CHARLES UNIVERSITY

Cryptocurrencies: Threats and Investigative Opportunities for Law Enforcement

31st July, 2018

2280960G
13899875

Presented in partial fulfilment of the requirement for the Degree of MSc International Security, Intelligence and Strategic Studies (SECINTEL)

Word Count: 22,050
Supervisor UofG: Dr. Eamonn Butler
Supervisor Charles Uni: Dr. Vítek Stritecky

Abstract

Cryptocurrencies have developed and widely spread within recent years. Their anonymous and decentralised characteristics have attracted criminals who leverage these technologies to sell and purchase illicit goods on the black market while concealing their identities and avoid prosecution. The new development of cryptocurrencies and their underlying architecture blockchain has had positive and negative effects on the success of law enforcement investigations. It is perceived as a threat when there are factors that increase the complexity of law enforcement investigations due to the use of highly anonymous cryptocurrencies and Bitcoin mixers. Cryptocurrencies are also perceived as a threat when criminals use them for money laundering purposes. Conversely, the rise of cryptocurrencies also introduces new opportunities for law enforcement investigations. Records of cryptocurrency transactions in the blockchain help law enforcement to trace suspicious addresses by the emergence and improvement of analysis tools. In parallel, anti-money laundering (AML) regulations and the financial authorities have proved to play a key role in fighting against money laundering and gather information on suspicious activities carried out through financial institutions. The analysis of this dissertation sets forth that cooperated efforts between regulatory entities, financial authorities and law enforcement agencies significantly enhance law enforcement capacities to fight against crime, cybercrime and money laundering related to cryptocurrencies.

Table of Contents

List of Abbreviations

5AMLD	5th Anti-Money Laundering Directive
AML	Anti-Money Laundering
BSA	Bank Secrecy Act
BTC	Bitcoin
CEO	Chief Executive Officer
CTF	Counter Terrorist Financing
CTR	Currency Transaction Report
D.C.	District of Columbia
DDoS	Distributed Denial of Service
EU	European Union
FATF	Financial Action Task Force
Ff	and following
FBI	Federal Bureau of Investigations
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
GB	Gigabyte
ID	Identification
IRS	Internal Revenue Service
KYC	Know Your Customer
MSB	Money Services Business
n.d.	no date
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TNO	The Netherlands Organisation for Applied Scientific Research
UNODC	United Nations Office on Drugs and Crime
US / USA	United States of America
USD	US-Dollar
VCPPS	Virtual Currency Payments and Product Services

Cryptocurrencies: Threats and Investigative Opportunities for Law Enforcement

I. Introduction

I.1. Bitcoin and the Global Security Agenda

Bitcoin[1] (BTC) is a peer-to-peer electronic currency that was developed in 2009 after the publication of the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" authored by the pseudonymous "Satoshi Nakamoto". In this white paper, the author outlined and detailed the principles of an electronic cash system which allows its users to anonymously and securely transfer virtual coins without the involvement of any third party financial institution (Nakamoto, 2008). One of the most particular facets of this system is its decentralisation, which is possible due to the underlying architecture of Bitcoin, the blockchain register. Blockchain is a public ledger where all transactions of Bitcoin are recorded and archived, using a complex code of letters and numbers – referred to as Bitcoin addresses – instead of direct identification information of the user. Soon after the launch of Bitcoin, other cryptocurrencies emerged, such as Ethereum, Dash, Zcash, Litecoin and Monero. As of July 2018, there were 1629 types of individual cryptocurrencies in circulation.

Cryptocurrencies do not have any legal tender status in any jurisdiction and therefore are not considered as fiat currencies. Initially, Bitcoin was valued less than one US penny. However, the number of investors and miners of these virtual coins has increased and Bitcoin is now the leading cryptocurrency in the world with a total market capitalisation of 109,699,391,589 USD (as of July 10, 2018). In 2017, Bitcoin experienced an exponential rise of its value in the market; on January 1 Bitcoin was worth roughly 1,000 USD and by December of the same year, it nearly reached

[1] This document uses the recommended nomenclature in Bitcoin Wiki: 'Bitcoin' written in singular form with upper case letter 'B' is used to label the protocol, software, and community, and 'bitcoin/s' with a lower case 'b' is used to label units of the currency (https://en.bitcoin.it/wiki/).

20,000 USD (see Figure 1 in the Appendix). This sharp growth attracted the interest of many people who saw investment opportunities and purchased bitcoins, promoting it to an object of speculation rather than a currency which could also be used to purchase goods and services online. As early as 2014, it was estimated that 70% of bitcoins were held in dormant accounts (Weber, 2014).

Nevertheless, this virtual coin has also been valued for its intrinsic characteristics of anonymity and decentralisation. Ever since its launch, Bitcoin has increasingly been leveraged by criminals to commit cyber-enabled crime and cybercrime. A recent study published in January 2018 investigated the scope of illegal activity financed by cryptocurrencies by analysing all transactions in blockchain from its foundation until mid-2017 (Foley et al, 2018). Through three different approaches to identify illicit transactions as well as its user base, the study estimated that 25 percent of Bitcoin users and nearly 50 percent of the transactions in Bitcoin are associated with illegal activities. In absolute numbers, in 2017 alone there were 24 million Bitcoin market participants using the cryptocurrency for illegal purposes, all conducting around 36 million transactions with a total value of 72 billion USD. According to another study a significant proportion of the illegal activity involving Bitcoin is likely to be associated with the illicit trade and trafficking of drugs through various online black markets. The study explores the sales between 2011 and 2015 and concludes that 90% of the revenue is produced by sales of narcotics across 16 anonymous marketplaces (Soska and Christin, 2015). The US White House Office of National Drug Control Policy estimated in 2010 that proceeds coming from illicit drug sales are approximately 100 billion USD per year. In the European market, Europol[2] together with the European Monitoring Centre for Drugs and Drug Addiction (2016) estimated this figure to amount to at least 24 billion Euros per year.

Bitcoin is by far the cryptocurrency that has developed and spread more widely within recent history, gaining a diversity of customers which seek increased anonymity in their purchases and transaction activity, speculators who try to make profits by leveraging the rise of value in Bitcoin, and criminals harnessing the digital currency and Darknet technologies to receive and send payments for illicit products and services (Brown, 2016). To put this data into context, some

[2] **Europol** is the European Union's law enforcement agency, giving support to the 28 EU Member States to fight against terrorism, cybercrime and other forms of crime.

experts and researchers consider cryptocurrencies and its blockchain technologies as disruptive to the international political economy which can be utilised as tools to empower and enable criminal activity – whether it is laundering of funds, transactions of illegal or illicit products or facilitating ransomware through cybercrimes- with much more ease. Other groups, including a small and growing community of law enforcement researchers see the use of cryptocurrencies and blockchain as an investigation opportunity due to its transparency as a public ledger where transactions are recorded and archived. In particular, it has proved to be an outlet for law enforcement agencies to trace and investigate suspicious transactions and ultimately unveil the identity of suspects through new de-anonymising techniques.

When Bitcoin emerged, criminals constituted a significant portion of the early users in the belief that it was a fully secure, untraceable coin that would keep their transactions anonymous. Nowadays, Bitcoin is known for being only partially anonymous because of the necessary components of online Bitcoin wallets and due to policies such as the Know Your Customer (KYC) and Anti-Money Laundering (AML) laws. Far from being an untraceable coin, many tools of analysis – some for law enforcement and others open to public use – are now available. Significant effort to curb illegal activity has signified a 180-degree turn in Bitcoin security and now could become a major risk for criminals, since all their transactions are forever recorded in the blockchain.

In harmony with the surge in popularity of other cryptocurrencies, some alternative coins offer much more anonymity than Bitcoin, which is attracting more criminals to using highly anonymous altcoins. In addition, the emergence of “bitcoin laundering services” as a response to the lower level of anonymity offered by Bitcoin, is significantly increasing the complexity of law enforcement investigations in efforts to trace criminal accounts and fraudulent transactions. The race between law enforcement forensic tools and new regulations against the emergence of new technologies that criminals can leverage on has led to a divergence of opinions toward the role that law enforcement has to safeguard and monitor the use of cryptocurrencies: some experts perceive cryptocurrencies as a threat because it enables crime with much more ease and anonymity while other groups see blockchain as an opportunity for law enforcement due to the fact that all transactions are forever recorded in a ledger which is publicly available, enabling a market for more advanced forensic tools and an opportunity for increased regulation.

The research presented in this thesis will examine to what extent the use and regulation of cryptocurrencies impact law enforcement agencies. By examining the impact of its utility as a positive opportunity or negative threat for law enforcement it can contribute to further the literature on this controversial matter.

I.2. Research Question

Considering the opportunities presented for law enforcement agencies through Bitcoin monitoring, there are two prevailing justifications**.** This dissertation aims to analyse the research question of whether cryptocurrencies are a threat or an investigative opportunity for law enforcement. It is perceived as a threat when there are factors that complicate law enforcement investigations due to the difficulty in tracing the criminals that use enhanced anonymisation techniques such as Bitcoin mixers or other altcoins which grant increased anonymity measures to users by omitting or disabling public ledger information to be accessed through transactions. Cryptocurrencies are also perceived as a threat that enables crime and criminals to go unnoticed and succeed in laundering their bitcoins through fiat exchanges. Conversely, blockchain is perceived as an investigative opportunity and tool for law enforcement when there is an ability to trace and track suspicious addresses, as is the case with AML regulations which require to money services businesses enhanced application of KYC and Due Diligence policies. These regulations have the potential to be effective tools for the identification of individuals involved in certain transactions, as well as for the detection of money laundering.

I.3. Methodology

The following thesis employs a methodology of mixed-methods, and presents a holistic, qualitative and analytical review of the opportunities and threats presented for law enforcement agencies regarding cryptocurrencies. In doing so, a literature review sets the basis for a theoretical framework on how the research question has been addressed in previous literature. Although the novelty and modernity of the topic presents a limited selection of resources and published literature, there is notable research and scholarship in the sector, especially considering proposed regulations outlined in official documents from cybercrime units of the US government and the European Commission, for example.

The research presented in the thesis cites notable cases that highlight the opportunities and threats presented for law enforcement agencies with the increased and widespread use of cryptocurrencies. Cases are set forth as a proof of the arguments mentioned and to clarify how different entities are interrelated.

I.4. General Thesis Structure

This dissertation comprises six chapters. After having introduced in Chapter I the relevance of Bitcoin and cryptocurrencies in the global security agenda, and having outlined the research question as well as the methodology, the structure of the work is as follows: Chapter II presents the state of the art of Bitcoin and blockchain technologies, and gives an overview of the businesses involved in the cryptocurrency market. Chapter III and chapter IV describe the main regulatory and financial actors involved and cite case studies on how the increased utility of cryptocurrencies are an opportunity and a threat for law enforcement agencies. Chapter V is an analysis of the preceding sections, providing a thorough analysis that examines the impact to which cryptocurrencies have on the facility of illegal activity and law enforcement agencies who are tasked with patrolling its use. The last chapter concludes with a summary of the main results.

II. Cryptocurrencies and Blockchain: State of the Art

II.1. Bitcoin and blockchain: an overview

This section presents a brief definition on Bitcoin and its underlying blockchain architecture. The purpose of this description is to familiarise and state the basic functioning of these technologies as well as present other related concepts that are crucial in understanding the relevance that each feature has in the "Bitcoin ecosystem". These terms are highlighted in bold, and will be repeatedly referenced throughout the study. Conversely, other related but non-essential, supportive concepts will be outlined in the footnotes.

Bitcoin is a peer-to-peer electronic cash system founded on the principle of public key cryptography and decentralsation (Nakamoto, 2008). It is the first implementation of a concept known as cryptographic currency and the first specification of the so-called "Bitcoin Protocol" which was published in 2009 under the alias of Satoshi Nakamoto. Bitcoin possesses a number of unique characteristics that are widely examined in existing literature that can be summarised in the following: 1) pseudonymity, 2) decentralisation, 3) non-legal tender.

II.1.1. Pseudonymity

Bitcoin offers a certain degree of anonymity to its users. Like conventional currencies, bitcoins (and other cryptocurrencies) can be used to purchase goods and services electronically. Users transact and exchange goods and services for money and are able to conceal their identities through a provided pseudonymous code, consisting of a "hash" or a series of letters and numbers commonly known as a 'public key' or 'Bitcoin address'. The information is recorded in a public ledger called 'blockchain' and can be used to trace, track and identify the change of hands of bitcoins and cryptocurrencies in a given network. While Bitcoin itself does not require identification and can be transferred anonymously among users, many transaction enablers, platforms and Bitcoin storage services require proper identification and documentation prior to use.

II.1.2. Decentralisation

Blockchain is the architecture behind Bitcoin. A blockchain is a distributed database where all transactions are recorded in 'blocks' and is therefore growing continuously. The only public information shared through a transaction within the blockchain is the Bitcoin addresses of the transacting users. Each user can generate a different address for each transaction, making it more difficult for each singular transaction to be traced back to them. Conversely, it is easier to follow the transactions of a user that uses the same address for multiple transactions. The visible information in the blockchain includes the Bitcoin address, the date and time of the transaction, whether it was sent or received, the amount of Bitcoin, and important information regarding origin, or mining of that particular Bitcoin. Furthermore, every type of cryptocurrency has its own specific blockchain, considered as a unique register for transactions in that particular cryptocurrency.

II.1.3. Non-legal Tender (financial sovereignty)

Currently, neither Bitcoin nor the numerous other cryptocurrencies do not have legal tender status. This means that there is no public-sector government or financial institution that sponsors cryptocurrencies or recognises it as an official, national currency. Sovereignty in its use does not belong to the State, but rather to each owner of Bitcoin, enabling its decentralised network. Essentially, when a public key is generated a private key is paired. This private key is required every time a transaction is made to confirm the transaction. If the private key is lost, the bitcoins associated with the paired address will no longer be recoverable. It is, therefore, the responsibility of the owner to keep the private key secure and secret, since anyone in possession of the private key would be able to sign a transaction and effectively use the bitcoins. For this reason, there are marketed services that offer secure cryptocurrency 'wallets' that store private keys and can retain them in a relatively protected manner. Wallets are commonly a free software that store the private key on a hard drive or private server (rather than storing Bitcoin and/or other cryptocurrencies through personal means), and have usually enhanced security measures of cryptography to avoid being hacked or accessed (Narayanan et al 2016). The original software wallet of Bitcoin is "Bitcoin Core protocol" which can be downloaded for free but requires additional memory from the operating system since it requires the downloading of the whole public ledger (which is currently around 145 GB). Other versions of wallets are cloud-based, which are much lighter in terms of memory resources but offer much less security and are prone to cyberattack due to their hosting on the public domain internet. In addition, hardware wallets are small devices that offer

high degree of security since they are generally offline but require a significant deal of personal security measures and cannot be guaranteed by a wallet provider or service.

II.2. Flows of Bitcoin and Other Cryptocurrencies

Bitcoins can be acquired in several different ways. The most common way to enter the Bitcoin ecosystem is by purchasing them in **fiat exchange services**, which are companies that offer trading services of Bitcoin (and sometimes Ethereum, another leading cryptocurrency) with government backed currencies such as Euros and Dollars. Bitcoins can also be self-generated by a mining process which requires high-powered computing technology which generates, or "uncovers" Bitcoin through the construction of complex algorithms or code. [3] Alternatively, once apart of the ecosystem, Bitcoin can be traded from other cryptocurrencies in **cryptocurrency to cryptocurrency (crypto-to-crypto) exchange services** which are companies that allow the exchange of a wider range of cryptocurrencies among its users. bitcoins can also be earned by selling products or services in the Clearnet (in which Paypal currently accepts) and in the black market sites on the Darknet (Shen, 2018). In addition, bitcoins can be earned in online gambling sites in which users buy credits with conventional currencies and can "cash out" their earnings in cryptocurrencies.

For the purpose of this study, the term **'cryptocurrency exchange service'** and **'virtual currency exchange'** will make a generic reference to both kinds of exchanges, and the aforementioned terms '**fiat exchange service**' and '**crypto-to-crypto exchange service**' will be used when a distinction is applied.

II.3. Legitimacy in the Intended Use of Bitcoin and other Cryptocurrencies

Bitcoin and other cryptocurrencies are an alternative to conventional bank payments and transfers which can potentially offer more anonymity, faster transactions and cheaper fees without directly involving a major financial institution or service provider. These are the main incentives (leaving aside Bitcoin as a speculation asset) that legitimise the intentions in the use of Bitcoin and other

[3] A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system (FATF Virtual Currencies. Key Definitions).

cryptocurrencies. Notably, activists concerned about their privacy use the same channels of anonymity as criminals, contributing to the debate that cryptocurrencies should not be criminalised or seen as something purely negative due to the potential externalities offered to its user base.

Embedded in the initial Bitcoin design was the intention of providing citizens of the international political economy with a mean of payment that is i) anonymous ii) enables the execution of rapid value transfers at minimal costs and iii) a currency that is outside the scope of control or manipulation by governments, central banks or financial institutions. In the original white paper outlining Bitcoin and blockchain, Nakamoto identifies the problem of the costs entailed for transactions among the sender and the receiver by mediating third parties such as financial institutions. While both these parties have an important role in maintaining the trust of both parties, it limits the transaction size to a certain minimum and maximum amount and incurs fees and transaction costs. The author compares the privacy measures offered by a bank and the ones offered by blockchain, whereas the traditional model relies on an entity which owns the money and the identity information of the person, and transactions are made directly through this private entity (keeping everything away from the "public"). Contradictorily, the new privacy model initiates the transactions publicly (as can be referenced in https://www.blockchain.com) by using a Bitcoin address, instead of the real identity of the person. This reduces the number of actors needed to complete a transaction, sidelining third parties while maintaining a degree of anonymity and facilitating a direct transaction between the involved parties. If anyone visits the website and public ledger, they can see individual transactions but cannot recover specific identification information that directly identify the sender nor receiver.

The entity or group behind the alias "Nakamoto" purposely created an anonymous electronic currency in the era where digitalisation and interconnectivity have endangered public privacy. When purchasing on the Internet is no longer anonymous, Bitcoin is the offered solution. Having said, Bitcoin is seen as a modern manifestation of the cyberpunk culture from the 1990s. In March 1993, the American mathematician and computer programmer Eric Hughes released a "cyberpunk manifesto" which included the following testament:

"*Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.*

(...) We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do."

As of today, this concern for public privacy in front of a "watching system" still remains. The ownership and sharing rights of personal data has been a hot topic of debate, especially in the wake of the revelations of US intelligence contractor Edward Snowden about the government-sponsored PRISM surveillance program which directly challenges and nullifies the fourth amendment of the US constitution (Lee, 2013a), and more recently following a data breach of Facebook by Cambridge Analytica in which information and disinformation was used to manipulate and influence the 2016 presidential election (Cadwalladr and Graham-Harrison, 2018).

Legitimate Bitcoin and more generally, cryptocurrency users, are in the market of new platforms to carry out financial transactions in a secure manner that better protects their personal data from financial institutions and tax regimes of public governments. In addition to this, the cheaper fees incurred through the use of cryptocurrencies (in comparison to bank transfers) are notable considering the transaction speed, which are the main traits that encourage its use.

II.4. Illicit Uses of Bitcoin and Other Cryptocurrencies

While it is extremely difficult to estimate the illicit activity hidden behind Bitcoin transactions, one study attempted to make an accurate estimation by analysing the whole blockchain through three different approaches to the identification of addresses linked to illegal activities. Results showed that 25 percent of Bitcoin users are linked to illicit activities, and nearly 50 percent of Bitcoin transactions entail some degree of illegal activity (Foley et al, 2018).

The largest criminal market to utilise cryptocurrencies rests in the drug trade, where the vast majority of proceeds generated is concentrated in only a few black-market sites. A recent study conducted by the Centre of Sanctions and Illicit Finance and Elliptic[4] named "Bitcoin Laundering:

[4] **Elliptic** is an investigative company focused on the detection and investigation of cybercrime involving cryptocurrencies. The company was created as an offshoot of the Foundation for Defence of Democracies' Centre on Sanctions and Illicit Finance, and they help in law enforcement investigations, as well as private companies which aim AML transaction screening.

An Analysis of illicit flows into digital currency services" found that between 2013 and 2016, the main source of bitcoins entering conversion services were coming from just two or three of the most popular marketplaces (Robinson and Fanusie, 2018). These findings are consistent with a previous study from RAND Corporation (2016), which estimates that the total monthly revenue – which ranges between 10.6 and 18.7 million Euros – is generated by the top eight black markets on the Darknet. Anonymous black markets are a great opportunity for lone vendors to 'start their business' in drug selling and trafficking and its features offer enhanced secrecy and privacy. According to a Europol report, the majority of the vendors in Darknet marketplaces are individuals operating alone. However, the top sellers are likely to be part of organised crime syndicates listing advertisements directly within the market and earning substantial amounts of profit (Europol, 2017b).

Silk Road was one of the first and largest anonymous market places that operated in the Darknet. It was founded in 2011 and utilised Bitcoin as the sole payment method. It was shut down by the United States Federal Bureau of Investigations (FBI) in 2013 and its founder, Ross Ulbricht, was arrested and charged. According to the FBI, the site had over 900,000 registered users, more than 13,000 listings and generated 9.5 million bitcoins during its operational time. The value of those Bitcoin at that time was of 1.3 billion USD (Pagliery, 2013). After its closure, a new market, AlphaBay, emerged and became the most popular black market, earning a significant portion of the Silk Road userbase. This market was ten times bigger than Silk Road in terms of listings and the amount of revenue. This success is partly attributed to the fact that it operated and accepted four different cryptocurrencies which included Monero, Zcash, Ethereum and Bitcoin. Some of these cryptocurrencies offered a higher degree of anonymity compared to Bitcoin, although they are not so popular among all black-market users. In July 2017, the AlphaBay domain was shut down by the FBI. Shortly thereafter, another market, Hansa, obtained the market-share of the obsolete AlphaBay and became one of the most popular black markets, until its closure by police in the Netherlands in March 2018 (Europol, 2017c).

In a recent operation in June 2018, the Spanish Guardia Civil and the Australian federal police dismantled and apprehended a criminal network which produced 'new neuropsychoactive substances' and distributed them across various platforms hosted on the Darknet. In total, more than 4.5 million Euro in cryptocurrencies were seized by authorities as part of the sting, which included Bitcoin, IOTA and Lumen from eight individuals that were arrested and charged. In

addition, the members of the organised crime group were also charged for their involvement in money laundering activities which involved fraudulent activity with cryptocurrencies (Europol, 2018b).

Marketplaces hosted on the Darknet are more complex than illicit drug trading. They are a key enabler for other types of crime such as the provision of counterfeit documents to facilitate fraud, illegal immigration, child sexual exploitation, and trafficking of weapons and humans (Europol, 2017). However, these communities are normally separated from the most popular black markets. For example, Silk Road's terms of service prohibited trading with certain items whose purpose was to "harm or defraud" (Zetter, 2013). Trading with child pornography, weapons and stolen credit cards was therefore forbidden. This type of material is sold or exchanged in other niches on the Darknet.

In June 2015 Europol and the Italian National Police shut down a hidden website that specialised in the distribution of child sexual abuse multimedia. Over 14,000 Bitcoin wallets were seized from the administrator when Europol shut down the service (Europol, 2015).

On the other hand, for-profit cybercriminal activities are considered another kind of illicit market which poses an increasing threat and generates a significant amount of revenue for criminals. More precisely, ransomware attacks[5] have dramatically increased in its scope and potency over the past years. Attacks have been on the rise, whereas there were over 4 million attacks recorded in 2015 and an estimated 638 million attacks were committed in 2016 (SonicWall, 2017). This dramatic increase can be explained by the amplified facility and ease of spreading malicious code from computer to computer as well as the increased dependency on digital computing systems across many different sectors, in addition to the emergence of Bitcoin and other anonymous payment methods. Basically, it allows the attacker to remain anonymous while receiving a victim's "ransom" payment for the restoration of files or the digital network that has been corrupted through means of a malicious code or program. Early ransomware developers typically wrote their own code, which implied high technical skills and an advanced knowledge of software vulnerabilities.

[5] **Ransomware** attacks are a complex type of malware that effectively restrict access to computer systems through means of encryption, which alter the way in which information is coded, restricting access and connectivity. Once the computer is locked down, there is a message displayed on the screen, which prompts the victim to make a ransom payment in order to gain access to the data of the system. Most often, the payments demanded are facilitated through the digital currency Bitcoin. If the victim does not pay the ransom by a specified date, the computer is programmed to crash, compromising the ability to recover any internal data stored on the infected system.

New attackers, however, are increasingly reliant on the ransomware-as-a-service program, in which the perpetrator is not required to have advanced technical skills. Rather, the author of the malicious software can make it available for anyone for free or charge a small fee up front, and often opt to take a cut of future ransom payments (Crowe, 2017). The cybersecurity firm BitDefender estimated that in 2017 the total revenue in ransom was 2 billion USD, a considerable market and source of income for cybercriminals.

II.5. Bitcoin Laundering

Bitcoin and other cryptocurrencies by themselves are not yet globally accepted for the majority of online payments and everyday transactions, including the Clearnet. However, Bitcoin is becoming a more popular form of payment and just now starting to be accepted in some businesses, rendering it to have a very limited threshold. This forces criminals who accumulate their wealth in bitcoins or other cryptocurrencies to look for ways to convert their funds into fiat currencies without leaving trace of theirs tainted coins or alarming tax of financial authorities with significant transfers. This process is commonly known as “money laundering” and alongside the emergence of Bitcoin, has opened a breach in the existing financial system that many criminals have leveraged.

As aforementioned, in 2017 around 36 million transactions were made using Bitcoin with a total value of 72 billion USD (Foley et al, 2018). This highlights the potential externalities that virtual currencies have for illegal activities, money laundering, as well as the vulnerabilities that financial institutions, payment systems and mediums of exchange have when there are no consistent regulations across the financial system. Setting these numbers into context, the illicit selling of goods and cybercrime weapons are generating massive cryptocurrency profits for criminals. The United Nations Office on Drugs and Crime (UNODC) conducted a study in 2011 which estimated to what extent illicit funds were generated by drug trafficking and organised crimes and to investigate to what extent these funds are laundered. The report estimates that in 2009, 1.9 trillion USD were laundered (representing 2.7% of the global GDP).

Converting high amounts of Bitcoin into fiat currencies is, however, not a simple task. Dealers with lucrative portfolios of Bitcoin might not be able to exchange their holdings into fiat currencies straight away since conversions in high volumes would be flagged as suspicious activity to financial institutions. For instance, when Ross Ulbricht was arrested in 2013 for his involvement

as an administrator of the Silk Road Darknet marketplace, he was far under the radar of authorities, living an ordinary life in San Francisco despite the fact that he owned 144,000 bitcoins – which at that time amounted to over 28.5 million USD (Greenberg, 2013). Even though he owned a substantial Bitcoin holding, sending money from an anonymous (and potentially suspicious) Bitcoin account to an identified bank account would have made it easy for the police to trace him and freeze his assets.

Money laundering is typically executed in three steps: placement, layering and integration. Placement is the introduction of money into the financial system. It is usually made in small amounts so that involved parties or accounts do not raise suspicions to the financial institutions through which criminals are conducting transfers. Second, layering is the process of moving and distributing funds throughout various accounts in small increments across an array of financial institutions around the world, transcending jurisdictions, rendering it very difficult for banks to detect due to lax policies about sharing sensitive information about their clients and holdings. The objective of the layering process is to obfuscate the original source of money. Finally, the funds are integrated in the economy and can be sent back to the beneficiary through other legal measures or payments.

Ownership of Bitcoin, unlike an account at an institution within a traditional banking system, are not directly linked to the specific identity of any individual but rather to a private key connected to a Bitcoin account and recorded in the blockchain. Due to its decentralised nature, there is no central entity such as a bank or a government that controls the transactions and who they belong to. The concealed identity and obfuscated transfer in the blockchain ledger can be beneficial to criminals, and when utilised, could lead to higher rates of money laundering with ease.

The previously mentioned study of Elliptic shed light on the various methods used by criminals for “cleaning” or laundering bitcoins earned from illicit activities (Robinson and Fanusie, 2018). Similar to what occurs with laundering fiat currencies, individuals move bitcoins from an address associated with illicit activity to a new address with the purpose of blurring the original source. Paired with the increased anonymity earned through the use of Bitcoin, transferring cryptocurrency through multiple accounts across a variety of service providers and Bitcoin wallets provides considerable cover to cybercriminals.

The entry-exit point where cryptocurrencies convert into fiat currencies and vice versa are called conversion services. There are different types of these specialised services depending on the type of currency and the aim of the conversion. Of all cryptocurrency exchange services, Bitcoin is by far the most utilised due to its popularity worldwide. These services convert fiat currencies to Bitcoin which can then be used to purchase other cryptocurrencies- this process is widely popular among Bitcoin investors that seek and expect to use bitcoins as an asset and sell them for profit when their value in the market has increased. This practice became especially popular in 2016 when the value of Bitcoin started to rise and a growing number of people invested in Bitcoin by using these services. Keeping this aside, Bitcoin conversion services are also very popular for criminals who seek to launder fiat currency by using it to purchase bitcoins and then later introducing the funds into the financial system as earnings from the increasing value of investments in cryptocurrency.

The aforementioned study calculated that nearly 90% of the total amount of bitcoins coming from illicit sources are directed and processed by Bitcoin exchanges. Most of these services, such as the widely popular Kraken and Coinbase platforms, also offer a specialised cryptocurrency to cryptocurrency exchange. When a virtual coin is converted into another type of virtual coin, transactions on the Bitcoin blockchain can no longer be traced, since every blockchain belongs to a specific cryptocurrency.

Services such as Kraken and Coinbase, as well as the vast majority of Bitcoin trading platforms, require user ID verification in order to make deposits or withdrawals; verification in this manner protects traders from scams and the financial system from money laundering. However, some exchanges allow their clients to remain anonymous and market their services accordingly. When conversion exchanges do not have appropriate anti-money laundering (AML) and know-your-customer (KYC) policies, authorities consider the conversion of Bitcoin into fiat currencies in these exchange services to be the physical act of money laundering. This can be considered a soft regulation due to the voluntary incorporation of these policies into the service agreements within cryptocurrency exchange service platforms. Failure to adopt these policies can be considered criminal in itself due to the apparent disregard for financial crime and compliance to existing banking laws.

Additionally, mixers and gambling sites are a highly used resource among criminals for concealing bitcoins coming from illicit trade. Bitcoin mixers, also known as Bitcoin laundering services, are a service provided to consolidate and aggregate cryptocurrencies in a singular account, much like a pooled investment or investment fund. Some service providers offer participation in a mixer as an additional, paid service and charge a fee that typically ranges from 1 to 3%. Precisely because cryptocurrencies provide a public ledger of all transactions, some users opt for disguising the source of their bitcoins through mixers, which are potentially identifiable but offer substantial coverage. By mixing their accounts, criminals can augment the anonymity of their bitcoins, making the labours of law enforcement harder from aggregated, more obfuscated layering. Proponents of cryptocurrency mixers assert that Bitcoin is not as anonymous as it once was at the beginning of its emergence. They use Bitcoin mixing services in order to gain more privacy and prevent hackers and other users to follow transactions. On the other hand, some experts claim that mixers should be a criminalised practice since they can potentially be used for and enable illegal activities in the cryptocurrency markets.

In conclusion, the main difference between traditional money laundering and Bitcoin laundering is that the layering process in Bitcoin laundering occurs when the user first makes purchases and makes transactions in cryptocurrencies, in different quantities and over different periods of time. It is after the layering process that the money is finally introduced to the financial system as clean money by utilising Bitcoin exchange services. This difference in its nature has further complicated the question of whether traditional anti-money laundering (AML) regulation can be applied and implemented in the effort to regulate cryptocurrencies and their exchanges.

Enhanced regulation measures and a stricter compliance from cryptocurrency transmitters and Bitcoin exchange services and marketplaces, as well as a cohesive collaboration between these entities and law enforcement agencies, should help in flagging and intercepting criminals trying to launder illicit funds. Not only this would prevent money laundering, but also the exit point of the network could help to trace the thread of criminals' transactions, facilitating the investigative labours of the police. In this regard, the US is one of the first countries that have implemented a considerable amount of advanced regulations in cryptocurrencies. Compliant financial institutions involved in this process, as well as early regulatory measures adopted in the international cryptocurrency services market are described and analyzed in further detail in the "Financial Authorities and AML Regulations" section, in chapter III.

III. Bitcoin as an Opportunity for State Law Enforcement Agencies

III.1. Bitcoin Investigative Advancements in Law Enforcement

III.1.1. Law Enforcement Analysis Tools

Legitimate users make transactions with Bitcoin and other cryptocurrencies every day, exchange money and purchase goods or services in a secure and anonymous way. However, as stated previously its pseudo/anonymous characteristics (providing sufficient cover) and decentralised nature make an ideal tool for criminals. Currently, law enforcement agencies are using and developing tools which allow the police to trace and track suspicious Bitcoin transactions. There are a number of websites which offer blockchain analysis services, such as "Chainalysis", that are able to index and analyse Bitcoin transactions and addresses, giving a valuable insight into the Bitcoin ecosystem, including the behaviour and patterns of their users. Another known firm which collaborates with law enforcement in cybercurrency intelligence is CipherTrace. CipherTrace is a blockchain technology security firm based in Menlo Park, California, which works with more than 40 companies and public sector governments to track and trace cryptocurrency transactions. CipherTrace is a pay-for-service that seeks to help cryptocurrency wallet hosts and exchanges avoid accepting money obtained illegally by tracing the transactions of each Bitcoin and signaling whether or not the funds come from Bitcoin mixers, Darknet marketplaces or digital wallets flagged as criminal or suspicious.

While these services can be useful, analyses performed by third-party actors are sometimes not able to produce evidence that can be used in court cases, since they do not comply with the established investigation policies or court-mandated evidence provisions in most countries. INTERPOL Global Complex for Innovation has proposed an analytical framework and software system to assist law enforcement agencies in the analysis of the Blockchain, providing legal coverage and helping to extend the value of these investigative tools in criminal cases (Kuzuno and Karam, 2017). The proposed framework relies and rests on three critical components: an indexer, an analysis module and a web interface. The indexer records Bitcoin addresses and transactions in real time and label them as "suspicious" when applicable. Sometimes an address is suspicious because it has already been reported by law enforcement agencies and has since been

flagged or frozen due to its activity. On other occasions, to determine if an address is involved in illegal activities, the tool uses a web-crawler to automatically search the Clearnet and the Darknet for connections or traces. The analysis module studies the behavioural patterns of a targeted Bitcoin address through the transaction history as recorded in the blockchain. Finally, the results from the analysis module are classified in four groups: i) statistics of the activity of an address (for example, the number of transactions, active months, etc.), ii) a graphical representation between various transactions and Bitcoin addresses, iii) transaction paths for each Bitcoin address, and iv) a cluster which contains all the Bitcoin addresses that belong to the same wallet. By providing this information, digital forensic analysts from law enforcement agencies can better identify criminal activity in the Blockchain as well as the time zone that a criminal is operation based at the time of the transactions. This tool was tested in the aforementioned study of INTERPOL, by comparing their findings with the forensic evidence previously reported from three solved cases: Silk Road, CryptoLocker ransomware and DD4BC extortion.

In the Silk Road case, INTERPOL selected an address involved in the Silk Road market and identified critical information related to that Bitcoin account, including an email address which led the investigators to posts in a Bitcoin forum. This combination of blockchain information and open source information provided them with the sufficient data to verify the involvement of the Bitcoin address with criminal activities. Secondly, in the analysis part, investigators found out that that specific Bitcoin address had repeatedly sent bitcoins to another address, reaching the amount of 111,111 bitcoins which has a substantial conversion rate. According to the investigators, the two addresses belonged to the same owner. Finally, there was enough information that linked the second Bitcoin address with the identity of the owner. In this case, the tool combines with open source information demonstrated to be useful for the identification of the owner of 111,111 BTC coming from illicit activities. Although the tool didn't provide new information, it proved to have at least the same effectivity as the forensic tools used by the FBI when the case was investigated.

In the CryptoLocker ransomware case, the tool proved to be more effective than preceding law enforcement forensic tools. CryptoLocker was a ransomware attack triggered in September 2013 which lasted until May 2014. It requested its victims a payment of 2.0 bitcoins (which was valued around 250 USD at that time) to a specific Bitcoin address. This time around, the aim of the investigation was to determine the number of victims and the total revenue of the criminals to then use to pinpoint specific Bitcoin users with similar holdings. Their methodology consisted in

searching for transactions for the value of 2.0 bitcoins that occurred between the given dates of the attacks. While the results of the indexing part came up with a large number of transactions that were unrelated to the ransomware attack, the analysis part revealed two addresses that were likely to be involved in the attack due to the large number of irregular transactions received (allegedly the victims' ransom) in that period time. Once the addresses were identified, further analysis of the transaction histories was conducted to verify the link between the addresses and the CryptoLocker attack. The main features examined were the timeline of the operations, the volume and frequency of the incoming transactions and the amount of the payments. Investigators also used open source information in various Darknet forums related to ransomware. Finally, the investigation revealed that the author of the ransomware forwarded the bitcoins to another address from which the bitcoins were exchanged to another cryptocurrency by using a well-known, compliant cryptocurrency exchange service.

Although there is no further information available concerning how the police managed to further track the perpetrator(s), in 2014, the Department of Justice issued an indictment against the Russian hacker Evgeniy Bogachev for his alleged involvement and he is currently in the upper tier of the FBI's "Most Wanted" list. The information revealed by the analytical framework tool showed that not only were law enforcement agencies able to index the number of victims through the Bitcoin addresses, but also were able to identify new suspicious Bitcoin addresses using deductive means of investigation of blockchain ledgers.

Finally, the "DD4BC extortion" case (meaning "DDoS[6] for Bitcoin") the attackers threatened the victims with an email warning the deployment of a DDoS in case a certain number of bitcoins were not sent set during the allotted time frame, stipulated by the attacker(s). The investigation started with tracking the given Bitcoin addresses provided to their victims by the attackers and a further follow-up of the thread of the transactions between different Bitcoin addresses during the specified time frame. INTERPOL found out the relation of numerous Bitcoin addresses to two main addresses, and then, from one of them, the remittance of the money in smaller quantities to an extensive number of addresses. According to their observations this is a typical behaviour of mixers or tumblers – in this case, the other main account sent the bitcoins to another Bitcoin

[6] DDoS stands for "Distributed Denial of Service" and is a cyberattack which renders websites and other online resources unavailable to intended users due to increased and overloaded traffic to its servers, causing an overload of activity and temporarily shuts down the site.

address and then exchanged them to another cryptocurrency. INTERPOL's analysis tool was able to trace the transactions further than previous investigations were able by evidencing that bitcoins were sent to mixers and highlighted the difficulty in its tracing. Although there is a rapid progress and developing of the methods and tools used by law enforcement to patrol and detect cybercrime, mixers and tumblers complicate and hinder the ability for law enforcement to track the criminals behind numerous Bitcoin addresses, as well as crypto-to-crypto exchanges. This development emphasizes a higher expertise from the side law enforcement and demonstrates the complexity and accuracy of new (even 'beta') tools for de-anonymization.

III.1.2. Behaviour Analysis in the Blockchain

Tools and specialised software are important in tracking the activity and can also help pinpoint known behaviours and trends of criminals in the Blockchain. By analysing this activity, law enforcement can provide and target certain activities, regarding patterns that indicate a potential willingness to conceal illicit money sources and/or laundering techniques. A recent study which identified some behaviours of users in illegal marketplaces concluded that 1) users tend to transact more and in smaller quantities each transaction; 2) they are also more likely to repeatedly transact with a given counterpart 3) they have a tendency to hold less Bitcoin in their accounts (Foley et al, 2018). Another relevant finding is the increase of activity immediately after the seizure of a marketplace, or after a scam that affects its userbase. Finally, the network of Bitcoin transactions between illegal users is three to four times denser than the network of legal users. Bitcoin users are also much more connected with one another through transactions. Activities such as repeated use or construction of Bitcoin mixers could potentially signal illegal activity.

The tendency to accumulate small amounts of Bitcoin or cybercurrency in numerous account might also indicate illegal activity. This is an increasingly common practice due to the fact that when law enforcement agencies seize Darknet marketplaces or online platforms hosting illegal activity, there are most likely associated, flagged accounts that are monitored by law enforcement due to the presence of a substantial amount of cryptocurrency and association with the shutdown site or service. Shocks in Darknet market places take place immediately following seizures or takedowns by law enforcement, hacks or scams that affect active users of a particular service, platform or marketplace. After a shutdown, users have to relocate their holdings, and turn to alternative marketplaces. At the same time, these shocks are unlikely to affect legal users.

When a marketplace is taken down, such as was the case with the Silk Road or AlphaBay, the demand for illicit products and services is maintained but its platform is interrupted. Due to the remaining (and possibly increased demand), its users simply migrate to another existing market or platform to ensure the flow of the goods and services. Although this might seem an endless or nonsensical task for the police to shut down market after market, this kind of operations can serve an additional purpose: law enforcement agencies can use the information of the seized bitcoins to identify its users such as the marketplace operators, customers and suppliers in post-seizure investigations. When law enforcement officials are able to analyse transactions in the blockchain through confiscated bitcoins or account information associated with illicit activity, there are certain patterns and behaviours that are explicitly marked or tagged as potentially criminal. By familiarising or knowing a series of behaviours beforehand, it increases the possibility for law enforcement agencies to develop and engineer advanced software that targets or pinpoint these peculiarities and isolate suspicious behaviours/transactions. This development would not only increase the potential of law enforcement to better regulate and patrol the use of cryptocurrency, it could also be fundamental in shaping the digital landscape of the use and legal parameters of cryptocurrencies.

III.2. Financial Authorities and AML Regulations

This section outlines the key institutions involved in the anti-money laundering procedures and presents the current regulations in the US and Europe that address AML measures related to virtual currencies.

Fiat exchanges are considered the sole entry and exit point of Bitcoin in the existing financial system. Cryptocurrencies with no jurisdiction become currencies with legal tender when converted to fiat currencies. The potential for its illegal use and the and the expansion of Bitcoin in the markets has raised concern among public sector financial officials, who have started to pay attention and to propose and implement regulatory measures. Fear of uncontrolled flows of wealth outside traditional boundaries of fiat currencies, as well as tax evasion and money laundering are some of the biggest concerns of governments around the world. For example, in 2017 China took action in banning Bitcoin mining and use in fear that the cryptocurrency would be fraudulent and used for aforementioned illicit activities and money laundering. Other countries like the US, while

acknowledging the same potential threats, advocate for adopting binding, regulatory measures which would further develop the cryptocurrency market. In order to prevent money laundering, terrorism financing and financial crime, financial intelligence institutions have a critical role in the proposal and implementation of regulatory policy.

Financial intelligence units (FIUs) are national entities which collect information on suspicious or unusual activity from the financial industry and other entities or professions required to report transactions suspicious of enabling money laundering or terrorism financing. Their mission is to process and analyse the information received and, if sufficient suspicious activity is found, they report it to public prosecution and tax services (Egmont Group, 2018). They collect raw transactional information as well as Suspicious Activity Reports (SAR) – further described below – which are usually provided by banks and other financial service institutions – which, to a certain extent, now also include cryptocurrency exchange platforms. Every country has its own national financial intelligence unit, and to a considerable degree collaborate together through international initiatives, such as that of the Egmont Group, an informal network of 155 FIUs that provide a commonplatform for financial intelligence and expertise to combat money laundering and trace the financing of organised crime and terrorism.

A **Suspicious Activity Report** (SAR) also known as **Suspicious Transaction Report** (STR) is a report generated and issued by a financial institution to its FIU when the financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing. In addition to Egmont Group, Europol recently founded the European Financial Intelligence Unit Network which is a decentralised computer network that created an information sharing platform between the FIU to the European Union and individual member state financial authorities. The classification and availability of information through this integrated database system makes it possible for FIUs to search, match and track names in order to find relevant data another FIU might possess.

Information sharing is especially relevant in the use of virtual currencies matter due to its defining, decentralised characteristic. A financial institution operating within a specific jurisdiction and a variety of national currencies might send a STR to its financial authority to further investigate a suspect. However, the person behind these transactions could have ongoing operations in other jurisdictions that would confirm or deny its involvement in money laundering. Information about

transactions, IP addresses, emails and personal information can help to put a small amount of information into context and consolidate cases against alleged criminal activity. Coalitions and collaborative efforts such as the Egmont Group have an increasingly relevant role in facilitating the flow of FIU information among multiple authorities when needed.

III.2.1. United States: FinCEN and the Bank Secrecy Act

In the United States, the **Financial Crimes Enforcement Network (FinCEN)** is "the body responsible to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities." (FinCEN, 2018). FinCEN is the financial intelligence institution within the US which exercises regulatory functions primarily under compliance to the US PATRIOT Act of 2001 and the **Bank Secrecy Act (BSA)** statute[7] by issuing, implementing and enforcing compliance of regulations requiring banks and other financial institutions to establish the necessary measures to prevent financial crime, money laundering and counter-terrorism financing. FinCEN is, therefore, the authority which implements AML programs and drafts reports of high value in criminal, tax, regulatory investigations, and counter-terrorism financing matters. To achieve its mission FinCEN includes the three interrelated strategies (FinCEN, 2013a):

- Administering the Bank Secrecy Act
- Sharing information collected as well as intelligence analysis with law enforcement, regulatory partners and other intelligence agencies
- Building global cooperation and technical expertise among financial intelligence units around the world

In March 2013, FinCEN issued an explanatory guidance to clarify to what extent regulations under the BSA regarding virtual currencies would be applicable under the framework of the financial system. This document focuses on the *definitions* of persons engaged in virtual currency transactions and determines who should and should not be applicable to the regulation for money service and exchange services (FinCEN, 2013a).

[7] The BSA is the nation's first and most comprehensive Federal anti-money laundering and counter-terrorism financing (AML/CFT) statute.

- A *user* is described as a person that obtains virtual currency to purchase goods or services.
- An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.
- An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.

The BSA defines ***money services businesses*** **(MSBs)** as "a person, wherever located, doing business, whether or not on a regular basis or as an organised or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section. This includes, but is not limited to maintenance of any agent, agency, branch, or office within the United States[8]." Currently there are six categories included in this definition, but for the purpose of narrowing the scope to virtual currencies administrators and exchangers, only the category of *money transmitter* will be considered and discussed. FinCEN defines the term *money transmitter* as "a person that provides money transmission services, or any other person engaged in the transfer of funds." Therefore, to clarify, a MSB is "a person wherever located doing business, whether or not on a regular basis or as an organised or licensed business concern, wholly or in substantial part within the United States, in the capacity of (…) money transmission services, (…) engaged in the transfer of funds (…) unless a limitation to or exemption from the definition applies to the person."

According to FinCEN, a user of Bitcoin is not considered an MSB under FinCEN's regulations, because the definition of *user* is someone who uses the cryptocurrency to purchase goods or services, and therefore does not fall into the category of money transmission services. Conversely, *exchanges* and *administrators* are money transmitters because they accept and transmit virtual currencies and buy or sell virtual currencies. This definition includes money transmitters who exchange fiat currencies to cryptocurrencies, as well as money transmitters who trade cryptocurrencies to other types of cryptocurrencies since a "convertible virtual currency" is defined as either having an equivalent value in real currency or acting as a substitute for real

[8] *Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011) (the "MSB Rule"). Full text available online: https://www.federalregister.gov/documents/2011/07/21/2011-18309/bank-secrecy-act-regulations-definitions-and-other-regulations-relating-to-money-services-businesses#sectno-citation-%E2%80%891010.100

currency. Having said, the definition of MSB encompasses not only just banks, but also fiat exchange services, crypto-to-crypto exchange services and mixers.

As of today, all MBSs within the US should comply FinCEN MSBs' regulations by registering, reporting and keeping record of their financial activities. The BSA states that MSBs are required to:

1. Register to FinCEN
2. Establish written anti-money laundering programs which would not only prevent money laundering but also terrorist financing activities,
3. Submit Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs).
4. Keep certain records, especially when related to monetary instruments with currency transactions by currency exchangers.
5. Moreover, MSBs are subject to examination and auditing by the Internal Revenue Service (IRS) to ensure appropriate BSA compliance.

In addition to this, an "Activity threshold" clarification was added to the MSB definition which outlines the conversion of a user into a MSB when the daily income of the dealer exceeds 1,000 USD, falling into the category of *Dealer in foreign exchange*.

"*Dealer in foreign exchange:* A person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more other countries in an amount greater than 1,000 USD for any other person on any day in one or more transactions, whether or not for same-day delivery".

When applicable, the MSB must then send a Currency Transaction Report (CTR)[9] to the Internal Revenue Service (IRS) to embody full compliance.

Following the case of the shutdown of the Silk Road marketplace in 2013, the director of FinCEN released a statement which made reference to the potential of virtual currencies to be exploited for money laundering – just as other currencies do– and its relevance to FinCEN's attention soon after the market was closed by the police (FinCEN, 2013b). Specifically, FinCEN warned financial

[9] **Currency Transaction Report**: cash transactions in excess of 10,000 USD during the same business day. The amount over 10,000 USD can be either from one transaction or a combination of cash transactions.

institutions that deal in virtual currency to implement effective AML/CFT controls to harden themselves and provide thorough protection from becoming the targets of illicit actors that could potentially exploit any identified vulnerabilities. One year after, in 2014, FinCEN applied an anti-money-laundering program including specific requirements and clauses applicable to Bitcoin exchanges. The following two cases exemplify a non-compliant and a compliant exchange service and their consequences.

Case Study 1: BTC-e Money Laundering and Stolen bitcoins from Mt Gox

In July 2017, FinCEN took its first action against a foreign operating MSB doing business within the US. Together with the U.S. Attorney's Office for the Northern District of California, FinCEN identified a Bitcoin exchange service called "BTC-e" under the shell company Canton Business Corporation, which willingly violated the Bank Secrecy Act. According to FinCEN press release, BTC-e did not comply with any of the FinCEN guidance established in 2013 under the BSA regulations. At the time of the report, the company was one of the biggest Bitcoin exchanges in the world in terms of volume of exchanges and it allowed trading between USD, Euros and Russian rubles, in addition to numerous cryptocurrencies including Bitcoin, Dash and Ethereum. Its intrinsic lack of basic anti-money laundering measures catered to evade criminal activity in services to launder funds coming from illicit proceeds, including drug trafficking in the dark market. FinCEN's assessment (2017) cites BTC-e for multiple BSA violations, including failures to: register as an MSB; implement a written AML program; verify customer identification; monitor for and report suspicious activity; and comply with recordkeeping requirements. Furthermore, the assessment states that users at BTC-e openly and explicitly discussed ways to conduct criminal activities in an internal messaging system from BTC-e's website. Furthermore, the same website and its administrators received inquiries from customers on how to launder proceeds obtained from selling products in the online black markets, including Silk Road, AlphaBay and Hansa. The estimated amount of deposits that BTC-e received during its existence is reportedly valued at over 4 billion USD. In addition to this, the FinCEN report also stated that BTC-e processed the stolen bitcoins from another Bitcoin exchange service "Mt Gox[10]", one of the largest Bitcoin exchange platforms in 2014.

[10] **Mt Gox** was created in 2010 and became one of the largest Bitcoin exchanges in the world, operating by 70% of transactions in 2014. Mt Gox was hacked in 2011, and almost 750,000 Bitcoins of its customers as well as 100,000 of its own Bitcoins were stolen.

Interestingly, in a parallel criminal investigation, the alleged founder of the company, Alexander Vinnik, was arrested and detained in Greece (Gibbs, 2017; Department of Justice of the United States, 2017). According to the superseding indictment[11], BTC-e operated as an unlicensed MSB which facilitated virtual currency transactions involving various crimes, including computer hacking, identity theft, tax refund fraud schemes, public corruption and drug trafficking. With regards to Vinnik, the indictment directly links him to the stolen Bitcoin from Mt Gox, asserting that Vinnik received the proceeds from a hack of Mt Gox and laundered them through various online exchanges under his ownership and supervision, including his companies BTC-e and Tradehill.

In summary, the indictment charged BTC-e and Vinnik with "one count of operation of an unlicensed money service business, (…) one count of conspiracy to commit money laundering, (…) seventeen counts of money laundering, (…) and two counts of engaging in unlawful monetary transactions (…)". The total penalties imposed by FinCEN on BTC-e was of 110,003,314 USD and 12,000,000 USD on Alexander Vinnik. FinCEN director, Jamal el-Hindi, asserted that this action "should be a strong deterrent to anyone who thinks that they can facilitate ransomware, Darknet drug sales, or conduct other illicit activity using encrypted virtual currency."

This operation took place only one week after the FBI seized the illicit marketplaces AlphaBay and Hansa, which in an indicator that probably some of the accounts targeted by the police belonged to Vinnik. As seen in the cryptocurrency money laundering layering step, Vinnik would be seeking to conceal the stolen funds through various transactions that might have included the use of mixing services and finally reach different fiat exchanges. Through this process he would have disguised the source of his bitcoins, including his connection to the hacking of Mt Gox. All the adopted measures were not effective enough to completely conceal it from law enforcement, nor from FinCEN. At the same time, this case has some similarities with the Silk Road case and the arrest of its administrator, Ross Ulbricht, especially considering the seizure of his Bitcoin holdings. Large sums of money, even when underground or in unregulated accounts, are difficult

It wasn't until 2014 that the company would realise and report this theft. The total loss constituted about seven percent of all available Bitcoins in circulation, and was worth around 473 million USD at that time. The company declared bankruptcy and closed in 2014.

[11] An **indictment** merely alleges that crimes have been committed, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in the court of law.

to conceal. This case is also a warning signal for other exchange services that, whether willingly or not, could be used to provide money laundering services to criminals. If these actions were unveiled, the CEO of a particular exchange service could be arrested and the business closed due to the corporate responsibility to comply with financial regulations of a certain jurisdiction.

Case Study 2: Example of a regulated cryptocurrency trading service: Coinbase

As previously stated, the platform Coinbase is one of the largest cryptocurrency exchange service providers, currently trading four types of cryptocurrencies - Bitcoin, Bitcoin Cash, Ethereum and Litecoin – all of which can be bought directly with fiat currencies using its interactive platform. Coinbase is also one of the most reliable and well reputed trading services in terms of compliance with AML regulations. Information regarding their compliance with regulations can easily be found on their website (https://www.coinbase.com), where they include the measures related to customers information and privacy they are required to take by law. First, the company is registered as a Money Service Business with FinCEN. Second, it applies an anti-money laundry program consisting of (1) the verification of their customer identities by sending a copy of the passport or ID, (2) maintaining records of currency transactions to a maximum of five years, (3) report suspicious transactions. In addition to this, they also comply with clauses stipulated under the USA Patriot Act which requires to designate a compliance officer, create protocols and procedures to ensure compliance, conduct trainings and periodically review the compliance program. Coinbase also possess the BitLicense which allows the company to engage the business as a money transmitter, registered and fully compliant in the state of New York (Suarez, 2017).

In March 2017, Coinbase was ordered by the US Internal Revenue Service (IRS) to report all customers moving more than 20,000 USD per year. The data of more than 14,000 users was reported to the US authority, including registered IDs, names and dates of birth as well as all the history of transactions made and links to other associated accounts (Brandom, 2017). The IRS made the petition in the wake of the sudden surge in market value of Bitcoin, which resulted in the generation of significant wealth among Bitcoin investors.

Finally, in compliance with the federal regulations as a registered MBS, Coinbase is required to ask each customer whether the funds are being sent to another digital currency service or not,

before making a transaction to an off-site address. This is intended to help the authorities to link cryptocurrencies and accounts even when they are sent to another MBS – and consequently switch between Blockchains of other cryptocurrencies. This is considered a crucial step for investigations given the fact that other cryptocurrencies such as Monero or Zcash cannot be purchased directly in fiat exchanges but rather are exclusively available and traded in crypto-to-crypto exchanges.

According to the chief legal and compliance officer of Coinbase, the company aims to be one of the most transparent and trusted cryptocurrency service providers in the world in order to create an open and compliant financial system and to ensure the cybersecurity of their customer assets, as well as market integrity (Lemper, 2018). Coinbase's close collaboration with regulators, law enforcement and financial institutions is part of their larger strategy to promote their growth and market their services as reliable and law-abiding. Conversely, Coinbase is a source of concern for those who look for anonymity at the same time they want to trade on a reliable platform. In informal channels such as "Bitcoin forum" hosted on the website "Bitcointalk"[12] some customers complain that after their exchange of Bitcoin to fiat currencies the bank statement specifies the source of their money: "COINBASE.COM/Bitcoin CREDIT". This contrasts with bank statements issued previous to 2013 when the message that appeared was only "Coinbase CREDIT" giving no further details about the source of the income. This increase in transparency by disclosure of the details provided to the bank when customers do their purchases can be negatively perceived as an invasion of customers' privacy by those who are mainly interested in hiding their identity. Companies following the same model of transparency are likely to be rejected by criminals who are avid proponents for extended privacy measures. At the same time, users who are more concerned about the security of their funds can find confidence in Coinbase and like-minded companies as a reliable platform in which they can store, utilise and to trade cryptocurrency holdings. This notion could result in extended compliance efforts for those who are indeed acting legally within the framework of existing finance law.

III.2.2. Europe: European Commission – 5th Anti-Money Laundering Directive

The Directive (EU) 2015/849 of the European Parliament constitutes the main legal instrument to prevent money laundering and terrorist financing within the EU financial system. This Directive sets out a comprehensive legal framework for preventing the collection of money for terrorist

[12] Bitcointalk forum can be found at: https://bitcointalk.org/index.php?topic=219354.msg2308960#msg2308960

purposes by requiring EU Member States to identify, understand and mitigate the risks related to money laundering and terrorist financing.

In February 2018, the European Commission held a roundtable to discuss the risks and opportunities in the wake of extended use of cryptocurrencies. This meeting was primarily focused on the financial impact associated with cryptocurrencies, and its generated outcomes which can greatly determine the openness of Europe to virtual coins, and therefore, its further utility across the continent. It was agreed that blockchain technology should be embraced by European leaders in order to remain competitive and robust. However, the European Commission acknowledged the risks of cryptocurrencies related to money laundering and financing of illicit activities, directly acknowledge its role in terrorism, and proposed that virtual currency exchanges and wallet providers should be regulated under the **5th Anti-Money Laundering Directive (5AMLD)** and subject to further regulation in compliance to terrorism and counter-terrorism measures (European Commission, 2018).

The 5AMLD is an amendment of the 4th AMLD and the new measures include:

- The prevention of risk associated with the anonymous use of virtual currencies for terrorist financing and limiting the use of pre-paid cards
- Enhancing the transparency on company ownerships by providing the accuracy of beneficial ownership registers
- Strengthening the monitoring of financial transaction to and from high-risk third countries
- Enhancing the powers of EU Financial Intelligence units and their access to information, including centralised bank account registers
- Ensuring centralised national bank and payment account registers or central data retrieval systems in all member states.

In terms of scope, the new AML regulations extend the EU Directive 2015/849 to virtual currencies and their respective exchange platforms as well as to providers of digital wallets for virtual currencies. The new amendment includes the following:

“Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.”

These new entities will have to i) register with the financial intelligence units of their jurisdiction, ii) identify and verify their customers and iii) report any suspicious activity to the financial intelligence unit of their jurisdiction.

In addition to this, to combat against anonymity of electronic money, a reduction in the threshold for identifying the holders of prepaid cards has been condensed from the last regulation. Financial institutions will be required to ask for customer identification when remote payments over 50 Euros are made using cryptocurrencies. The only cases when physical vendors and markets in EU member states will have the possibility to allow the use of cryptocurrencies will be i) when users use a prepaid card directly in the shop, for a maximum amount of 150 Euros (instead of 250 Euros); ii) in an online transaction with a prepaid card below 50 Euros.

The 5AMLD also aims to enhance the transparency of the beneficial ownership registers for legal entities, by making them accessible from any competent authority, professional sector or person who can demonstrate a legitimate interest. In addition to this, national registers will enhance their interconnectivity to facilitate exchange of information between member states. This measure is expected to prevent the use of legal entities for money laundering and terrorist financing purposes.

Since some countries outside the EU lack of the effective measures to prevent anti-money laundering, and for this, the commission has established a list of non-EU countries associated with high-risk of money laundering destinations. This list builds upon the one published by the Financial Action Task Force (FATF) and is updated on a regular basis. As of 29 June 2018, the FATF listed 72 high-risk and non-cooperative jurisdictions, constituting a "cryptocurrency black list". These new rules entered into force on 9 July 2018, and member states are expected to implement these new rules into their national legislation by 10 January 2020. This common framework should facilitate the competent authorities of any country within the EU to monitor individuals behind suspicious virtual currency transactions.

In one instance, before the application of the new regulations, a virtual currency exchanger sent a STR to Europol (Europol, 2017a), even when the exchanger was not required to file the report because the legislation at that time did not require so. The exchanger voluntarily conducted a customer due diligence, monitored the activity and notified law enforcement the transactions believed to be linked with criminal activities. Finally, the analysis conducted by the exchanger revealed the that the source of the income originated in illegal markets in the Darknet. Just days

before, Europol had been informed about a money laundering and drug trafficking organised crime group investigation which corresponded to the same individual using the virtual currency exchange. Furthermore, the money exchanger provided critical assistance to Europol by providing all the necessary evidence and history of transactions to better and more effectively analyse the money flow within the crime syndicate. This example shows the effectiveness of information sharing, especially when virtual currency exchanges are willing to collaborate with financial regulators and investigative units.

III.3. Expansion of Cooperation Networks

III.3.1. Financial Action Task Force

The **Financial Action Task Force (FATF)** is an inter-governmental organisation in which its member countries promote the effective implementation of legal, regulatory and operational measures against money laundering, terrorist financing and related threats involving the integrity of the international financial system. Its members are composed of the Ministers of its member jurisdictions (currently 35 jurisdictions and 2 regional organisations), and they work to generate recommendations to bring about national legislative and regulatory reforms. In 1989, FATF created and consistently updates a published series of recommendations to reflect the changing context. The last version of the FATF recommendations was issued in 2012, as it did not take into consideration the utility of virtual currencies. For this reason, in June 2014, FATF issued a new report which conducted a preliminary assessment on Money Laundering and Terrorism Funding risks, providing a substantial framework and the definition of some concepts associated with virtual currencies. Their assessment is based on to assumptions that 1) the revolution of virtual currencies as a payment method is favorable 2) virtual currencies are a powerful tool for criminals, organised groups and terrorist financers who store and move illicit funds in the shape of bitcoins and other cryptocurrencies.

First, FATF recognises the necessity to establish a common set of definitions reflecting the terms which are involved in the operations of virtual currencies. They also note that vocabulary should be subject to change as cryptocurrency and its use evolve to better fit the market and its userbase. Interestingly, the FATF defines ‘virtual currency’ as “a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status (…) in any jurisdiction”. Since it is not

issued by any jurisdiction, it is also not guaranteed by any jurisdiction. This makes virtual currency different from e-money, which is a digital representation of fiat currencies used to make digital transfers. Digital currency can be interpreted as either virtual currency (non-fiat) or e-money.

Bitcoin enters in the category of convertible decentralised virtual currencies. 'Convertible virtual currencies' have an equivalent value in fiat currencies and can be exchanged for real money and vice versa. 'Decentralised virtual currencies' such as Bitcoin are also referred to as cryptocurrencies since they are "distributed, open source, math-based peer-to-peer virtual currencies" with no central administrator and no central oversight.

An 'exchanger' (also known as a 'virtual currency exchange') is a "person or entity engaged as a business in the exchange of virtual currency for real currency, funds or other forms of virtual currency (…)".

A user is a person or entity who "obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment".

The FATF also considers decentralised systems particularly risky for the integrity of financial systems because the lack of a central provider of Bitcoin does not require any identification and verification of its participants. Law enforcement investigative tasks have to rely on exchange platforms for client's information, and not all of them are compliant to the emerging new regulations. These exchangers are the gateways which permit access back and forth the financial system by the exchange of cryptocurrencies and fiat currencies. The assessment suggests that AML and Counter Terrorism Financing (CTF) controls should target those exchange platforms rather than the users.

One year later, in 2015, the FATF issued a guidance which intended to clarify the application of the FATF Recommendations set forth in 2012, directly applying elements to cryptocurrencies virtual currency exchangers by a risk-based approach to AML and CTF measures. This guidance is intended to serve as a basis from which national authorities can develop their regulatory responses, including the amendment of current AML and CTF laws. In addition, the guidance is also addressed to those companies in the private sector who are involved in virtual currency payments and product services (VCPPS) and how they should comply with the AML requirements.

III.3.2. Law Enforcement Cooperation

Law enforcement cooperation agencies such as INTERPOL and Europol are actively involved in fighting against cybercrime and cyber-enabled crime related to cryptocurrencies, blockchain and Darknet. These agencies are a key player on the dissemination of awareness of the emergent threats and providing trainings and tools to the National Central Bureaus of their member countries.

INTERPOL[13] Global Complex for Innovation provides training to the police is subjects such as the Darknet, black markets, cryptocurrencies and the Blockchain. In July 2015, INTERPOL provided the first five-day training specialised on the Darknet, in cooperation with the Netherlands Organisation for Applied Scientific Research (TNO) (Interpol, 2015). For that purpose, the Cyberspace lab created its own Darknet network, its own private cryptocurrency and recreated a similar black-market environment to those typically found in the Darknet. During the training participants role-played as sellers, buyers and administrators, and simulations of "take downs" from law enforcement. These exercises helped participants to improve their understanding of the technical infrastructure as well as the functioning of these technologies. Representatives from Australia, Finland, France, Ghana, Hong Kong, Indonesia, Japan, Netherlands, Singapore, Sri Lanka and Sweden attended the first training session. A second training was performed that same year in Brussels, along with a supplemental training event focused on senior law enforcement officials who needed to raise awareness of new threats to a less technical degree among a greater and more extensive audience.

In March 2018, INTERPOL held a two-day working group on implications presented through extended use of the Darknet and cryptocurrencies, covering subjects such as the surge in popularity and utility of altcoins as a potential substitution for Bitcoin, cryptocurrency mixers, lack of altcoin tracing tools and decentralised escrow services (peer-to-peer markets) (INTERPOL, 2018). Participants included police agents from over 18 countries as well as members from cyber departments of Europol. Case examples of cryptocurrency investigations were shared, along with the legal and technical challenges they faced in their corresponding jurisdictions. There was a general consensus shared on the importance of information sharing through knowledge databases, not only to facilitate investigations, but also to avoid duplication efforts. In addition to this, the

[13] INTERPOL is the world's largest international police organisation, with 192-member countries. Its role is to "connect the police to help preventing and fighting crime through enhanced cooperation and innovation on police and security matters."

working group agreed on the collective usefulness of commercial and law enforcement tools for the investigation criminal cases, reaffirming the need for compliance and corroboration in its practice. An example of these tools will be further explained later in the section *Blockchain investigations in law enforcement*.

In addition to this, INTERPOL has available a web-based learning portal called INTERPOL Global Learning Centre, which allows authorised users to access to a comprehensive offer of trainings, including Darknet investigations. Furthermore, the agency is actively conducting research on new technological advancements in cooperation with experts in Darknet, blockchain and cybercrime working in innovation companies such as the aforementioned TNO and Kaspersky Lab.

In 2016 INTERPOL, Europol and Basel Institute of Governance established a tripartite partnership to conduct a working group focusing on money laundering and the misuse of digital currencies (Europol, 2016b). The main aims for the working group were to:

1. Gather, analyse and exchange non-operational information regarding the use of cryptocurrencies as a means of money laundering, and the investigation recovery of proceed of crime;
2. Organise annual workshops and meetings for the representatives of the above-mentioned Law Enforcement Agencies and institutions to increase the capacity to successfully investigate crimes in which virtual currencies are involved;
3. Create a network of practitioners and experts in this field, who can collectively establish best practices and aid assistance and recommendations inside and outside the working group.

Continuing with this collaboration, two global workshops were held in the subsequent years. In January 2017, there were more than 400 financial investigators directly involved in uncovering money laundering and cybercrime through financial intelligence units, alongside experts on asset recovery and relevant representatives from the private sector. The two-day event had a generic focus on countering money laundering through digital currencies, with the participants reaching the following conclusions:

- There is a need of increased information sharing in the field of money laundering and digital currencies. In particular, suspicious Bitcoin addresses that threaten economic stability should be shared
- Digital currency exchangers and wallet providers should be regulated under current anti-money laundering and counter-terrorism financing legislations
- The need to take action against digital currency mixers/tumblers, designed to anonymise transactions, which hinders the work of law enforcement agencies to detect and trace suspicious transactions

The working group of 2018 had a more specific focus on "Financial Investigators on Detection, Investigation Seizure and Confiscation of Cryptocurrencies" (Europol, 2018a). Participants engaged in a more technical working group where they shared several relevant cases and best practices to solve them. Conclusions reached at the end of the event were, however, very similar to those from 2017 with the difference that 1) information sharing this time includes (additionally to the tripartite partnership) the Egmont Group and Financial Intelligence Unit Network (FIU.net) and 2) the need of a consensus for the definition of "cryptocurrencies", "digital currency exchanger", "wallet provider" and "mixer" to be included in the EU legal framework.

Europol has also a prominent role on the fostering discussion and raising awareness about cryptocurrencies. As of today, Europol has held five conferences in the last years regarding the use of cryptocurrencies of illicit activities. The 5th and most recent conference was related to the topics of tracing, attribution and demixing cryptocurrencies. Among the vast majority of law enforcement participants in the conference, a small proportion of attendants were representing select cryptocurrency exchanges and institutions such as Blockchin.info. Similar to INTERPOL, Europol brings together a variety of experts from different disciplines and practitioners of law enforcement to contribute to the development of the expert community of investigators and prosecutors. In addition to this, the European Cybercrime Centre of Europol offers trainings on the areas of cybercrime and digital forensics.

III.3.3. Private Tech and Research Companies

There is an increasing number of startups that are facilitating and creating forensic analysis software for direct use by law enforcement agencies, such as the one offered by Elliptic. Designed specifically to help law enforcement agencies delivering leads, insights and evidence of

cryptocurrency-enabled crimes, the software was designed and offered exclusively to public sector security services investigating cybercrime through cryptocurrencies. Elliptic, along with other crime-fighting software start-ups, help law enforcement agencies such as Europol and the FBI to trace cryptocurrency transactions finding patterns or clustering digital wallets associated with the targeted accounts or known criminal activity. Once they can connect wallets to specific crimes, money can be tracked across the Bitcoin blockchain network to pinpoint specific exit points through exchanges and lead investigators directly to bank accounts housing those funds (Yakowicz, 2018).

Blockchain Alliance is an organisation created in 2015 as a response to the criminalised stigma of Bitcoin after the Silk Road case. The organisation is led by the Coin Center[14] and the Digital Chamber of Commerce, in which representatives from the biggest, most important companies in the Bitcoin industry actively participate. The group aims to foster and develop a reliable forum in which authorities and regulators can consult to help combat the criminal activity related to Bitcoin by sharing information and getting technical assistance from industry experts in the aim to further develop the understanding of blockchain (Parker, 2015).

[14] **Coin Center** is a leading non-profit research and advocacy centre based in Washington, D.C., focused on the public policy issues facing cryptocurrency and decentralised computing technologies like Bitcoin and Ethereum.

IV. Threat to State Law Enforcement

The previous section outlined the way in which law enforcement has developed effective tools and methods of investigation to trace suspicious transactions in the blockchain by using a combination of aggregate data which includes IP addresses, Bitcoin keys, information provided by virtual currency exchanges, etc. However, anonymity and the ease of obfuscation is still one of the biggest problems facing investigative and regulatory agencies. There are many anonymisation techniques that help criminals conceal their identity and at the same rate that law enforcement specialists are gaining traction in busting criminal activity, criminal specialists- including their teams of coders and software developers are making significant headway in outsmarting authorities and bypassing jurisdictional laws. These techniques range from mixing bitcoins in a Bitcoin-laundry process, using more anonymous cryptocurrencies or purchasing bitcoins in rogue platforms that remain outside the scope of legal frameworks and do not comply with the Know Your Customer regulations, offering significant reward to criminals and holders of illicit cryptocurrency funds.

IV.1. Decentralisation of Cryptocurrency Exchanges

Although the entry-exit points to the cryptocurrency ecosystem are fiat exchanges, most platforms require some sort of identification proof from their customers to establish an account or open a wallet. While Bitcoin addresses are still anonymous (despite being publicly listed) in the peer-powered Blockchain, any entity having access to the data can potentially find out what and how many bitcoins were spent on certain goods or services. Due to the perceived logging of activity, many customers are not willing to use regulated fiat exchanges that seem to be compliant with law enforcement officials or regulating agencies. Rather, these proponents of an anonymous cryptocurrency seek platforms, service providers and start-up companies that operate outside the scope of the conventional financial system.

IV.1.1. Peer-to-Peer Markets

One of the most popular peer-to-peer market options is the online platform “LocalBitcoins”, run by a company based in Helsinki and currently operating in 248 countries. LocalBitcoin permits users to buy and sell their Bitcoin with fiat currencies, without limitations regarding the size of transactions. Users post advertisements and anonymous payments can be made in cash either by

meeting in person or by depositing fiat currency into a bank account of the seller. Trust is generated based on the reputation and feedback of the sellers, and embedded in an escrow and conflict-resolution service feature on the platform. Since the transactions are considered peer-to-peer, both parties count as a "user" under the FinCEN regulations. Since neither the users nor the platform LocalBitcoins fall into the category of *money services business*, both parties are exempt from providing a valid identity documentation and do not require a record of the transaction.

In August 2016, LocalBitcoins operated a volume of transactions of roughly 14 million USD per week. The company ceased to operate in Germany after being contacted by the German Federal Financial Supervisory Authority which stated that their business model directly conflicted with regulations implemented in the country (Rizzo, 2014). Two men were charged for money laundering and for running an unlicensed money transmission business in Florida that operated in unison with LocalBitcoins, where the men reportedly moved over 150 Bitcoin in a six-month span through the platform. After this suspicious activity, the CEO of LocalBitcoins, Jeremias Kangas, stated that the company wasn't aware of those charges and that they relied in the users to follow the laws of their country and that the company was working on implementing the proper tools to have more scrutiny over the users' activities. Interestingly, when LocalBitcoins was blocked in Russia because of a finance ministry proposal to criminalise the use of Bitcoin, LocalBitcoins published specific indications to avoid the access restrictions. As of today, LocalBitcoins requires ID verification documents for listing and advertisements hosted on its site but does not for users replying to an advertisement. This loophole still leaves an open door for customers who want to buy cryptocurrency with total anonymity. Moreover, there is still no limit in the total amount of LocalBitcoin transactions.

IV.1.2. Decentralised Exchanges

Due to the difficulties in maintaining privacy in protocols like Bitcoin and Ethereum, software developers have designed a tool to trade cryptocurrencies without the need of a central exchange. Bisq is a decentralised exchange also known as peer-to-peer exchange network (Bisq.network, 2018). This **decentralised exchange** is a tool based on an open source software from which the user can buy or sell both fiat currencies and cryptocurrencies with no previous registration. Bisq is not a company but an open source project. On its website, it states that "Bisq does not know the traders. No data is stored on who trades with whom." and "Bisq does not require registration. This

means privacy is maintained, there are no "approval" wait times, and identity theft becomes impossible." Although this initiative differs in many aspects from the previously described platforms, all of the aforementioned services directly bypass regulations for money services business in the US and Europe. Users must take the responsibility to make sure they are not evading the law or applicable regulations. For instance, in a Bisq forum there are multiple posts where customers voice their concerns about the limits of cryptocurrencies that users can receive per day in USD. If users sell cryptocurrencies for more than 1,000 USD, they would not qualify as a monetary service provider at FinCEN and would therefore be a violation of the law. Having said, many users operate multiple accounts at lesser values to evade this policy.

Regulations are structured in a way that the force of the law applies to cryptocurrency exchangers: they are responsible for their customers and therefore, reserve their rights to inform them about or suspend/delete an account that does not comply with their listed requirements. Contradictorily, companies such as LocalBitcoins and Bisq have a business strategy that transfers the responsibility from the platform to the individual users, making every customer responsible for its actions since they are peer-to-peer markets. This leaves an open tool for money laundering opportunities and their customers responsible for their actions and any breach of applicable regulation enacted in a certain jurisdiction.

IV.2. Proliferation of Highly Anonymous Altcoins

After the successful launch of Bitcoin, alternative cryptocurrencies (known as altcoins) emerged. Altcoins typically function the same as Bitcoin: they are peer-to-peer electronic coins, supported by a unique blockchain architecture, are created through a complex computational mining process, and offer cheaper alternatives to conventional banks or financial institutions.

The innovations introduced through some altcoins include enhanced transaction speed, enhanced connectivity – DNS resolution, and improved privacy, among others. As in the case of Bitcoin, depending on the use that its customers give them, altcoins can behave as an asset for investment or they can be used as actual currencies with enhanced characteristics, usually building on the simplistic model created by Bitcoin. While some of these cryptocurrencies focus more on the benefits for business purposes, others are more focused on aspects such as privacy and anonymity.

Altcoins such as Bitcoin Cash, Litecoin, Ethereum and Ethereum Cash have become the most popular altcoins at the present moment, and many cryptocurrency exchange platforms support these in their exchanges. For instance, Bitcoin cash reportedly processes more transactions per day at a faster speed, and reduced fees as compared to traditional Bitcoin (Bitcoin.com, 2018), which can make this alternative more attractive to cryptocurrency users.

The emergence of altcoins with specific and unique features can be considered a holistic response to the shortcomings of Bitcoin in direct relation to privacy and prospective regulation. As previously stated, with advanced analysis apparatuses, Bitcoin addresses in the blockchain can be traced, and with enough regulatory measures, Bitcoin owners might ultimately be identified by authorities or financial regulators through timestamps and specific transactions linked to specific accounts or wallets. Having said, there are some altcoins created specifically to address these issues- Dash, Monero and Zcash have been listed among the top most anonymous cryptocurrencies (Corcoran, 2018). A higher degree of anonymity is usually payed through higher fees and tariffs on every transaction, as well as longer (and allegedly more secure) processing time.

Enhanced anonymity is a source of concern and poses a direct threat for law enforcement operations. According to a report from Europol (2017b), even though Bitcoin is still the preferred cryptocurrency in criminal markets, Monero, Ethereum and Zcash are amongst the most popular altcoins used for illicit purposes, specifically in the selling drugs and firearms in black markets. The exchange of Bitcoin to these more anonymous cryptocurrencies in small increments augment the complexity of cryptocurrency investigations of the police and is considered one of the most effective techniques to conceal criminals' identity online.

Monero is growing in popularity thanks to its offered security and privacy features. The cryptocurrency is essentially a privacy-centric coin which includes transactions in its main offering, meaning that a single coin cannot have its entire transaction history revealed. Therefore, transactions cannot be attributed to any particular address and the amount being transferred is hidden, as well as all transaction histories. This strict secrecy has made the coin very popular in the Darknet. AlphaBay was one of the few markets in the Darknet which offered the possibility of buying and selling in Monero. When the online market was shut down in July 2017, the authorities confirmed that the owner held Monero cryptocurrencies, but the amount remains uncertain even after his arrest. Due to its growing popularity, Monero is increasingly being accepted in a number

of black market exchanges, and in 2017 the first ransomware attack asking for Monero was deployed (Abrams, 2017). According to one of its core developers, "even with big data analysis, the ability to farm anything out of the metadata is cryptographically negligible" (Greenberg, 2017). This is essentially the main reason why the extended use of this cryptocurrency poses a serious threat for law enforcement, given the fact that there are no available analysis tools yet that are capable to trace Monero.

Another popular alternative to Bitcoin, Ethereum, was launched in July 2015 and is considered the second most popular cryptocurrency after Bitcoin in the market. Due to its original characteristics, Ethereum might reinforce cybercrime-as-a-service models in the Darknet (Europol, 2016). While this has yet to be seen, Europol has spotted at least at least one black market in the Darknet accepting the altcoin for payments. In addition, Zcash is additional cryptocurrency that focuses on improved privacy in transactions. This virtual coin hides the sender, recipient and the amount of the transaction. With enhanced layers of security and anonymity, Zcash is another cryptocurrency currently accepted in many black market sites which is expected to gain popularity over the following years with increased use and more refined reputation.

To acquire such coins, however, is a multi-faceted task since it requires a series of prior verification and initiative. Moreover, its use is restricted only to marketplaces which accept such coins. For example, if a user wants to buy Monero, first they are required to purchase Bitcoin in a fiat exchange service – such as Coinbase – in order to purchase the altcoin via a crypto-to-crypto exchange service. Having said, it is important to restate the fact that through the first step of buying Bitcoin, all companies providing this service are liable to comply with regulations under their jurisdiction and, as seen in the example of Coinbase, there are KYC procedures that weaken the anonymity of the user through direct identification measures. Certainly, a criminal could initially provide false information about his/her identity, but after a certain amount of revenue, service providers would require that he/she provide further documentation to verify identity and ownership of the wallet. Large transactions and accumulated incomes would inevitably be flagged through the Coinbase network and be reviewed by the service provider and forwarded to competent authorities for corroboration.

As an asset, alternative cryptocurrencies are becoming increasingly popular, for both investors and idealistic users looking for more private and secure currencies. They have also gained the backing

of large and reputable multinational companies such as JP Morgan and Microsoft and have even been adopted by banks such as Santander, Bank of America and UBS (Harris, 2018). Their increasing popularity and credence predicts a promising future for virtual currencies. Even when Bitcoin has the advantage of being the most popular and widely used coin, improved features on new cryptocurrencies will compete in the market whether or not governments and the competent authorities are prepared for their proliferation.

Regardless of the legality of use that people give to such cryptocurrencies, new features and consequential utility may influence the userbase, and this will increase the risk of triggering a new speculative bubble (Greenberg, 2018). As market capitalisation of some cryptocurrencies mature, it is possible that in their legitimate pursuit for profit, some investors will be unknowingly contributing to coins that are used for illegal services and by criminals and their syndicates.

IV.3. Bitcoin Mixers

When it comes to cryptocurrencies, there are certain variations with respect to traditional money laundering. First, money "does not go anywhere" but it is crossed with other people's money hosted online in a digital wallet or account. This is enough to make tracking difficult, even through the Blockchain.

Bitcoin mixers, also known as Bitcoin laundry services and Bitcoin tumblers, are services used to enhance the anonymity of the Bitcoin's owner by mixing the funds of the customer with those of the other customer. These services are often used with the intention of obscuring the traceability of the transactions made. In the world of Bitcoin, this is would be the analog of money laundering since it directly hides the flow of money and does not keep a record of the transaction at all. Since all transactions are recorded publicly in the Blockchain, some users want to ensure their anonymity and, therefore, resort to these services to pool their coin holdings and use a collective account so that they are not individually pinpointed through the use of their cryptocurrency.

These services never operate with national currencies but only with virtual currencies. According to the definition on FinCEN guidance report (2013) "An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency". A mixer exchanges virtual currency for virtual currency, and therefore, even if it does not operate with state-backed currencies, it counts as an exchanger, and should comply with the regulations.

According to the CipherTrace software start-up, services that allegedly "clean dirty funds" are widely available and some of them have even been featured and advertised in Google AdWords (Kharif, 2018). Bitcoin mixers are highly valued by criminals who want to launder their bitcoins because of the perceived coverage offered through participation. Following the findings of the aforementioned study of Elliptic, Bitcoin mixers are widely used by dark market users, and cybercriminals who engage ransomware attacks. In their case anonymity is not only a matter of privacy, but a key step to complicate police or tax authority investigations (Robinson and Fanusie, 2018).

In essence, when bitcoins are mixed, the user is sending its money to an anonymous service that will then respond by sending the same amount (minus a fee) but composed of cryptocurrencies which belonged to other users. This way, the currencies of user A can be traced back to user B and those of the latter are traceable to user A. This will highly complicate the act of tracing transactions and funds since the mixer multiplies the number of users involved in the operation and, as a result, complicates the exact holding and use of each participant in the mixer. To get the best possible privacy, many mixers recommend sending multiple payments to different addresses. This step makes it necessary to have various Bitcoin accounts and to be willing to pay the fees for each transaction. In addition to this, to make it even more untraceable, mixer services offer to option to receive the payments with a certain amount of time difference.

For instance, Bitcoin mixers were first uncovered as a widely used tactic by users of the Silk Road. To register as a selling user, an amount must be paid in bitcoins as a deposit to verify the legitimacy of the seller. Sellers would then use mixers to make this payment anonymously. A section of the Elliptic website, Law Enforcement, offers an application in which bitcoins can be tracked. This particular service better legitimises the existing connection between the old Silk Road portal and the services of mixers like Bitcoin Fog, one of the oldest services in existence.

One particular case which directly relates bitcoin mixers with money laundering is the shut down of Coin.mx case. Coin.mx was running bitcoin laundry services under a shell company in Florida and in 2016 its two owners were accused of not registering their company as a MSB and knowingly laundering bitcoins which were coming from ransomware attacks. Although they were facing an initial imprisonment of twenty years, they finally were sentenced for only five years and a half (Nichols, 2017).

Bitmixer, the most popular bitcoin mixer in 2017 earned revenues of 65,000 Bitcoin per month until their closure just three days after AlphaBay and Hansa were shut down by American authorities. The owner of the mixing service stated that the shutdown was due to his own convictions in order to contribute to a cleaner Bitcoin ecosystem. However, some users of Bitmixer speculated that the real reason was due to pressure from law enforcement and potential fear of being linked to illegal activity from their role in facilitating payments and transfers in illegal marketplaces (Southurst, 2017).

The main problem with Bitcoin mixers is extra-judicial status and their inadvertent ability to facilitate criminal transactions. These services are usually run by experts in digital anonymity and are most commonly headquartered in remote countries were Bitcoin lacks value as a currency. These characteristics enable administrators to run and operate their businesses free of regulation from third parties and normally outside the scope of conventional financial law. These advantages are strongly reflected in the previously mentioned study conducted by Elliptic: Table 1 in Appendix displays in percentages the distribution of illicit Bitcoin volume into conversion services by region. Between years 2013-2016 the highest percentage of illicit Bitcoin flows into conversion services was conducted in unknown countries, being 52.03% the average. Some law enforcement entities advocate the banning Bitcoin mixers- for instance, in a global conference organized by the Basel Institute on Governance, Europol and Interpol, dedicated to countering money laundering and digital currencies, the following recommendation was made:

"*All countries are advised to take action against digital currency mixers and tumblers. Such services are designed exclusively to anonymize transactions and to make it impossible for Law Enforcement Agencies to detect and trace suspicious transactions. The existence of such companies should not continue to be tolerated…"*

Banning the use of mixers would imply an inconvenience for those who are concerned about their anonymity, but at the same time would potentially facilitate law enforcement labours.

V. Analysis

The complexity and dynamism of the cryptocurrency system make it difficult to determine whether their use and existence pose a direct threat or act as an investigative opportunity for law enforcement and financial agencies. In what ways will the internationalisation and increased use of cryptocurrencies empower or hurt state actors and criminals? Even so, how will law enforcement agencies maintain their ability to govern and regulate cryptocurrencies and blockchain transactions under the currently ambiguous legal framework? While some judgements can be made with a fair degree of certainty, other considerations need to be taken more carefully due to the changing environment of cryptocurrencies. Having said, it is important to highlight and present the utility of cryptocurrencies from the perspective of law enforcement agencies and cybercriminals alike.

V.1. Cryptocurrencies as an opportunity for law enforcement: tools and regulation

First, Bitcoin is still the preferred cryptocurrency on fiat exchange services. This creates a bottleneck effect that enables tougher controls over the conversion points between state backed currencies and the cryptocurrency ecosystem. This increases the opportunities for financial institutions applying KYC measures and forensic analysis tools to detect suspicious transactions that would be covering money laundering operations. In this regard, Bitcoin, as a “gateway” to other cryptocurrencies, has become an ally of law enforcement because of the relevance it has gained over the years. Governments have put the attention it deserves to establish the necessary research and development in tightening surveillance of the service and implementing regulations on service providers involved in facilitating cryptocurrency transactions.

At the same time, many private sector startups have begun to flourish in the new market for forensic analysis tools in regards to the newly empowered blockchains. This alone represents a step forward, towards a more transparent cryptocurrency framework. It is in the best interest of law enforcement specialists and by extension, to public sector governments to continue fostering Bitcoin as a way to surveil cybercrime by establishing norms and identifying or detecting criminal behaviours before the coins can be converted into fiat currencies.

Records of cryptocurrency transactions in the blockchain become an opportunity for law enforcement investigations with the emergence and improvement of analysis tools. Some firms can already count on software which can detect whether bitcoins are coming from Bitcoin mixer services or black markets in the Darknet. As long as technologies continue improving in this direction, anonymising techniques will be less effective and law enforcement will benefit from that.

Likewise, the enhancement of law enforcement investigations is related to the knowledge of the behavioural study of transactions and wallets. There are some patterns that might indicate potential criminal activities involved. Identification of patterns, as well as clustering are tasks that currently are carrying out a set of algorithms in blockchain analysis software, such as the publicly available "Chainalysis" or other more specialized law enforcement tools seen in the "Law enforcement tools" section in chapter II. As these technologies progress, it would be possible that algorithms not only implement a model, but also gets refined with experience. This technology is known as *machine learning* and it has full potential for development in the field of cryptocurrencies to help law enforcement investigations. This could prove extremely useful in the detection and deterrence of criminal activity through online financial services and cryptocurrency holdings.

In light of momentum and development in regulating cryptocurrencies, criminals are adapting to the current environment by adopting new techniques to commit their illicit activities utilising the Darknet. The disruptive emergence of cryptocurrencies and anonymising techniques pose a greater challenge for law enforcement agencies to fight against crimes leveraging in such technologies, including the purchase of illicit goods in the various marketplaces online, especially considering the ability for them to be used to purchase ransomware attacks and cybercrime-as-a-service. All national centre bureaus should become acquainted with this problem and its implications for the general public, and they should count on the expertise and tools to conduct the necessary investigations. In this regard, international cooperation between law enforcement agencies is key to disseminate valuable information and share knowledge on best practices.

In the US, fiat exchanges and crypto-to-crypto exchanges have implemented new KYC policies and other AML guidelines to comply with the regulations issued by the Bank Secrecy Act in 2013. The FinCEN assessment against the foreign-located cryptocurrency exchange BTC-e proved that US agencies and regulations are being effective to combat cryptocurrency laundering. Generally,

most of the exchanges are getting more compliant and rely on good reputation and trustworthiness as a business strategy to attract more Bitcoin users with added features of more transparency and security in its holding and use. Nevertheless, not all countries are yet implementing virtual currency regulations with the same solidity. In Europe, the 5th Anti-Money Laundering Directive entered into force on the 9th July 2018, and Member States of the European Union will still have time to implement it into existing frameworks until January 2020 when it is enforced across the EU. This uneven action increases the challenges to target criminals attempting to launder their funds, as well as to conduct successful law enforcement investigations. This difference between the enforcement of regulations has been reflected in the prevalence of Bitcoin laundering in Europe over the US in the last years (Robinson and Fanusie, 2018). Referring again to Table1 in the Appendix, between years 2013-2016 Europe accounted for approximately 37% of the distribution of illicit Bitcoin volume into conversion services on average, largely exceeding the percentage of north America. It is expected that with the enforcement of the 5th Anti-Money Laundering Directive by its Member States these numbers will decrease.

Nevertheless, this new regulation only includes exchange services that deal between virtual currencies and fiat currencies but does not take into consideration businesses that exchange virtual currencies with virtual currencies (crypto-to-crypto exchanges). This flaw makes the AML regulations in Europe less robust than in the US since Bitcoin mixers and other crypto-to-crypto exchanges are under no obligation to comply with AML polices within the EU jurisdiction. Lack of AML programs such as the application of KYC policies in crypto-to-crypto exchanges could permit significant cryptocurrency laundering.

The US government is currently leading the way in terms of cryptocurrency regulation, closely working with international financial institutions operating cryptocurrency exchanges. However, the proportion of laundered coins has kept steady since 2015 when anti-laundering measures were first introduced. This indicates a learning curve of criminals due to the maintained success rate of laundering money. A possible loophole is still a significant rate of bitcoins that are being laundered through exchanges and gambling sites which are often outside the scope of traditional cryptocurrency financial platforms (Robinson and Fanusie, 2018). Poor law enforcement in conversion service types results in successful illegal operations and undermines the effectiveness of finance law and order. Therefore, it is important to include all kinds of exchanges, platforms and markets accepting cryptocurrencies when implementing regulatory policy.

For instance, a former director of FinCEN noted in a statement in 2013 that "legitimate financial institutions including virtual currency providers do not go into business with the aim of laundering money on behalf criminals" (Lee, 2013b). However, three years after the application of the anti-money laundering program which included virtual currencies, FinCEN detected that the company BTC-e was operating illegally outside the jurisdiction of the US. By then, BTC-e was a virtual currency exchange platform which accounted for 3% of the total bitcoins in circulation. Contrarily to the former director of FinCEN, BTC-e was run by a criminal who used his own company to launder money and willingly provided services of money laundering to other cyber criminals. While this should not be assumed as a rule for all the existing exchange platforms**,** it should constitute a substantial warning sign for competent authorities to increase the level of scrutiny for these exchange platforms which serve as a gateway to the financial system. This illustrates the need of FinCEN and equivalent financial authorities in other countries around the world to increase the monitoring of existing exchange platforms and keep record of the new ones wherever the exchange platforms trade with the currency under the jurisdiction of that financial authority. This indicates the specific need for collaboration on the level of policy and regulation across state, regional and continental borders.

In this regard, the 5th Anti-Money Laundering Directive of the European Commission proposes that transparency should be enhanced by providing enough information regarding the ownership of the exchange services. These actions should help to detect suspicious behaviours and investigate connections between exchange platforms at early stages to thwart money laundering and disable criminal activity before it is committed. As previously seen, Coin mx and BTC-e cases have some similarities. Both operations are conducted by high profile cybercriminals who first conduct a cybercrime. The stolen Bitcoin funds at Mt Gox in the BTC-e case, and a ransomware attack in the Coin mx case. Later, the criminals run their own company of Bitcoin mixing services and Bitcoin exchanger in order to launder their funds and finally convert them into fiat currencies.

This signifies the need for regulatory and investigative initiatives to comply with various departments of homeland and international security and include them in their ranks to ensure that cryptocurrency specialists are working alongside, not simultaneously with organised crime or terrorism units.

There are concerns that tough regulations could encourage Bitcoin businesses into secrecy (Salmon, 2014). It is important that FinCEN and the financial intelligence units in Europe take

enforcement actions to make sure that MSB are registered and are compliant with effective identification measures. Only by strengthening AML reporting obligations from financial companies law enforcement will have the necessary information when required. On the contrary, a failure on detecting non-compliant exchange companies would be a blind spot for law enforcement investigations. The application of Know Your Customer and Customer Due Diligence procedures is especially relevant to Financial Institutions which issue and implement the regulations; to both types of exchange platforms which are obliged to comply with the AML regulations, and for law enforcement agencies which could use an unexplained massive wealth income as a source of evidence for investigations on illicit trading in black markets. Progressive compliance from virtual currency exchange companies might lead to a divergence of customers: customers willing to invest or purchase with a less degree of anonymity, in return of a reliable company with a good reputation of market integrity and lower fees; and customers who value privacy above all and prefer to engage with companies who do not ask for identification details but ask for much higher fees (sometimes up to 50%).

In order to enhance the effectivity of European AML regulations, regulators in each EU Member State should work to improve the current national regulatory structure by focusing on specific rules for cryptocurrencies and exchange platforms, in unison with other policies enacted within the European Union. First, by fostering and ensuring cooperation between Bitcoin exchangers and financial regulators; second, promoting the widespread use of SARs with the aim of alerting law enforcement regarding a potential illicit activity; and third by including in the AML regulations exchange services that involve cryptocurrency to cryptocurrency exchanges. This could also be a way in which cyberdefense and cybercrime units can incorporate the expertise of the private sector by engaging them and including them in their spheres of influence over the regulation of cryptocurrencies and its proper use within the current legal and financial framework.

V.2. Current and future challenges

As of today, highly anonymous altcoins pose a direct threat to law enforcement agencies. A few days before the dark market AlphaBay was closed, it was announced that the market would soon accept the highly anonymous altcoin Zcash. Although this change would never be implemented, it is something likely to happen in the near future and law enforcement agencies have expressed

their concern about this matter (Europol, 2017b). If future black markets start supporting Monero, Zcash, Dash and other highly anonymous cryptocurrencies, the police and other authorities could face serious difficulties to trace illicit transactions and arrest the criminals behind it – not only people involved in the drug and arms trade, but also in cybercrimes such as ransomwares as well as bitcoins laundering, which would go undetected and could potentially result in the creation of obscure altcoins that have advanced criminal protections embedded in their functionality. Nevertheless, the adoption of altcoins into existing platforms is not a simple step. For example, Zcash has many technical similarities with Bitcoin which is partly the reason why it is supported by most wallets and cryptocurrency markets. However, Zcash offers various anonymity "shields" and in order to be fully anonymous, Zcash requires significantly more wallet development than most currently offered on the market. In the example of Monero, it experiences similar difficulties in terms of finding wallets that can support the complexity and advanced coding rooted in its blockchain (Knight, 2018). As technologies available to support these coins emerge, they will become more popular in term of usability and it might not be long before they are considered mainstream currencies. Before this happens, the police and financial authorities will need to have the latest and most advanced software analysis tools in their arsenal as well as new advancements in tracing techniques to prepare them for future challenges and cybercrimes. A failure in doing so would create a great advantage for criminals in the foreseeable future due to the constant competition to outsmart the respective authorities.

Bitcoin mixers are still one of the current challenges for law enforcement investigations. As previously stated, Bitcoin mixers are laundry services for Bitcoin that are usually located in remote countries which do not have effective legislation concerning financial crime or established a sound cryptocurrency framework. Their status falls into the "exchanger" category of the US regulation, but they are offshore and outside the jurisdiction. Trying to establish a KYC policy in a Bitcoin mixer is contradictory in its nature because the service would lose its fundamental purpose.

After the shutdown of AlphaBay and Hansa, the closing of Bitmixer in 2017 could be a warning sign for other Bitcoin mixers. After the police operation, many accounts, names and Bitcoin addresses were identified. Further investigations from law enforcement could have led to the arrest of the owner of Bitmixer, provided that enough evidence would have linked the company to illegal activity in dark markets. Due to its popularity, it is very likely that Bitmixer was involved in Bitcoin laundering coming directly from those markets by its userbase. The decision of closing the

mixer was possibly a self-defense move in the fear of being caught by the police, as many Bitcoin users assert, and could be the first of many other cases in the future where law enforcement use coercive or threatening measures to ensure the closure of criminally-charged facets of cryptocurrencies and its support network.

Nevertheless, some of these services suffer from serious limitations. One of their flaws is the tendency to fail when dealing with large amounts of money (Smith, 2016). In such cases the laundering process can be itself identified in the blockchain because when a large amount of money is sent, even to various accounts, this can be seen in the blockchain. In addition to this, a study which analysed several Bitcoin laundry services found out that even the most well-established mixers have security and privacy limitations (Balthasar and Hernandez-Castro, 2017). The study ultilised a series of blockchain analysis tools, including Chainalysis, and found out that the worst Bitcoin mixers have an algorithm that is itself quite poor in its design. In addition to this the scarcity of transactions makes it even easier to identify Bitcoin addresses. These mixers are characterised also for having also security weaknesses that make it easy to find IP addresses from users and, therefore, to establish a link with the individual. The most reputable mixers were more difficult to trace with commercially available tools, however, the study suggests that with a few more steps in an investigation it would be possible to uncover the identity of a user of this service. These limitations constitute an advantage for law enforcement investigations when tracing Bitcoin transactions coming from illicit black markets.

As is the case with black markets, when a bitcoin mixer closes, the flow of bitcoins redirects to other mixers. Criminalising these services is an alternative that has been already put on the table by some experts from INTERPOL, Europol, the Basel Institute on Governance. While proponents of these services would claim that this would undermine the possibilities for Bitcoin users to keep their privacy, there are other means to maintain privacy which do not entail the use of Bitcoin mixers. By using wallet services, users of Bitcoin can prevent being traced with blockchain analysis tools by any third party. This is possible because many wallet services have a similar anonymising functionality. When a wallet service guards the funds of a client, bitcoins are kept in a "pool" with other bitcoins, and whenever they are withdrawn, the bitcoins are different from the ones deposited (Robinson, 2018). Contrary to mixers, wallet services ask for identification information from their customers and keep record of their transactions. While this information, like in the exchange services cases, is not publicly available, if required by law enforcement

agencies or financial intelligence units, they would be obligated to send and forward the information to authorities in the case of suspicious activity. If such alternative would be widely accepted as an anonymisation measure within the "public" sphere of blockchain, mixers would be one step closer to be criminalised.

Although this could potentially solve the problem of privacy versus AML compliance, users concerned by their privacy are more keen to use methods that give them total anonymisation from public access to blockchain as well as from government entities. Yet, it cannot be assumed that mixers are entirely illegal and used to conceal illicit sources of Bitcoin. For instance, Elliptic found out that only 16% of the funds entering mixers were coming directly from illicit sources. This percentage might increase when taking into consideration transactions made in between, as well as within a bigger sample[15]. As of today, Bitcoin mixers as still widely available, and represent an increased challenge to law enforcement investigation when tracking suspicious transactions. While mixers are a powerful tool for criminals, its use should justify further investigation in the source of funds when someone is using it. Paradoxically, whoever wants to keep more anonymous might be the one in the spotlight.

In addition, decentralised exchanges are another powerful tool for anonymity. Compared to regular cryptocurrency exchanges, decentralised exchanges account for a very small proportion of cryptocurrency transactions and many of them are still in the experimental stages. This leaves these types of exchanges in a position that does not fall inside the regulation framework for cryptocurrency exchangers and, therefore, implies that decentralised exchanges do not need to have KYC procedures. As is the case with highly anonymous cryptocurrencies, it is very unlikely that the growing transparent ecosystem will embrace these technologies if they cannot be regulated and implement identification procedures. In fact, many decentralised exchanges highlight their lack of KYC policies as a marketing strategy to stand out among other exchanges (Medium, n.d.). It is likely that criminals will increasingly rely on them in the search for avoiding identification measures. If such case happened there is the chance that users could easily transact large amounts of funds across national borders with no limits and with a decreased chance of being discovered. In such case, similar to what has happened with regular exchanges, regulatory authorities should

[15] "The parameters of the study were purposefully narrow to keep the data manageable, which likely minimized the volume of illicit bitcoins considered for analysis" (Robinson and Fanusie, 2018).

draft the necessary amendments and ratify them as laws before these types of exchanges become more widespread.

Being caught does not seem a deterrent measure for criminals to stop. Going back again to the succession of AlphaBay after Silk Road market, the arrest of Ulbricht did not seem to stop the "business model" of the black market, but rather to improve it. When black markets are shut down, users and administrators migrate to other markets. Shutting down a market does not put an end to criminality in the Darknet, but rather it is a stimulus for developing of new ways to disguise from the police. The first online black market, Silk Road, was innovative in the sense that it was run exclusively with Bitcoin. After its shutdown by the FBI AlphaBay took over the leading role in the black market. In addition to Bitcoin, AlphaBay supported other cryptocurrencies such as Ethereum and Monero. These new features added another degree of complexity for the police: not only they would have to investigate transactions in Bitcoin but also in other cryptocurrencies. Bringing in new altcoins did not impede the police to target the administrator and shut down of the market with enhanced analytic tools. This escalation of techniques for hiding and catching has a reminiscence to "the cat and the mouse game", which is fostering innovation from both sides and where the eventual winner will be the player that counts on the most relentless technology.

Criminals engaging in illicit drug selling businesses, cybercrime and money laundering, have a lot to lose if they are caught by the police. While Ulbricht's fortune in USD was 1.3 billion, he was sentenced for a lifetime in prison. Alexandre Cazes, the co-founder of AlphaBay committed suicide when arrested in Thailand. Vinnick, from BTC-e and Mt Gox case was arrested in Greece and has recently been extradited to France were he will be judged for defrauding thousands of people including 100 French nationals (Kantouris, 2018). Beyond the abilities of the police for tracing and arresting criminals, the severity of the measures taken by judges on repeated cases will have an in impact on the potential deterrence for future cases. In the meantime, the opening and shutdown of black markets will continue offering opportunities for law enforcement to further track and arrest criminals, and for criminals to conduct their illegal activities while hiding from the police.

V.3. Potential future scenario of cryptocurrencies

The cryptocurrency ecosystem is diverging into two worlds; one is characterised for its compliance with the law and its transparency and the other is going underground where the potential for committing illegal activities gathers.

Between the two diverging worlds of transparent vs. anonymous cryptocurrency ecosystems, the most prevalent one is the transparent ecosystem. Amidst the growing highly-capitalised firms and financial institutions calling for AML compliance it is unlikely that they will support initiatives aiming for full privacy. However, the growth of Monero, Zcash and other coins is undeniable. Cryptocurrencies are becoming a true threat when their partial anonymity turns into true anonymity. The rise of highly anonymous altcoins is a real threat for law enforcement investigations, because it is extremely complex for the police to develop further knowledge on multiple, smaller and more obscure cryptocurrencies. As of today, law enforcement is able to link transactions once bitcoins have been exchanged with coins such as Monero and potentially trace them. However, if analysis software does not advance at the rate of the complexity of criminal activity, it will be unable to face this challenge when coins such as Monero are more widely used by criminals. Having said, there is a big chance that this altcoin will be greatly stigmatised, as it happened with Bitcoin in the aftermath of the first major Darknet shutdown, the Silk Road market. Conversely, this could positively affect the Bitcoin perception and trust, by broadening the breach between the "transparent ecosystem" and the "anonymous ecosystem", augmenting the popularity of the former, and worsening the reputation of the latter.

While a more anonymous ecosystem should not necessarily be linked with illegal activity, its lack of transparency regarding the identity and its mismatch within the AML laws takes cryptocurrency ecosystem completely underground. The two ecosystems will be connected by the "nodes" of the variety of centralised and decentralised exchanges, by offering the user the possibility to buy Bitcoin and then trade it to Monero (or other altcoins). But the second underground ecosystem will be more likely the operational environment for illicit activities. This dichotomy could serve as a clearance filter leading the efforts of law enforcement investigations towards the underground world of cryptocurrencies. In the meantime, financial institutions and financial intelligence units would continue "patrolling" cryptocurrency transactions, with blockchain analysis tools and KYC procedures. Since these two worlds are not disconnected, the analysis tools already available

should be effective enough to link transactions. For instance, a suspicious activity report is not very effective on its own, but it could be a powerful tool in combination with an analysis in the blockchain and a law enforcement investigation. As seen in the previous example of Europol in the "Expansion of Cooperation Networks" and in the Case Study 1 "BTC-e money laundering and stolen bitcoins from Mt. Gox", cooperation between law enforcement and FIUs was key to target the criminals. This inclusion and collaboration among existing agencies can better protect the peer-to-peer network and keep an advantage for law enforcement agencies if there are voluntary or specialised private sector experts working to curb cybercrime and the misuse of cryptocurrencies.

VI. Conclusion

Cryptocurrencies and their related technologies are constantly evolving. As of today, most cryptocurrencies and especially Bitcoin and its respective blockchain technology have proved to be an ally for law enforcement investigations. The mainstream of Bitcoin has been leveraged first by criminals and later by law enforcement agencies which rely on blockchain to conduct their investigations. Available analytic tools for law enforcement are sufficiently effective to detect and reveal the identity of criminals behind many illegal operations. Some of these tools have been developed for the explicit purpose of law enforcement investigations, such as the Analysis Framework of INTERPOL, and others for commercial purposes, such as Chainalysis. These softwares have the capacity to detect suspicious transactions, determine whether an address is involved in illegal activities and identify the transaction patterns of criminals. In addition to being an investigation opportunity for law enforcement, these tools can give valuable insights on the behaviour patterns in the blockchain that can be utilised in further investigations.

Likewise, regulatory bodies have issued and enforced the necessary AML measures to fight against money laundrering and gather information of suspicious activities carried out through financial institutions. Many cases have proven that collaboration between financial intelligence units and law enforcement can be significantly beneficial to detect transactions coming from illicit sources.

In Europe, as the 5th anti-money laundering directive has been issued very recently and its Member Countries will gradually enforce it, with the deadline of January 2020. A successful implementation of the 5AMLD will depend on the cohesiveness of its Member States on enforcing it as well as on the collaboration of financial institutions with the financial intelligence units. An interesting point of the new regulations is the demand for more transparency regarding the ownership of exchange services, given the previous involvement of some cryptocurrency exchangers in money laundering and cybercrime, such as in the BTC-e and Coin.mx cases. On the other hand, the lack of specification of crypto-to-crypto exchanges within the EU regulatory framework constitutes a loophole that will enable Bitcoin mixers and other related services to operate within the European jurisdiction without applying KYC measures. This leaves an open breach that increases the complexity of law enforcement investigations.

In addition to this, Bitcoin laundry services are commonly used by criminals trying to obscure the source of their funds. These services have proved less effective than they claim as well as having some important security flaws. Law enforcement can greatly benefit from these weak points when tracing Bitcoin addresses coming from black markets.

The near future envisions the potential widespread adoption of fully anonymous altcoins such as Monero and Zcash. This poses a serious threat for law enforcement investigations. With such features, criminals are able to hide behind fully anonymous coins that can avoid analytic and the identification techniques utilised so far. Technological advancements will determine the effectiveness of law enforcement agencies in coping with it. Additionally, decentralised exchanges are another threat factor for law enforcement. However, today's lack of popularity of these platforms has not kept the attention of regulation authorities. Depending on their evolution in the future, they might be subject to restrictive laws in order to prevent money laundering.

Finally, with the increasing adoption of AML programs from many cryptocurrency exchanges, the cryptocurrency world is diverging into a more transparent and a more obscure ecosystem. This dichotomy is likely to channer illegal activities in the cryptocurrency underground.

Bibliography

Abrams, L. (2017). *Star Trek Themed Kirk Ransomware Brings us Monero and a Spock Decryptor!*. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/star-trek-themed-kirk-ransomware-brings-us-monero-and-a-spock-decryptor/ [Accessed 14 Jul. 2018].

Balthasar T., Hernandez-Castro J. (2017). *An Analysis of Bitcoin Laundry Services*: NordSec2017 - Nordic Conference on Secure IT Systems, At Tartu, Estonia pp. 297-312

Bitcoin.com. (2018). *Bitcoin Cash compared to Bitcoin Core* – Bitcoin.com. [online] Available at: https://www.bitcoin.com/info/bitcoin-cash-compared-to-bitcoin-core [Accessed 24 Jul. 2018].

Bisq.network. (2018). *Bisq - The decentralized Bitcoin exchange.* [online] Available at: https://bisq.network/ [Accessed 29 Jul. 2018].

Brown, S. (2016). *Cryptocurrency and criminality: The Bitcoin opportunity.* The Police Journal: Theory, Practice and Principles, 89(4), pp.327-339.

Breu, Stephan and Seitz, Theodor G.,(2017). *Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society* (November 27, 2017). Forthcoming, Legal Impact on the Economy: Methods, Results, Perspectives, (eds. Vaypan, Egorova) Moscow, 2018. Available at SSRN: https://ssrn.com/abstract=3081911

Brandom, R. (2017). *Coinbase ordered to report 14,355 users to the IRS.* [online] The Verge. Available at: https://www.theverge.com/2017/11/29/16717416/us-coinbase-irs-records [Accessed 24 Jul. 2018].

Cadwalladr, C. and Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* The Guardian. [online] Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [Accessed 14 Jul. 2018].

Corcoran, K. (2018). *Law enforcement has a massive problem with these 3 cryptocurrencies.* [online] Business Insider Singapore. Available at: https://www.businessinsider.sg/law-enforcement-problems-with-monero-zcash-dash-cryptocurrencies-2018-2/?r=US&IR=T [Accessed 13 Jun. 2018].

Christin, N., 2013, *Traveling the silk road: A measurement analysis of a large anonymous online marketplace*, In Proceedings of the 22nd International Conference on World Wide Web.

Crowe, J. (2017). *Ransomware-as-a-Service is Booming: Here's What You Need to Know.* [online] Available at: https://blog.barkly.com/how-ransomware-as-a-service-works.

Department of Justice of the United States (2017). *Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox.* Northern District of California: US Government.

Egmontgroup.org. (2018). *Financial Intelligence Units (FIUs)* - The Egmont Group. [online] Available at: https://egmontgroup.org/en/content/financial-intelligence-units-fius [Accessed 24 Jul. 2018].

Europol (2015). *Darknet hidden service for child sexual abuse material shutdown.* [online] Available at: https://www.europol.europa.eu/newsroom/news/darknet-hidden-service-for-child-sexual-abuse-material-shut-down [Accessed 13 Jul. 2018].

Europol (2016). *EU Drug Markets Report. In-depth analysis.* [online] Luxembourg: Publications Office of the European Union. Available at: http://www.emcdda.europa.eu/system/files/publications/2373/TD0216072ENN.PDF [Accessed 3 Jul. 2018].

Europol (2016a). *Internet Organised Crime Threat Assessment* (IOCTA) 2016. European Cybercrime Centre. [online] Available at: https://www.europol.europa.eu/iocta/2016/index.html [Accessed 3 Jun. 2018].

Europol (2016b). *Money laundering with digital currencies: working group established.* [online] Available at: https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established [Accessed 24 Jul. 2018].

Europol (2017a). *From suspicion to action. Converting financial intelligence into greater operational impact.* Financial Intelligence Group. Luxembourg: Publications Office of the European Union.

Europol (2017b). *Internet Organised Crime Threat Assessment (IOCTA) 2017. European Cybercrime Centre.* [online] Available at: https://www.europol.europa.eu/iocta/2017/index.html [Accessed 13 Jun. 2018].

Europol (2017c). *Massive blow to criminal dark web activities after globally coordinated operation.* [online] Available at: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation [Accessed 21 Jul. 2018].

Europol (2018a). *Global workshop for financial investigators on detection, investigation, seizure and confiscation of cryptocurrencies.* [online] Available at: https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigators-detection-investigation-seizure-and-confiscation-of-cryptocurrencies [Accessed 24 Jul. 2018].

Europol (2018b). *Police seize more than Eur 4.5 million in cryptocurrencies in Europe's biggest ever LSD bust.* [online] Available at: https://www.europol.europa.eu/newsroom/news/police-seize-more-eur-45-million-in-cryptocurrencies-in-europe%E2%80%99s-biggest-ever-lsd-bust [Accessed 28 Jun. 2018].

FinCEN (2013a). *Application of FinCEN's Regulations to Persons Administering*, Exchanging, or Using Virtual Currencies. Department of the Treasury, United States.

FinCEN (2013b). *Statement of Jennifer Shasky Calvery*, Director Financial Crimes Enforcement Network United States Department of the Treasury. Washington DC: fincen.gov.

FinCEN (2017) *Assessment on civil money penalty*. Financial Crimes Enforcement Network. Department of Treasury. United States of America.

Fincen.gov. (2018). *What We Do* | FinCEN.gov. [online] Available at: https://www.fincen.gov/what-we-do [Accessed 24 Jul. 2018].

Foley, S., Karlsen, J. and Putniii, T. (2018). *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?*. SSRN Electronic Journal.

Gibbs, S. (2017). *'Criminal mastermind' of $4bn bitcoin laundering scheme arrested. [online] the Guardian.* Available at: https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik [Accessed 13 Jul. 2018].

Greenberg, A. (2013). *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road*. Forbes. [online] Available at: https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#732434452765 [Accessed 3 Jul. 2018].

Greenberg, A. (2017). *Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire*. [online] WIRED. Available at: https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/ [Accessed 24 Jul. 2018].

Harris, B. (2018). *What are the alternative cryptocurrencies to Bitcoin?*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2018/01/introducing-ripple-the-second-most-valuable-digital-currency-after-bitcoin/ [Accessed 14 Jul. 2018].

INTERPOL (2015). *INTERPOL Darknet training shines light on underground criminal activities.* [online] Available at: https://www.interpol.int/News-and-media/News/2015/N2015-108 [Accessed 24 Jul. 2018].

INTERPOL (2018). *INTERPOL holds first DarkNet and Cryptocurrencies Working Group.* [online] Available at: https://www.interpol.int/News-and-media/News/2018/N2018-022 [Accessed 24 Jul. 2018].

Kantouris, C. (2018). *Russia blasts Greece's decision to extradite a Russian bitcoin operator and cybercrime suspect to France.* [online] Business Insider Deutschland. Available at: https://www.businessinsider.de/alexander-vinnik-greece-russia-extradite-2018-7-2?r=US&IR=T [Accessed 25 Jul. 2018].

Kharif, O. (2018). *Crypto Thefts Triple as Coin Money-Laundering Industry Grows Up*. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2018-07-05/crypto-thefts-triple-as-coin-money-laundering-industry-grows-up [Accessed 24 Jul. 2018].

Knight, G. (2018). *Monero vs. Zcash and the Race to Anonymity* . [online] Medium. Available at: https://medium.com/coinmonks/monero-vs-zcash-and-the-race-to-anonymity-4322b0a9bd90 [Accessed 25 Jul. 2018].

Kruithof, K., J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso, and S. Hoorens, (2016) *Internet-facilitated drugs trade.* RAND Corporation

Kuzuno, H., & Karam, C. (2017). *Blockchain explorer: An analytical process and investigation environment for bitcoin.* 2017 APWG Symposium on Electronic Crime Research (eCrime), 9-16.

Lee, T. (2013a). *Here's everything we know about PRISM to date. The Washington Post.* [online] Available at: https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?noredirect=on&utm_term=.02fc7ceefd68 [Accessed 14 Jul. 2018].

Lee, T. (2013b). *Here's how Bitcoin charmed Washington.* [online] Washington Post. Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington/?noredirect=on&utm_term=.f04cc097f891 [Accessed 29 Jul. 2018].

Lempres, M. (2018). *Building Trust Through Compliance – The Coinbase Blog.* [online] The Coinbase Blog. Available at: https://blog.coinbase.com/building-trust-through-compliance-10d0ee00cff5 [Accessed 24 Jul. 2018].

Medium. (n.d.). *Understanding a Decentralized Exchange*. [online] Available at: https://medium.com/@theblocknetchannel/understanding-a-decentralized-exchange-eee9e1043f45 [Accessed 29 Jun. 2018].

Mullany, G. (2013). *China Restricts Banks' use of Bitcoin. The New York Times.* [online] Available at: https://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html [Accessed 6 Jul. 2018].

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin, [online] Available at: https://bitcoin.org/ bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction.* 1st ed. New Jersey: Princeton University Press

Nichols, S. (2017). *See you in 2023 – Bitcoin exchange Coin.mx bigwig gets 66 months in the slammer.* [online] Theregister.co.uk. Available at: https://www.theregister.co.uk/2017/06/27/coinmx_boss_gets_66_months/ [Accessed 13 Jul. 2018].

Pagliery, J. (2013). *FBI shuts down online drug market Silk Road.* CNN. [online] Available at: http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html [Accessed 3 Jul. 2018].

Parker, L. (2015). *Controversy arises as new Blockchain Alliance engages with US law enforcement* Brave New Coin. [online] Bravenewcoin. Available at: https://bravenewcoin.com/news/controversy-arises-as-new-blockchain-alliance-engages-with-us-law-enforcement/ [Accessed 24 Jul. 2018].

Perper, R. (2018). *China eliminates all cryptocurrency trading.* Business Insider. [online] Available at: https://www.businessinsider.de/china-eliminates-all-cryptocurrency-trading-2018-2?r=US&IR=T [Accessed 6 Jul. 2018].

Roberts, J. (2018). *Bitcoin and Taxes: What You Need to Know About Cryptocurrency and the IRS. Fortune.* [online] Available at: http://fortune.com/2018/01/29/bitcoin-taxes-cryptocurrency-irs/ [Accessed 6 Jul. 2018].

Robinson, T. (2018). *Bitcoin Mixers: Assessing Risks in Bitcoin Transactions.* [online] Elliptic.co. Available at: https://www.elliptic.co/our-thinking/bitcoin-mixers-assessing-risk-bitcoin-transactions [Accessed 24 Jul. 2018].

Robinson, T. and Fanusie, Y. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services.* [online] Elliptic. Available at: https://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf [Accessed 15 Jun. 2018].

Ron, D. and Shamir, A., 2013, April. *Quantitative analysis of the full bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security* (pp. 6-24). Springer, Berlin, Heidelberg.

Salmon, F. (2014). *When Disruption Meets Regulation,* REUTERS (Jan. 30, 2014), Available at: http://blogs.reuters.com/felix-salmon/2014/01/30/when-disruption-meets-regulation

Smith, J. (2016). *Bitcoin is Not Anonymous*. [online] Elliptic.co. Available at: https://www.elliptic.co/our-thinking/bitcoin-transactions-money-laundering [Accessed 15 Jul. 2018].

Sonicwall.com (2017). *2017 SonicWall Annual Threat Report* | Landing Pages | SonicWall. [online] Available at: https://www.sonicwall.com/en-us/lp/2017-sonicwall-annual-threat-report

Soska, K., and N. Christin, (2015). *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem*. In Proceedings of the 24th USENIX Conference on Security Symposium

Southurst, J. (2017). *Sudden Bitmixer Shutdown a Red Flag for Bitcoin 'Anonymity'*. [online] Bitsonline. Available at: https://bitsonline.com/bitmixer-shutdown-bitcoin-anonymity/ [Accessed 24 Jul. 2018].

Suarez, J. (2017). *Coinbase Obtains the Bitlicense – The Coinbase Blog.* [online] The Coinbase Blog. Available at: https://blog.coinbase.com/coinbase-obtains-the-bitlicense-f1c3e35c4d75 [Accessed 24 Jul. 2018].

UNODC (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes.* [online] Vienna: United Nations Office on Drugs and Crime. Available at: http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf [Accessed 5 Jul. 2018].

Yakowicz, W. (2018). *Startups Helping the FBI Catch Cryptocurrency Criminals*. [online] Inc.com. Available at: https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html [Accessed 24 Jul. 2018].

Zetter, K. (2013). *Feds Arrest Alleged 'Dread Pirate Roberts,' the Brain Behind the Silk Road Drug Site.* [online] WIRED. Available at: https://www.wired.com/2013/10/silk-road-raided/ [Accessed 30 Jul. 2018].

Appendix

Figure 1. History of Bitcoin market capitalisation between 2015 - 2018
(data extracted from Coinmarketcom.com)

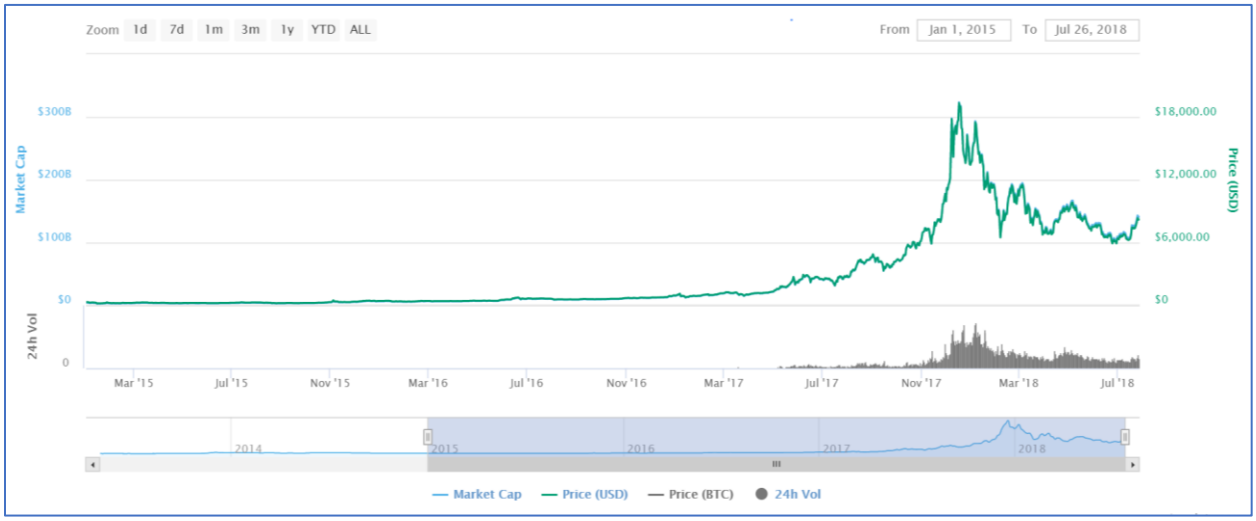

Table 1. Distribution of Illicit Bitcoin Volume into conversion services, by region.

DISTRIBUTION OF ILLICIT BITCOIN VOLUME INTO CONVERSION SERVICES, BY REGION					
	2013	2014	2015	2016	All years
Africa	0.00%	0.00%	0.09%	0.00%	0.00%
Asia	7.14%	0.51%	1.61%	1.21%	3.29%
Europe	43.31%	21.90%	38.31%	56.65%	37.33%
North America	6.26%	7.42%	8.19%	5.28%	7.12%
Oceania	0.00%	0.09%	0.47%	0.35%	0.20%
South America	0.02%	0.01%	0.07%	0.07%	0.04%
Unkown	43.27%	70.07%	51.36%	36.44%	52.03%
Grand Total	100.00%	100.00%	100.00%	100.00%	100.00%

(data extracted from "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services" p. 10 by Robinson and Fanusie, 2018)

CHARLES UNIVERSITY

MSc International Security, Intelligence and Strategic Studies
2016-2018

Dissertation Archive Permission Form

I give the School of Social and Political Sciences, University of Glasgow permission to archive an e-copy/soft-bound copy of my MSc dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name: EVA GONZALEZ MARQUES

Student Number: 2280960G

Student Signature:  Date: 30th July 2018