

2017 Virtual Currencies Money Laundering Typologies

Targeting Exchanges and other CyberGatekeepers



Unit O50
AP Sustrans, FIG
The Hague, 31/12/2017

Table of Contents

LIST OF ABBREVIATIONS	3
I – INTRODUCTION	4
II – CONVERTIBILITY.....	4
III – CURRENT LEGISLATION	5
IV –OPPORTUNITIES VS VULNERABILITIES	5
V –DETECTED TYPOLOGIES.....	6
VI – CONCLUSION	12

LIST OF ABBREVIATIONS

ATM	Automated Teller Machine
AMLD	Anti-Money Laundering Directive
BTC	Bitcoin
BTM	Bitcoin Teller Machine
CDD	Customer Due Diligence
EU	European Union
EUR	Euro
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ID	Identity Document
IP	Internet Protocol
LEA	Law Enforcement Agency
KYC	Know-Your-Customer
ML	Money Laundering
MSB	Money Service Businesses
OCG	Organised Criminal Group
STR	Suspicious Transaction Report
TF	Terrorism Financing
VC	Virtual Currency

I – Introduction

The daily transaction volume of virtual currencies, more precisely bitcoins, already exceeds that of major Money Service Businesses (MSBs) like PayPal and Western Union¹. Despite bitcoins popular use as a means of payment, from a legal perspective, they are not defined as currency, electronic money or payment instruments. The regulatory framework does not classify virtual currencies in any category of traditional fiat currency or legal tender, making them an unregulated payment instrument with manifold opportunities for exploitation for money laundering purposes. Due to the certain degree of anonymity they allow, the lack of a legal obligation to conduct Customer Due Diligence (CDD), to monitor and identify suspicious transactions as well as due to their global reach – from the users perspective but also from the suppliers point of view – they represent a powerful tool for criminals to convert, move and store illicit funds, out of the reach of law enforcement agencies (LEAs).

II – Convertibility

Virtual currencies can be convertible or non-convertible. Convertible virtual currencies can be exchanged for fiat currency and vice versa, whereas non-convertible virtual currencies can only be used in the closed environment for which they were designed and cannot be exchanged for fiat currency. A good example of non-convertible currencies are video game credits which can only be used within the respective game.

Alongside other possibilities, the easiest way to obtain virtual currencies, such as bitcoins, is to use online exchanges. According to the definition of the EU Commission², “virtual currency exchange platforms can be considered as 'electronic' currency exchange offices that trade virtual currencies for fiat currencies. Virtual currency wallet providers hold virtual currency accounts on behalf of their customers. In the 'virtual currency' world, they are the equivalent of a bank offering a current account on which fiat currencies can be deposited. They store virtual currencies and allow for their transfers to other wallets/virtual currency accounts”. There are hundreds of available online exchanges such as:



¹ The daily transaction volume of bitcoins exceeded 240 million EUR during February 2017

² Communication from the Commission to the European Parliament and the Council on an action plan for strengthening the fight against terrorist financing COM(2016) 50

They act as brokers between the virtual and the real world and offer a way in which one can buy or sell virtual currencies for a variable fee. A virtual currencies exchange works like any other currency exchange: Customers can convert a fiat currency into a virtual one or the other way around. An increasing number of exchanges also allows for users to perform exchanges between the different types of virtual currencies.

Virtual currencies exchanges are not regulated in a harmonized way in the EU and since they constitute the intersection between unregulated virtual currencies and the regulated fiat currency financial system, they represent a potential strategic point for intervention by law enforcement authorities in order to mitigate the risk of money laundering.

III – Current legislation

The EU decided that regulatory efforts should especially focus on virtual currencies exchanges:

*"Transactions with virtual currencies benefit from a higher degree of anonymity than classical financial fund transfers and therefore entail a risk that virtual currency may be used by terrorist organisations to conceal financial transfers. There is no reporting mechanism equivalent to that found in the mainstream banking system to identify suspicious activity. Possible further risks relate to the irreversibility of transactions, means of dealing with fraudulent operations, the opaque and technologically complex nature of the industry, and the lack of regulatory safeguards"*³.

Currently virtual currencies are not regulated at EU level. However this does not imply that they are unregulated in all Member States as national legislation may exist. As such, the European Commission put forth a proposal to amend the current 4th Anti-Money Laundering Directive (AMLD) with specific provisions dedicated to the prevention of the misuse of virtual currencies for money laundering and terrorism financing (TF) purposes. In July 2016 the Commission proposed to include virtual currency exchange platforms and custodian wallet providers⁴ as obliged entities under the AMLD.

It is thus expected that in the near future virtual currencies exchanges and virtual currencies "wallet providers" will have to apply Customer Due Diligence (CDD) when conducting their activities. They will also be obliged to implement preventive measures, to monitor and to report suspicious transactions to their FIU.

IV – Opportunities vs Vulnerabilities

From a law enforcement perspective, virtual currencies exchanges are a substantial source of information on individual clients - typically storing name, contact details including verified email and phone number, IP logs, activity logs comprising all transactions on the exchange as well as deposits and withdrawals, all bitcoin and other cryptocurrency addresses used by the client, personal messages, payment information, proofs of ID, sometimes complemented by a self-generated image of a person holding the ID and proofs of home address. Europol maintains an updated list of contact points from all major virtual currencies exchanges and provides these contacts to Member States upon request. Most exchanges cooperate with law

³ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, 2016/0208 (COD), 05.07.2016, European Commission, p. 10

⁴ A *wallet provider* is an entity that provides means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency (FATF Report on Virtual Currencies).

enforcement authorities and respond to their enquiries either directly to a request coming from LE email address or upon presentation of a court order.

Even though the clear majority of virtual currencies exchanges already requires identification and conducts CDD, there are still a few that aligned their services towards the needs of criminal clients by enabling the purchase and sell of virtual currencies without requiring a proper form of identification or verifying the provided identities.

Additionally, criminals using legitimate exchanges opt to apply various techniques to circumvent pre-set verification processes and also take advantage of the payment methods offered by exchanges.

Fake identity documents are available online and via Darknet markets enabling criminals to stay anonymous.

Some exchanges have already upgraded their CDD requirements and are now putting in place Skype verification calls or require customers to produce self-generated images holding their ID and papers with a random text written on it. However criminals will almost certainly find new ways to bypass the current verification processes.

Virtual currencies exchanges offer different payment methods to buy or sell virtual currencies, predominately bank transfers and credit or debit card payments. Some also offer the use of Money Service Businesses (such as Western Union and MoneyGram), PayPal, bank cheques and even cash (i.e. cash deposits, cash in mail).

Money laundering vulnerabilities associated with the use of cash are commonly known. The use of cash is widely recommended by criminals discussing in online forums as a simple means of avoiding tracing or detection. Suspects can engage in bitcoin to cash transactions either with their associates or with third parties they encounter on localbitcoins.com or on various bitcoin events, such as regular bitcoin meetups in larger cities.

Another simple way to stay anonymous is the use of prepaid credit and debit cards which can be bought in supermarkets, stores or online.

At 247exchange.com and Cex.io customers can buy bitcoins with a prepaid credit and debit cards instantly without the need to supply any proper form of identification.

V –Detected Typologies

A number of investigations carried out in 2017 demonstrate how virtual currencies are used to conduct money laundering operations, most of them, via the abuse of virtual currency exchanges and at times with their complicity.

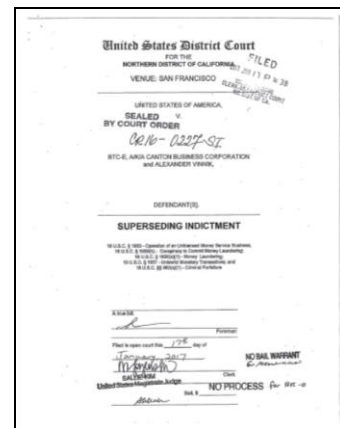


Operation AVARICIOUS

A virtual currencies exchange complicit with money laundering activities.

Following an investigation led by US authorities a Russian national operating one of the largest virtual currency exchanges in the world⁵ BTC-e was arrested in Greece in July 2017.

According to the publicly available indictment⁶ against BTC-e the operator *"BTC-e was an exchange for cybercriminals worldwide, and one of the principal entities used to launder and liquidate criminal proceeds from digital currencies, including Bitcoin, to fiat currencies, including U.S. dollars, Euros, and Rubles. [...] BTC-e facilitated crimes, including computer hacking, ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. BTC-e lacked basic anti-money laundering controls and policies [such as Know-Your-Customer] and, as such, was attractive to those who desired to conceal criminal proceeds."*



The modus operandi was described as follows: To use BTC-e a customer created an account by accessing the respective website. Usually virtual exchanges require identity information such as name, date of birth and address including identity verification. Once a user places funds into his account, he can conduct transactions with other users; exchange virtual currencies into fiat currency and vice versa or simply use the exchanger to store virtual currencies.

Unlike the majority of virtual currency exchanges *"BTC-e's business model obscured and anonymized transactions and source of funds."* BTC-e though allowed opening accounts anonymously as they did not require providing basic identity information, but only a username, password and an email address.

Reportedly, *"BTC-e users could not fund an account by directly transferring money [from their bank accounts] to [a bank account of BTC-e] itself, but rather had to wire funds to [bank accounts of] one of BTC-e's shells or affiliate entities."* It was also possible to send and/ or receive fiat currencies and virtual currencies from other users. Users of BTC-e could not furthermore withdraw funds from their accounts directly, but instead *"were required to make deposits or withdrawals through the use of third-party 'exchanges', thus enabling BTC-e to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail."*

Thus BTC-e was *"extensively used for illegal purposes"* and *"functioned as the exchanger of choice [...] for the criminal world."*

⁵<https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware>

⁶ <https://www.justice.gov/usao-ndca/press-release/file/984661/download>

According to FinCen "users openly and explicitly discussed criminal activity on BTC-e's user chat. BTC-e's customer service representatives offered advice on how to process and access money obtained from illegal drug sales on darknet markets like Silk Road, Hansa Market, and AlphaBay."



Another recent investigation shows that criminals/ criminal groups nowadays make use of money mules to exploit different virtual currency exchange services to convert i.e. "dirty" bitcoins into fiat currency.

Operation ARGENTI

The use of money mules, bank accounts and virtual currencies exchanges for money laundering activities.

The following modus operandi was detected in the framework of a cybercrime investigation:

Stage 1: Opening of verified accounts at bitcoin exchanges.

In order to convert bitcoins directly deriving from illegal activities such as ransomware and fraud into fiat currency (such as euro currency) the criminal organisation opens an account with an exchanger using money mules as frontman with false identity documents for verification.

Stage 2: Opening of bank accounts by money mules.

At the same time money mules from Baltic States, working for the criminal organisation, opened several bank accounts in a third country (i.e. in Spain) with false foreign identity documents. All the documentation associated with the opening of these bank accounts is then delivered to the criminal organisation and the money mules simply return to their country of origin.

Stage 3: Transfer of the "dirty" bitcoins from bitcoin addresses to exchanges.

The criminal organisation then using tumblers/mixers transfers the bitcoins from the bitcoin addresses directly linked to the criminal activities to the verified account opened at the exchanger with false identity documents.

Stage 4: Transfer of bitcoins from the exchanger to the local bank accounts opened by money mules.

At this stage since the criminal money was already separated from its original source, criminals simply request a transaction from the exchange to the local bank account that was opened by the money mules. Then criminals can manage the money at their own convenience (i.e. cashing out or purchasing goods and services), as they have all of the documentation necessary to do so (online credentials, debit and credit cards). Usually these bank accounts are used for short periods of time and their balance typically does not exceed EUR 30,000.



Money mules are increasingly making use of Bitcoin ATMs (also referred to as “BTMs”) to launder illegally obtained money⁷. Whereas previously banking transfers or remittance services such as Western Union or MoneyGram were used, criminals now instruct their mules to withdraw money from compromised bank accounts and to use it to buy bitcoins via a BTM.

BTMs allow the insertion of cash in exchange for bitcoins that are provided as a paper receipt (a paper wallet) or transferred to a Bitcoin address. Two different types of bitcoin ATM enable users either only to buy or to buy and sell bitcoins, mostly in exchange for cash as they are not set up to process debit or credit card transactions. BTMs allow for quick purchases as the buyer receives bitcoins to his address almost instantly. Currently there are 1.560 bitcoin ATMs in 58 countries worldwide run by 265 operators⁸.

Operation GLUTONS

The use of Bitcoin ATMs to launder criminal money.

According to information provided by Spanish Guardia Civil, bitcoin ATMs operated by a particular company were being frequently used by a group of individuals with extensive criminal backgrounds in drugs trafficking to convert criminal cash into virtual currency.

To avoid any identification procedures the criminal depositors would apply smurfing techniques to split the funds to batches of under EUR 1.000. On the same day they would make multiple deposits in several bitcoin ATM machines in different locations, at a rate of approximately 200.000 EUR per month and with a total of 3 million EUR already detected.

The majority of the funds deposited were in EUR 500 banknotes. Such a considerable discard of EUR 500 banknotes might be explained by the decision of the European Central Bank⁹ to discontinue the production of this banknote by the end of 2018 due to Europol’s proposal¹⁰,

⁷ <https://krebsonsecurity.com/2016/09/money-mule-gangs-turn-to-bitcoin-atms/>

⁸ www.coinatmradar.com

⁹ <https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html>

¹⁰ <https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering>

because of its known association with criminal activities. It is therefore likely that more concerned criminals are now interested in getting rid of their EUR 500 banknotes without making use of the banking system.

Strong suspicions exist that the company managing these Bitcoin ATMs is complicit with the on-going money laundering activities (no CDD is being performed or STRs are being submitted).



In addition to using the traditional virtual currency exchanges the possibility also exists to trade bitcoins "Face-to-Face". Online it's possible to find private vendors that wish to sell bitcoins for a small fee. Several sites on the Internet offer to match individuals willing to buy or sell bitcoins in person. LocalBitcoins.com is the most famous of such market places. Some sellers prefer cash as payment while others may allow various forms of payment such as online payment service, bank or MSB transfers, etc.

Operation TULIPAN BLANCA

The use of LocalBitcoins for money laundering purposes.

According to information provided by Spanish Guardia Civil, it was found that a money laundering OCG traditionally dedicated to place and layer criminal funds derived from the trafficking of cocaine from Spain to Colombia via the use of bank account smurfing techniques had updated its modus operandi and was now using LocalBitcoins.com to carry out its international transfers.

After picking up considerable amounts of criminal cash from drug traffickers in Europe the OCG continues to use its smurfing techniques to split and deposit funds into a large number of bank accounts under their control. After several transfers to other bank accounts funds are ultimately used for the purchase of bitcoins from private vendors located in different EU countries, via the use of the LocalBitcoins platform.

In order to move the value of the recently obtained bitcoins to Colombia the OCG uses two simple alternatives:

Option 1: On the same day (to prevent price fluctuations) the exact amount of purchased bitcoins in the EU is resold by the OCG – again using the services of Local.Bitcoins.com – but this time to private buyers in Colombia that pay with bank transfers directly into Colombian bank accounts, in Colombian pesos.

Option 2: On the same day the LocalBitcoin wallet where the purchased bitcoins are stored and the necessary information to access and use the wallet, is delivered to the cocaine trafficking

OCG in Colombia that can then use the value stored in that wallet in Colombia or anywhere in the world, as they wish.

Example of Localbitcoins sellers accepting cash

Seller	Distance	Location	Price/BTC	Limits
	6.4 km	Madrid, Spain	210.29 EUR	10000 - 10000 EUR
	6.4 km	Madrid, Spain	206.28 EUR	20000 - 180000 EUR
	6.5 km	Madrid, Madrid, Spain	197.05 EUR	400 - 9000 EUR
	6.5 km	Madrid, Madrid, Spain	201.07 EUR	4500 - 25000 EUR
	6.5 km	Madrid, Madrid, Spain	207.11 EUR	50 - 10000 EUR

Seller	Payment method	Price / BTC	Limits
thom2639 (6, 100%)	Paypal	3,884.02 EUR	0 - 305 EUR
Induba (100+, 100%)	SEPA (EU) bank transfer	4,119.10 EUR	100 - 994 EUR
bitcoin (100+, 100%)	SEPA (EU) bank transfer	4,129.32 EUR	50 - 2,865 EUR
mlindro (1000+, 100%)	SEPA (EU) bank transfer	4,149.04 EUR	200 - 1,000 EUR

Finally it is also important to bear in mind that virtual currency exchanges do not only serve the purpose of converting virtual into fiat currency and vice versa, but they can also be used for the conversion of a virtual currency into another, including the more recent and with enhanced anonymity virtual currencies.

New cryptocurrencies such as monero, zcash, dash or pivx allow anonymous transactions. monero and zcash provide private transactions keeping amounts, balances, source and destination addresses anonymous and thus making it hardly possible to trace back transactions or identify their real owner. dash and pivx simply mix transactions involving multiple sources into a single transaction.



Operation WANNACRY

The use of exchanges to convert bitcoins into untraceable moneros.

Since March 2017 two global cyber-attacks have affected more than 300.000 computers in over 150 countries. The so-called "WannaCry" 1.0 and 2.0 ransomware took control of computers, encrypted their contents and demanded that victims pay a ransom between USD 300 to USD 500 in bitcoins to regain control of their computers and decrypt their files.

In September 2017 Neutrino S.r.l. a cyberlab dedicated to the research of innovative solutions in the security sector, revealed that a percentage of the bitcoins that had been paid as ransom was exchanged by criminals into moneros, an alternative cryptocurrency "well-known for its wide adoption on darknet markets". Monero is virtually impossible to trace complicating the task of identifying the true identity of their users/owners.

The criminals used two different exchanges, Shapeshift and Changelly. ShapeShift started blacklisting Wannacry addresses after the first exchanges¹¹.

¹¹ <http://www.neutrino.nu/single-post/2017/09/01/WannaShift-to-Monero>

VI – Conclusions

There has been a considerable increase in the use of virtual currencies to perform money laundering activities. No longer an exclusive tool for cybercriminals, EU traditional drug trafficking OCGs and major Colombian drug trafficking cartels have now acquired the necessary technical expertise and confidence levels to use virtual currencies as an instrument of their criminal finances.

As already foreseen by Europol in 2014¹², due to their global availability, ease of access, reliable and irreversible transactions, low cost, high international transfer speed and especially because of their potential to obfuscate the true identity of their owners – virtual currencies are an ideal tool for money laundering.

It is expected that over the next year the number of cases involving virtual currencies for money laundering purposes will increase exponentially.

In light of these developments, there is an urgent need to add virtual currencies exchanges to the list of obliged entities as part of the 5th AMLD¹³. As obliged entities they will have to request, obtain and process personal data from all potential clients to conduct their CDD similar to financial institutions. They will become obliged to implement preventive measures (monitor transactions) and to report suspicious transactions to FIUs.

Nonetheless the inclusion of these new obliged entities will not entirely address the issues of difficult traceability and in some cases enhanced anonymity¹⁴ associated with the usage of virtual currencies.

Bitcoin ATMs, bitcoin loaded debit cards, crypto-gambling websites and “Face-to-Face” facilitators such as the website LocalBitcoins.com (a venue for private “Face-to-Face” transactions, often with the use of cash) are emerging as money laundering facilitators.

Monitoring and understanding the use of virtual currencies will continue to be of the utmost importance to detect its usage for money laundering and TF purposes. It is therefore necessary that all EU money laundering and TF investigative units provide training, promote expertise and practical knowledge to their financial investigators on the tools and investigative techniques needed to understand, identify and monitor the use of new payment systems, including virtual currencies.

This growing threat demonstrates also the pan-European need of supplementary financial intelligence in general and for virtual currencies in particular. Such collection should permit to detect, prevent and investigate red flag indicators, leads and high value targets, making sure all pieces of financial intelligence in the EU could be timely available to those in need on the fight against money laundering and TF. Thus to mirror such threat in its changing nature and level of gravity the launch of new international public/private partnerships/initiatives under the umbrella of Europol should be strongly considered.

In addition, financial institutions should vigilantly monitor all of the bank accounts held by virtual currency exchanges, bitcoin ATMs companies, companies that provide bitcoin loaded

¹² “Bitcoin Exchanges, innovations in tackling the problem of digital currency and money laundering” Europol, AP SUSTRANS 17/02/2014

¹³ On the 15/12/2017 the European Parliament and the Council reached a political agreement on the Commission's proposal of July 2016 for the 5th AMLD. Publication is now expected to follow and then the transposition period for the National Legislations http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=610991.

¹⁴ Via the use of mixers or cryptocurrencies as Monero and Dash.

debit cards and crypto-gambling websites as well as “Face-to-Face” facilitator Internet websites such as LocalBitcoins.com. Upon the detection of any suspicious activity STRs should be rapidly submitted to their local FIU.