to charge between 7% and 15% of the transaction value; at a normal exchange office about 0.3% is charged. In spite of the high commission there is still a market for these traders. The same criminal investigations show that after selling bitcoins to exchange offices or through exchanges, the traders withdraw most or all of the money received on their bank account immediately in cash. In this way the trader probably provides for his need for cash so that he can buy more bitcoins. The investigations also show that the banks ask bitcoin traders to clarify the large amounts received by them from a money changer or an exchange which have then been withdrawn in cash (as shown by their profile). Repeated failure to answer these questions to the satisfaction of the bank will lead to termination of the client-bank relationship. Exchanges terminate their client relationships for similar reasons, so that the general picture which emerges is one of successive money changers, exchanges and banks.

### 4.2 Money laundering

Why would someone use a bitcoin trader when there are cheaper and more reliable alternatives available? The answer to this question lies in the anonymity and the cash payment for bitcoin sales and in the original source of the bitcoins themselves. An average private individual or business person is not likely to conduct such large transactions against such high bill charges and in cash. Several criminal investigations clearly show that criminals converted their bitcoins using traders of this kind. Millions of Euros worth of bitcoins have been exchanged for cash in this way, with high commissions for the traders. These bitcoins invariably originate from illegal activities on the dark web.<sup>27</sup> In those investigations the bitcoin trader acted as a connecting link in the

---

<sup>23</sup> Wwft Section 1 in conjunction with Section 16. Supervisor De Nederlandsche Bank (DNB) warned banks and payment institutions of integrity risks with virtual currencies in 2014. DNB qualifies the current virtual currencies as products with an extremely high risk profile whereby as currencies they are attractive as links in a money laundering process. Source: *Nieuwsbrief banken* June 2014, 'DNB warns banks and payment institutions of integrity risks with virtual currencies', 3 June 2014, <http://nieuwsbrief.dnb.nl/edition/nieuwsbrief-nieuwsbrief-2014/152> (consulted 31 July 2017).

<sup>24</sup> One possible explanation for a suspect with a large volume of bitcoins is that the person in question may be a miner. However mining is becoming less profitable due to the associated energy costs. According to Baukema: 'The more computing power a user makes available to the bitcoin network, the more likely it is that this user will generate a new bitcoin, which the user then "acquires" and can bring into circulation. In view of the enormous amount of computer power and energy required for this, it is almost impossible for most consumers to earn bitcoins in this way.' Source: J. Baukema, 'Bitcoin: een (ongereguleerd) betaalmiddel van de toekomst?', *Tijdschrift voor Financieel Recht*, December 2013, number 12. In Mongolia for example – mainly because of the cheap energy – 'bitcoin mines' are built in which bitcoins are mined in large sheds full of computers, see S. den Daas, 'De mijnwerkers van de 21e eeuw komen uit Binnen-Mongolië', *Het Financieel Dagblad* 21 January 2017. Such an explanation from a suspect should therefore be supported by the energy bill of the suspect, the hardware and software present, and his transaction data from the bank and the Blockchain.

<sup>25</sup> The most commonly used minimum for a purchase in cash by a trader varies from 2000 to 5000 Euros per transaction.

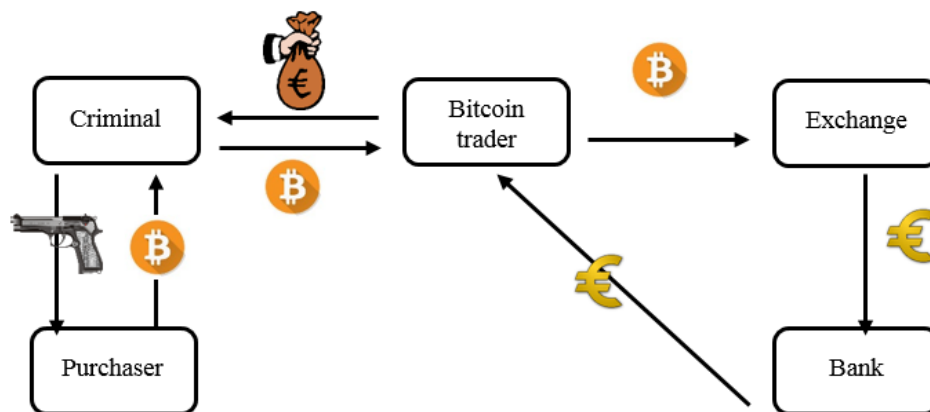
The highest minimum referred to is 30,000 Euros. The most commonly used limits for a sale lie between a minimum of 500 Euros and a maximum of 10,000 Euros, with a maximum cash purchase peak of 50,000 Euros. Date of consultation localbitcoins.com 15 August 2017.

<sup>26</sup> Criminal investigations by the money laundering teams of FIOD Haarlem and FIOD Zwolle and by the Central Netherlands Police Force.

<sup>27</sup> Criminal investigations by the money laundering teams of FIOD Haarlem and FIOD Zwolle and by the Central Netherlands Police Force. See also the press release on the website of the Dutch tax authorities, '10 arrests in international bitcoin investigation', 20 January 2016

money laundering process for criminals. It is a well-known fact and a money laundering typology that ready cash (in large amounts) is used often in criminal circles.<sup>28</sup> It is also a well-known fact and a money laundering typology that the physical transportation of large amounts of cash is associated with considerable security risks.<sup>29</sup> The trader profiles himself anonymously on the 'surface' web and the dark web. It is well-known that activities on the dark web are often of a criminal nature.<sup>30</sup>

The trader meets his clients in a public place such as a fast food restaurant where the transaction is conducted. Here there is free wifi and both parties feel safe due to the public nature of the location and the number of people present. Often the trader cannot be found under his own name on the internet, is not registered (with regard to his actual trading activities) at the Chamber of Commerce and/or is not known to the tax authorities in relation to his exchange activities. The trader actively recruits his clients on the dark web and keeps no administration (with respect to his clients). The communication to the client is often screened off using Threema<sup>31</sup> or Blackberry Messenger for example. The bitcoin trader who fits the profile set out above will generally be regarded as a criminal bitcoin trader who helps to facilitate the money laundering process of criminals.



## 5. The bitcoin mixer<sup>32</sup>

A bitcoin mixer is also a means of increasing your anonymity when using bitcoin. Here online services referred to as 'mixing services' are involved. Bitcoins are exchanged for other bitcoins against payment of a commission to the mixer.<sup>33</sup> The commission is several percent (2 to 3.5% for example) of the total amount in bitcoins.<sup>34</sup> Since bitcoin transactions are updated in a public register, the Blockchain, it is possible to trace the origin of

(consulted 1 August 2017).

<sup>28</sup> The money laundering typology is construed as follows: 'For large quantities of cash in various currencies: it is a generally known fact that various forms of criminality are associated with large amounts of cash in various currencies.' The generally known fact is construed as follows: 'The Court deems it to be a generally known fact that various forms of criminality are associated with large amounts of cash in large denominations, whereas denominations of € 500 are rare in normal payment transactions.' (Central Netherlands Court 19 March 2015, ECLI:NL:RBMNE:2015:1838). See <https://www.amlc.nl/producten/witwasindicatoren/>. Cash plays a major role in money laundering in particular, according to A. Verhage, A. Jorissen, R. Prins & J. Jaspers (eds.), *Criminele organisaties en organisatiecriminaliteit*, Apeldoorn: Maklu 2016, p. 116.

<sup>29</sup> The money laundering typology is construed as follows: 'For the physical transportation of large amounts in cash: the physical transportation of large amounts of cash brings substantial security risks.' The generally known fact is construed as follows: 'The Court deems it to be a generally known fact that the possession of large amounts of cash by private individuals is highly unusual due to the risk of among other things theft, for which the money is not insured.' (Central Netherlands Court 19 March 2015, ECLI:NL:RBMNE:2015:1838) and 'It is a generally known fact that the physical transportation of large amounts of cash brings substantial security risks.' ('s-Hertogenbosch Court 25 March 2015, ECLI:NL:GHSHE: 2015:1181). See <https://www.amlc.nl/producten/witwasindicatoren/>.

<sup>30</sup> See also D. Moore and 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* February-March 2016, issue 58, no. 1, p. 15-22.

<sup>31</sup> 'Threema – Seriously secure messaging', <https://threema.ch/> (consulted 1 August 2018).

<sup>32</sup> This paragraph describes the bitcoin mixer. There are also mixing services available for other virtual currencies. See for example <https://ethermixer.com/> (consulted 26 September 2017).

<sup>33</sup> J. Redman, 'Tumbling Bitcoins: A Guide Through the Rinse Cycle', 21 July 2016, <https://news.bitcoin.com/tumbling-bitcoins-guide-rinse-cycle/> (consulted 9 August 2017).

<sup>34</sup> R.S. van Wegberg, J.J. Oerlemans and 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, p. 9.

bitcoins. By using the mixer your transaction history (nature thereof, scale, wallets and parties involved) is made invisible and cannot be reconstructed. In order to keep the service provider and the client anonymous, mixing services often work through a Tor network. Mixing services also appear to operate mainly from jurisdictions with which there is little or no judicial cooperation.<sup>35</sup> The mixer is designed in such a way that you do not get your own bitcoins back even if you put your bitcoins through the mixer in several portions. The bitcoins you receive back after 'mixing' originate from other persons who also use the service. It can be seen from the bitcoins whether or not they have been through a mixer. The fact that bitcoin mixers are conducive to concealment with an associated risk of money laundering is also discussed by Schoonbeek, Shreki and Van der Wulp.<sup>36</sup> In my opinion mixing services – considering the foregoing – have no purpose other than to conceal the original source of the bitcoins.<sup>37</sup> Some of these mixing services, such as BitLaundry, also state as much explicitly: 'Secure Launder renders your bitcoins completely untraceable, even to the most persistent forensic investigator.'<sup>38</sup> Concealing the origin of bitcoins is extremely relevant if the origin of those bitcoins is illegal. For that reason criminals in particular will use mixing services. According to TNO (Netherlands Organization for Applied Scientific Research) researcher Rolf van Wegberg it is indeed likely that many of the bitcoins present in mixers have a criminal origin.<sup>39</sup> According to Van Wegberg situations can also arise in which there is a legitimate reason for using a mixer. However this will not happen very often.<sup>40</sup> De Jong wrote as follows about the bitcoin mixer:

'The use of a bitcoin mixer is comparable, as an indicator, to the only roof on a row of terraced houses which has no snow on it. This, together with an anonymous tip about the presence of a hemp farm, permits the police to enter the building to establish whether the (strong) suspicion is correct. There may of course be legitimate reasons for using the services of bitcoin mixers. In practice however, bitcoin mixers use trade names which do little to conceal their purpose, such as 'BitLaunder', whereby it is clear that they have a particular target group in mind.'<sup>41</sup>

## 6. Money laundering typologies

In connection with the various criminal investigations the Anti Money Laundering Centre (AMLC)<sup>42</sup> wrote the following phenomenon description: 'the bitcoin trader, a facilitating role during the cash-out of criminal gains'.<sup>43</sup> The phenomenon description is based on literature study, interviews with experts and the data and experiences from criminal investigations in which underlying criminality was confirmed. On the initiative of the AMLC a proposal was put forward on the basis of that description to the FIU (Netherlands Financial Intelligence Unit) for three money laundering typologies relating to the trade in virtual currencies, such as bitcoin, and to the mixer of virtual currencies.<sup>44</sup>

---

<sup>35</sup> B.H.M. Custers, J.J. Oerlemans and R.L.D. Pool, 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 2016, no. 2, issue 15 with references to: M. Möser, R. Böhme and D. Breuker, 'An inquiry into money laundering tools in the Bitcoin ecosystem', eCrime Researchers Summit (eCRS) September 2013, p. 1-14, (<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6805780>).

<sup>36</sup> A.B. Schoonbeek, W.M. Shreki and M.T. van der Wulp, 'Bitcoins, witwassen & integriteitsrisico's', *Tijdschrift voor Compliance* April 2017, p. 90.

<sup>37</sup> See also B.H.M. Custers, J.J. Oerlemans and R.L.D. Pool, 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 2016, no. 2, issue 15.

<sup>38</sup> <https://bitlaunder.com/launder-bitcoin> (consulted 1 August 2018).

<sup>39</sup> S. Eikelenboom and J. Dobber, 'Bitcoin is reservemunt van de onderwereld geworden', *Het Financieele Dagblad* 3 February 2017. Van Wegberg, Oerlemans and Van Deventer state as follows about the mixer in their study: 'Bitcoin mixing services are services that aim to disassociate bitcoins from their often-criminal source.' R.S. van Wegberg, J.J. Oerlemans and 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, p. 2.

<sup>40</sup> 'According to TNO researcher Van Wegberg many of the bitcoins in mixers probably do have a criminal origin. He points out however that may also be legitimate reasons for using such a mixer. "What if you are a foreign journalist in a country like Myanmar for example? There it is probably not a good idea to work publicly as a journalist and if you receive your salary from a foreign medium you will be noticed. Bitcoin offers a solution, and by using such a bitcoin mixer you can conceal the fact that your money comes from a foreign media company.'" Source: S. Eikelenboom and J. Dobber, 'Bitcoin is reservemunt van de onderwereld geworden', *Het Financieele Dagblad* 3 February 2017.

<sup>41</sup> R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *TBS&H* March 2017, no. 1, p. 5.

<sup>42</sup> The Anti Money Laundering Centre (AMLC) is the centre of knowledge and expertise in the field of money laundering which works in cooperation with public and private parties to combat money laundering at the national and international level, [www.amlc.nl](http://www.amlc.nl) (consulted 1 August 2017).

<sup>43</sup> A phenomenon description is an expert report drawn up by the AMLC (in cooperation with partners) with the aim of providing insight into a particular phenomenon and the money laundering risks associated with that phenomenon. This phenomenon description can be found at [https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/notitie\\_de\\_bitcoinhandelaar\\_amlc\\_20170825.pdf](https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/notitie_de_bitcoinhandelaar_amlc_20170825.pdf).

<sup>44</sup> See in this regard S. Eikelenboom and J. Dobber, 'OM voert strijd op tegen witwassen via bitcoin', *Het Financieele Dagblad* 3 February

The following three typologies have since been accepted and published by the FIU:<sup>45</sup>

Typologies in connection with research into the purchase and sale of virtual currencies:

1. The repeated withdrawal from one or more bank accounts of substantial amounts in cash, as a whole or in parts and within a relatively short period of time, without any apparent necessity and in combination with the repeated cashless receipt of sums of money (whereby the amounts received in the case of the trader in virtual currencies apparently originate from the sale of virtual currencies).
2. The purchase of virtual currencies whereby at least two of the following characteristics are fulfilled:
  - a. the buyer offers his services through the internet by means of supply and demand sites;
  - b. the buyer does not ascertain the identity of the seller;
  - c. the buyer screens off his own identity;
  - d. the buyer pays in cash;
  - e. the buyer charges an unusually high exchange fee percentage;
  - f. the transaction takes place in a (public) space where there are many members of the public present, thereby reducing the security risk for the buyer;
  - g. there is no plausible legal, economic explanation for the method of exchange;
  - h. the scale of the virtual currencies purchased is not plausible with respect to average private use;
  - i. the buyer is not known to the Chamber of Commerce or the tax authorities for his exchange establishment.
3. The buyer and/or seller makes use of a so-called 'mixer' during the sale of virtual currencies.

The role of money laundering typologies is to give concrete and unambiguous form to activities which have the characteristics and character traits of money laundering. For that reason they are of great importance in combating money laundering.<sup>46</sup> Money laundering typologies may also contribute to a reasonable suspicion of money laundering.<sup>47</sup> They provide points of reference when it comes to giving substance to the subjective indicator for those institutions which are under an obligation to report pursuant to the Wwft.<sup>48</sup> Finally, money laundering typologies can be used for the evidence in a criminal case.<sup>49</sup> They can be used to give substance to the component relating to the knowledge of the suspect for example.<sup>50</sup> Or to make plausible the illegal source of the objects to which the money laundering relates.<sup>51</sup> Ultimately it is up to the Court to decide on the basis of all the circumstances of the case whether it deems it to be plausible that the objects originate directly from a crime.<sup>52</sup>

## 7. Conclusion

On the one hand bitcoin provides a high degree of anonymity since the bitcoin address and the bitcoin wallet are not linked to a name. Bitcoin makes it possible to make payments and transfer funds anonymously, which means there are money laundering risks associated with the use of bitcoin. On the other hand bitcoin is transparent since all transactions can be found with the date and amount of the transaction in the public ledger (the Blockchain). Anonymity ceases at the moment when bitcoins are exchanged for Euros or some other currency. The bitcoin exchange transfers the bitcoins to a bank account number which is registered under a name. Those who regard their anonymity as essential, such as criminals, consider this lack of anonymity during the cash-out to be highly undesirable. The bitcoin trader addresses this lack of anonymity by accepting

---

2017 and also S. Eikelenboom and J. Dobber, 'Bitcoin is reservemunt van de onderwereld geworden', *Het Financieele Dagblad* 3 February 2017. The FIU has a central role in developing new money laundering typologies, see *Kamerstukken II* (Parliamentary Papers II) 1999/00, 27159, no. 3 (Explanatory Memorandum), p. 9. The FIU determines new typologies on the basis of presentation by a standing committee allied to the AMLC, see <https://www.fiu-nederland.nl/nl/witwas-typologieen-0> (consulted 1 August 2017).

<sup>45</sup> <https://www.fiu-nederland.nl/nl/witwas-typologieen-0> (consulted 12 September 2017).

<sup>46</sup> Annual Statement 2016 of FIU-Netherlands, p. 9, attached as an appendix to *Kamerstukken II* 2016/17, 29911, no. 155.

<sup>47</sup> See for example Supreme Court 13 July 2010, ECLI:NL:HR:2010:BM0787, *NJ* 2010, 456 and Noord-Nederland Court 15 April 2016, ECLI:NL:RBNHO:2016:3876.

<sup>48</sup> Annual Statement 2016 of FIU-Netherlands, p. 9, attached as an appendix to *Kamerstukken II* 2016/17, 29911, no. 155.

<sup>49</sup> Parliamentary Papers II 1999/00, 27159, no. 3, p. 9 (Explanatory Memorandum).

<sup>50</sup> For an example in case law of a money laundering indicator which according to the judges contributed to the proof of the knowledge of the accused, see Amsterdam Court 11 February 2015, ECLI:NL:RBAMS:2015:714.

<sup>51</sup> The component 'originating from a crime'. Numerous examples of the use of this component by the courts in their judgements are to be found on [www.rechtspraak.nl](http://www.rechtspraak.nl). See for example Amsterdam Court of Appeal 4 May 2016, ECLI:NL:GHAMS:2016:1887; Arnhem-Leeuwarden Court of Appeal 18 March 2014, ECLI:NL:GHARL:2014:2268 and Overijssel Court 9 June 2015, ECLI:NL:RBOVE:2015:2771.

<sup>52</sup> See also *Kamerstukken II* 2015/16, 34294, no. 6, p. 13.

bitcoins for others in exchange for cash and changing those bitcoins at a bitcoin exchange. The bitcoin trader charges a high commission for this service. Whereas a normal exchange charges about 0.3%, the bitcoin trader charges between 7% and 15% of the transaction amount. The clients of the bitcoin trader are willing to pay this high commission for the sake of anonymity when selling bitcoins (cash-out). Usually the trader does not know who his clients are. He receives large quantities of bitcoins from his clients in each transaction. The bitcoins have often been in contact with the dark web. The trader sells the bitcoins to exchange offices and exchanges while the equivalent value is paid into his bank account. The credit balance is then withdrawn in cash so that he can buy more bitcoins. The bitcoin trader with this profile may be regarded as a criminal bitcoin trader who facilitates the money laundering process of criminals. Apart from bitcoin traders, bitcoin mixers also come up in the criminal investigations. These are services which ensure that the history of the bitcoins can no longer be traced. The sole purpose of the mixer is therefore to conceal the origin of the bitcoins and in view of that purpose it is precisely criminals who will make use of these services. As a result of the research carried out into both phenomena the FIU has since come to regard both the trade in virtual currencies (such as bitcoin) and the use of the mixer of virtual currencies as a money laundering typology. Considering the observation of Europol that 40% of intra-criminal payments are made in bitcoins, it is important for the parties involved in combating money laundering to keep a close eye on such new developments. Hopefully the typologies and the research on which they are based will prove to be useful in combating money laundering by means of virtual currencies such as bitcoin.