Andrés Hinojal Fraile
Guardia Civil Lieutenant

CRYPTOCURRENCIES AND MONEY LAUNDERING

CRYPTOCURRENCIES AND MONEY LAUNDERING

Abstract: Because of their global availability, ease of access, reliability and irreversibility of transactions, speed of international transfers and ability to obfuscate the identity of the owners of the funds, cryptocurrencies are an ideal tool for money laundering. Virtually all types of criminal proceeds can be laundered using cryptocurrencies.

The analysis of techniques for using cryptocurrencies for money laundering, as well as the analysis of current legislation, will make it possible to determine whether greater police efforts are needed to modernise technology for the investigation of this type of crime.

Resumen: Debido a su disponibilidad mundial, a la facilidad de acceso, a la fiabilidad e irreversibilidad de las transacciones, a la rapidez de las transferencias internacionales y a la capacidad de ocultar la identidad de los propietarios de los fondos, las criptomonedas son una herramienta ideal para el blanqueo de capitales. Prácticamente todo tipo de beneficios delictivos se pueden blanquear utilizando criptomonedas.

El análisis de las técnicas de uso de criptomonedas para el blanqueo de capitales, así como el análisis de la legislación vigente, permitirá determinar si es necesario un mayor esfuerzo policial de modernización tecnológica para la investigación de este tipo de delitos.

Keywords: Cryptocurrencies, Money Laundering, Guardia Civil, Blockchain, Drug Trafficking.

Palabras clave: Criptomonedas, Blanqueo de Capitales, Guardia Civil, Blockchain, Tráfico de Drogas.

1.- INTRODUCTION

Cryptocurrencies are a technological and financial breakthrough with significant global economic potential. However, in the absence of adequate regulation, they are also used for illegal purposes. They are attractive to those wishing to avoid detection by law enforcement but innovative investigation and analysis techniques make it easier to detect suspicious transactions and identify users.

The use of this virtual currency for criminal activities and money laundering has increased and become more sophisticated in recent years. Tools that facilitate the use of cryptocurrencies are now widely available and services devoted to channelling criminal proceeds are well established. As a result, the criminal use of cryptocurrencies is no longer limited to cybercrime, but now relates to all types of crime that require the transmission of monetary value.

Cryptocurrency tracking is key in many law enforcement investigations and has led to successful operations in cases that would otherwise have gone unsolved. The number of requests for cryptocurrency analysis addressed to Europol has been steadily increasing over the years. Until 2019, such requests mainly concerned cybercrime. Today, however, cryptocurrency tracking requests are linked to many areas of crime. Investigations regarding the dismantling of encrypted communication services that are widely used by criminals have confirmed the use of cryptocurrency for large-scale transactions and/or money laundering in connection with several criminal activities.

Law enforcement agencies, to a greater or lesser extent and at a national and international level, have units specialised in the study of economic crime and specifically in the investigation of crimes related to money laundering. It is very difficult to start analysing money laundering through cryptocurrencies from scratch for all these actors that specialise in the traditional criminal offence of money laundering due to the high technical capacity needed to process the information and data that remain on the blockchain and to be able to trace the transactions carried out on it.

2.- BLOCKCHAIN

Blockchain is a subset of what is known as distributed ledger technology (DLT). It is a method of recording and exchanging data using data warehouses, also known as ledgers, which all contain the same data records and are collectively maintained and controlled by a distributed network of computer servers known as nodes.

"Blockchain is a mechanism that employs a method of encryption known as cryptography and uses specific mathematical algorithms to create and verify an ongoingly growing data structure –to which only data can be added and from which existing data cannot be removed– that takes the form of a blockchain of transactions, which works as a distributed ledger." (Natarajan, Krause and Gradstein, 2017)

In practice, blockchain is a multifaceted technology. It can include a variety of features and cover a wide range of systems, from fully open ones and without permissions to with permissions:

Someone on a blockchain without permissions can join or leave the network at any time without needing to be authorised by any institution. All you need is a computer with the required software installed to connect to the network and contribute transactions to the ledger. There is no single owner of the network or software and identical copies of the ledger are distributed to all nodes in the network. The vast majority of cryptocurrencies in circulation today are without permission and blockchain-based (e.g. Bitcoin, Litecoin). (Natarajan, Krause and Gradstein, 2017)

In order to join an authorised blockchain, transaction validators have to be pre-selected by a network administrator, who sets the rules of the ledger. This enables, among other things, easy verification of the identification of network participants. However, it also requires that network participants rely on a central coordinating body to choose reliable network nodes. Licensed blockchains are classified into two classes. (Shobhit, 2018)

Public or open blockchain with permission, which can be accessed and viewed by anyone, but where only authorised network participants can generate transactions and/or update the status of the ledger. (Witzig and Salomon, 2018)

Blockchain with closed permissions, where only the network administrator has access to generate transactions and change the ledger status. It should be noted that, as in an open blockchain without permissions, transactions on an open blockchain with permissions can be validated and executed without the need for a third party.

2.1.- How a chain of blocks works.

One distributed database that can be considered as such is blockchain. One member initiates additions to the database by creating a new "block" of data, which can contain any type of data. This new block is then transmitted to all parties in the network in encrypted form using cryptography, which ensures the privacy of the transaction.

Network members use a pre-defined algorithmic validation process, generally referred to as a "consensus mechanism", to collectively assess the validity of the block. The new "block" is added to the blockchain once it has been validated, essentially updating the ledger of transactions circulating on the network. This technology can be used with any asset that can be represented digitally and used for any type of value exchange. (Natarajan, Krause and Gradstein, 2017)

In a blockchain network, each user has a pair of keys. There are two types of keys: a private key that is used to produce a digital signature for a transaction, and a public key that is known to everyone in the network. A public key can be used for two purposes:

a) "It serves as an address in the blockchain network.
b) It is used to verify a digital signature/validate the identity of the sender."

A digital wallet, often referred to as an e-wallet, stores a user's public and private keys. This wallet can be held or stored online (sometimes referred to as "hot storage") or offline (often referred to as "cold storage"). (FATF, 2014)

One of the most significant advantages of blockchain technology is that it simplifies the execution of a wide variety of transactions that would otherwise require the intervention of a third party. (In essence, blockchain is about decentralising trust and enabling decentralised transaction authentication). It simply cuts out the middleman. (Witzig & Salomon, 2018)

Cryptocurrencies. Cryptocurrencies are not easy to define. Like blockchain, cryptocurrencies have become a buzzword for a wide range of technological advances that use a method known as cryptography. A critical review of the definitions that have already been created by several interested policy makers at European and international level will be undertaken in the following in an attempt to provide an acceptable definition of cryptocurrencies.

The issue of cryptocurrencies has been analysed by various bodies, each of which has handled it in a different way. The main and most useful definition is that provided by the Financial Action Task Force:

2.2.- Financial action task force

"The Financial Action Task Force (FATF) is the global watchdog on money laundering and terrorist financing. This intergovernmental body sets international standards aimed at preventing these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the political will required for national legislative and regulatory reforms in these areas.

With over 200 countries and jurisdictions committed to implementing them, the FATF has developed the FATF Recommendations or FATF Standards, which ensure a coordinated global response to prevent organised crime, corruption and terrorism. They help authorities pursue the money of criminals trafficking illegal drugs, humans and other crimes. The FATF also works to stop the financing of weapons of mass destruction.

The FATF reviews money laundering and terrorist financing techniques and strengthens its standards on an ongoing basis to address new risks, such as the regulation of virtual assets, which have become more widespread as cryptocurrencies gain popularity. The FATF monitors countries to ensure that they fully and effectively implement the FATF standards and holds countries accountable if they fail to do so." (Financial Action Task Force, 2022)

Like many other policy makers, the FATF has addressed cryptocurrencies as a subset of virtual currencies, which it defines as digital representations of value that can be digitally traded and work as a medium of exchange, and/or an account unit, and/or a value deposit, but are not legal tender in any jurisdiction. (FATF, 2014)

"Virtual currency is a digital representation of value that can be digitally traded and works as an exchange medium, account unit or value deposit, but is not legal tender in any jurisdiction. It is not issued or guaranteed by any jurisdiction and performs the above functions only by agreement within the community of virtual currency users"

"Online currency is distinguished from fiat currency, which is the currency and paper money of a country that is designated as its legal tender, circulates, and is

commonly used and accepted as a medium of exchange in the issuing country. It is different from e-money, which is a digital representation of fiat currency used to electronically transfer value designated in fiat currency. E-money is a digital fiat currency transfer mechanism, i.e. it transfers legal tender value electronically."

"Digital currency" can mean a digital representation of virtual (non-fiat) currency or electronic (fiat) money, and is therefore often used interchangeably with the term virtual currency.

It further states that virtual currencies fall into two categories:

a) "Convertible virtual currencies that have an equivalent value in real currency and can be exchanged for real currency –these virtual currencies can be centralised or decentralised in nature.
b) Non-convertible virtual currencies that are specific to a certain domain or virtual world (multiplayer online game) and under the rules governing their use, cannot be exchanged for fiat currency. (FATF, 2014)

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority which sets rules that make them non-convertible. In contrast, convertible virtual currencies can be of two sub-types: centralised or decentralised.

a) "Centralised virtual currencies have a single managing authority that controls the system. An administrator issues the currency, sets the rules for its use, keeps a central ledger of payments and has the authority to redeem the currency. Currently, the vast majority of virtual currency payment transactions are undertaken with centralised virtual currencies.
b) Decentralised virtual currencies (also known as cryptocurrencies) are distributed, open-source, mathematics-based virtual currencies that have no central authority to administer them and no central control or supervision. Example: Bitcoin, Litecoin and Ripple."

"Cryptocurrency refers to a convertible, decentralised, mathematically based virtual currency that is protected by cryptography. Cryptocurrency relies on public and private keys to transfer value from one (natural or legal) person to another and must be cryptographically signed each time it is transferred. The security, integrity and balance of cryptocurrency ledgers are guaranteed by a network of mutually distrusting parties who protect the network in exchange for the opportunity to earn a randomly distributed commission. Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the blockchain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in the development of alternative, potentially more efficient methods, such as proof-of-stake based systems." (FATF, 2014)

2.3.- Cryptocurrencies today.

The cryptocurrency market has surpassed USD 3 trillion for the first time in its history in 2021 according to the website Coin Gecko, which monitors the market for more than 10,500 cryptocurrencies.

Bitcoin is by far the largest cryptocurrency and currently accounts for 41% of the total cryptocurrency market capitalisation, while the second largest, Ethereum, accounts for around 18%. Among the smaller players in this market is Binance Coin, with a current value of USD 109 billion, followed by Tether, which ranks fourth with a market capitalisation of USD 75 billion.

Although the cryptocurrency industry remains largely unregulated, the authorities are becoming increasingly interested, opening the way to a widening circle of investors and the possibility of future democratisation. An increasing number of companies are allowing and accepting Bitcoin payments, while one of the largest exchange platforms, Coinbase, went public in April 2021. (Roa)

3.- MONEY LAUNDERING

Money laundering tends to be an international, professionalised and sophisticated activity that is not confined to one state. The economic trend towards what has come to be known as globalisation drags many human activities towards interdependence; however, criminal enforcement mechanisms are still limited by borders.

Technical developments and deregulation make it possible to transfer huge amounts of money in a matter of minutes and with minimal traceability. The ease of transporting people and goods can improve the global economy but it also favours the expansion of crime and the ability of criminal organisations to establish themselves in countries without diminishing the ability to control them.

However, the huge sums generated and the increasing difficulties in concealing the illicit origin of money and assets have encouraged criminals to seek out those with the knowledge, skills and experience to circumvent state control mechanisms. The infrastructure related to tax avoidance has thus been put at the service of hiding money of criminal origin. Tax evasion is not socially considered as a criminal activity, although it is a serious form of unscrupulous behaviour as it hinders the redistribution of wealth.

Finally, the increasing attention of institutions to money from organised crime has led to the transformation of laundering mechanisms from simple laundering to the configuration of genuine and complex laundering networks, in which the most sophisticated and imaginative means are used to make the money legal. (Fernandez, 2022)

3.1.- Stages in the money laundering process

The model proposed by the Financial Action Task Force is based on three phases: placement (concealment), diversification or layering, and integration.

a) Placement / Concealment

Placement is defined as the act of physically disposing of large amounts of cash without yet concealing the identity of the holders. The Executive Service states that concealment implies that the laundering process is initiated by converting the money into cash, another good or moving it to a different location. In its simplest sense, placement involves the deposit with an institution of the cash generated by the last traffic step. Placement mechanisms are:

1) Traditional financial institutions. Banks.

   By splitting cash income (structuring), buying financial instruments ("smurfing"), exchanging small banknotes for large banknotes, etc. (The term "smurfing" is usually limited to the exchange of currency in small amounts of cash).

2) Non-traditional financial institutions. Institutions that provide services like banks but can be used in the same way.

   Using companies or businesses with high cash receipts, whether or not they correspond to reality, the purchase of goods with cash or smuggling cash or documents of equal value.

3) Other placement mechanisms.

   Money exchange bureaux, insurance brokers, gemstone dealers, prize buyers, stockbrokers, money transfer companies, etc.

b) Diversification or layering

It consists of concealing the origin of the money or the goods acquired with it through a certain number of financial transactions, i.e. stratifying the movement of capital by preventing the trail that could identify it with its origin to be followed. Diversification mechanisms are:

a) Creation of a fake paper trail.
b) Acquisition of financial instruments with easy physical transportation and immediate liquidity.
c) Resale of goods purchased for cash.
d) Electronic funds transfer. (FATF, 2014)

c) Integration phase

It consists of the introduction into legal economic circuits of goods of criminal origin, pretending that they come from licit activities. Integration mechanisms are:

a) Real estate transactions.
b) Creation of fake companies and simulated credits.
c) Investment in and control of legitimate businesses. (FATF, 2014)

3.2.- Generic systems of money laundering

Some activities that are most commonly employed to achieve the desired results. Some fund laundering methods are:

a) Use of tax havens. There are certain countries with rather permissive and low-pressure tax legislation while their banking regulations allow the opening of secret accounts in which the names of the depositors remain anonymous.
b) Application for secured loans. The method consists of depositing the proceeds

of illicit activities in a country that observes banking secrecy. Then going to the bank and applying for a loan backed by money deposited in another country as collateral. It can be argued that they have set up some companies or businesses abroad when asked to explain this sudden enrichment.

c) Cash business. The Costa del Sol and the Costa Brava have been a paradise for foreign criminals for decades, where a large part of the millions obtained have been invested in housing estates, hotels or placed in bank vaults.
d) Many of these people have set up businesses such as restaurants, cafés, supermarkets, nightclubs, etc., as it is difficult to determine the exact turnover in these businesses. Money can be laundered by mixing dirty money with legally earned profits.
e) Casino gambling. Playing with dirty money means laundering funds.
f) Use of banks. Several smaller deposits made in different banks and in the names of family members may go unnoticed.
g) Purchase of winning tickets. Buying a prize by paying an extra and thus justifying that the investor is the person who won the prize is another method of money laundering.
h) The use of cryptocurrencies by criminal organisations is on the rise, in line with their adoption as a payment system by society. (Fernandez, 2022)

3.3.- The money laundering process and cryptocurrencies

The placement step in the cryptocurrency laundering process involves the use of exchanges. Money brokers open several accounts using money mules as front men and fake identity documents. A money broker receives cash from criminals to exchange into cryptocurrencies; alternatively, the broker uses cryptocurrencies that have already been obtained to move that amount to other jurisdictions. In some cases, intermediaries contact private sellers on cryptocurrency exchange platforms. Criminals have used these marketplaces to buy cryptocurrencies from private sellers in different EU countries.

The layering phase provides for the exchange of primary currencies for other currencies so that intermediaries hide the origin of the cryptocurrency. This process is also known as "chain hopping", whereby money moves from one cryptocurrency to another, across exchanges –the less regulated the better– and jurisdictions to create a money trail that is difficult to trace. The stratification process may also involve the use of blending services. The new cryptocurrency looks "clean" after this process.

The integration of funds can be carried out in several ways, depending on the client's wishes. In some cases, money mules open several bank accounts in one or more countries. Documents and identity information from bank accounts remain in the possession of the criminal network. The transfer of funds from the exchanges to these bank accounts is processed on the same day, to avoid price fluctuations. This means that the exact amount of purchased cryptocurrencies is exchanged and transferred to the bank accounts operated by the criminals. Alternatively, criminals set up online companies that accept cryptocurrency payments to legitimise their profits.

4.- METHODS FOR MONEY LAUNDERING WITH CRYPTOCURRENCIES

"With cryptocurrencies, new methodologies for money laundering are emerging that make it difficult for countries to combat this type of organised crime. The risks arising

from the use of cryptocurrencies for illicit purposes can be grouped under the following three headings:" (Navarro Cardoso, 2019)

1. Use of cryptocurrencies to pay for criminal services.

2. Use of virtual currencies as a form of fraud.

3. Use of virtual currencies to launder money of illicit origin.

Modern technologies have encouraged criminal behaviour in the areas of money laundering and tax fraud, as well as other types of crime, due to anonymity, speed, trans-nationality and non-presence. Virtual currencies have clearly established themselves as a relatively safe tool for criminals to move illicit wealth around the world with less risk than traditional techniques. (Navarro Cardoso, 2019)

5.- MODUS OPERANDI OF MONEY LAUNDERING

Cryptocurrencies are a technological and financial breakthrough with significant global economic potential. However, in the absence of adequate regulation, they are also used for illegal purposes. Cryptocurrencies are attractive to individuals seeking to escape detection by law enforcement. Moreover, innovative investigation and analysis techniques enable the detection of dubious transactions and the identification of users.

The use of this virtual money for illegal operations and profit laundering has increased in recent years in terms of volume and sophistication. Tools that facilitate the use of cryptocurrencies are now widely available and services specialised in channelling illegal gains are well established. As a result, the criminal use of cryptocurrencies is no longer limited to cybercrime, but increasingly encompasses all types of crime involving the transmission of monetary value. (Europol, 2020).

The illicit use of cryptocurrencies covers a wide range of activities. They have been used in money laundering schemes and linked to a number of underlying crimes such as fraud and drug trafficking. They are also commonly used to pay for illegal goods and services sold online and offline.

Money laundering is the most common criminal activity related to the illegal use of cryptocurrencies. Due to their growing popularity and use, cryptocurrencies are increasingly used in money laundering activities. Other criminal acts related to cryptocurrencies include using them as a payment method for illegal goods and services, making fraudulent investments in bitcoins and engaging in cybercrime. In all cases, criminals use them to disguise the origin of illicit assets. (Chainalysis, 2022)

There are a large number of criminal offences involving cryptocurrencies. The methods used to launder money and to convert money obtained illegally in different ways into legal money are explained below.

Criminals committing fraud rely heavily on the use of cryptocurrencies. The number of requests to Europol for support in tracing cryptocurrency-related fraud has increased considerably in recent years. It involves the deposit, transfer and laundering of the proceeds of fraud, as well as specific scams that lure victims into investing money in

a newly created currency that later turns out to be a scam. (Europol, 2020)

Cryptocurrencies are also the preferred method of payment for illegal goods and services such as drugs and child sexual abuse material purchased online, especially on dark web marketplaces, where they are the primary payment method. Several malware strains target cryptocurrency theft as well as coin mining in a network of unwitting victims and cybercriminal extortion schemes, among other things.

5.1.- Mining

"Mining in the cryptocurrency world can be defined as the set of processes required to process and validate transactions of a cryptoasset using a blockchain network. The protocol only allows these transactions to be processed by specialised users called miners. Within such a network, for a transaction to be validated, a complex mathematical problem needs to be solved. The key has to be cracked by making random attempts, earning the right to decide the block. By writing that block down in the ledger, these computers are the miners of the cryptocurrency." (Barroilhet, 2019)

Once the mathematical problem is solved, the transaction is added as another block, making it irreversible. The first person to solve the mathematical puzzle is rewarded with many cryptocurrencies, which are then distributed to the public. Miners not only unlock money and contribute it to the network but also audit the transactions. Almost all cryptocurrencies are created through mining.

Mining equipment is expensive, costing more than €1,500 per unit, is noisy and consumes a lot of electricity. Today, it is vital to have a high technological capacity to mine virtual currencies, so it is essential to have a high processing capacity to mine many cryptocurrencies at the same time. Considerable infrastructure and a soundproofed area are required.

"For these reasons, companies and organisations carrying out this activity tend to choose countries where electricity is cheaper or colder countries where less refrigeration is needed. It is estimated that 75% of BTC mining takes place in China due to the proximity to hardware manufacturers and lower electricity costs." (Jiang, et al., 2021)

Organisations that obtain illicit funds through several criminal activities and need to launder them use the funds to purchase cryptocurrency mining equipment. Moreover, as mining requires a large amount of electricity, it often leads to electricity fraud. Mining revenues can be reinvested in any asset or in an apparently legal enterprise with profits that can be justified to the authorities. (Barroilhet, 2019)

5.2.- Mixers

A service provided by virtual platforms to ensure that their customers can hide the origin of cryptocurrencies registered on the blockchain, it is marketed as a way to boost the anonymity of transactions. All members' money is mixed on these platforms and exchanged, erasing transaction tracking. (Albrecht, Duffin, Hawkins and Morales Rocha, 2019).

5.3.- Local traders

People who advertise to exchange virtual currency for real currency buying and selling cryptocurrencies in exchange for cash are called exchanges. Some of the indicators that could be related to money laundering include the following:

1. "Trading virtual currency against cash in significant volumes.
2. Exchanging virtual currency against cash using channels that involve paying high fees and/or enduring worse exchange rates.
3. Exchanges made in unusual and anonymous places. In many cases, trades are organised through internet forums and exchanges take place physically to ensure the buyer of the cryptocurrencies pays cash and the seller merely provides their account password.
4. The purchase is made with direct profits from other illicit activities." (Sanz-Bas, Carlos del Rosal, Núñez Alonso and Echarte Fernández, 2021).

5.4.- Online video games

The use of online video games to launder money is the most recent and relatively simple trend, which can be found in tutorials on several digital video platforms such as YouTube. To launder money, criminals use several online video games. This method is demonstrated in the video game "Fortnite", which allows users to acquire V-Bucks, the game's virtual money, by purchasing cards containing a security code. The cards are resold to customers on the Dark Web at a cheaper price in exchange for Bitcoins.

5.5.- Exchanges

Customers deposit their funds on exchange platforms, which works as wallets for them. The use of the services of an exchange is usually subject to a fee. The risks involved in the use of exchanges in terms of money laundering are the following:

1. "The principals do not operate from Spain; however, Royal Decree-Law 7/2021 establishes that natural or legal persons offering or providing services in Spain are required to be registered.
2. They may be directly controlled by the laundering organisation." (Sanz-Bas, Carlos del Rosal, Núñez Alonso and Echarte Fernández, 2021).

5.6.- ATMS

These ATMs accept cash and convert it into virtual currency, which is then sent to the user's wallet; cryptocurrencies can also be sold in exchange for cash. The operation of an ATM is as follows:

1. "The customer inserts cash that they want to convert into virtual cash into the ATM.
2. The ATM sends the customer the equivalent amount in virtual currency, minus the commission charged for the transaction, to a wallet indicated by the customer.
3. The exchange linked to the ATM delivers the same amount of virtual currency to the operator at market price.

4. The operator tops up the ATM's purse by transferring virtual currency from the exchange.
5. The operator collects the money from the ATM.
6. The trader deposits the cash in the bank and makes a transfer to the stock exchange.

Following the entry into force of Royal Decree-Law 7/2021, which establishes that persons providing services for the exchange of virtual currency for legal tender must be subject to preventive obligations, the installation of cryptocurrency ATMs, their maintenance, security measures and the supervision they must carry will be regulated. (Sanz-Bas, Carlos del Rosal, Nuñez Alonso and Echarte Fernandez, 2021)

5.7.- Fraud

The most common underlying crime for the illicit use of cryptocurrencies is fraud, which accounts for over half of all documented criminal transactions. Fraudsters use professional money laundering services (cryptocurrencies) or devise their own laundering strategies.

"The annual report on the criminal use of cryptocurrency by Chainalysis reports that fraud accounts for 54% of detected illicit activities in 2020, amounting to USD 2.6 billion. Online fraudsters, in particular, make frequent use of gambling platforms to launder funds. Gaming platforms can be used in a similar way to mixers to hide the origins and flows of illicitly obtained funds." (Chainalysis, 2021)

"In 2021, revenue from scams increased by 82% to USD 7.8 billion in cryptocurrencies stolen from victims. More than USD 2.8 billion of this total, which is almost equal to the increase over the 2020 total, came from rug pulls, a relatively new type of scam in which developers build what appear to be legitimate cryptocurrency projects –meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investment opportunities– before taking investors' money and disappearing." It should be noted that the loss figures only reflect the value of the money stolen from investors, not the losses resulting from the subsequent loss of value of the DeFi tokens as a result of the theft.

Police operations Laundering the proceeds of fraud. French and Israeli security forces have dismantled a criminal network involved in benefit fraud by usurping the identities of over 200 companies to fraudulently apply for COVID-19-related state subsidies. This criminal organisation is believed to have defrauded the French state of EUR 12 million in unemployment benefits related to COVID-19. The fraudulently obtained benefits were paid into French bank accounts, before being immediately transferred via Belgian, Dutch and British bank accounts to Lithuanian bank accounts and then to cryptocurrency wallets. (Europol, 2021)

6.- DRUG TRAFFICKING

While money launderers continue to rely primarily on cash, cryptocurrencies are increasingly being used to launder the proceeds of drug trafficking. In recent years, EU law enforcement agencies have conducted several investigations into the laundering of drug money using cryptocurrencies.

These large-scale money laundering operations are often carried out by criminal networks specialising in laundering cryptocurrencies. Given the cross-border nature of drug trafficking, criminal networks providing laundering services operate on an international scale, collecting and transferring funds in several cryptocurrencies and fiat currencies across several jurisdictions. Investigations into drug trafficking operations triggered by the recent dismantling of encrypted communication platforms confirm that profits are often collected by or delivered directly to service providers. (Pastor, 2022)

Among the transactions analysed as part of EncroChat's research, 95% of users were found to be using Bitcoin, followed by anonymous emerging currencies, such as Monero and Dash. Analysis of the use of cryptocurrency addresses included in the SKY CC and Anom related research datasets also shows a very marginal use of altcoins[1]. In these two datasets, most of the addresses analysed were transferring directly to and from exchanges, often of large size, making very limited use of obfuscation techniques. These addresses had received large amounts of Bitcoin, showing transactions worth millions of euros on some occasions. (Villanueva, 2022)

This analysis is based on cryptocurrency addresses extracted from chats in the Operations Limit and Greenlight datasets. The addresses were analysed with a cryptocurrency tracking tool, which showed the amounts of the addresses and the services that were linked to them. Further analysis led to a better understanding of address reuse and a number of tactical recommendations for similar datasets. An analysis of SKY CC datasets by Europol's EC3 revealed 673 addresses that received more than 4866 Bitcoins (worth over EUR 54 million). One account received more than EUR 4 million. (Europol, 2021)

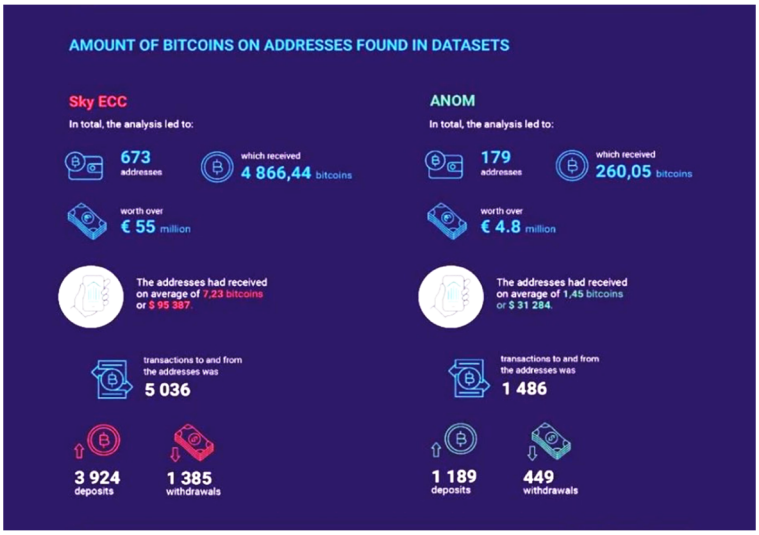

Figure 1. Results of the analysis of cryptocurrency addresses. Source: Europol

6.1.- Modus operandi of drug trafficking with cryptocurrencies

The relevance of cryptocurrencies in the laundering of the proceeds of traditional offline crime is difficult to assess. This is because cryptocurrency is originally deposited as fiat

[1] An altcoin is an alternative cryptocurrency to the traditional and most popular ones. They are currently on the rise due to the volatility of the cryptocurrency market, which carries many risks.

currency with no evidence of its illicit origins visible on the blockchain, rather than moving from addresses that have previously been recognised as criminal-related.

Only if someone were already investigating the criminals in question would they know where these funds come from, aside from knowing anecdotally that at least some criminals do.

a) How cryptocurrency can be used to launder money from offline crime

A common strategy used by many criminal enterprises is the following:

1. "The organised criminal group (OCG) contacts a controller who is in charge of a money laundering operation and tells them how much illicit cash they need to move, the counterpart receiving it and where that counterpart is located.
2. The controller will then contact one of the many coordinators they work with, whose job it is to ensure that the money reaches the right counterpart.
3. The OCG sends the controller and SMS with an image of a banknote with the serial number visible. The controller sends the image to the coordinator, who sends it to the collector in charge of physically receiving the cash.
4. Through the controller, the coordinator communicates to the OCG where the cash will be delivered. The two parties share other details, such as the make and model of the vehicles to be driven by the exchange partners. This is done to limit the risk of police infiltration at the meeting.
5. The OCG will then pass on the photo of the invoice in step 4, together with the cash to be transferred to a courier. Next, the courier meets the collector at the designated place and time.
6. When they meet, the messenger passes the note in the photo to the collector. The collector then checks that the serial number matches the photo they received. The transaction will not take place if they do not match. This is done to assure the collector that the messenger, whom they have never seen, is the right person.
7. If the serial numbers match, the courier delivers the full amount of money to the collector.
8. The collector informs the controller that the cash has been delivered. At that point, the controller carries out a value transfer process, whereby the money is electronically transferred to a coordinator at the location of the OCG counterpart. Traditionally, the wire transfer is done through banks or traditional money service businesses (MSBs).
9. The controller and the new coordinator then ensure that the same process described in steps 1 to 7 is carried out in reverse at the OCG's counterpart location, so that the counterpart receives an equivalent amount of cash – importantly, not the same cash delivered at the OCG's location." (Chainalysis, 2021)

Multiple members of a drug trafficking ring operating in the UK and Australia were arrested by authorities in 2019. In this case, drug traffickers smuggled cocaine in items into Harrod's and then had unwitting employees ship the items to addresses in Australia where the conspirators could retrieve them. The Harrod's drug ring followed this exact procedure, with one exception: instead of bank or MSB transfers, value transfers were made through Bitcoin transactions.

The collectors, in particular, were in charge of carrying out the cryptocurrency transactions. Following a cash drop, police tracking the Harrod's drug ring caught one of these collectors, collected the cash and discovered evidence on them person identifying the serial numbers of the aforementioned banknotes, as well as a list of multiple Bitcoin addresses.

Police discovered a hardware cryptocurrency wallet with a six-month transaction history showing the transfer of USD 8 million in cryptocurrencies to a major exchange house. Blockchain analysis alone will never enable an investigator or compliance officer to identify this money as dangerous because it entered the Bitcoin ecosystem as fiat currency. (Chainalysis, 2021)

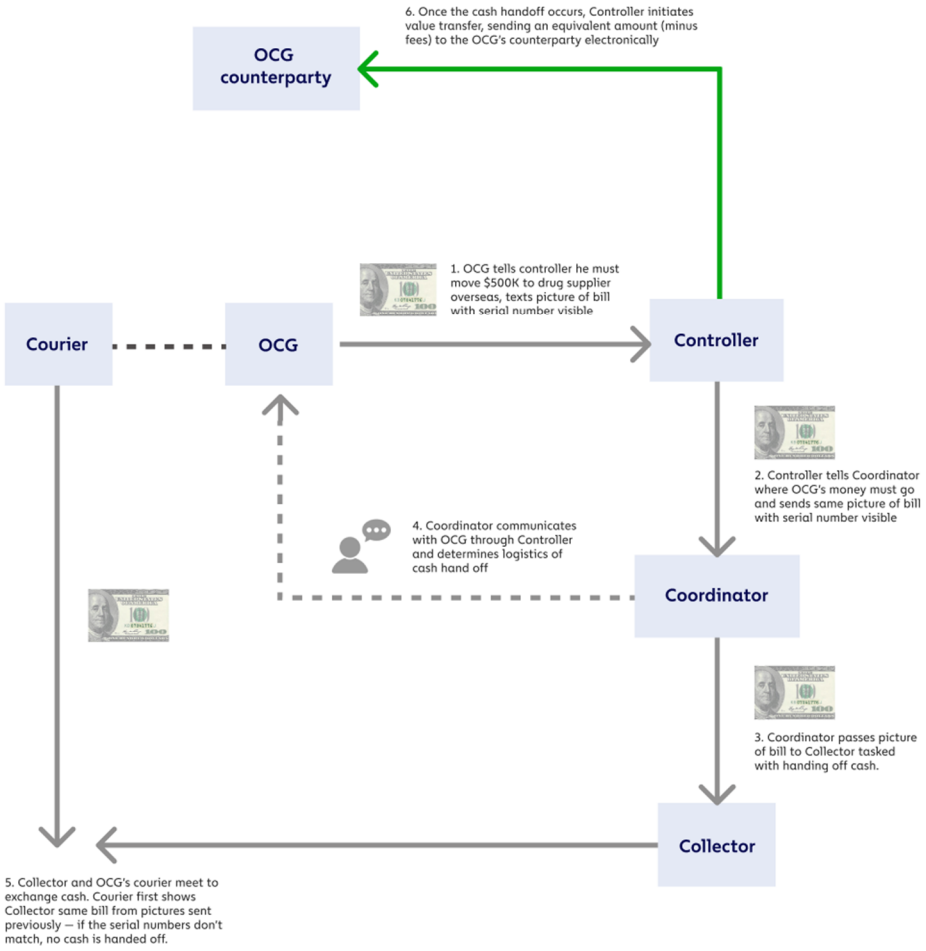

Figure 2. Common strategy used by many criminal enterprises. Source: Chainalysis.

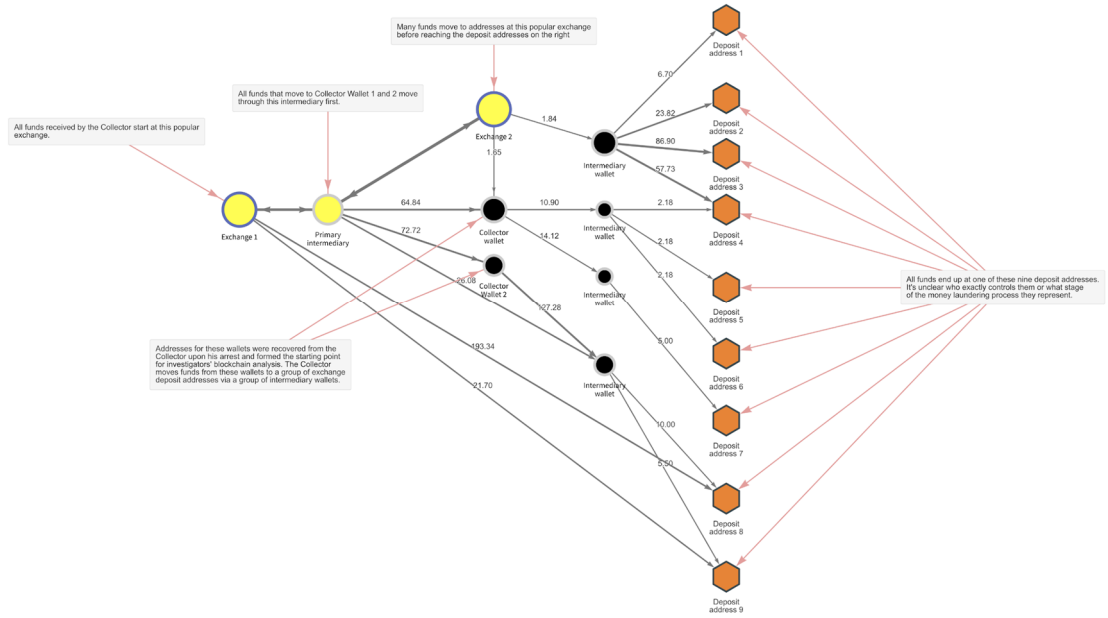

Figure 3. Reactor graph showing Bitcoin transactions related to money laundering network activity. Source: Chainalysis.

6.2.- Money laundering between the EU and South America

A high-profile money broker is coordinating the collection of cash on behalf of a drug trafficking network operating in Europe, where the cash collected is quickly exchanged into cryptocurrencies and credited to a wallet controlled by a Colombian money broker, who then pays the drug trafficking network. The payment itself is handled through legal commercial structures and the usual banking system. In this case, the Colombian money broker appears to be linked to legal structures run by a Chinese network.

The latter does not appear to have direct access to customers, but oversees the actual collection of cash by serving the money broker as a banking network. The Chinese criminal network exchanges the cash collected into Bitcoins and credits the funds to the Colombian broker's wallet. The process between the cash pick-up in Europe and collection takes between 24 and 48 hours. The broker charges 9%. (Gart, 2022)

In another case, a money laundering network organises the transfer and laundering of funds between the EU and Latin America. The network arranges for the proceeds of crime to be collected in Europe and delivered to Latin America via cryptocurrencies and bank transfers. Funds are transferred through shell companies set up in China and Turkey before reaching the customer, adding steps to the money laundering process. (Pastor, 2022)

7.- CONCLUSIONS

The main findings based on research related to money laundering and crypto-currencies are as follows:

Increased use of cryptocurrencies: The use of cryptocurrencies in money laundering activities has increased in recent years. The pseudo-anonymous nature and ease of cross-

border transfer of cryptocurrencies have made them an attractive tool for criminals who wish to hide the illicit origin of funds.

Regulatory challenges: Economic crime related to cryptocurrencies presents significant regulatory challenges. As cryptocurrencies operate across national borders and are decentralised, traditional anti-money laundering regulations are difficult to enforce.

Blockchain technology and tracking: Although cryptocurrencies offer a degree of anonymity, the underlying blockchain technology can also be used to trace transactions. Law enforcement agencies have been working on blockchain forensic analysis techniques to trace transactions and enable the money trail in money laundering activities.

International collaboration: As cryptocurrency-related economic crime crosses borders, international collaboration is key. Joint efforts between different countries, financial institutions and law enforcement agencies are required to effectively combat money laundering in the cryptocurrency environment.

Improvements in regulation and supervision: Regulation and supervision of cryptocurrencies should be strengthened to prevent and detect money laundering.

In summary, money laundering using cryptocurrencies poses significant challenges in the fight against economic crime. However, efforts are being made at both the technological and regulatory levels to address this issue and improve the effectiveness of prevention and detection of money laundering in the cryptocurrency environment. International collaboration and improved regulation and supervision are crucial to combating this type of crime.

Some proposals, ideas or solutions that may be useful to combat this practice to some extent, which is increasingly used by Criminal Organisations, are the following:

Improve regulation and supervision: Regulations and compliance requirements for cryptocurrency exchange platforms and related financial service providers should be strengthened. This includes implementing robust know-your-customer measures, ensuring that users' identities are verified and suspicious transactions are reported.

International cooperation: Collaboration among countries is crucial to tackle money laundering through cryptocurrencies. Governments should promote international cooperation and share relevant information on suspicious transactions, investigations and best practices. This can help track and dismantle criminal networks operating globally.

Cryptocurrency forensics technology: It is key to invest in the development of advanced blockchain forensic analysis tools and techniques. This technology can help to trace transactions and follow the trail of illicit money. By having experts trained in the analysis of cryptocurrency transactions, suspicious patterns and behaviour can be identified, enabling detection and early intervention.

Education and awareness-raising: It is important to raise awareness among cryptocurrency users of the risks associated with money laundering and promote safe practices. Education efforts can include awareness-raising campaigns on economic crime.

Collaboration with industry: Financial institutions and cryptocurrency exchange platforms should be allies in the fight against money laundering. Establishing partnerships and collaborative arrangements with these entities can help to share knowledge and best practices, as well as implement more effective measures to prevent and detect suspicious transactions.

These solutions can go some way towards combating money laundering using cryptocurrencies. However, it is important to recognise that this is a complex and evolving challenge, requiring a multi-faceted and ongoing approach to keep up with the practices of criminal organisations and mitigate the associated risks.

BIBLIOGRAPHY

Albrecht, C., Duffin, K., Hawkins, S. and Morales Rocha, V. (2019). Money Laundering Control Review. From The use of cryptocurrencies in the money laundering process: https://doi.org/10.1108/JMLC-12-2017-0074

Bank for International Settlements. (2015). CPMI. From Digital currencies: https://www.bis.org/cpmi/publ/d137.pdf

Barroilhet, A. (2019). Revista Chilena de Derecho y Tecnología. From Cryptocurrencies, economic and legal aspects: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51584

Chainalysis. (2021). Chainalysis. From The 2021 Crypto Crime Report: https://go.chainalysis.com/2021-Crypto-Crime-Report.html

Chainalysis. (2022). Chainalysis. From The 2022 Crypto Crime Report: https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Ciphertrace. (2021). Ciphertrace. From Cryptocurrency Crime and Anti-Money Laundering Report: https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/

CPMI. (2015). CPMI. From Digital currencies: https://www.bis.org/cpmi/publ/d137.pdf

Custers, B., Oerlemans, J. and Pool, R. (2020). Papers.ssrn.com. From Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282

European Banking Authority. (2018). European Banking Authority. From Designing a Regulatory and Supervisory Roadmap for FinTech: http://www.eba.europa.eu/documents/10180/2151635/Andrea+Enria%27s+speech+on+FinTech+at+Copenhagen+Business+School+ 090318.pdf.

European Central Bank. (2012). Virtual currency schemes. From the European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank. (2015). Virtual currency schemes –a more detailed analysis. From the European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

European Centre for Financial and Economic Crime. (2019). Virtual currencies, EFIPPP typologies.

European Securities and Markets Authority. (2017). European Securities and Markets Authority. From ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies: https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf

Europol. (2021). A corrupting influence: the infiltration and undermining of the European economy and society by organised crime. From European Union Serious and Organised Crime Threat Assessment 2021: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Europol. (2021). Encrochat: a glimpse into the world of global high-risk organised crime.

Europol. (2021). Europol. From https://www.europol.europa.eu/media-press/newsroom/news/six-arrested-for-siphoning-€12-million-in-fraudulent-covid-19-unemployment-payments-france

Europol. (2021). Europol. From Europol helps Belgian and Swiss authorities unravel Vitae Ponzi scheme: https://www.europol.europa.eu/media-press/newsroom/news/europol-helps-belgian-and-swiss-authorities-unravel-vitae-ponzi-scheme

Europol. (2022). Europol. From https://www.europol.europa.eu/media-press/newsroom/news/six-arrested-for-siphoning-€12-million-in-fraudulent-covid-19-unemployment-payments-france

EY. (2018). EY. From IFRS - Accounting for crypto-assets: http://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf

FATF. (2014). FATF. From Virtual Currencies - Key Definitions and Potential AML/CFT Risks: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Federal Trade Commission. (2021). Federal Trade Commission. From What To Know About Cryptocurrency and Scams: https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

Fernández, J. C. (2022). Judicial Police Manual III. Money laundering. CUGC.

Financial Action Task Force. (2022). Financial Action Task Force. From the Financial Action Task Force: https://www.fatf-gafi.org/about/

Flashpoint and Chainalysis. (2021). Flashpoint. From Hydra: Where the crypto money laundering trail goes dark: https://www.flashpoint-intel.com/blog/chainalysis-hydra-cryptocurrency-research/

Gart, J. (2022). Meeting on cryptocurrencies at Europol. (A. H. Fraile, Interviewer)

Guardia Civil. (2018). A criminal organisation dedicated to the production and distribution of New Psychoactive Substances (NPS) dismantled. From Guardia Civil: https://www.guardiacivil.es/es/prensa/noticias/6654.html

Hernández de Cos, P. (2021, 20 December). Interview with the Governor of the Banco de España. (P. Expansion, Interviewer)

Institute for Security and Technology. (2021). Institute for Security and Technology. From Combating Ransomware: https://securityandtechnology.org/ransomwaretaskforce/report/

International Monetary Fund. (2016). International Monetary Fund. From Virtual Currencies and Beyond: Initial considerations: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Jiang, S., Yuze, L., Quanying, L., Yongmiao , H., Dabo, G., Yu , X., & Shouyang, W. (2021). Nature Communications. From Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China: https://www.nature.com/articles/s41467-021-22256-3

Natarajan, H., Krause, S. and Gradstein, H. (2017). World Bank Group. From Distributed Ledger Technology (DLT) and blockchain: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed- Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

Navarro Cardoso, F. (2019). Electronic Journal of Criminal Science and Criminology. From Cryptocurrencies and Money Laundering. : Available online: http://criminet.ugr.es/recpc/21/recpc21-14.pdf

Pastor, C. D. (2022). European Centre for Economic and Financial Crime. (A. H. Fraile, Interviewer)

RAND Europe. (2020). Exploration of the use of the Zcash cryptocurrency for illicit or criminal purposes.

Roa, M. M. (2021). Statista. From The cryptocurrency market now exceeds USD 3 trillion: https://es.statista.com/grafico/26156/capitalizacion-de-mercado-de-las-principales-criptomonedas/

UNODC. (2014). A basic manual on detecting and investigating the laundering of crime proceeds through the use of virtual currencies. From Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies.

LEGISLATION

Treaty on the Functioning of the European Union (Official Journal of the European Union C 326 of 26 October 2012).

Council Directive 91/308/EEC of 10 June 1991 on the prevention of the use of the financial system for the purpose of money laundering (Official Journal of the European Union C 166 of 28 June 1991).

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (Official Journal of the European Union C 344 of 28 December 2001).

Instrument of Ratification of the United Nations Convention against Transnational Organised Crime, in New York on 15 November 2000 (BOE No 233 of 29 September 2003).

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Official Journal of the European Union C 309 of 25 November 2005).

Spanish Constitution (BOE No. 311 of 29 December 1978).

Organic Law 1/1988, of 24 March 1988, on the Reform of the Criminal Code with regard to illicit drug trafficking (BOE no. 74, 26 March 1988).

Organic Law 10/1995 of 23 November 1995 on the Penal Code (BOE no. 281 of 24 November 1995).

Act 10/2010 of 28 April 2010 on the prevention of money laundering and terrorist financing (BOE no. 103 of 29 April 2010).

Royal Decree 304/2014 of 5 May, approving the Regulations of Act 10/2010 of 28 April, on the prevention of money laundering and terrorist financing (BOE no. 110, of 6 May 2014).

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (BOE No. 155 of 26 June 2010).

Circular 4/2010 of 30 December, on the functions of the Prosecutor in the investigation of assets in criminal proceedings (State Prosecutor's Office Doctrine C- 2010-00004, of 30 December 2010).

ABBREVIATIONS

ATM	Automated Teller Machine
BTC	Bitcoin
CPMI	Committee on Payments and Market Infrastructures
DDW	DeepDotWeb
DLT	Distributed Ledger Technology
EBA	European Banking Authority
CE3	Europol's European Cybercrime Centre
ECB	European Central Bank
EFECC	Europol's European Financial and Economic Crime Centre
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
EU	European Union
FATF	Financial Action Task Force
GC	Guardia Civil
ID	Identity Card
OCG	Organised Crime Group
UNODC	United Nations Office on Drugs and Crime