Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin

1. Introduction

Nowadays, cryptocurrencies - like bitcoin - are commonly used in a variety of cybercrimes. Bitcoins are used in both (1) cyber enabled crime, i.e., crimes that are enabled by computers and the Internet (such as hacking and malware), and (2) cyber assisted crime, i.e., criminal behaviours in which computers and the Internet assist in committing crimes (such as drug trade on online forums) (McQuade, 2002; Burden and Palmer, 2003). In both types of cybercrime, bitcoin can be seen as an enabler of the digital criminal enterprise. The main instigators of their popularity among cybercriminals is that they are straightforward to use, relatively anonymous, and their use is unimpeded by borders or legislation (Shcherbak, 2013; Bryans, 2014). Steadily, bitcoin has proven itself to be a vital part of the criminal enterprises. For instance, ransomware victims are pressed to exchange the ransom from fiat currency to bitcoin and transfer this amount to a specific bitcoin address that is provided by the criminals. On underground markets, large amounts of goods and services - like drugs, weapons and DDoS-attacks - are bought and sold using bitcoin as method of payment. In online underground markets, bitcoins are therefore to be seen as the preferred currency of criminals (Motoyama *et al.*, 2011; Sood, Bansal and Enbody, 2013; Moore and Rid, 2016). And recently, criminals start to embrace bitcoin as a partner in their cash-out strategy and launder money aided by bitcoin (Möser, Böhme and Breuker, 2013).

Criminals need a solid cash-out strategy to launder cybercrime proceeds, in this case bitcoin, without getting connected to the associated crime (Levi, 2015). A cybercriminal seldom starts his cash-out with bitcoins. Usually, his cybercrime proceeds exist of fiat currency, such as euros or dollars. Regardless of the source, nature, and size of the cybercrime proceeds, the bitcoin ecosystem is utilized as part of the anonymisation or layering process a cash-out strategy entails. Already upon exchanging these proceeds for bitcoin, the money trail becomes obfuscated (Europol, 2015c).

On the Dark Web, services are being offered to anonymize bitcoins even further, by mixing them, or in this case: launder them. Two key components in this 'bitcoin laundering' are bitcoin mixers and bitcoin exchanges (Moore and Christin, 2013; Möser, Böhme and Breuker, 2013; Christopher, 2014; Brenig, Accorsi and Muller, 2015). Bitcoin mixing services are services that aim to disassociate bitcoins from their often-criminal source. Bitcoin exchange services are services that aim to anonymously convert bitcoins to spendable money. In this paper we focus on the use of the cryptocurrency bitcoin facilitating the cash-out and laundering of cybercrime proceeds.

Until now, there is little experimental, empirical research into the working of these bitcoins mixers, let alone explorative research into its usability for cash-out strategies. Only Möser, Böhme & Breuker (2013) tested five bitcoin mixers to analyze their technical method of operation. But how do you identify and select a reputable service? And what percentage of your crime proceeds do you 'lose' in the laundering process? To answer those and similar questions, we set up an experiment that in addtition to testing the mixers itself, illustrates a cash-out strategy using bitcoin mixers. The experiment will allow us to further determine the likeliness of integration of these potential criminal strategies in an actual criminal scheme. Doing so, we were able to analyse these cash-out strategies, as it would provide an opportunity to study how the different elements of such a strategy are

connectable and how they operate together as a (successful) cash-out strategy.

The goal of this paper is not only to test the method of operation of bitcoin mixers, but also to make a first attempt to identify the usability of these mixers in a cash-out strategy. Understanding the strengths and weaknesses in this strategy, will enable creating better evidence-based countermeasures for money laundering, ideally corrupting the underlying business models. The question we attempt to answer is: To what extent are those bitcoin mixing- and exchange services being offered on the DarkWeb reputable and cost-efficient to be used in a money laundering scheme?

The remainder of this paper is divided in five sections. Section II provides an overview of money laundering, related to bitcoin and underground markets. Section III considers bitcoins and bitcoin laundering as a part of a cybercrime cash-out strategy. The approach and methodology of the underlying experiment are outlined in section IV. The results of the experiment are presented in section V. Finally, we present our conclusion and implications thereof for both law enforcement efforts as for the policies on cryptocurrencies in section VI.

2. Money laundering, bitcoin and underground markets

Money laundering is not a new criminal phenomenon. It is a constantly changing criminal phenomenon, with updated modus operandi and evolving business models (Savona, 2014). To the criminal enterprise, a decent cash-out strategy is not easy to achieve. Crime proceeds without the means to launder these proceeds, would make the criminal business an unprofitable one, unless it is carried out purely for lifestyle expenditure. Traditionally, the laundering of crime money is facilitated by (1) money mules, (2) offshore accounts, or (3) luxuries products, i.e. art, houses, boats, or a combination of those (Levi and Reuter, 2006; Aston *et al.*, 2009; Florencio and Herley, 2010; Levi, 2015). Alternative payment methods, such as WesternUnion or Perfect Money, allegedly have a prominent place in money laundering schemes. Prepaid credit cards, gift vouchers or other easily exchangeable non-traditional value items are also often associated with the laundering of crime money.[1] Today, so called new-payment methods are becoming a more important factor in actual money laundering schemes (Europol, 2015a, 2015b, 2015c; FATF, 2015). Within the category of new-payments methods, cryptocurrencies stand out. A shift is apparent, in which criminals more frequently make use of cryptocurrencies in the cash-out of crime proceeds (FATF, 2015). Bitcoins are also a popular form of payment between criminals. Europol (2015b, p. 46) even reports that bitcoin is "accounting for over 40% of all identified criminal-to-criminal payments" in cybercrime investigations. The extent to which this can be seen as evidence that there is an influx in the use of bitcoin as the prominent 'criminal' payment method, remains to be seen.

Underground markets can be seen as a facilitator for using cryptocurrencies in current and future money laundering schemes. These underground markets are easily accessible, and are gaining popularity amongst (cyber)criminals to deploy and set-up criminal activities. Anonymous browsing has become available for the general public using the Tor-protocol (The onion router). The Tor system routes internet traffic to several Tor nodes, encrypting the network traffic in between (Dingledine, Mathewson and Syverson, 2004). Only the IP-address of the previous Tor node in a

[1] See for more typologies on money laundering <http://www.fatf-gafi.com>

chain is visible to a connecting computer. Therefore, Tor makes it possible to use the Internet without revealing the originating IP address of the computer that is used to access the Internet by a computer user.[2] In this way the so-called DarkWeb came into existence, which attracts growing amounts of criminals seeking the advantages of moving their activities to the Dark Web. Quantitative research on the DarkWeb indicates that more than fifty percent of all content on the Dark Web is illegal (Moore and Rid, 2016, p. 21).

Criminals set-up entire business models and create a whole new, online underground economy (Christin, 2013; Holt, 2013; Holt and Smirnova, 2014). An underground economy has emerged that is based on buying and selling criminal techniques and services on the Internet (Holz, Engelberth and Freiling, 2009; Motoyama *et al.*, 2011). Criminals flock to the platform, even those that scam each other. "No honour amongst thieves", as the saying goes. A review system – comparable with for instance eBay - is put in place to reduce this scamming risk (Décary-Hétu and Dupont, 2013; Holt *et al.*, 2015). This review system can be seen as the most prominent element of the reputation-mechanism in underground markets, wherein services are reviewed and flagged as verified and working, a scam or to be cautious. An example of existing, accumulated reviews can be found in the figure below (Figure 1).

FIGURE 1

Next, research indicates that these marketplaces are extensively used by criminals to buy and offer illegal goods and services (Motoyama *et al.*, 2011; Sood, Bansal and Enbody, 2013; Thomas *et al.*, 2015). Van Eeten and Bauer (2008) already indicated that a specific underground economy of cybercrime has emerged, where individuals can buy and offer services that play a certain function within a cybercrime scheme. For example, some criminals author the malicious software that other individuals can utilize to infect computer and steal personal or financial information (Eeten and Bauer, 2008; Anderson *et al.*, 2012). Many of that software is subsequently offered as a 'kit' on the Dark Web that individuals can buy or rent (Caballero *et al.*, 2011; Grier *et al.*, 2012; Sood and Enbody, 2013). Other individuals specialize in laundering the proceeds obtained through cybercrime by offering bitcoin mixing and underground exchange services (Möser, Böhme and Breuker, 2013). Europol (2015a, p. 31) predicts that "individuals with computer skills or other skill that are valuable to criminal organisations are expected to advertise their services for payment in cryptocurrencies".

The above supports the image that a majority of these marketplaces are involved with criminal activity and that the use of bitcoin - as method of payment and facilitator for money laundering – is popular among cybercriminals. Our research therefore aims to provide insight in the process of money laundering by the use of the virtual currency and their involvement in cash out strategies used by criminals. Bitcoins are chosen as the virtual currency of interest, because bitcoin is presumably the preferred cryptocurrency among cybercriminals (Möser, Böhme and Breuker, 2014; Europol, 2015b). Yet, little is known about cash-out strategies using bitcoins to launder crime proceeds that are obtained through cybercrime.

[2] However, some researchers suggest Tor users can be de-anonymised. See for instance Chakravarty and Barbera (2014). See also Larry Hardesty, 'Shoring up Tor. Researchers mount successful attacks against popular anonymity network — and show how to prevent them', 28 June 2015. <https://news.mit.edu/2015/tor-vulnerability-0729> (last visited at 18 December 2015).

3. 'Bitcoin Money Laundering'

We now shift to the characteristics of the bitcoin ecosystem, to make clear why and how bitcoin facilitates the laundering of cybercrime proceeds. Blockchain is the fundament of bitcoin. The bitcoin blockchain operates as a decentralized bank for the bitcoin cryptocurrency (Nakamoto, 2008). This means banks are no longer necessary in interpersonal transactions with bitcoins. As a result, bitcoin transactions are made between bitcoin addresses directly (Decker and Wattenhofer, 2013). In this sense, the blockchain can be seen as a publicly visible and verifiable ledger. All transactions are logged in the blockchain and can be inspected via public websites, such as *blockchain.info* and other open source websites. Anyone, anywhere, can see all bitcoin transactions from one bitcoin address to another in real time. The current balance of the amount of bitcoins in a bitcoin address is also visible in the blockchain. Despite its openness, the bitcoin system does provide a high level of anonymity. The reason for this anonymity is that bitcoin addresses are not registered to individuals, in contrast to bank accounts. Comparable with numbered Swiss banking accounts, the bitcoin address itself acts as a unique identifier and the account is only accessible by the owner who has the login details to the bitcoin wallet. Yet, no names are connected to the bitcoin address and wallet. In addition to its high degree of anonymity, bitcoin relies on the instant creating of new bitcoin addresses. This in sharp contrast to bank accounts, which take time to set-up, next to the obligatory registration of personal information to name the account. This level of anonymity explains why bitcoin has become so popular in illegal activities. The total system however – from a criminal perspective - has one 'downside'. Due to the blockchain concept, all historic information on any bitcoin address and transactional information is just one mouse-click away for law enforcement authorities (UNODC, 2014).

Figure 2 illustrates the workings of the blockchain model for bitcoin transactions.

FIGURE 2

A bitcoin transaction constitutes of several elements: it has one or more inputs, one or more outputs and holds the cryptographic protection of this information. Each input and output consists of a bitcoin address and a bitcoin amount. As bitcoin transactions are linked to each other, each input is automatically an output of a previous transaction. This way, the value of a bitcoin output can be traced back to previous transactions.

Obviously, this poses a potential risk - from a criminal perspective - as the transaction that is used to cash-out cybercrime proceeds, links back to transaction(s) that are associated with illegal activity. For instance, transactions can potentially be linked to the receipt of ransom, the selling of illegal goods or other cybercrimes. This risk is the instigator of technologies designed to break the transnational link between the bitcoin transaction and illegal activity. For that reason, bitcoin mixing services are created that aim to break the transactional link – or in this case the money trail - of bitcoins. [3] Figure 3 illustrates the working of a typical bitcoin mixer.

FIGURE 3

[3] Bitcoin mixing services are also called -laundering, -tumbling', or –cleaning services.

The typical mode of operation is that bitcoin mixing services provide customers with a newly-generated bitcoin address to make a deposit. The bitcoin mixing service pays out other bitcoins from its reserve to bitcoin addresses provided by the customer, after deducting a mixing fee. In order to provide more anonymity, the pay-outs are spread out over time and some randomness is introduced in the division of amounts and/or the mixing fee.

An operational bitcoin mixer makes it virtually impossible to trace back mixed bitcoin to their tainted source. The customer can check the taint of the received bitcoins at the blockchain, e.g. at blockchain.info. If the bitcoin mixing is performed correctly, there is no link ("zero percent taint") between the deposited bitcoins and the received bitcoins. Some bitcoin mixing services offer a service to returning customers to ensure that (earlier) deposited tainted bitcoins in their reserve are not accidently paid out to the same customer in a subsequent use of the mixing service. After each 'mix' the customer is issued a returning customer number. This number can be presented when reusing the mixing service. The mixer then knows which bitcoins in the reserve were earlier deposited and will not pay out these same bitcoins to the client. This service-model is suitable for returning customers, or, said differently: frequent launderers. In this manner a sophisticated strategy can be set-up, using bitcoin as a facilitator in laundering cybercrime proceeds. When individuals successfully use a bitcoin mixer and subsequently an underground bitcoin exchange, only mistakes will leave sparse traces to your true identity or the fruits of your crime.

In summary, we have shown that the cryptocurrency bitcoin is used in many forms of cybercrimes. We have also explained the rise in popularity of bitcoins amongst cybercriminals. A potentially toxic combination – of anonymous browsing, trading, paying and laundering - becomes apparent. To determine the extent to which bitcoin laundering is feasible and – looking at reputation-mechanisms and service-percentage – actually usable in the criminal enterprise, we set up a bitcoin laundering experiment.

4. Approach

In this section, we first lay down the approach to our experiment and used to get an overview of both the available mixing and (underground) exchange services. We outline their individual characteristics and the selection criteria for the underground services to be included in the experiment. Thereafter, we elaborate on the set-up of the actual experiment, describing our methodology step-by-step.

4.1 Set-up

To set up the underlying experiment for this paper, we needed to address three conditional methodological questions. First, how do we get an overview of both underground bitcoin mixing and exchange services and its reputation and service-percentage. Second, how do we select bitcoin mixing and exchange services for this experiment? And third and last, how do we determine the effectiveness of these services?

4.1.1 Overview of available bitcoin mixing and exchange services

In order to gain insight into the underground economy of bitcoin laundering services we made use of

the TNO Dark Web Monitor[4]. The TNO Dark Web Monitor makes use of a 'crawling' technique to collect and analyse data on the Dark Web. This system therefore provides a solid basis for both exploratory and longitudinal research, as the data is collected over a longer period of time and is independent of the hidden services that are still online. Using this technique, we have discovered over 25.000 hidden services, i.e. Dark Web-sites. By use of the TNO Dark Web Monitor we obtained a solid overview of the total supply of Dark Web services offering bitcoin mixing and exchange from bitcoin to other non-virtual currency via a diversity of anonymous output platforms. This overview enabled us to see a number of notable differences in the offered services.

First, the analysis revealed that bitcoin mixers differentiate in (1) service percentage, (2) registration and authentication process, (3) reviews and (4) time delay. The service percentage relates to the percentage the service takes for mixing bitcoins. The registration and authentication process relates to how you register for the process and whether there is any form of authentication involved. The reviews relate to how the service is reviewed by other users and the time delay regards the question how much time it takes to receive mixed bitcoins.

Second, Bitcoin exchange services also differ in (1) service percentage, (2) registration and authentication process, (3) reviews and (4) time delay. Importantly, exchange services also show a variation in output platform. In other words, they offer, for instance, PayPal or PerfectMoney, to allow a client to anonymously receive the exchanged bitcoins. Keep in mind that these payment services themselves often do not offer this type of service. Using a bitcoin mixer and subsequently an underground bitcoin exchange service, make up together a cash-out strategy for cybercriminals (see Figure 4). The aim of the cash-out strategy is to provide a spendable proceeds of the crime that cannot be traced back to its origin.

FIGURE 4

4.1.2 Selection of services

Following the first question, we addressed the second question: how do we select the services to be included in our experiment. Starting from the paper of Möser (2013) and desk research into known mixers and exchange services, we added the currently available mixers and underground exchanges and generated a list of still active services. Due to budget restraints, we settled on selecting five mixing services and five exchange services.[5] The five services were selected on the basis of the three criteria: (1) function and fee, (2) positive/negative reviews and (3) (laundering/mixing) reputation in general. [6] Note that we indeed purposively included negatively reviewed services, e.g. potential

[4] TNO DarkWeb MoniTOR is an interactive tool designed for indexing and visualizing crawled DarkWeb data. See <dws.pm>.

[5] Allowing us to use 0.5 or 1 BTC per service.

[6] In this paper we have chosen not to disclose the names nor the onion-addresses of both the bitcoin mixers and the exchange services we used. As we are aware of the fact that these services can be (easily) found, adding more context information on usability and working cash-out schemes would have turned this paper into a user manual for bitcoin laundering, which is not our intention. Please do not hesitate however to contact us if you do have a scientific interest in the data used in this paper.

scams, into our sample.[7] The selected mixing services can be categorized as follows (see Table 1).

TABLE 1

By use of this sample, we belief we have selected these services that best reflect the total population of services on the Dark Web. The sample covers a variation in reviews, namely from scams to verified services. In addition, this sample provides a differentiation in the charged fee, namely from nearly no fee up to more 'expensive' services.

For the underground exchange services however, no such well-documented and reviewed overview of services was present. Therefore, we selected the underground exchanges that we came across in our search for bitcoin mixing services and underlying desk research.

Now that we have answered the first of two conditional questions, we can create the following model depicting the process of the experiment. [8]

FIGURE 5

4.1.3 Testing the effectiveness of the services

Third and finally, we had to decide how to determine the effectiveness of the tested services. For the mixing services we stick with the 'product description' or 'product promise' of many of these services: no taint. In that case, no taint refers to the taint a transaction has between bitcoin addresses in the blockchain. As the blockchain is easily accessible and a taint analysis is just one mouse-click away, we assume that this is a solid identifier for success and is also used or usable by cybercriminals who want to assess the service on its operational excellence. The first indicator for 'success' is the actual transferring of the bitcoins. Being scammed would count as unsuccessful. The underground exchange services are only effective when the bitcoins are (1) exchanged to fiat currency and (2) anonymously transferred to the output platform specified. In that case both the used service as the used output platform (such as WesternUnion and PayPal) needs to be assessed. Again, success counts here as not being scammed.

4.2 Experiment

We operated the experiment on one day, to minimize both the loss of value in bitcoin due to fluctuating currency exchange rates and moreover to test the speed and user-friendliness of the total cash-out strategy. First, we bought the necessary bitcoin via the Dutch payment service iDeal and started the experiment with these bitcoins stored in Wallet X on one bitcoin address. Hence, this can be seen as our 'control' address – where all the bitcoins used in the experiment originate from. After this first step, all the following steps are undertaken via the Tor-network to guarantee the most anonymous process. Second, we set-up a Lelantos email-account – which is a form of Tor-mail - for possible future communication with certain services. Third, we created Wallet Y, wherein we generate one or more new, clean bitcoin address per mixing service depending on the variety of services offered by the mixer. Fourth, we used all of the five selected mixing services one by one.

[7] The third criteria of 'reputation in general' was determined by the analysis of open sources about bitcoin laundering services.

[8] As we did not have the opportunity of actually starting our money laundering scheme with real crime proceeds – neither in bitcoin nor euros/dollars – we opted to use the research budget to acquire the bitcoins to use in this experiment via a reputable bitcoin exchange – using the Dutch Payment service iDeal.

Nearly all following the procedure of a) transferring bitcoin to a new – by the mixer provided – bitcoin address from our Wallet X and b) requesting the mixed coins to be transferred to one or multiple bitcoin addresses in our Wallet Y. Fifth, after we confirmed the actual transferring of the (mixed) coins, we 8nalysed the taint of the incoming transaction by cross-checking the traceability to our 'control address'. Sixth, we consecutively used the five exchange services. Following a procedure comparable to the mixing services of a) transferring bitcoin to a new – by the exchange service provided – bitcoin address from our Wallet Y b) selecting the output platform and c) providing details for this platform.

All these steps we could fit in the time-span of one day. The actual cash-out however takes 1 to 3 days, depending upon the output platform used. However, we were able to 'consume' one output platform right away. Therefore we used, without registering an account, the Dutch online food ordering service Thuisbezorgd.nl to order Sushi and paid – of course – with mixed bitcoins. A few days later, we were able to assess the success of the other exchange services and thereby the entire cash-out. We cashed out our mixed bitcoins using the following five service platforms: (1) PayPal, (2) PerfectMoney, (3) WesternUnion, (4) Bitonic, (5) and Thuisbezorgd.nl.

5. (Mixed) Results

We present the results of the experiment in two ways. First, we show the results in terms of bitcoin transferring by use of bitcoin mixing services. Second, we show the results of our exchange services. Based on these results, we describe our overarching conclusions based on the experiment and the overall cash-out strategy.

5.1 Mixing services

In this section we show the results of our bitcoins transfers using five bitcoin mixing services.

In Table 2 we have plotted the results of the experiment for these five specific mixing services.

TABLE 2

Noticeably, we fell for a scam three out of five times. Resulting in an immediate loss of 2.5 BTC. In all of these three cases the bitcoins were successfully transferred from our 'control address' to the bitcoin address the mixing services provided. Yet, we have not received any of the bitcoins we provided to the addresses belonging to the Mixers 1, 2 and 3.

Next, we used the Numisight blockchain explorer[9] to see what further information we could extract on all the mixing services and what happened to the bitcoins that went 'missing'. We discovered that the deposit address for Mixer 1 had already been used in a transaction three days before our experiment. Reuse of bitcoin addresses should be considered a deadly sin in the world of bitcoin mixing, as it provides correlations that could be used in forensic analysis.[10] Bear in mind that exactly these types of correlations are the main reason of using a bitcoin mixer to begin with. In curious contrast to this sole purpose, this mixer (willingly) made a mistake thereby annulling our efforts to prevent just these types of correlations. The same deposit address of Mixer 1 was used three more

[9] <http://numisight.com>

[10] See the report by UNODC (2014) for an overview of forensic techniques used in bitcoin money laundering investigations.

times during the next two weeks. We discovered a similar pattern of bitcoin address reuse by Mixer 2. When looking more closely into the outputs of Mixer 1 and Mixer 2, we discovered that they were combined in a transaction 12 days after our experiment. All of this strongly suggests that Mixer 1 and Mixer 2 are closely collaborating, and that they are very likely to be the same entity. This result, that Mixer 1 and Mixer 2 are closely collaborating and made use of the same bitcoin address at one point, is visualised in Figure 6.

FIGURE 6

To have a complete picture, we performed the same analysis for Mixers 3, 4 and 5. Mixers 3 and 4 each used their deposit address exactly once. Mixer 5 required the payment of an entry fee at the bitcoin address that was also used as deposit address, but there was no other bitcoin address reuse.

Another relevant result of the experiment regards to the question how long a deposit remains unspent. This is an indication for how much time worth of reserve a bitcoin mixer has. Or in other words, how large the reserve of a bitcoin mixer is in terms of the amount of bitcoins available for future mixing. When having a large reserve, a bitcoin mixer is not forced to reuse its deposits quickly as output in another 'mix'. For Mixers 1, 2 and 3, the wait time was four days (just after the weekend, as we operated the experiment on a Friday). For Mixer 4, the wait time was 17 hours. For Mixer 5, the wait time was 3 hours.

Furthermore, two out of the five tested services, i.e., all of the successful mixing attempts, operated conform to their own description. We received the same amount of bitcoins that we transferred to the service minus the percentage for the use of this service. Of both of these services, no taint is observable between the bitcoins we received from the mixers on the addresses we specified and our bitcoin 'control address'.[11] This means that there is – in retrospect – no way of linking these two addresses to each other, i.e., the money trail is obfuscated and in all probability impossible to follow. So despite the fact that we actually transferred bitcoins – via a mixer – from Wallet X to Wallet Y no trail can be found that reconstructs that we did precisely that.

5.2 Exchange services

In this section, we show the results of the use of five exchange services we used to cash-out our mixed bitcoins.

In contrary to the mixing services, exchanges services are based on both a service and an output platform. The service refers to the supplier that offers to receive bitcoin and will exchange this to a currency of your choosing. An output platform, such as PayPal of WesternUnion, is used to make sure this exchanged currency ends up in your possession.[12] In Table 3 we have plotted the results of the experiment for these five individual services and the platform used by this service.

TABLE 3

[11] Using the blockchain.info web based 'taint analysis' comparing the receiving bitcoin addresses in our Wallet Y with our 'control address' in Wallet X.

[12] Note that the platforms used, i.e. PayPal, are not offering these types of services themselves and should be seen as (relative) innocent bystander. However, it is known that WesternUnion is a prominent element in money laundering typologies, as might be expected form its domination of the legitimate financial transfer market globally, see FATF (2010).

At first glance, it is clear that all but one of the exchange services tested was operational and successful in its promise to exchange our mixed coins for currency or food. Only the service-platform combination that makes use of PerfectMoney did not came through. This could be due to the fact that the service is a scam or that the platform itself – PerfectMoney - has blocked the transaction.[13] Next, we used PayPal and Western Union as a cash-out strategy. The platform that facilitated this transaction charged a high percentage for the transfer. In exchange, we expected a better anonymization of this part of the cash-out strategy. This turned out to be the case. In order to use PayPal as a cash-out strategy we needed to provide a valid and active PayPal account, which can be bought online on underground markets or generated without leaving anything more than an (Tor) e-mail address. As promised, we received the exchanged funds on the PayPal account we provided. The service-platform combination that used WesternUnion asked us to provide a name and place for the collection of the funds. After we provided this information, we could pick-up the exchanged funds at a WesternUnion office of our choosing without leaving a signature. When comparing both cash-out strategies, it is important to note that the method via PayPal does not include a physical hand-over of the exchanged funds, where this is the case with the WesterUnion method. This is why we rated the PayPal service-platform combination slightly more anonymous than its WesterUnion alternative.

From a 'criminal perspective', we did make a vital mistake in our cash-out. Whereas there was no link between our "tainted" bitcoins and "laundered" bitcoins at the day of the experiment, we cleaned up the experiment and retrieved the invested bitcoins four days later. In this clean-up, remaining "tainted" bitcoins and "laundered" bitcoins were sent to our bitcoin address at a regular bitcoin exchange. This 'mistake' linked our identity directly back to the "tainted" bitcoins, negating all our previous efforts to stay anonymous. Of course, this step was intentional – as the experiment was completed and remaining bitcoins were to be collected – it does show how easily it is to make a mistake and render the attempted launderer vulnerable.

5.3 Overarching results

In this section, we discuss the overarching results of our experiment. Our first conclusion is that bitcoin laundering services offered on the dark web are partly scams and partly operational services. Reviews are of the utmost importance to reduce the chance of being scammed. The trustworthiness of this review system is solidified in our experiment, because the services that were flagged 'orange' or 'red', indicating to be cautious or be alarmed not to use these services, actually corresponded with our three mixing service scams.[14] In addition, the two operational mixing services were ranked 'green' in reviews. This means that if you read and use reviews of these specific services carefully, the risk of getting scammed is minimized. It would be wise for criminals to use these review systems,

[13] We described earlier our use of an exchange to buy the bitcoins used in this experiment. This regular exchange we also used to exchange our mixed coins back to euros. This specific service required us fill out a form wherein we had to specify a bank account to which the funds upon exchange should be transferred to. This in turn logically lowered the level of anonymity, as a bank account of course leaves a trace to an actual person or company. But on the other hand this service did not charge us with a high commission for the use of this exchange service.

[14] Figure 1 shows an example of accumulated reviews on a single platform, in this case for gambling services. We have chosen not to show the actual accumulated reviews of the services we used - to demonstrate the importance and accuracy of reviews - as this would neglect all previous efforts not do disclose the actual names of the tested services.

since it helps them to keep costs of scams low. The attractiveness of the examined type of case-out strategy is clear, since these services work as advertised and were straightforward to use in an anonymous manner (since no taint was present in the blockchain).

The exchange services show us a different pattern. All exchange services operated as they promised, except one. However, the level of anonymity differs a lot from service to service and from platform to platform. The exchange Bitonic[15] connects the mixed coins directly to a bank account, as this is required to use a regular bitcoin exchange. Of course, it is not obligated and it would not be wise to provide your own bank account for an exchange. A name and bank account number provides an interesting lead for law enforcement authorities. Using output platforms which are often integrated in other cash-out and more physically oriented laundering strategies, like PayPal and WesternUnion, build on an already established reputation in that area. The examined exchange services allow their clients to receive money in any shape and form with minimal registration requirement that may lead back to the identity of individuals.

Finally, it is important to point out that mistakes are made easily in the examined cash-out strategy. For instance, (1) not using the Tor browser, (2) using the same bitcoin address for different purposes or (3) providing an email address are detrimental to an anonymous transaction, are possible mistakes. This is however no different from other cash-out strategies, where mistakes also leave (extra) traces for law enforcement authorities.

In our view, the most significant difference compared to other money laundering strategies is the total percentage that covers the costs of this particular cash-out strategy. In many other cases these percentages add up to nearly 50 percent. In this case, looking at the maximum costs of all services and adjusting for potential value drops regarding exchange rates, we can safely estimate the total percentage of costs will not exceed 15 percent in this specific cash-out strategy. Again, we thereby assess that the strategy itself pre-includes trial-and-error and users reviews to find and use operational mixing and exchange services. Therefore, we do not contemplate the risk of getting scammed in our experiment as one to be very cost-increasing in these strategies as the full scale operation of the strategy will be build on positively-reviewed operational services. Therefore, we conclude that 15 percent is a good estimate of the total cost of this type of cash-out strategy based on the underlying experiment.

Keep in mind however, that intermediary cash out services may block transactions that exceed a certain threshold, for instance 5,000 or 10,000 dollars. Therefore, it is not certain this cash-out method works when larger amounts of money are laundered. Yet, potentially, the low commission of 15 percent for laundering services may make it interesting for cybercriminals to use bitcoins, mixing services and exchanges for money laundering purposes. As a result, this would significantly change the profitability of money laundering models that are now often used by criminals. In conclusion, these operational bitcoin laundering services provide a hassle-free and mostly anonymized exchange of mixed coins in an easy and consumer-friendly manner.

6. Discussion

Bitcoin has reportedly established itself as ‘a single common currency for cybercriminals within the

[15] <http://www.bitonic.nl>

EU'. The virtual currency potentially provides the means to launder the obtained proceeds without the strict requirements of (international) financial institutions. This paper aimed to examine in which ways cybercrime proceeds that are obtained in the form of bitcoin or converted to bitcoin can be laundered. Following up on previous studies, we focused in particular on money laundering services – both mixing as exchanging - offered for bitcoin on the Dark Web.

In order to examine bitcoin laundering, we used bitcoin mixing services and exchange services and integrated these services in a working cash-out strategy. We examined the usability of these services in a cash-out strategy by analysing the service-percentages and reputation-mechanisms. This aided us in determining the likeliness of integration of these bitcoin laundering services in an actual criminal scheme. We believe that in our experiment we have shown that laundering cybercrime proceeds using bitcoin is a user-friendly and working criminal service-model. However, it is not clear whether the model will work when larger amounts of money are laundered. Yet, for smaller amounts it clearly offers an easy to use and good value-for-money service, as long as criminals keep an eye out for scams.

We conclude that bitcoin money laundering is a practically conceivable concept and has a high degree of likeness to be integrated in current-day and future money laundering schemes. Recent cases and Europol reports support the conclusion that bitcoins are used for money laundering by cybercriminals. Most notably, the ability to lower the cost of laundering, whilst providing more anonymity, make it an interesting money laundering technique for criminals.

This brings us to the following questions. First, the question arises what does this mean for the profitability of criminal business models. Obviously, we have a limited overview of criminals actually using this very method. However, from this small-scale experiment, we do know that at least in theory the cost of money laundering can be lowered using bitcoin. That could make certain criminal business models potentially more profitable, which is of course attractive for the cybercriminal enterprise.

Second, the question arises how law enforcement should deal with this new money laundering technique. The start- and endpoint of bitcoin money laundering (often) includes the exchange in currencies. Law enforcement authorities may be able to gather evidence at these exchanges. Therein lies the possibility of intervening as current police measures provide sufficient means to do so, but future research is necessary to study this possibility to its full extent. In addition, law enforcement authorities may be able to seize and analyse bitcoin wallets of identified criminals to identify bitcoin addresses in order to trace back bitcoin transfers.

Finally, the question remains on how bitcoin should be treated from a legal perspective. Generally speaking, we can see that bitcoin is in a sort of twilight zone. In many states, bitcoins are not banned, nor regulated. Because governments do not recognize bitcoin as a currency, anti-money rules and regulations – such as 'know your customer' (KYC) rules and the reporting of suspicious transactions – do not apply apply for companies and institutions trading in bitcoin. Ironically, mainstream bitcoin exchanges, are lobbying to become regulated.[16] When bitcoin will move out of the twilight zone and will end up regulated, we cannot foresee. Current imagery of bitcoin as a

[16] <http://www.cnbc.com/2015/09/18/bitcoin-now-classed-as-a-commodity-in-the-us.html>; <http://www.cnbc.com/2015/02/25/bitcoin-futures-market-just-changed-the-game-commentary.html>

criminal currency might lead to regulation of bitcoin exchange services. However, that will not stop criminals in using bitcoin exchange services that are located in jurisdictions that have no or less strict regulations. The degree to which banning or regulating will have any effect on the facilitating role currently plays in the criminal enterprise, has yet to be determined.

7. Future work

We identify three research questions that can be used for future research. These are as follows:

How widespread is the use of using bitcoin in a cash-out strategy?
We extensively reported on the precise workings of bitcoin mixers and exchange services in a cash-out strategy for cybercrime proceeds. Concluding that the laundering of these proceeds can be facilitated by the use of bitcoin and underground laundering services. Consecutively we concluded that this provides a challenge for law enforcement, as the money trail becomes highly obfuscated. However, we do not know how widespread this specific cash-out strategy is, and how big of a challenge law enforcement is actually facing. Future research efforts could or should therefore also focus on the size, nature and impact of these strategies.

Which criminal business models (would) actually use this cash-out method?
Another step forward, follows-up on the question which criminal business models use this cash-out method. Next to size, nature and impact, research efforts should focus on further advancing the groundwork of 'bitcoin money laundering' and seek to identify criminal business models that could be using this cash-out method.

What are the weak links in the strategy? Or in other terms, where to intervene?
The next step is to study how the results of the experiment in this paper, can be used to create evidence-based intervention strategies for this type of cash-out strategies. We know that certain elements of the tested cash-out strategy are less anonymous, technically feasible to monitor or have the potential to be regulated. Following the previous section, not only criminological or technical, but also legal research into 'exploiting' the weak links in the tested cash-out strategy, will enable creating better countermeasures, including rules and regulations, to combat the underlying business models.

Acknowledgement

The authors are thankful to Willem Pino for his contribution to the Numisight analysis on the included bitcoin mixers in the experiment. Likewise, we would like to thank Michel van Eeten, Bram Klievink and Thijmen Verburgh for their valuable input on earlier versions of this paper.

References

Anderson, R., Barton, C., Boehme, R., Clayton, R., Eeten, M. van, Levi, M., Moore, T. and Savage, S. (2012) 'Measuring the cost of cybercrime', in *Workshop on the Economics of Information Security*.

Aston, M., McCombie, S., Reardon, B. and Watters, P. (2009) 'A Preliminary Profiling of Internet Money Mules: An Australian Perspective', in *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*.

Brenig, C., Accorsi, R. and Muller, G. (2015) 'Economic Analysis of Cryptocurrency Backed', *ECIS 2015 Proceedings*, (Ecb 2012), pp. 1–18.

Bryans, D. (2014) 'Bitcoin and money laundering: Mining for an effective solution', *Indiana Law Journal*, 89, pp. 441–472.

Burden, K. and Palmer, C. (2003) 'Internet crime: Cyber crime - A new breed of criminal?', *Computer Law and Security Report*, pp. 222–227. doi: 10.1016/S0267-3649(03)00306-6.

Caballero, J., Grier, C., Kreibich, C. and Paxson, V. (2011) 'Measuring Pay-per-Install: The Commoditization of Malware Distribution', in *Usenix Security Symposium*.

Chakravarty, S. and Barbera, M. (2014) 'On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records', in *PAM*. doi: 10.1007/978-3-319-04918-2.

Christin, N. (2013) 'Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace', in *World Wide Web*, pp. 213–224.

Christopher, C. M. (2014) 'Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering', *Lewis & Clark Law Review*, 18(1), pp. 1–36. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312787.

Décary-Hétu, D. and Dupont, B. (2013) 'Reputation in a dark network of online criminals', *Global Crime*, 14(2–3), pp. 175–196. doi: 10.1080/17440572.2013.801015.

Decker, C. and Wattenhofer, R. (2013) 'Information propagation in the Bitcoin network', *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*, pp. 1–10. doi: 10.1109/P2P.2013.6688704.

Dingledine, R., Mathewson, N. and Syverson, P. (2004) 'Tor: The second-generation onion router', *SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium*, 13, p. 21. doi: 10.1.1.4.6896.

Eeten, M. van and Bauer, J. (2008) *Economics of malware: Security decisions, incentives and externalities*. Report. OECD Science, Technology and Industry Working Papers.

Europol (2015a) *Exploring Tomorrow's Organised Crime*. Available at: https://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web-final.pdf.

Europol (2015b) *The Internet Organised Crime Threat Assessment*. Available at: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf.

Europol (2015c) *Why Cash is Still King?* Available at: https://www.europol.europa.eu/sites/default/files/publications/europolcik.pdf.

FATF (2010) *Money Laundering Using New Payment Methods*. Available at: http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf.

FATF (2015) *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. Available at: http://fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Florencio, D. and Herley, C. (2010) 'Phishing and Money Mules', in *International Workshop on Information Forensics and Security (WIFS)*.

Grier, C., Ballard, L., Caballero, J., Chachra, N., Dietrich, C. J., Levchenko, K., Mavrommatis, P., McCoy, D., Nappa, A., Pitsillidis, A., Provos, N., Rafique, M. Z., Rajab, M. A., Rossow, C., Thomas, K., Paxson, V., Savage, S. and Voelker, G. M. (2012) 'Manufacturing Compromise: The Emergence of Exploit-as-a-Service', in *ACM Conference on Computer Communications Security*.

Holt, T. J. (2013) 'Exploring the social organisation and structure of stolen data markets', *Global Crime*, 14(2–3), pp. 155–174. doi: 10.1080/17440572.2013.787925.

Holt, T. J. and Smirnova, O. (2014) *Examining the Structure, Organization, and Processes of the International Market for Stolen Data*. Report. US Department of Justice.

Holt, T. J., Smirnova, O., Chua, Y. T. and Copes, H. (2015) 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime*, 16(2), pp. 81–103. doi: 10.1080/17440572.2015.1013211.

Holz, T., Engelberth, M. and Freiling, F. (2009) 'Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones', in *Computer Security–ESORICS*.

Levi, M. (2015) 'Money for Crime and Money from Crime: Financing Crime and Laundering Crime Proceeds', *European Journal on Criminal Policy and Research*, 21(2), pp. 275–297.

Levi, M. and Reuter, P. (2006) 'Money laundering', *Crime and justice*, 34(1), pp. 289–375. doi: 10.1086/501508.

McQuade, S. (2002) *Encyclopedia of Cybercrime*, *Symploke*. doi: 10.1353/sym.2002.0018.

Moore, D. and Rid, T. (2016) 'Cryptopolitik and the Darknet', *Survival*. Routledge, 58(1), pp. 7–38. doi: 10.1080/00396338.2016.1142085.

Moore, T. and Christin, N. (2013) 'Beware the middleman: Empirical analysis of Bitcoin-exchange risk', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7859 LNCS, pp. 25–33. doi: 10.1007/978-3-642-39884-1_3.

Möser, M., Böhme, R. and Breuker, D. (2013) 'An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem', in *Procedings of the 2013 e-Crime Researches Summit*, pp. 1–14. doi: 10.1109/eCRS.2013.6805780.

Möser, M., Böhme, R. and Breuker, D. (2014) 'Towards Risk Scoring of Bitcoin Transactions', *First Workshop on Bitcoin*. doi: DOI: 10.1007/978-3-662-44774-1 2.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. and Voelker, G. M. (2011) 'An Analysis of Underground Forums', *ICM*.

Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', *Consulted*, pp. 1–9. doi: 10.1007/s10838-008-9062-0.

Savona, E. (2014) 'Organised crime numbers', *Global Crime*, 15(1–2), pp. 1–9. doi: 10.1080/17440572.2014.886512.

Shcherbak, S. (2013) 'How Should bitcoin be regulated?', *European Journal of Legal Studies*, 7(1), pp. 45–91. Available at: http://cadmus.eui.eu/bitstream/handle/1814/32273/183UK.pdf?sequence=1.

Sood, A. K., Bansal, R. and Enbody, R. J. (2013) 'Cybercrime: Dissecting the State of Underground Enterprise', *IEEE INTERNET COMPUTING*. Edited by I. C. Society.

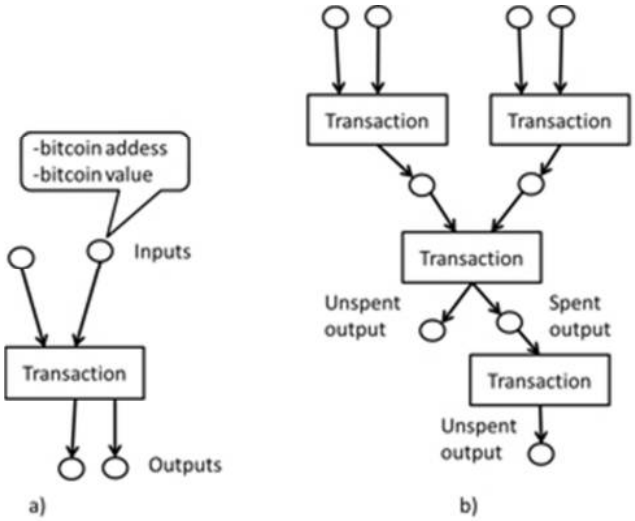
Sood, A. K. and Enbody, R. J. (2013) 'Crimeware-as-a-service—A survey of commoditized crimeware in the underground market', *INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION*, 6, pp. 28–38.

Thomas, K., Huang, D. Y., Wang, D., Burszstein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S. and Vigna, G. (2015) 'Framing Dependencies Introduced by Underground Commoditization', in *Workshop on the Economics of Information Security (WEIS)*.

UNODC (2014) *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*.

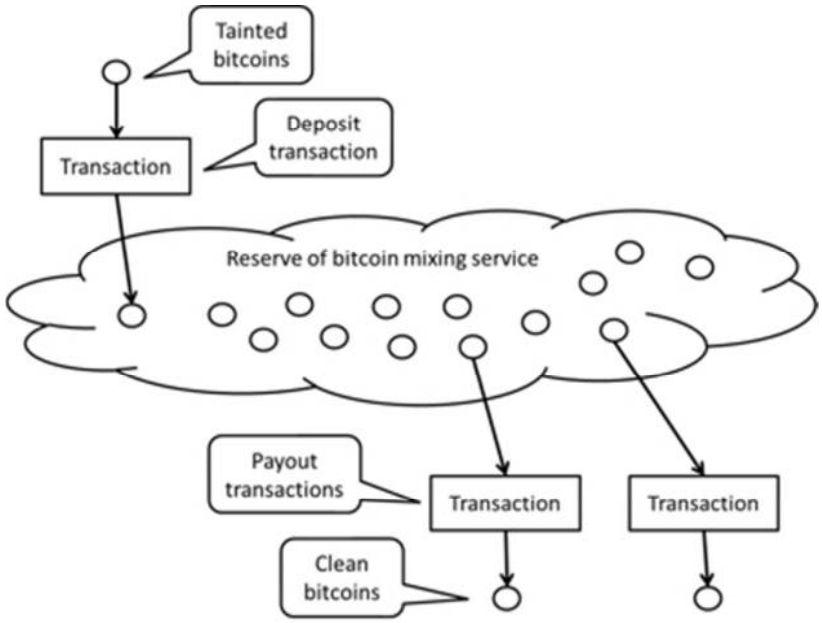
Example of reviews with accompanying labels

275x55mm (72 x 72 DPI)



a) Bitcoin transactions has inputs and outputs b) Bitcoin transactions are linked to each other

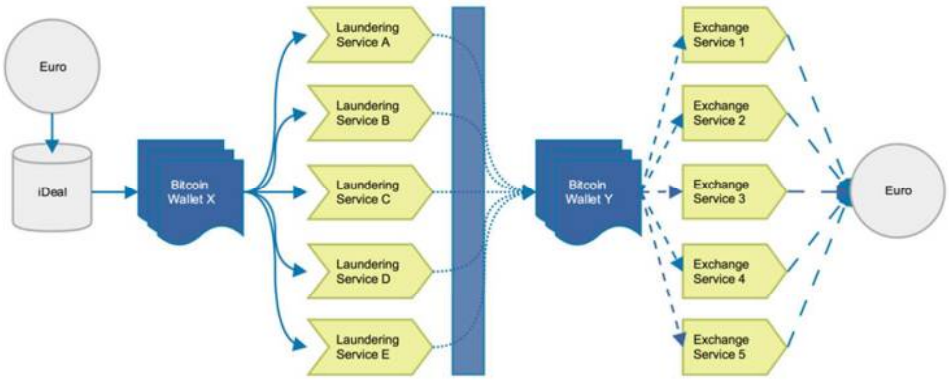
111x93mm (72 x 72 DPI)



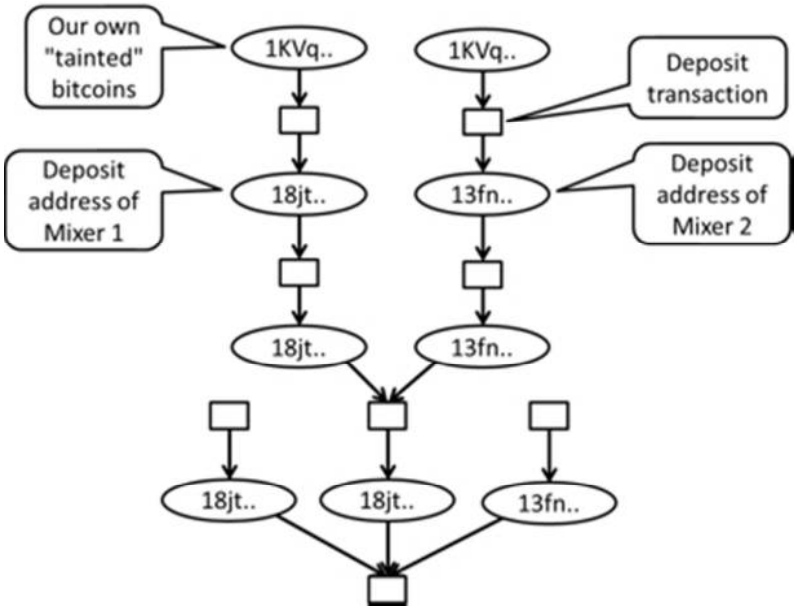
Bitcoin mixing service, deposit tainted bitcoin and receive clean ones

143x108mm (72 x 72 DPI)

Mixing- and underground exchange services form the cash-out strategy



Model of the process of the experiment



An illustration of how the blockchain analysis strongly suggests that Mixer 1 and Mixer 2 are controlled by the same entity

138x106mm (72 x 72 DPI)

Mixer	Review	Advertised fee
Mixer 1	-	0.5 – 3.5 %
Mixer 2	CAUTION	2 %
Mixer 3	SCAM	0.1 %
Mixer 4	VERIFIED	1 – 3 %
Mixer 5	VERIFIED	1 – 2.5 %

Overview of included mixing services in the experiment

Mixing Service	BTC IN	BTC OUT	Percentage	Blockchain-taint
Mixer 1	1.0	0	-	-
Mixer 2	1.0	0	-	-
Mixer 3	0.5	0	-	-
Mixer 4	0.5	0.4931291	-1.37%	0%
Mixer 5	0.5	0.497509	-0.5%	0%

Output and taint of mixing services

Exchange Service[a]	BTC IN	OUT[b]	Percentage	Anonymous?
1/PayPal	0.233933	$ 52.42	-6 %	+
2/PerfectMoney	0.1	0	-6.9%	?
3/WesternUnion	1.220364	$ 197	-10% + $50	+/-
4/Bitonic	0.33740872	$ 71	-0.25%	-
5/Thuisbezorgd.nl	0.109509	€ 23,50	-	+/-

[a] Notwithstanding the fact that we choose not to name the used mixing services by name, a solid overview of the results would be impossible without naming the output platforms as they have very distinct procedures and regulations that make the analysis more in-depth and understandable.

[b] Based on currency rates on 29 to 31 May 2015.

Overview of output and anonymity of the selected exchange services

165x228mm (72 x 72 DPI)