Trabajo Fin de Grado

CRIMINOLOGÍA Y CRIPTOMONEDAS

Presentado por:

Nerea Orta Rodríguez

Tutor/a:

Ricardo Chalmeta Rosaleñ

Grado en Criminología y Seguridad

Curso académico 2022/23

ÍNDICE:

Extended Summary.

This TFG's goal is to find out what types of crimes are most frequently committed using cryptocurrencies in order to educate the public about the risks that go along with using them as a form of payment as well as a way to earn a lot of money quickly through investments. the crimes that are committed both through the cryptocurrency itself and when it is used as a payment method. These crimes are described, along with a description of the typical methodology used to commit them. Additionally, there are some examples to help to better understand the priceless information. Additionally, some preventative measures are suggested for these crimes, including current international, European, and national law. However, in order to prevent becoming a victim of these crimes as much as possible, the author of this work has raised a number of self-protection measures for which the application is deemed necessary for those who engage in activities in the world of crypto-assets.

This work was created through the reading and analysis of numerous books and websites where the authors included details about the operation of cryptocurrencies and the crimes that were frequently committed using them. In order to attach the examples, it has also referenced some legal precedent, including the penal code of 1995 and a number of newspapers. After gathering the data deemed pertinent to this work, it was contrasted and joined to this work.

A cryptocurrency is a digital token or unit of value that can be used as money but is not controlled by a bank or other financial institution. The cryptonet operates under its own set of rules, enabling peer-to-peer transactions without the need for a middleman and connecting monetary policy to social and economic reality.

These tokens were produced in 2008, the same year that Satoshi Nakamoto released an article titled "Bitcoin: A Peer-to-Peer Electronic Cash System" and invented Bitcoin. Because it was introduced to the market after a severe financial crisis during which everyone began to distrust banks, Bitcoin had a significant social impact. It provided a simple means of moving money without going through a bank.

In order for Nakamoto's cryptocurrency, Bitcoin (BTC), to function, he also had to create the Cryptonet, a digital location, and its internal workings. Blockchain technology uses the peer-to-peer network to store cryptocurrencies, keeping track of all token transactions on a ledger. Each user needs two keys to be able to conduct transactions using the cryptocurrency; one of the keys is public and serves as the user ID on the cryptonet, and the other is private and serves as the password. Every user's clues are

kept in online wallets, wgghich can either be hot (on the internet) or cold (on hardware) and guard against theft and cyberattacks. The cold wallet is more secure because it is kept on hardware, which the user can disconnect from the PC to make it harder for hackers to access.

Because so many new ones are created every day, it is currently impossible to estimate the number of different types of cryptocurrencies. The three that currently have the highest capital ratios will be discussed in this section. The first is Bitcoin, the original cryptocurrency and the driving force behind the economic revolution that made it simpler for other cryptocurrencies to be developed and accepted by the general public. The second one is Ether, a token from the Ethereum network that enables it to perform the same operations as Bitcoin while also enabling software creation. The final cryptocurrency that will be discussed is Tether, which was founded in 2014 and is a stablecoin, meaning that, unlike Bitcoin and Ether, it has a fixed value (1 tether=1 dollar). Blockchain and Ethereum networks are used to operate Tether tokens.

Due to the benefits they offered—three of which were the most significant—cryptocurrencies have had a revolutionary impact on society. The first benefit is that because they are decentralized and independent, they offer greater privacy since clients themselves carry out transactions. The second benefit of tokens is that they are less expensive than banks, making it more affordable to conduct transactions using tokens than through banks. The ability to move objects with tokens more quickly and easily than if you had to use a middleman is the final significant benefit.

Since the invention of cryptocurrencies, their use and application have grown exponentially. Initially, only businesses and a small number of people with specialized knowledge used them. However, today, just a few years later, anyone who wants to increase their knowledge or begin investing in tokens has access to training.

However, because of the globalization they have experienced, pre-existing crime types have been modified to fit the new, and new crime types have been developed so that some crimes can be committed using tokens. These crimes can be split into two categories: those that involve the use of cryptocurrencies for payment and those that are merely an outcome of the operation conducted with the token.

Scamming and money laundering are two felonies that fall into the first category. The criminal code of Spain's Article 248 defines a scam as any action that uses deceit to cause another person to make a mistake. Two new types of this crime have been developed to fit the new cryptocurrency era. The first is a scam that involves the use of

fictitious cryptocurrency services; with this approach, markets or wallets are frequently exchanged because the benefit is substantial without the need for much work or exposure. The second new type is the advance payment scam, which is similar to those that already existed but significantly more sophisticated because it ensures both the buyer's and the seller's anonymity.

According to INTERPOL, money laundering refers to the practice of hiding the source of goods or benefits whose provenance is unlawful. Three phases can be distinguished in how this crime is committed (GAFI). The first is the introduction of money into the financial system while being aware of its illegal origins. In the second, the author purchases items or transfers money between national or international societies. This is known as the capital conversion or concealment phase. The final stage involves reintegrating the cleaned-up money into society and treating it as such. Because they guarantee anonymity, Crypto Actives have made this process significantly simpler and it is now more difficult to trace the "dirty money" because no one needs to know where the money comes from."

Numerous felonies could be found in the second category—those that accept cryptocurrencies as payment—but only two are discussed in this article. The first one is extortion, which is defined in the Spanish penal code's article 243 as the act of coercing another person—either physically or psychologically—to perform or refrain from performing a legal act or transaction in order to protect one's own property or the property of another. In 2014, Europol found that Bitcoin was now used as ransom in about a third of cyber extortions because it was harder to track than physical currency.

The second crime in this category is narcotrafficking, which is also known as a crime against public health. Articles 359 to 378 of the Spanish Penal Code serve as a good example. In many parts of the world, this crime is currently paid for using cryptocurrencies because it creates a low-risk drug market for both the buyer and the seller because they do not need to come into direct contact. UNDOC claims that a system has been developed in which users can agree on the location of drug pickup using encrypted messages and tokens to purchase drugs, the darknet.

The existing tools for preventing and controlling the aforementioned illegal behaviours are included in this TFG in addition to felonies and their classification. These are included because it is important to understand how these crimes are regulated and any potential preventative measures because it is impossible to completely eradicate these crimes. In this TFG, two distinct blocks of media are analysed. On the one hand,

there are some steps that the populace can take to protect themselves, and among them, there are three steps.

- Good understanding about how do cryptocurrencies operate.
- Verification of identity.
- Wallet security.

The first is being well-versed in the operation of cryptocurrencies. This precaution is seen as the cornerstone of self-defense against these crimes because, without the knowledge necessary to understand how cryptocurrencies work, a person runs the risk of falling for scams both virtually on the internet and by phony advisors.

In addition to attempting to keep a record of the transactions that are carried out and the value of each one, the second self-protection measure entails verifying the identity of the people with whom the transactions are being carried out. By realizing the recurring disappearance of their cryptocurrency in this way, the person who was being conned into using a fake wallet could alert the authorities in time to stop the problem.

he third and final step is to safeguard the wallet where the cryptocurrencies used to calculate it are kept. Since this kind of cryptocurrency wallet is hardware and cannot be accessed by a hacker even if he gained access to the computer, it is the best place for it to be protected. There is also no need to be concerned if cryptocurrencies are kept in a hot wallet (one that stays on the computer), as there is a double identification system in place for all types of cryptocurrency transactions and wallet access. The best way to safeguard your digital wallet is to create challenging passwords and keep the codes hidden from prying eyes.

On the other hand, there are the legal actions taken to regulate cryptocurrencies, and on this TFG, three of these have been examined:

- Global measures.
- European measures.
- Spanish units.

Since cryptocurrencies are a relatively new invention, every nation had to create its own law to regulate them at the time they were developed due to the lack of standards to do so. This resulted in a patchwork of laws around the world because some nations, like Ecuador, wanted to promote the use of cryptocurrencies while others did not want their citizens to have any contact with them. This is the reason why the International

Monetary Fund is currently developing some guidelines to harmonize the laws of various nations and, in doing so, give everyone the same opportunities

In order to try to make it easier for users and investors to make transactions with them and to reduce the risks that can arise from their use, criptoactives will be regulated in Europe by the Markets in Crypto-Assets (MiCA) regulation. This proposal has some measures to manage the optimization and regulation of the accounting of virtual assets within the European Union.

The law 11/2021 of July 9 on measures to prevent and combat tax fraud, which transposed Directive (EU) 2016/1164 of the Council of July 12, 2016, is currently in effect in Spain. Through this law, regulations aimed at the implementation of tax avoidance schemes, regulations aimed at the modification of some currently in effect tax regulations, and regulations aimed at the control of gambling are all introduced.

The three main conclusions from this work are as follows: First, society needs to be aware of how crime has changed in recent years as a result of the development of the Internet. Today, anyone can commit a crime from their home using only a computer or smartphone, and the criminal can now commit multiple crimes simultaneously without having to confront the victims. The profile of cybercriminals has significantly changed as a result of this change; rather than needing to be quick and intimidating to their targets, they now need to demonstrate a higher level of intelligence and computing knowledge.

On the other hand, and related to the first conclusion, it can be said that despite the fact that cryptocurrencies have been around since 2008, people have only recently started to invest in and conduct transactions using them. This is because anyone can do it now, and there are numerous courses available to train in this field. But the introduction of cryptocurrencies also brought about an evolution in some crimes, including fraud and money laundering, posing new dangers for those who work in this field and necessitating new legislation.

The third and final major finding relates to the regulation of cryptocurrencies because, despite the fact that they have been around for 15 years, it is only now that the International Monetary Fund is developing guidelines to try to harmonize national laws so that everyone has equal access to opportunities in this area. However, no self-protection measures that could be offered to users of cryptocurrency networks to keep them from becoming victims of these crimes have been discovered; for this reason, they have been suggested in this work by the author.

Resumen:

Las criptomonedas y la criminología son áreas que cada vez comparten más interconexiones debido a las nuevas oportunidades que los criptoactivos han creado para poder cometer conductas ilícitas y a la falta de legislación que actualmente existe.

Las criptomonedas son una unidad de valor digital descentralizadas y cuyo cometido es servir como un método de pago alternativo al dinero tradicional. La creación de los criptoactivos ha generado una conexión entre la realidad económica y social, ya que ofrece la posibilidad de llevar a cabo transacciones monetarias sin necesidad de recurrir a un banco, de tú a tú.

En lo que a la clasificación de delitos respecta, estos pueden dividirse en dos grupos. Por un lado, los que utilizan las criptomonedas como medio de pago, y por otro, los que son consecuencia de la propia operativa con criptomonedas. Dentro de este último grupo, se encuentra la estafa, que es de los más usuales, encontrando dentro de este aquellos que se llevan a cabo mediante el uso de cripto-servicios falsos o, las estafas de pago por adelantado.

Para todos estos delitos, es necesario establecer medidas de prevención y regulación, pudiendo ser estas o bien de autoprotección para las personas, o, legislativas. A pesar de ser necesarias, como la criptoweb es relativamente nueva, por el momento se encuentra un gran vacío legal. Para resolver estas carencias, en este TFG se ha realizado una búsqueda sobre la legislación existente que regula las criptomonedas a diferentes niveles, y, se proponen una serie de medidas de autoprotección para la población. Se considera que, de esta manera, al encontrarse todas las medidas de prevención y los riesgos recogidos en un mismo documento, va a facilitarse la labor de concienciación a la población.

Palabras clave: Criptomonedas, delitos, criminología, bitcoin.

Abstract:

Due to the additional options that crypto assets have generated to engage in illegal behavior and the existing lack of legislation, there is a developing connection between the fields of criminology and cryptocurrencies.

For use as an alternative payment mechanism to fiat currency, cryptocurrencies are a decentralized unit of digital value. Due to the ability to conduct financial transactions directly amongst peers instead of through a bank, the development of crypto assets has established a link between economic reality and social reality.

Crimes can be classified into two types as far as classification is concerned. Those that utilize cryptocurrencies as a form of payment, and those that are a result of dealing with cryptocurrencies. The scam is one of the most prevalent within this last category, and it includes those that involve using phony crypto-services or advance payment schemes.

It is vital to implement prevention and regulating measures for all of these offenses, which may take the form of either legislation or individual self-defense. Despite being necessary, there is now a significant legal void because of how nascent the cryptoweb is. In order to address these shortcomings, a review of the current laws governing cryptocurrencies at various levels has been conducted in this TFG, and a number of populace self-protection measures are suggested. It is believed that doing things this way will make raising public awareness easier because all the prevention strategies and hazards are contained in one document.

Keywords**:** Cryptocurrencies, crime, criminology, bitcoin.

1 Introducción.

Las criptomonedas son unidades digitales de valor que no se encuentran reguladas por ninguna entidad bancaria, contando con su propio mecanismo para poder llevar a cabo transacciones entre dos usuarios sin necesidad de tener un tercero que tome el rol de intermediario como podría ser un banco. Estas monedas digitales aparecieron en el año 2008, cuando Satoshi Nakamoto creó el Bitcoin y lo dio a conocer mediante un artículo que él mismo publicó. El bitcoin tuvo una gran repercusión social, abriéndoles paso al resto de criptoactivos que fueron creándose de manera posterior, ya que su lanzamiento se produjo de manera posterior a una gran crisis económica mundial en la cual la población desarrolló una gran desconfianza hacia las autoridades bancarias, y las criptomonedas se planteaban como solución a eso.

Desde el lanzamiento de estos activos digitales, su uso y expansión han aumentado de manera exponencial, comenzando en sus inicios a ser utilizados únicamente por empresas y personas conocedoras de ese ámbito, y evolucionando a que hoy en día, tan solo unos años más tarde, existen cursillos tanto presenciales como online que forman a cualquier persona que quiera invertir en estos activos.

En lo que a las ventajas que las criptomonedas presentan, y en concreto, es importante destacar tres: por un lado, la descentralización previamente nombrada, ya que al ser independientes, pueden brindar una mayor privacidad y autonomía a los usuarios, al ser ellos mismos los que realizan sus transacciones. En segundo lugar, estas monedas digitales cuentan con unos costes mucho menores que los de los bancos para las transacciones que pueden llevarse a cabo con ellas, suponiendo esto otro beneficio para los usuarios. Como tercera y última ventaja, aparece la facilidad y rapidez con la que pueden llevarse a cabo las transacciones (Ayllón, 2022).

Es importante tener en cuenta que además de las ventajas nombradas previamente, las criptomonedas también cuentan con algunos riesgos, y es que, su globalización ha sido total en estos años (Cediel. Pérez, 2020), influyendo esta en las formas de delinquir ya existentes, y, generándose otras nuevas (Roca, 2023). Dentro de los delitos que implican el uso de criptoactivos, se ha realizado una diferenciación entre aquellos que las utilizan como medio de pago, entre los cuales se encontrarían los delitos de narcotráfico y los de extorsión entre otros y aquellos consecuencia de la operativa con criptomonedas, donde se encuentran englobados las estafas y los blanqueos de capitales (United Nations Office on Drugs and Crime).

Debido a la evolución que el mundo criminal ha sufrido y a la relativa novedad que suponen las criptomonedas, es muy importante llevar a cabo medidas de prevención para

estos delitos. Estas medidas de prevención pueden clasificarse en enfocadas a la autoprotección de las personas y dirigidas a la legislación que se está estableciendo a nivel mundial, europeo y nacional.

El método de investigación llevado a cabo para realizar el presente trabajo ha sido el de revisión de bibliografía, siendo esta tanto física como digital. La física ha sido extraída de la biblioteca de la universidad, y la digital, realizando la búsqueda en bases de datos como *Web of Science* o *Google Académico*. Esta búsqueda se ha enfocado a encontrar artículos y libros escritos por autores con amplios conocimientos sobre criptomonedas, su funcionamiento, los riesgos que suponen, y aquellas medidas de prevención que es posible aplicar para que estos no se den.

Además, para la selección de las noticias sobre los delitos que se han cometido con estos criptoactivos, se ha llevado a cabo una búsqueda por diferentes periódicos digitales nacionales e internacionales.

Se estima que el presente TFG puede ser útil para aquellos sectores de la sociedad que hoy en día se encuentran formándose para poder adentrarse en el mundo de las criptomonedas, pudiendo servir este como recordatorio de los conocimientos que han adquirido o están adquiriendo y como aportación de nuevos conocimientos sobre los delitos que pueden cometerse con ellas y las acciones que pueden llevarse a cabo para evitar ser víctima de estos.

Por ese motivo se considera oportuno realizar el presente TFG, que tienen como objetivo fundamental analizar los principales delitos que se cometen relacionados con las criptomonedas y proponer soluciones para evitarlos. Este objetivo principal se desglosa en los siguientes objetivos específicos:

- Objetivo uno. Comprender el funcionamiento de las criptodivisas y el alcance que estas tienen.
- Objetivo dos. Realizar un análisis exhaustivo de la relación existente entre la criminología y las criptomonedas llevando a cabo una investigación sobre los delitos que se llevan a cabo tanto mediante el uso de las criptodivisas como utilizando estas como medio de pago.
- Objetivo tres. Concienciar a la población de los riesgos que el uso de las criptomonedas puede suponer.

- Objetivo cuatro. Analizar las medidas de prevención existentes y crear una serie de medidas de autoprotección.

El documento se estructura del siguiente modo. En el capítulo 2 se describen las características principales de las criptomonedas. En el capítulo 3 se identifican los principales delitos que pueden cometerse, diferenciando entre aquellos en los que la criptomoneda simplemente es el medio de pago y aquellos en los que es el medio para cometer el delito. También se presentan los principales casos mediáticos producidos como ejemplo para facilitar la comprensión de los diferentes delitos. En el capítulo 4 se recopilan las medidas propuestas por los organismos reguladores, junto con otras propuestas realizadas por la autora de este TFG, para evitar la comisión de estos delitos. Finalmente, en el capítulo 5, se muestran las conclusiones obtenidas.

2 *Conceptos básicos sobre criptomonedas.*

A continuación se va a realizar una introducción sobre cuándo y por qué aparecieron las criptomonedas, la manera en la que funcionan, las formas de protegerlas y almacenarlas y, finalmente, una breve descripción de las tres criptomonedas que cuentan actualmente con mayor capitalización.

2.1 Definición e historia.

Una criptomoneda (del inglés *cryptocurrencies*), es "*una unidad digital de valor, no emitida por ninguna autoridad bancaria central o institución, que en ciertas ocasiones puede ser utilizada como medio de pago alternativo al dinero*" (Banco Central Europeo, 2018). Las criptomonedas, son por tanto, archivos digitales (como podría serlo un PDF), que nacen para conseguir operar con dinero sin necesidad de intermediarios, creando un vínculo entre la realidad económica y social, y la política monetaria (Cediel, Pérez. 2020).

El nacimiento de las criptomonedas fue el 1 de noviembre de 2008 cuando Satoshi Nakamoto publicó una reseña titulada "Bitcoin: A Peer - to - Peer Electronic Cash System". Por aquel entonces la población se encontraba en un entorno incierto de crisis económica que supuso una pérdida de confianza en las instituciones políticas y económicas, viéndose por tanto la relación con estas afectadas. En el artículo publicado por Nakamoto se plantea un sistema alternativo en el cual sería posible llevar a cabo transacciones económicas careciendo de terceros, que, hasta este momento, eran considerados imprescindibles para esto (Cediel, Pérez. 2020).

El crecimiento de las criptomonedas ha sido exponencial ya que el 3 de enero de 2009, dos meses después de la publicación del documento, la red de los Bitcoin (las primeras

criptomonedas) entra en funcionamiento, comenzando en sus inicios a realizar intercambios con las criptomonedas creadas y en octubre de ese mismo año, comenzaron las compras de los Bitcoin (BTC) con dinero en curso legal y el 22 de mayo del año 2010, se registró la primera compra de bienes mediante el uso de BTC, siendo esta la compra de unas pizzas por 10.000 BTC, que en aquel entonces equivalían a unos 25 dólares.

2.2 Funcionamiento.

Para lograr comprender cómo llegan a cometerse crímenes mediante el uso de las criptomonedas, es importante tener en consideración cuál es el funcionamiento de estas, ya que, puede resultar complejo de entender al funcionar de manera virtual, sin tener un soporte físico en el que observar estos movimientos.

Las criptomonedas se encuentran almacenadas mediante la tecnología *Blockchain o cadena de bloques* dentro de la red Peer to Peer (de ahora en adelante P2P), llevándose a cabo las transacciones, compras o ventas que se llevan a cabo con las criptomonedas entre dos iguales, sin necesidad ninguna de contar con un tercero como intermediario.

En lo que al sistema *Blockchain* respecta es importante tener en cuenta que el elemento más importante de esta tecnología es la capacidad de transmitir, además de información, valor de manera digital, suponiendo una revolución para la época digital. (González de Frutos, 2018). Además, cabe destacar que es un mecanismo de seguridad ante los posibles ataques de hackers, ya que al llevarse a cabo los movimientos vía internet y sin ningún tipo de intermediario, en caso de no existir un mecanismo de seguridad de este tipo, los dueños de los tokens se encontrarían expuestos a los ataques de estos profesionales, pudiendo verse sus claves vulneradas o incluso sus criptomonedas robadas.

2.2.1 Protección y almacenamiento

Dentro del sistema de Cadena de Bloques, cada usuario no es registrado con su nombre o número de identificación personal, sino que se generan dos claves, una pública y otra privada. (Cediel. Pérez, 2020). La clave pública corresponde a la identidad del usuario en dicha red y, por tanto, la que queda registrada en el Libro Mayor junto a los tokens que tiene en su poder. Por otro lado, la clave privada es una contraseña que va ligada a esa clave pública y es necesaria para llevar a cabo transacciones y movimientos con las criptomonedas que, junto a un SMS que se envía a un número de teléfono asociado a dicho usuario, forman la identificación de doble factor.

Estas claves y usuarios se encuentran almacenadas en unos *wallets* o monederos digitales para protegerlas tanto de robos como de los ataques de hackers. Estos monederos se dividen en dos tipologías, monederos fríos y monederos calientes. En los monederos fríos, las claves se almacenan en dispositivos electrónicos sin acceso a internet, siendo conocidos estos también como hardware y pudiendo ser por ejemplo un USB o un disco duro. Por otro lado, los denominados monederos calientes son aquellos en los que se utiliza un almacenamiento criptográfico en línea para proteger dichas claves, contando por tanto con menos seguridad.

2.3 Ejemplos de criptomonedas.

Debido a la facilidad y la velocidad con la que se crean a día de hoy las criptomonedas, no es posible determinar qué número de estas existen, ya que, prácticamente se crean varias cada día.

Las tres criptomonedas que a continuación van a explicarse son las que cuentan con la mayor capitalización a día de hoy, siendo el Bitcoin el que preside la lista , seguido del Ether y del Tether. Es importante tener en cuenta que el valor de las criptomonedas funciona por especulación y por la ley de oferta y demanda, por lo que este pódium de capitalización puede variar en cualquier momento.

2.3.1 Bitcoin.

El Bitcoin (BTC) fue la primera criptomoneda existente, creada por Satoshi Nakamoto el 1 de noviembre de 2008, y suponiendo su creación una gran revolución económica a nivel mundial.

La creación de BTC no solo supuso la creación de una criptomoneda, sino la de todo el círculo en el que estas se mueven, como es el sistema P2P o el blockchain, que, de manera posterior, cuando se han creado nuevas criptomonedas, han adaptado sistemas similares para su funcionamiento.

2.3.2 Ether.

El Ether es un token de la red Ethereum, que fue creada el 30 de julio de 2015 por el programador Vitalik Buterin. La finalidad con la que esta criptomoneda se creó fue principalmente para llevar a cabo transacciones (como el BTC), aunque no es la única función que esta permite llevar a cabo ya que, el Ether permite crear programas informáticos nuevamente sin necesidad de intermediarios.

2.3.3 Tether**.**

Moneda creada en 2014 por Brock Pierce, Reeve Collins y Craig Sellers bajo el nombre "*Real Coin*". Los tokens de esta criptomoneda fueron creados como stablecoins, contando estas por tanto desde el momento de su creación, con un valor fijo y sin permitir que este se encuentre sujeto a la oferta y demanda del mercado, quedando establecido dicho valor en la proporción 1 token: 1 dólar (Binance Academy, 2020)

Inicialmente el lanzamiento de estos tokens fue en el blockchain de BTC, pero, conforme fue desarrollándose, esta realizó una migración hacia otras cadenas de bloques pertenecientes a otras criptomonedas, encontrándose ahora la mayor parte de su valor en la red Ethereum.

3 Tipologías delictivas más comunes en este ámbito.

Las criptomonedas han supuesto una evolución económica a nivel mundial, incluyendo en esto un importante cambio en la manera de cometer algunos delitos como podrían ser estafas, extorsiones, blanqueo de capitales o delitos contra la salud pública entre otros.

A continuación se va a proceder a explicar las tipologías más comunes que guardan relación con las criptomonedas (tabla 1), diferenciando dos grupos diferentes. Por un lado se encuentran aquellos delitos en los cuales las criptomonedas se utilizan como medio para llevar a cabo el delito, encontrándose ubicados dentro de este grupo la estafa y el blanqueo de capitales. El segundo grupo, se encontrarían englobados aquellos delitos que se cometen de una manera tradicional, pero que han evolucionado de tal manera, que pueden utilizarse las criptodivisas como medio de pago, encontrándose agrupados en este los delitos contra la salud pública y las extorsiones.

Clasificación de los delitos		
Consecuencia de la operativa con criptomonedas.	Estafa	Cripto-servicios falsos
		De pago por adelantado
	Blanqueo de capitales	
Uso de las criptomonedas como medio de pago.	Extorsión	
	Contra la salud pública: Narcotráfico	

Tabla 1. Clasificación de los delitos más comunes llevados a cabo con criptomonedas.

3.1 Delitos consecuencia de la operativa con criptomonedas.

En esta tipología de delitos la criptomoneda es el objeto del delito, ya que es el medio para poder llevar a cabo la conducta ilícita. La posibilidad de delinquir vía criptoactivos ha generado la creación de nuevos delitos y la adaptación de los ya existentes. A continuación se presentan los dos delitos identificados en esta categoría: estafa y blanqueo de capitales.

3.1.1 Estafa.

Según se encuentra recogido en el artículo 248 del Código Penal Español, "*cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno*". La regulación legal de este delito se encuentra del artículo 248 al 251 bis del mismo Código Penal, estableciendo las tipologías de estafa que se pueden encontrar y las consecuencias jurídicas establecidas para cada una de ellas, pudiendo ser pena o multa dependiendo de la cuantía económica que se haya estafado. En este delito, el bien jurídico que se encuentra protegido es el patrimonio ajeno, pudiendo ser este tanto bien mueble como inmueble.

Para comenzar a hablar de los tipos de estafas que pueden llevarse a cabo en el ámbito de las criptomoneda, es importante tener en cuenta que estas se llevan a cabo mayoritariamente en el *Exchange*, es decir, en el mercado en el cual se realiza la compraventa de los tokens. Dentro de este mercado, se pueden diferenciar tres tipos de mercados de intercambio. Por un lado, se encuentran los Exchange centralizado (CEX), el cual se encuentra dirigido por una organización o compañía, seguidamente aparecen los Exchange descentralizados (DEX), que son aquellos en los que el intercambio se realiza mediante el sistema P2P sin necesidad de regulación por parte de terceros y para terminar, existen los Exchange híbridos, que, como su nombre indica, son una combinación de los mercados centralizados y de los descentralizados (Xia et al., 2020).

Uno de los métodos más utilizados en este ámbito es el de los cripto-servicios falsos (Bartoletti et al., 2021), y es que, para llevar a cabo una estafa mediante el uso de este método, suele recurrirse un porcentaje muy alto de veces a los mercados de intercambio o a las carteras, ya que es una manera mediante la cual el beneficio va a ser elevado sin necesidad de llevar a cabo mucho esfuerzo ni verse expuesto. Los estafadores, en los casos en los que se acude al mercado para llevar a cabo las estafas, suelen engañar a los compradores realizando ofertas muy competitivas para

conseguir algunos tipos de criptomonedas, viéndose los compradores tentados ante semejante oferta.

Por otro lado, en aquellos casos en los que se prefiere estafar mediante el uso de falsos wallet, puede realizarse de diferentes maneras, siendo una de ellas la posibilidad de llevar a cabo el robo de la cuantía completa en el momento en el que el estafador tiene acceso al wallet, y siendo esta una tarea nada complicada ya que, en este se encuentran tanto el código de identificación personal como la contraseña necesarios para poder llevar a cabo todas las acciones que se quiera con los tokens. El segundo tipo de estafa que se lleva a cabo con la cartera es la que correspondería a un delito continuado de hurto, extrayendo el estafador de manera periódica un pequeño porcentaje del depósito con el que cuenta esa cartera. Finalmente, existe otra tipología en la cual se procede a vaciar el depósito cuando llega a cierto umbral establecido por el hacker, resultando desconocido por el dueño de la wallet que un tercero tiene acceso a su cuenta, y vaciándose esta de manera repentina al llegar a esa cantidad, como en el primer caso.

Otra de las estafas frecuentes que implican el uso de criptomonedas son las estafas de pago por adelantado, que, a pesar de ser un delito previamente existente, hoy en día se encuentra enfocado también al ámbito de las criptomonedas, siendo estas similares a las tradicionales pero mucho más sofisticadas debido al anonimato que garantiza tanto para el vendedor como para el comprador. En estas campañas suelen compartirse por correo electrónico y mediante el uso de tácticas de ingeniería social enfocadas al BTC, que es la moneda por excelencia para llevarlas a cabo (Montes, 2021).

Esta tipología de estafas suele encontrarse enfocada a aquellas personas que ya cuentan con cierta soltura en el ámbito de las criptomonedas y resulta muy tentadora para el comprador debido a la garantía de conseguir el dinero de manera anónima y sin necesidad de pagar impuestos, prometiendo esta una gran cantidad de bitcoin a cambio de un pequeña cantidad de estos, otorgando además una falsa sensación de seguridad, ya que una vez la víctima accede a la web que se le indica en el email, se le solicita que realice un cambio de contraseña para que de esta manera sus transacciones no puedan verse vulneradas.

3.1.2 Blanqueo de capitales.

La Organización Internacional de Policía Criminal (Interpol) establece que el blanqueo de capitales es la acción de encubrir u ocultar el origen de bienes o beneficios

cuyos orígenes sean ilícitos, encontrándose generalmente este delito aunado al de tráfico de drogas o robo con violencia.

El Grupo de Acción Financiera Internacional (GAFI), tomando como referencia la sentencia del Tribunal Supremo n.º 685/2013, de 24 de septiembre, ECLI:ES:TS:2013:4888, establece que dentro de este delito pueden diferenciarse tres fases o etapas:

- Fase de introducción o colocación del capital en el sistema financiero, teniendo como finalidad la desvinculación de la actividad ilícita de proveniencia.
- Fase de conversión o encubrimiento de capitales: esta se lleva a cabo mediante la compra de bienes, transferencia del caudal o, transferencias entre sociedades tanto nacionales como internacionales.
- Fase final de reintegración del capital que ha sido blanqueado, considerándose este como "capital limpio" y llevándose a cabo esta reinserción mediante la utilización de empresas ficticias en paraísos fiscales o, mediante la compra de inmuebles.

El uso de las criptomonedas garantiza un mayor anonimato que cualquier medio tradicional que no sea el dinero en efectivo, dificultando por tanto la persecución del "dinero sucio", e impidiendo la aplicación de las medidas antilavado *KYC* (Know Your Costumer), conoce a tu cliente (GAFI). La razón por la que las criptomonedas ofrecen un mayor anonimato es porque, a pesar de quedar registrado en la cadena de bloques las pertenencias de estas, no se realiza el registro con el nombre de la persona, sino con la clave pública que el sistema ofrece, coincidiendo en todos los casos la clave con la identidad de la persona, pero resultando imposible para un comprador de criptomonedas saber quién es el usuario al que se le está comprando o vendiendo el token.

Lo que se obtiene como una clara conclusión de la intervención de las criptomonedas en el blanqueo de capitales es que se facilita enormemente la tercera fase, en la que el capital es reintegrado, ya que facilitando la posible actividad de un testaferro[1] y, complicando por tanto nuevamente conocer la identidad del presunto autor del crimen (Navarro, 2019).

3.2 Delitos que utilizan las criptomonedas como medio de pago.

En esta tipología delictiva, la criptomoneda se utiliza simplemente como medio de

[1] Dícese de la persona que en un negocio o asunto jurídico ajeno, cede su nombre para aparecer como titular, encubriendo por tanto a los dueños originales REAL ACADEMIA ESPAÑOLA:

pago para llevar a cabo el delito, provocando esto que la conducta delictiva sea la misma que de manera previa a la existencia de estos criptoactivos, simplemente llevando a cabo la modificación del pago para garantizar un mayor anonimato y de esta manera dificultar el rastreo del autor o autores en las investigaciones posteriores. A continuación se presentan los dos delitos identificados en esta categoría: extorsión, y dentro de los delitos contra la salud pública, narcotráfico.

3.2.1 Extorsión.

El delito de extorsión se encuentra recogido en el artículo 243 del Código Penal español, y en este se determina que "*El que, con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero (…)"*

En cuanto a la naturaleza de este delito respecta, podría denominarse un delito "híbrido", ya que se encuentra dentro de los delitos patrimoniales, concretamente podría englobarse dentro de las estafas, debido a que, el ánimo de lucro, es un elemento necesario para la comisión de este delito pero por otro lado, podría igualmente englobarse dentro del delito de amenazas condicionales, ya que, el sujeto en cuestión expondría una amenaza y la condición para no cumplirla sería el capital a cambio.

En el año 2014, la Oficina Europea de Policía (Europol), realizó un estudio en el cual se descubrió que en aproximadamente un tercio de las extorsiones cibernéticas, el Bitcoin era utilizado como rescate. Esta investigación también desveló que esta misma criptomoneda también era contemplado como una opción de rescate en los casos de extorsión llevados a cabo fuera de la red, como podrían ser los secuestros, pudiendo determinarse por tanto que Bitcoin es, de todas las criptomonedas, el token descentralizado más usado en los delitos de extorsión (Europol).

3.2.2 Delitos contra la salud pública.

Los delitos contra la salud pública son aquellos que afectan de una manera negativa al bienestar social provocando daños a la salud del colectivo. Esta tipología delictiva se encuentra regulada en el Título XVII, Capítulo III del Código Penal, concretamente en los artículos del 359 al 378. Es importante tener en cuenta, que dentro del Código Penal se encuentran diferenciados los delitos relacionados con el comercio de sustancias que puedan resultar nocivas para la salud (artículos 359-367) y por otro lado, aquellas conductas relacionadas con el narcotráfico (artículos 368-378). Es esta

segunda tipología delictiva la que más sencilla es de cometer mediante el uso de criptomonedas, reduciendo el uso de estas la posibilidad de resolver el delito.

En el año 2017, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNDOC, siglas en inglés) publicó un apartado en su Informe Mundial de Drogas un apartado dedicado al uso de los tokens en el narcotráfico. En este informe se determina que la tecnología está generando un mercado de droga de bajo riesgo ya que gracias a las comunicaciones telefónicas, los traficantes de estas sustancias no tienen necesidad de mantener un contacto personal con los clientes, de manera que estos delegan en unos traficantes de un inferior nivel que hacen de intermediarios entre los grandes traficantes y los compradores, de tal manera que estos transportan la droga y el dinero. Al igual que la posibilidad de comunicarse mediante mensajes encriptados supuso una revolución, lo mismo sucedió con el uso de las criptomonedas, ya que conforme este fue normalizándose, la "*darknet*" como la denomina la UNDOC, ofrece la posibilidad de realizar la compra de sustancias ilícitas por medio de tokens y acordar el punto de recogida de la mercancía.

La UNDOC especifica que estas acciones son de momento un pequeño porcentaje dentro de todos los movimientos que se realizan con los tokens, pero, a pesar de ello, en los últimos años ha crecido de manera notable gracias al anonimato, tanto para comprador como para vendedor, que este mercado ofrece, y siendo esta característica una disminución del riesgo de ser detenidos por llevar a cabo esas acciones ilícitas.

3.3 Casos mediáticos.

A continuación, van a recogerse algunas noticias resumidas de algunos delitos que se han llevado a cabo o bien mediante el uso de las criptodivisas, o bien con estas como medio de pago. El objetivo de este apartado es que sirva como ejemplo y refuerzo de los delitos explicados de manera anterior.

3.3.1 A nivel nacional.

El 3 de junio de 2022, el periódico digital *Noticias de Navarra* publicó una noticia titulada "Detenido un pamplonés por estafar 143.650 euros como asesor de criptomonedas" en la cual se relata el caso de un joven de 25 años que lleva a cabo una estafa piramidal conocida como Estafa Piramidal de Ponzi[2], con bitcoin, mediante

[2] Esta estafa se lleva a cabo mediante las promesas a los clientes de elevadas rentabilidades, mucho más altas de lo que se obtienen en el mercado, comprometiéndose a invertir las cantidades que las víctimas le proporcionaban, pero esto finalmente no sucede, ya que esta cantidad se ve incorporada al patrimonio del autor. Al inicio de la estafa, los pagos de vuelta a los clientes sí que se realizan con

el ofrecimiento de asesoramiento sobre cómo invertir con estas. Además otro de los delitos cuya autoría se le atribuye es el de extorsión, ya que prometía una compensación económica a cabio de mantener relaciones sexuales con él.

Tras la investigación llevada a cabo por la Policía Judicial se descubrió que había 14 personas afectadas y que la captación de estas se llevaba a cabo mediante la exhibición, por parte del autor, del manejo de dinero en efectivo con el que contaba, alardeándose de que no contaba con un empleo y de que él se consideraba un "*inversor en bolsa y cocaína*". Mediante este embaucamiento, los afectados le confiaban sus ahorros para que consiguiera ese elevado tipo de rentabilidad mediante la inversión de estas en criptomonedas.

Estas tres noticias que se van a describir a continuación como casos mediáticos acaecidos en nuestro país, fueron publicadas el 22 de mayo de 2022 en el periódico digital *Madrid Actual*, de un artículo en el que se relatan las mayores estafas que se han cometido mediante el uso de criptomonedas en España.

"Javier Biosca superó los 250 millones de euros estafados a los inversores". La captación de las víctimas se realizaba ofreciendo una elevada rentabilidad (20-25%) por WhatsApp. Javier Biosca se encontraba al frente de la empresa Algorithmics Group, siendo considerado un bróker español y encontrándose acusado de un delito continuado de estafa, apropiación indebida y falsedad de documentos públicos, elevándose el número de víctimas a 300, elevándose la cantidad a más de 250 millones de euros y siendo por tanto el mayor fraude en nuestro país hasta el momento relacionado con los tokens.

"Caso Bitchain, pioneros en Bitcoin y estafas". Jordi y Miguel Alcaraz, en 2018 y utilizando como tapadera su empresa llamada Bitchain, comenzaron la búsqueda de fuentes que financiaran el proyecto de manera externa para poder llevar a cabo un proyecto basado en el intercambio de BTC, contando hasta con el apoyo de la Generalitat de Cataluña para instalar cajeros en los que pudiera extraerse el dinero procedente de Bitcoins. Los acusados no destinaron el dinero a las inversiones prometidas sino que lo gastaron en otros asuntos, estafando 180.000€ a una empresa y dos particulares.

---

intereses, sirviendo como incentivo para invertir cantidades más grandes, ya que así, la ganancia aumentará. Cuando se consigue que la víctima invierta una importante cantidad de dinero, el estafador les comenta que en ese momento no puede parar de invertir, ya que sino todo lo que ya ha sido invertido se perderá, continuando las víctimas esa ficticia inversión, y, no recuperando las últimas grandes inversiones.

“Caso Arbistar, la mayor estafa piramidal con criptomonedas de España”. El caso toma su nombre de una empresa cuya sede se encuentra en Tenerife, Arbistar 2.0 SL. Estas consiguieron atraer a las víctimas mediante la promesa de unas rentabilidades mensuales que podían llegar al 15%, viéndose esta promesa cumplida hasta que el uno de los administradores de la sociedad congeló las cuentas en septiembre de 2021. El número de víctimas al que afecta esta gran estafa piramidal es de unas 30.000 personas, basándose en la cantidad de cuentas que se ha visto afectada. La cantidad de fondos involucrados en esta causa sería de más de 10.000 BTC, un total más de 100 millones de euros.

3.3.2 A nivel internacional.

“Phishing por un valor de un millón de euros anual”. Bajo este titular publicaba el 22 de mayo de 2022 el periódico *Madrid* Digital el artículo en el que se narran los siguientes hechos. En 2019 se detuvieron de manera simultánea a 47 ciberdelincuentes, 24 de ellos en España y 23 en Marruecos. Todos ellos eran miembros de una red internacional y llevaban a cabo delitos de phishing, robando datos bancarios de unas 300 personas, consiguiendo estafar aproximadamente 1.000.000€ de manera anual y utilizando las criptomonedas como elemento de blanqueo para evitar levantar sospechas.

“La gran estafa con criptomoneda: 20 millones y cientos de afectados en España y otros países”. Según establece el periódico digital *La Razón*, la Macroestafa fue cometida por un conjunto de empresas localizadas en unos 30 países, pero con un mayor arraigo en Bulgaria y Estonia, utilizando estas falsas noticias en las que se aseguraban que junto a ellas invertían personajes públicos como Leo Messi, Pedro Sánchez o Amancio Ortega ente otros, sirviendo estas como cebo para que los inversores se animasen y acabaran perdiendo todo el dinero. Esta estafa, al igual que en la del resto de noticias mencionadas en el trabajo, es una Estafa Piramidal de Ponzi, y, se estima que la organización que la llevaba a cabo estaría compuesta por unas 120 personas, 235 cuentas bancarias (99 en nuestro país) y 237 empresas.

4 Propuestas para la prevención de estos delitos.

La prevención de los delitos que mantienen relación con las criptodivisas, es un asunto que necesita mantenerse en constante evolución, ya que, las criptomonedas se encuentran en plena expansión y son relativamente “nuevas”, por lo que, poco a poco van a ir apareciendo nuevas aplicaciones para estas, encontrándose incluidos dentro de estas nuevas aplicaciones, nuevos delitos.

A continuación se muestran las medidas que se encuentran en la Tabla 2. Medidas de autoprotección enfocadas a la población y medidas enfocadas a las leyes reguladoras a nivel mundial, europeo y nacional.

Medidas de protección	
Autoprotección Población	Buen conocimiento sobre el funcionamiento de las criptomonedas.
	Verificar la identidad de las personas con las que se están llevando a cabo las transacciones.
	Proteger el wallet en el que se encuentran almacenadas las criptodivisas
Leyes reguladoras	A nivel mundial: pautas homogeneizadoras de las legislaciones de los diferentes países (FMI)
	A nivel europeo: Reglamento MiCA
	En España: Ley 11/2021 de 9 de julio de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016.

Tabla 2. Medidas de protección.

4.1 Enfocadas a las personas.

Observando las noticias sobre los casos reales y más mediáticos que han ocurrido tanto a nivel nacional como internacional, se podría determinar que una de las propuestas para la prevención de los delitos que se cometen con criptomonedas, ya sea mediante ellas, o utilizándolas como medio de pago, el objetivo sería intentar concienciar a la población de los riesgos a los que pueden estar expuestos, para, de esta manera evitar ser una posible víctima, ya que como puede apreciarse, la mayoría de delitos que se cometen suelen ser de estafa, apelando por tanto a que las personas que se encuentran en el mundo de las criptomonedas sean un poco menos confiadas con las ofertas que puedan llegarles.

En este apartado van a plantearse medidas de prevención enfocadas a la población en general, pudiendo definirse estas como medidas de autoprotección, ya que la finalidad es que ellos mismos intenten, mediante las pautas que aquí se les proporcionan, detectar los delitos que previamente se han explicado para evitar ser las

víctimas.

No existen iniciativas internacionales ni nacionales enfocadas a la autoprotección de las personas a diferencia de lo que sucede con las medidas legislativas, que sí que se encuentran propuestas por parte de diferentes organismos gubernamentales. A pesar de ello, a partir de la experiencia del autor de este TFG se considera que podrían llevarse a cabo las siguientes:

- Conocimiento sobre el funcionamiento de las criptomonedas.
- Verificación de la identidad.
- Protección del wallet.

En primer lugar y, haciendo una apelación al sentido común, una de las medidas de autoprotección básicas dirigidas a la población es tener un buen conocimiento sobre el funcionamiento de las criptomonedas. Esta medida se considera la base de la autoprotección ante estos delitos, ya que, en caso de no tener los conocimientos necesarios sobre el funcionamiento de las criptomonedas, la persona se convierte en una potencial víctima de ser estafada tanto de manera virtual en la cybernet, como, por falsos asesores que lleven a cabo estafas piramidales, ya que, al no contar con información suficiente sobre las criptodivisas, cualquier porcentaje de rentabilidad que pueda ofrecérsele y sea un poco elevado, lo va a visualizar como una ganga.

La segunda medida de autoprotección, es la de verificación de la identidad de las personas con las que se están llevando a cabo las transacciones, además de intentar llevar a cabo un registro de las transacciones que se llevan a cabo y del valor de cada una de ellas. De esta manera, en el caso de que la persona estuviera siendo objeto de una estafa mediante el uso de falso wallet, si esta notase una periódica desaparición de sus criptodivisas, podría avisar a tiempo a las autoridades para ponerle solución al problema.

La tercera medida es proteger el wallet en el que se encuentran almacenadas las criptodivisas con las que se cuenta. La mejor manera para que estas se encuentren protegidas es en un wallet frío, ya que este tipo de billetera de criptomonedas es un hardware, de tal manera, que, en el caso de que un hacker tuviese acceso a su ordenador, estas no se encontrarían en el interior de este. En el caso de que las criptodivisas se encuentren almacenadas en un Wallet caliente (aquel que permanece en el interior del equipo informático), tampoco hay por qué preocuparse, ya que se cuenta con un sistema de doble identificación a la hora de llevar a cabo cualquier tipo de transacción con criptomonedas y acceder al monedero, da igual del tipo que sea.

La mejor manera de proteger el monedero digital es generar contraseñas difíciles de adivinar, y, almacenar los códigos en lugares seguros por si se sufriera un ataque informático.

4.2 Enfocadas a las leyes reguladoras.

Otra de las maneras existentes para intentar prevenir la comisión de crímenes relacionados con los activos digitales, es la implantación de leyes y reglamentos que regulen, por ejemplo, el funcionamiento de estas, o la manera en la que hay que declararlas, para de esta manera, contar con otro factor de control, para conseguir que el funcionamiento de estas criptodivisas sea un poco más transparente y, por tanto, suponiendo esto una dificultad añadida para cometer crímenes mediante el uso de estas.

4.2.1 A nivel mundial.

La creación de las criptomonedas y la globalización de estas sucedieron de manera fugaz, suponiendo esto un gran vacío legal que cada país solucionó de la manera que más correcta consideraba, por lo que en cada uno de ellos se comenzó a regular este asunto de una manera diferente, encontrándose por ejemplo países que prohibieron a sus habitantes la posibilidad de tener criptoactivos, o de contar con la capacidad para llevar a cabo acciones con estos y por otro lado, países que fueron un poco más progresistas, y que llegaron a contratar empresas para poder facilitar que la población que estuviera interesada, pudiera llevar a cabo las acciones que considerase pertinentes con las criptomonedas, implementando por tanto su uso (Fondo Monetario Internacional, 2022).

Ante la heterogeneidad observada en las diferentes leyes que los países han generado para la regulación de estos activos digitales, el FMI está intentando generar unas pautas que deban seguir las normas reguladoras de los criptoactivos, para que estas no difieran tanto las unas de las otras. A pesar de esto, la gran preocupación que les abruma, es que si la creación de una legislación común se prolonga mucho en el tiempo, serán muchos los países que ya hayan generado su propia normativa, contando por tanto con marcos regulatorios distintos. Ante este dilema el FMI ha solicitado que se lleve a cabo una respuesta globalizada para obtener mejores resultados. Esta respuesta debe ser coordinada, para evitar las brechas entre regulaciones de diferentes países y de esta manera, generar unas condiciones homogéneas, también debe ser congruente, para conseguir una concordancia con las normas tradicionales en lo que respecta a las acciones que se pueden llevar con estas

y los riesgos que suponen y para finalizar, esta respuesta debe ser integral, de manera que consiga abarcar todos los aspectos del ecosistema que las criptomonedas presentan (Narain & Moretti, 2022).

Uno de los ejemplos de la heterogeneidad en la legislación de los diferentes países es que en septiembre de 2021, El Salvador se convirtió en el primer país en utilizar la criptomoneda Bitcoin como moneda de curso legal, al igual que el dólar (Barría, 2023). Esto supuso grandes cambios a nivel social, ya que, las empresas y establecimientos, se vieron obligados a aceptar la criptomoneda como medio de pago. Por otro lado, para poder utilizar esta criptomoneda como moneda digital, Bukele (el mandatario), ha comprado BTC con fondos públicos, confiando mucho en esta y son tener en cuenta las advertencias que sugieren el alto riesgo al que se ven expuestos, ya que, BTC, funciona por especulación.

Por otro lado y en abril de ese mismo año, Turquía prohibía llevar a cabo las transacciones con criptoactivos, siendo esto una consecuencia de la escasa regulación con la que contaban, siendo esta una muestra de la heterogeneidad con la que contaban las regulaciones en los diferentes países. A pesar de esto y según apuntan los medios de comunicación, a lo largo de este año, Turquía va a crear una lira turca digital para poder llevar a cabo transacciones dentro del propio país.

4.2.2 En la Unión Europea.

La Autoridad Bancaria Europea comenzó en el año 2020 a desarrollar el Reglamento MiCA (Markets in Crypto-Assets). Este es, por el momento, una propuesta que cuenta con medidas para lograr optimizar y regular la contabilidad de los activos virtuales dentro de la Unión Europea, para, de esta manera intentar facilitar los movimientos que usuarios e inversores llevan a cabo, intentando abordar de una manera correcta los riesgos que puedan derivarse de la compra-venta de criptomonedas. Este reglamento se encuentra actualmente en periodo de revisión por parte del Parlamento Europeo y del Consejo de la Unión Europea, ya que, se prevé su entrada en vigor para el año 2024.

En la 6ª conferencia mundial sobre Finanzas Criminales y Criptodivisas que impartió la Europol el 1 y 2 de septiembre del pasado año, se expuso que el sector privado, las fuerzas del orden y los reguladores, se encuentran trabajando de manera exhausta para adelantarse a los criminales que se dedican a cometer delitos y blanqueos de capitales mediante el abuso de los criptoactivos. Europol también expuso que cada vez la normativa es más estricta, utilizando como ejemplo la nueva normativa

de la UE, mediante la cual se pretende garantizar que a las criptomonedas se les ofrezca el mismo trato que a cualquier otro activo para facilitar las medidas de control sobre estas. Además, expusieron cómo se han logrado resolver múltiples casos de una manera exitosa, ya que, los investigadores, se encuentran actualmente aprovechando las características únicas que presenta la cadena de bloques para de esta manera poder realizar un seguimiento del dinero, permitiéndoles esto identificar delitos como estafas, además de a redes especializadas en el blanqueo de capitales, y a grupos de delincuencia organizada.

Las autoridades tanto policiales como judiciales, con el paso del tiempo, han cambiado el trato que les daban a los activos virtuales, siendo este ahora cada vez más similar al de los activos físicos visto desde el punto de vista legal. De esta manera, se consiguen facilidades para incautarlos y gestionarlos. Por otro lado, las empresas privadas reman en la misma dirección, innovando velozmente las herramientas con las que cuentan para poder rastrear los activos blanqueados mediante varias blockchain.

Desde Europol concluyeron que, conseguir que se aumente la comprensión y la capacidad de la criptoweb entre los reguladores, fuerzas de seguridad y el sector privado, es la clave para conseguir combatir el blanqueo de capitales y la delincuencia organizada.

4.2.3 En España.

En España, actualmente se encuentra activa la Ley 11/2021 de 9 de julio de medidas de prevención y lucha contra el fraude fiscal, de transposición de la Directiva (UE) 2016/1164, del Consejo, de 12 de julio de 2016. Mediante esta ley, se introducen normas enfocadas contra la comisión de prácticas de elusión fiscal, normas enfocadas a la transformación de algunas normas tributarias que ya se encuentran activas y normas dedicadas a la regulación del juego.

Esta ley se creó con el objetivo de ser un elemento para combatir el fraude, blanqueo de capitales y delitos patrimoniales que se llevan a cabo con los criptoactivos, ya que, desde el 1 de enero de este año, es necesario que las personas que posean criptoactivos con un valor conjunto que supere los 50.000€ los tributen. Esto supone un elemento de control fiscal sobre cuánto invierte el individuo en cuestión y la rentabilidad que estas presentan, haciendo entonces saltar las alarmas en el supuesto de que un individuo con un nivel de vida estándar pueda invertir una cantidad económica muy elevada.

CONCLUSIONES

En este TFG se han analizado los delitos relacionados con las criptomonedas y se han identificado las principales medidas que pueden llevarse a cabo para prevenirlos. A continuación se enumeran las principales conclusiones que pueden extraerse de este trabajo:

PRIMERA: La creación de la primera criptomoneda en el año 2008, BTC, se produjo como solución a la necesidad de encontrar otro medio para poder llevar a cabo movimientos de dinero sin tener que contar con el control, en ocasiones excesivo, de las autoridades monetarias. Además del control que la banca ejercía, debido al contexto de crisis internacional que se dio en la época, la población había disminuido notablemente su confianza en los bancos, suponiendo las criptomonedas una nueva solución a este problema, y ofertando la posibilidad de no necesitarlos.

SEGUNDA: Desde el lanzamiento del bitcoin, el fenómeno de las criptomonedas ha crecido de manera exponencial, aumentándose el número de criptoactivos que se encuentran en el mercado, y, el número de compradores para estas, ya que, hoy en día, cualquier individuo puede comprarlas, sin necesitar acreditar ningún tipo de conocimiento o formación sobre el tema.

TERCERA: Con la globalización de estas criptodivisas, además de beneficios, se han generado riesgos, estando estos causados por la adaptación de delitos ya existentes para poder llevarlos a cabo mediante el uso de estos tokens, o, la creación de nuevos. Este factor aunado a que hoy en día cualquier persona puede formar parte del mundo de las criptomonedas genera la necesidad de que cualquier individuo que vaya a hacerlo, se forme de manera adecuada para evitar ser víctima potencial de aquellos delitos.

CUARTA: La evolución no se ha visto solamente reflejada en los delitos, sino también en los delincuentes, ya que, antiguamente los delitos se cometían de manera física y por tanto requerían un mayor esfuerzo. Hoy en día, gracias a internet, un delincuente puede llevar a cabo varios delitos de manera simultánea y si necesidad de abandonar su domicilio ni de enfrentarse cara a cara a la víctima, simplemente encontrándose frente a una pantalla. Esto le resta importancia a la capacidad de intimidar y a la apariencia física del delincuente, y, provoca que actualmente haya que centrarse más en la capacidad intelectual y los conocimientos que tenga sobre informática.

QUINTA: A pesar de que las criptomonedas llevan instauradas desde 2008, no existen, por el momento, unas directrices globales, para que los países generen las normas con

las que se regulan los criptoactivos, derivando esto en una legislación muy heterogénea entre las diferentes naciones, y provocando esto una desigualdad entre los habitantes de estas. Asimismo, tampoco se recomiendan medidas de autoprotección que la población debería llevar a cabo. Es por ello por lo que la autora de este TFG propone las siguientes: Buen conocimiento sobre el funcionamiento de las criptomonedas; Verificar la identidad de las personas con las que se están llevando a cabo las transacciones; y Proteger el wallet en el que se encuentran almacenadas las criptodivisas.

SEXTA: A pesar de lo necesaria que es una regulación sobre las criptomonedas, es importante tener en cuenta que estas triunfaron entre la población por su descentralización e independencia con respecto de las instituciones bancarias y los gobiernos, por lo que, por el momento, es difícil saber los cambios que esta regulación provocará en el mercado y la demanda de las criptodivisas.

En lo que a mi experiencia personal respecta, elegí este tema para realizar mi trabajo de fin de grado, ya que considero que es una de las maneras en la que se delinque hoy en día, y que se va a seguir haciendo, considero que cada vez más. A pesar de ello, como he remarcado en varias ocasiones durante la escritura de mi trabajo, considero que ni la población ni los poderes públicos se encuentran suficientemente concienciados del peligro que puede suponer esta nueva forma de inversión, y es por ello por lo que he decidido enfocarlo de esta manera. Además, realizar este trabajo me ha permitido desarrollar labores de investigación sobre el mundo de las criptomonedas y ampliar mis conocimientos con respecto a su funcionamiento, tanto lícito como ilícito de estas, y, relacionarlo con los conocimientos que he adquirido durante los 4 años de carrera.

BIBLIOGRAFÍA

Ayllón, L. E. (2022). Principios básicos en criptomonedas y estudio sobre su conocimiento y manejo. Trabajo de Fin de Grado, Universidad de Valladolid. Disponible en: https://uvadoc.uva.es/bitstream/handle/10324/54532/TFG-J-375.pdf?sequence=1 [Consultado: 20-03-2023]

Barría, C. (2023). "Bitcoin en El Salvador: qué busca la inédita y controvertida ley que redobla la apuesta de Bukele por las criptomonedas". *BBC News Mundo*, 19 de enero. Disponible en: https://acortar.link/RDftQK [Consultado: 19-04-2023]

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., y Serusi, S. (2021). *Cryptocurrency scams: analysis and perspectives*. Ieee Access, *9*, 148353-148373. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634

Bokovnya, A. Y., Shutova, A. A., Zhukova, T. G., y Ryabova, L. V. (2020). *Legal measures for crimes in the field of cryptocurrency billing. Utopía y Praxis Latinoamericana*, 25(7), 270-275. https://www.redalyc.org/journal/279/27964362028/27964362028.pdf

[Consultado: 05-03-2023]

Calleja, T. (2021). "La gran estafa con criptomoneda: 20 millones y cientos de afectados en España y otros países". *La Razón*, 10 de abril. Disponible en:

https://www.larazon.es/espana/20210409/a4byhutxrbfynblbcx6md5yxwi.html
[Consultado: 13-03-2023]

Cediel, A. y Pérez, E.P (2020). "*Fiscalidad de las criptomonedas*": Atelier Libros Jurídicos.

Diccionario de la lengua española, 23.ª ed., [versión 23.6 en línea]. Disponible en: https://dle.rae.es [Consultado: 15-02-2023].

EFE. (2022). "Turquía empezará a utilizar una moneda digital propia a partir de 2023". *El Liberal*, 30 de diciembre. Disponible en: https://www.elliberal.com/turquia-empezara-a-utilizar-una-moneda-digital-propia-a-partir-del-proximo-ano/ [Consultado: 19-04-2023]

Fernández Civenta, O. (2021). *50 conceptos relacionados con las criptomonedas que deberías conocer antes de invertir*. Bussines Insider. Disponible en: https://www.businessinsider.es/50-conceptos-criptomonedas-tienes-conocer-935297

[Consultado: 07/02/2023]

Fernández, J (2022). "Un repaso por las mayores estafas de criptomonedas en España".

Madrid Actual, 22 de mayo. Disponible en : https://www.madridactual.es/7836812-un-repaso-por-las-mayores-estafas-de-criptomonedas-en-espana [Consultado: 14-03-2023]

GAFI: Directrices para un enfoque basado en riesgo para monedas virtuales.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Montes, S. (2021). *Las estafas de pago por adelantado evolucionan con el uso de supuestas plataformas para ganar criptomonedas*. Disponible en : https://is.gd/OCfbka [Consultado: 26-02-2023]

Morales, J. (2022). "Detenido un pamplonés por estafar 143.650 euros como asesor de criptomonedas". *Noticias de Navarra*, 3 de junio. Disponible en:

https://www.noticiasdenavarra.com/actualidad/2022/06/03/detenido-pamplones-estafar-143-650-3559560.html [Consultado: 13-03-2023]

Nakamoto, S. (2009). Bitcoin: *A peer-to-peer electronic cash system Bitcoin*. Disponible en https://bitcoin.org/en/bitcoin-paper [Consultado: 05-02-2023]

Narain, A., Moretti, M. (2022). "La regulación de los criptoactivos". *Fondo Monetario Internacional*, 22 de septiembre. Disponible en:

https://www.imf.org/es/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti [Consultado: 25-03-2023]

Navarro Cardoso, F. C. (2019). "Criptomonedas (en especial, bitcoin) y blanqueo de dinero". *Revista electrónica de ciencia penal y criminología,* 21-14, pp. 16-40. Disponible en: http://criminet.ugr.es/recpc/21/recpc21-14.pdf [Consultado: 08-02-2023]

Oficina Europea de Policía (Europol). (2022). *Cryptocurrencies key to tackling organised crime – Europol and Basel Institute on Governance*. Disponible en:

https://acortar.link/U3lsTJ [Consultado: 17-03-2023]

Oficina Europea de Policía (Europol). (2014). *Internet organized crime threat assessment*. Disponible en:

https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2015.pdf [Consultado: 05-03-2023]

Organización Nacional de Policía Criminal (INTERPOL). (s.f.). *Blanqueo de capitales.* Disponible en: https://acortar.link/zbZcmc [Consultado: 17-03-2023]

Reddy, E. y Minnaar, A. (2018). "Cryptocurrency: A tool and target for cybercrime". *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3), 71-92.

https://is.gd/l6NI20 [Consultado: 14-02-2023]

Roca, C. (2023). *Invertir en criptomonedas: Guía completa [2023].* Disponible en: https://www.thepowermba.com/es/blog/invertir-en-criptomonedas [Consultado: 20-03-2023]

Romero, N. (2022). "El mercado de criptoactivos y el Reglamento MiCA". *INEAF Bussines School*, 12 de diciembre. Disponible en: https://www.ineaf.es/tribuna/el-mercado-de-criptoactivos-y-el-reglamento-mica/ [Consultado: 20-03-2023]

Sánchez, L.J. (2022). "El Reglamento MiCa obligará a las empresas de criptoactivos a notificar operaciones de M&A por su relevancia al regulador". *Confilegal*, 7 de septiembre. Disponible en: https://acortar.link/7mZYGI [Consultado: 20-03-2023]

United Nations Office on Drugs and Crime (2014): *Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*. Disponible en:https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf [Consultado: 17-02-2023]

United Nations Office on Drugs and Crime: World Drug Report 2017, Book 5 (2017): *The drug problem and organized crime, illicit financial flows, corruption and terrorism*, pp. 16 y ss. Disponible en: https://www.unodc.org/wdr2017/field/Booklet_5_NEXUS.pdf

[Consultado: 07/02/2023]

Vives Antón/ Orts Berenguer/ Carbonell Mateu/ González Cussac/ Martínez-Buján Pérez: Derecho Penal. Parte Especial. 3a ed. Tirant lo Blanch. Valencia, 2011.

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). "Characterizing cryptocurrency exchange scams". *Computers & Security*, 98, (101993), pp. 1-3. Disponible en: https://is.gd/Zrr0hh [Consultado: 03-03-2023]

A Anexo 1: Glosario.

- Blockchain (cadena de bloques): tipo de Libro Mayor de contabilidad digital y universal en el cual se registran todas los movimientos (transacciones, operaciones de compra-venta…) y las titularidades de manera cronológica, suponiendo esto un plus de transparencia y seguridad dentro de la red entre pares (P2P). (Cediel. Pérez, 2020)

  El elemento más importante de esta tecnología es que es capaz de transmitir, además de información, valor de manera digital, suponiendo una revolución para la época digital. (González de Frutos, 2018)
- Brokers de criptomonedas: plataforma digital que adquiere la posición de intermediario para que sea posible llevar a cabo operaciones con activos digitales. (Fernández, 2021)
- Exchange: plataforma digital en la cual se llevan a cabo tanto compras como ventas de criptomonedas. (Fernández, 2021)
- Red Peer to Peer: Sistema de intercambio entre pares en el cual no es necesario contar con una autoridad central como podría ser un banco en el caso del intercambio de dinero. Es el sistema base utilizado en el funcionamiento de Bitcoin y del resto de criptomonedas. (Nakamoto, 2008)
- Tokens: son objetos parecidos a las monedas, pero carecientes de valor de curso legal, ya que se crean en una comunidad privada y en un estado de necesidad contando por tanto con poco valor. A pesar de que inicialmente el valor con el que estos cuentan es escaso, este puede volverse elevado dentro de la comunidad en la que se utilizan, como, por ejemplo, el del Bitcoin. (Maldonado, 2018)
- Wallet: cartera digital en la cual se almacenan tanto el usuario como las claves necesarias para poder llevar a cabo diferentes transacciones, ventas y compras de criptomonedas. (Fernández, 2021). Estos pueden ser de dos tipos:
  - Frío: las claves se almacenan en dispositivos electrónicos sin acceso a internet, siendo conocidos estos también como hardware, y, pudiendo ser por ejemplo un USB o un disco duro.
  - Caliente: se utiliza un almacenamiento criptográfico en línea para proteger dichas claves.