



TRABAJO FIN DE GRADO
GRADO EN CRIMINOLOGÍA
CURSO ACADÉMICO 2021/2022
CONVOCATORIA OCTUBRE

TÍTULO:

ALUMNO:

DNI: 48054014E

GRADO: Criminología

TUTOR:

Fecha: 3/10/2021

ÍNDICE DE CONTENIDOS

I.	INTRODUCCIÓN...	3
1.	Justificación del tema.....	3
2.	Objetivos.....	4
3.	Metodología.....	5
II.	LAS CRIPTOMONEDAS...	5
1.	Definición y características principales.....	5
2.	Tipos de criptomonedas.....	7
III.	LEGISLACIÓN CRIPTOMONEDAS...	8
1.	Criptomonedas en España.....	8
2.	Criptomonedas en Europa.....	10
2.1.	Regulaciones de la Unión Europea.....	10
2.2.	Consideraciones específicas sobre la regulación de las criptomonedas en los países de la UE.....	11
3.	Criptomonedas en el resto del mundo.....	14
IV.	LOS DELITOS ECONÓMICOS...	15
1.	Tipología.....	15
2.	Ejemplos de delitos económicos cibernéticos con criptomonedas.....	19
2.1.	Estafas. Arbistar 2.0 S.L., suplantación de personajes televisivos y sorteos de criptomonedas.....	19
2.2.	Extorsión. Secuestro de ordenadores mediante ransomware.....	24
2.3.	Blanqueo de capitales. Caso Mixers y Operación Tulipán Blanca.....	26
2.4.	Financiación de organizaciones criminales o grupos terroristas como el ISIS.....	30
2.5.	Robos. 2gether, Pony y Bitfinex.....	31
2.6.	Especulación. “Pump and Dump”, Caso Tubacex y especulación por influencia.....	32
V.	MECANISMOS PARA EVITAR Y AFRONTAR DELITOS ECONÓMICOS CON CRIPTOMONEDAS...	33
1.	La Legislación.....	33
2.	Prevención: Mecanismos para evitar posibles delitos económicos con monedas digitales.....	35
VI.	CONCLUSIONES...	38
VII.	BIBLIOGRAFÍA.....	40

ÍNDICE DE ILUSTRACIONES

Ilustración 1. <i>La Audiencia Nacional investigará el caso Arbistar, la mayor estafa piramidal con criptomonedas</i>	20
Ilustración 2. <i>Casos de correos electrónicos de Phishing</i>	21
Ilustración 3. <i>Fases de la estafa con criptomonedas</i>	23
Ilustración 4. <i>El timo de las criptomonedas usa a Jordi Évole y El Hormiguero</i>	24
Ilustración 5. <i>Los 6 principales métodos de estafa de criptomonedas</i>	24
Ilustración 6. <i>Fake Elon Musk Crypto Giveaway Scam Gets 0.4 BTC as Twitter Fails to Vet Advert</i>	25
Ilustración 7. <i>Elon Musk, Jeff Bezos, and Bill Gates appear to have had their Twitter accounts hacked as part of a bitcoin-giveaway scam</i>	25
Ilustración 8. <i>Y, como estaba anunciado, la burbuja del bitcoin pinchó</i>	26
Ilustración 9. <i>Wanna Decryptor: así funciona el ransomware que se ha usado en el ciberataque a Telefónica</i>	26
Ilustración 10. <i>La Guardia Civil desarticula una organización criminal dedicada al blanqueo de capitales procedentes del narcotráfico mediante el uso de criptomonedas</i>	29
Ilustración 11. <i>Los terroristas ahora se financian con Bitcoin</i>	31
Ilustración 12. <i>“Pony” botnet pilfers digital coins worth \$220,000 in sustained attack</i>	31
Ilustración 13. <i>Elliptic Follows the \$7 Billion in Bitcoin stolen from Bitfinex in 2016</i>	32
Ilustración 14. <i>Elliptic Follows the \$7 Billion in Bitcoin stolen from Bitfinex in 2016</i>	32
Ilustración 15. <i>Tubacex, el fabricante de tubos sin soldadura que perdió más de 18 millones por la crisis</i>	34

I. INTRODUCCIÓN

El surgimiento de las nuevas tecnologías y el auge de los nuevos métodos de pago virtuales, es decir, los no físicos (como las criptomonedas), ha provocado que los delitos que se cometían antiguamente con el dinero fiduciario sean distintos a los actualmente se pueden cometer. Más específicamente, cambian las herramientas o técnicas que se emplean, y con ello la manera en la que se producen los delitos económicos.

Por tanto, el objetivo general de esta investigación es averiguar, a través de una revisión documental y bibliográfica, cuáles son los principales delitos económicos cibernéticos con criptomonedas que pueden perpetrarse actualmente y los mecanismos que se podrían implantar para evitarlos. En este caso, el Bitcoin (la criptomoneda más famosa y con mayor capitalización del mercado actualmente) puede aprovechar esos vacíos legales, al no ser una moneda de curso legal ni estar bajo el amparo de las jurisdicciones de cada país. Este hecho es el que puede provocar que sea más cómodo cometer delitos con esta moneda y que pase desapercibido por las autoridades policiales, judiciales e incluso de los gobiernos de todo el mundo, ya que están, en muchos casos, exentas de cualquier control fiscal.

Actualmente, el auge del Bitcoin y de las criptomonedas en general en todo el mundo ha generado un gran revuelo. Mientras algunos países están a favor de su uso, otros se encuentran en contra, pero también algunos de ellos estudian la manera de poder encontrar una legislación que se ajuste a la nueva realidad social con tal de tener un buen uso por parte de la población de las criptomonedas, así como evitar que se produzcan hechos delictivos mediante dichas monedas digitales. Este fin se investigará en este estudio, es decir, se analizará, tras conocer el funcionamiento de las criptomonedas y sus distintos tipos, la legislación existente o la ausencia de esta para encontrar vacíos legales que puedan permitir a los criminales utilizar las criptomonedas para lucrarse. Seguidamente, se evaluarán por tipologías de delitos económicos que puedan darse con criptomonedas con ejemplos que demuestran su uso fraudulento por distintos grupos de personas. A continuación, se analizará la posible prevención aplicable para disminuir la producción de este tipo de delitos, con tal de salvaguardar el dinero de la población, así como aumentar la seguridad de los cripto inversores. Finalmente, se detallarán las conclusiones y líneas de investigación futuras que puedan surgir tras la investigación.

1. Justificación del tema

En este estudio documental y bibliográfico se pretende conocer el mal uso que le puede dar la sociedad a las criptomonedas, dada la importancia que éstas están adquiriendo en la actualidad como posibles nuevas formas de pago que se puedan instaurar en un futuro. Para investigar el uso fraudulento de las criptomonedas, se puede estudiar el uso de éstas como método para blanquear dinero, ya sea por particulares, empresas, gobiernos, organizaciones criminales o terroristas. Pero también para cometer otro tipo de delitos, como las estafas, que se producen con monedas virtuales donde se pretende que la gente invierta su dinero con la promesa de ganancias sustanciales, las cuales no se realizan nunca. También se producen amenazas y extorsiones, donde secuestran ordenadores mediante hackeos masivos que solamente pueden ser desbloqueados mediante un pago realizado con Bitcoins. Pero estos no son los únicos hechos delictivos que se pueden cometer con las criptomonedas, sino que

también pueden darse delitos contra la Hacienda Pública por el hecho de no declarar ganancias con las criptomonedas por parte de ciertos cripto inversores.

Todo ello, hace que sea necesario conocer la legislación vigente que regula el uso de las criptomonedas tanto en España como en Europa y en resto del mundo, con especial hincapié en las grandes potencias mundiales como Estados Unidos y China, así como averiguar cuáles son los entornos en los que más se reproducen e intentar incidir en éstos con tal de evitar escenarios proclives a que se comentan este tipo de actos delictivos con monedas digitales.

Como comentaba Juan Ramón Rallo, economista y profesor en la Universidad Francisco Marroquín, las criptomonedas están consideradas “un activo que surge debido a las nuevas tecnologías que tenemos disponibles y que ha llegado para quedarse”¹. Por otra parte, Kenneth Rogoff, profesor de Economía en la Universidad de Harvard y antiguo economista jefe del Fondo Monetario Internacional, considera que las criptomonedas deben ser reguladas lo antes posible dado “los bajos tipos de interés y la búsqueda ansiosa de los inversores por lograr rentabilidad en los mercados”². Cataloga, por tanto, al Bitcoin y al resto de criptomonedas como una burbuja que, además, permite delinquir fácilmente.

En resumen, nos interesa conocer si se puede blanquear dinero o no por medio de las criptomonedas, conociendo también qué plataformas se usan para comprar y vender monedas digitales. Asimismo, también conviene conocer cómo estas páginas webs utilizan mecanismos tanto para evitar ser víctimas de *hack* de manera masiva, como para salvaguardar la identidad de los inversores o para evitar blanqueo de capitales. Por tanto, nos podemos hacer las siguientes preguntas, que se podrán responder a lo largo del presente estudio y que son útiles para justificar el tema de nuestra investigación: ¿Es más fácil cometer un delito económico con monedas de curso legal que con las digitales? ¿Se puede evitar mediante alguna herramienta legislativa que sirva como método preventivo para la lucha contra el fraude fiscal realizado con cryptoactivos? ¿Y para evitar estafas o extorsiones? Lo que parece evidente, es la necesidad de una regulación conjunta por parte de los gobiernos para evitar el fraude fiscal con criptomonedas entre otro tipo de delitos.

2. Objetivos

2.1. Objetivo general

El objetivo principal de nuestro estudio es investigar el alcance delictivo de las criptomonedas y averiguar qué mecanismos legislativos o de otro tipo existen para prevenir el aumento de este tipo de delitos.

2.2. Objetivos específicos

Destacan los siguientes:

- Profundizar en el concepto “criptomoneda” y ahondar en sus características principales, así como en los tipos más importantes de criptomonedas que existen.
- Conocer la legislación vigente sobre las criptomonedas tanto en España como en Europa y el resto del mundo (principalmente Estados Unidos y China). Con ello se pretende intuir las intenciones futuras de dichos países en cuanto a su regulación.

¹ AGENCIA EFE (2021). *Las criptomonedas han llegado para quedarse, según los economistas*.

² ELECONOMISTA (2021). *Rogoff, sobre el bitcoin y las criptomonedas: "Las autoridades tienen que despertar antes de que sea tarde"*.

- Averiguar, por tipologías, los delitos económicos que se pueden cometer y cuáles de todos ellos pueden reproducirse mediante el uso de las nuevas tecnologías en general y las criptomonedas en particular, así como exponer varios ejemplos sobre ello.

Con todos estos objetivos, se persigue establecer unas pautas preventivas que puedan servir a los Estados para evitar este tipo de uso fraudulento de las monedas digitales dado el auge de éstas en el mundo y su posible implementación en la sociedad, y con una seguridad jurídica para los cripto inversores.

3. Metodología

Esta investigación se basa en una revisión documental y bibliográfica relativa al tema de las criptomonedas y los nuevos delitos económicos cibernéticos que se pueden cometer con ellas. Para hacer dicha revisión se han utilizado, por un lado, medios más convencionales como artículos de prensa o noticias y, por otro, investigaciones más académicas. Las primeras se han empleado con el objetivo de buscar información, por ejemplo, sobre las intenciones que tienen varios países a la hora de regular las criptomonedas o para ejemplificar los delitos económicos que se pueden cometer con este tipo de monedas digitales. Al existir información escasa sobre nuestro tema, este tipo de información nos ha facilitado realizar una aproximación al objeto de nuestra investigación. Las segundas, por su parte, nos han permitido dar un enfoque a la investigación más académica y objetiva. Para ello, se han empleado bases de datos típicas como Dialnet o Google Académico.

Durante la búsqueda de información se han utilizado distintos filtros que nos han ayudado a encontrar los documentos y estudios que se precisaban. Algunos de estos filtros han sido los siguientes: (1) por año, ya que al ser un tema bastante novedoso era preciso buscar información reciente; (2) por autor/a, procurando buscar expertos en la materia como legisladores o economistas; y (3) por palabras clave como “Bitcoin”, “Blanqueo de Capitales”, “Estafas”, “Ciberdelincuencia”, “Criptomonedas”, “Criptodivisas”, “Monedas digitales”, “Regulación” o “Financiación del Terrorismo”, entre otras, siendo preciso en algunas ocasiones la combinación de varias para poder obtener la información buscada.

En conclusión, la metodología empleada nos resultará útil, ya que nos permitirá alcanzar los objetivos propuestos con anterioridad al ofrecernos una amplia visión sobre los aspectos más importantes desarrollados en el presente estudio.

II. LAS CRIPTOMONEDAS

1. Definición y características principales

Desde los inicios de la civilización humana, han existido métodos que permitían intercambiar unas mercancías por otras. Al principio solamente se realizaban intercambios relacionados con la agricultura y la ganadería, es decir, si una persona poseía una serie de alimentos que no tenía otra y viceversa, podían realizar un trueque que les servía, formalizando un contrato privado mediante la palabra, para obtener algo que no tenían a cambio de dar una parte de lo que poseían en exceso. Posteriormente, se implantó el oro, la plata y el cobre como medios de pago entre particulares o comercios, los cuales, dichos metales fueron acuñados como monedas donde cada país acababa formalizando las suyas propias y las marcaba como monedas de curso legal. Con el paso de los siglos, se instauraron los billetes, ya que eran más

fácil transportar. Con ello, el dinero dejó de estar respaldado por el oro para estar basado en la confianza que tenían las personas en cuanto al valor de dichos billetes o monedas pese a que éstas no estuvieran construidas con materiales de gran valor. En la actualidad, y con el surgimiento de la tecnología, estos métodos de pago continúan cambiando y, por tanto, aparecen nuevas herramientas que sirven para realizar la función de comprar o vender, ya sea por personas individuales o empresas. Así surgen las criptomonedas en 2009, tras la crisis financiera que azotó el mundo entero.

El Bitcoin³ fue la primera criptomoneda que apareció. Surgió en 2009 por primera vez en la *Deep Web* (Internet Profundo) como método de pago con el que se podían comprar armas, drogas, pasaportes falsos o contratar sicarios y hackers, entre otro tipo de delitos que se cometían sin que las autoridades pudieran identificar a los cibercriminales. Silk Road, es la primera página que suministraba dichos materiales en la *Deep Web* y, por tanto, es la más conocida⁴. Aunque este fue el uso inicial que se le dieron a las criptomonedas, éstas “nacieron con la finalidad de permitir la realización de transacciones económicas o intercambios de bienes (físicos o virtuales) y servicios sin necesidad de intermediarios”⁵.

El funcionamiento del Bitcoin y del resto de criptomonedas permite la llegada de dinero a cualquier parte del mundo de manera casi inmediata y sin apenas comisiones. Además, puede favorecer que esas transacciones no estén reguladas ni controladas por ningún tipo de gobierno, ya que se producen de particular a particular, es decir, de manera privada entre dos personas. Tampoco es gestionada ni emitida por ninguna entidad central, sino que es pública, por lo que se considera, por ese hecho, que está descentralizada. De hecho, se considera “mineros” a aquellos que crean bitcoin mediante cálculos matemáticos, es decir, “transmiten y confirman las transacciones pendientes a ser incluidas en la cadena de bloques.”⁶. Por tanto, las características principales del Bitcoin y las criptomonedas son: “la descentralización, la imposibilidad de falsificación o duplicación, que es directa sin intermediarios, irreversible en sus transacciones, privada y permite el cambio con monedas como el euro o el dólar”.⁷

Para el Banco Central Europeo (*European Central Bank*, 2012) es considerado como dinero digital “aquel que no está regulado y que es emitido y controlado por sus creadores y que, además, es utilizado entre los miembros de una comunidad específica, la cual debe ser virtual”.

La Blockchain o cadena de bloques es la tecnología en la que se sustenta el Bitcoin y el resto de las criptomonedas. Es como un libro mayor donde se registran las transacciones que aprovecha la red *peer to peer* para realizar dichas transacciones. Se caracteriza por ser descentralizada o distribuida, es decir, que el control no está centralizado por una entidad concreta sino por un conjunto de personas que en un principio eran voluntarios, que son los conocidos mineros de Bitcoins. En segundo lugar, es público, ya que cualquiera puede

⁴ OLVERA RODRÍGUEZ, PATRICIA (2016). *Término CRIMPEDIA: Web profunda, darknet y Tor*.

⁵ OLIVA LEÓN, RICARDO (2021). Regulación legal del bitcoin y de otras criptomonedas en España. *Algoritmo legal*

⁶ JIMÉNEZ, M. N. P. (2016). *Criptodivisas: del bitcoin al MUFUG. El potencial de la tecnología blockchain*. Pp.10

⁷ *Ibidem*, Pp.9

visitarlo. Y, por último, está encriptado con tal de favorecer la privacidad y la seguridad de los que emplean dicha tecnología⁸.

Los *Wallets* o Monederos y *Exchanges* o Intercambiadores son los dos medios más utilizados en el mundo de las criptomonedas. El primero sirve para guardar las criptodivisas y existe el modelo online, como Coinbase⁹, o el modelo offline como el Ledger Nano S, la cual es un monedero de hardware que se asemeja a un *pen drive* y que solamente se conecta al ordenador para transferir las monedas digitales, mientras que el resto del tiempo lo puedes guardar de manera física sin estar conectado a Internet. Con lo cual, este modelo se vende como más seguro, ya que evita posibles ataques informáticos que sí que pueden sufrir aquellos monederos que son online. En cuanto a los intercambiadores, son plataformas online donde se permite la compra y la venta de Bitcoins y cualquier otra criptomoneda. De hecho, son las páginas webs que utilizan los cripto inversores que realizan *trading*. La plataforma más conocida en la actualidad es Binance¹⁰.

En definitiva, el Bitcoin ha terminado convirtiéndose en una especie de oro, es decir, como reserva de dinero donde las personas pueden salvaguardar su capital en épocas de crisis. Pero no solo existe el Bitcoin, en la actualidad existen una gran cantidad de criptomonedas con distintas funcionalidades o con mejoras con base en las carencias o limitaciones que podía tener el Bitcoin como moneda de cambio. Este tipo de criptomonedas se verán en el siguiente apartado.

2. Tipos de criptomonedas

Existen distintos tipos de criptomonedas y no todas funcionan de la misma manera. Por un lado, existen las monedas digitales que no tienen respaldo con monedas fiduciarias como podría ser el propio Bitcoin, el cual se entiende por el mercado como un activo que sirve de resguardo (como el oro), es decir, como reserva de dinero, ya que “las mercancías por excedencia elegidas como dinero en los últimos 4000 años han sido el oro, la plata y los metales preciosos”¹¹. Pero también, por otro lado, existen tipos de monedas que tienen una funcionalidad dentro de una aplicación y que está controlada y gestionada por una empresa, como podría ser la criptodivisa Status¹², la cual está conformada para ser una aplicación de mensajería instantánea descentralizada o, también, Theta¹³, otra moneda digital que pretenden que funcione como una red social con las mismas características respecto a la descentralización que Status.

También existen otro tipo de monedas, como Tether (USDT)¹⁴. Este tipo de criptodivisas están respaldadas por monedas físicas basadas en la confianza como en este caso el dólar, ya que un Tether tiene el mismo valor que un dólar y no aumentará ni disminuirá su valor si no lo hace con anterioridad el dólar. Por tanto, pueden dar una sensación de seguridad si se tiene

⁸ CORREDOR HIGUERA, J. A., & DÍAZ GUZMÁN, D. (2018). Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina. *Derecho pucp*, (81), 405-439.

¹⁰ <https://www.binance.com/es>

¹¹ MUÑOZ ESTEBAN, M. (2017). *La moneda digital: El bitcoin*. Pp. 13

pensado implementarlas en la sociedad como monedas de curso legal con los que poder hacer transacciones, compras o ventas, es decir, como medio de intercambio de bienes e inmuebles.

En conclusión, como tipologías de criptomonedas tenemos, por un lado, el Bitcoin que es entendido por la comunidad de cripto inversores como una reserva de capital; el resto de criptomonedas con distintas funcionalidades, ya sea por tener una empresa detrás, como por estar pensadas para soportar mayores transacciones y más rápidas que el propio Bitcoin; y, por último, las conocidas como *stablecoins*, las cuales están respaldadas por monedas fiduciarias como el dólar y que se caracterizan por no tener la volatilidad que el resto de criptomonedas y, por ende, son más fáciles de implementar en la sociedad como monedas de cambio digitales. De hecho, Facebook ha presentado varios proyectos para implementar una *stablecoin* que funcione en sus aplicaciones con varios intentos fallidos, el último, este mismo año con la moneda Diem.¹⁵

III. LEGISLACIÓN DE LAS CRIPTOMONEDAS

1. Criptomonedas en España

En España existe la obligación de marcar en la declaración de la renta las ganancias de los cripto inversores, ya que el Bitcoin y el resto de las criptomonedas son consideradas un activo en nuestro país. 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, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, de modificación de diversas normas tributarias y en materia de regulación del juego, es la que regula la obligación de declarar las criptomonedas en España.

En la Modificación de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio, se regula la obligación de presentar en la Declaración de la Renta la posesión de monedas virtuales. En su interior se muestra la modificación, en el apartado 4, del artículo 91, el cual trata los temas de imputación de rentas en el régimen de transparencia fiscal internacional, donde se modifica el apartado 6 y 7 a la disposición adicional decimotercera, la cual es específica sobre las monedas virtuales.

En el apartado 6 de dicho artículo, se indica que “las personas y entidades residentes en España y los establecimientos permanentes en territorio español de personas o entidades residentes en el extranjero, que proporcionen servicios para salvaguardar claves criptográficas privadas en nombre de terceros, para mantener, almacenar y transferir monedas virtuales, ya se preste dicho servicio con carácter principal o en conexión con otra actividad, vendrán obligadas a suministrar a la Administración Tributaria, en los términos que reglamentariamente se establezcan, información sobre la totalidad de las monedas virtuales que mantengan custodiadas. Este suministro comprenderá información sobre saldos en cada

¹⁵ ELECONOMISTA (2021). *La stablecoin de Facebook (Diem) que iba a cambiarlo todo se desinfla antes de nacer.*

moneda virtual diferente y, en su caso, en dinero de curso legal, así como la identificación de los titulares, autorizados o beneficiarios de dichos saldos”.

Mientras, en el apartado 7 del mismo artículo, se especifica que “las personas y entidades residentes en España y los establecimientos permanentes en territorio español de personas o entidades residentes en el extranjero, que proporcionen servicios de cambio entre monedas virtuales y dinero de curso legal o entre diferentes monedas virtuales, o intermedien de cualquier forma en la realización de dichas operaciones, o proporcionen servicios para salvaguardar claves criptográficas privadas en nombre de terceros, para mantener, almacenar y transferir monedas virtuales, vendrán obligados, en los términos que reglamentariamente se establezcan, a comunicar a la Administración Tributaria las operaciones de adquisición, transmisión, permuta y transferencia, relativas a monedas virtuales, así como los cobros y pagos realizados en dichas monedas, en las que intervengan o medien, presentando relación nominal de sujetos intervinientes con indicación de su domicilio y número de identificación fiscal, clase y número de monedas virtuales, así como precio y fecha de la operación”. Asimismo, se aclara que “la misma obligación anterior tendrán las personas y entidades residentes en España y los establecimientos permanentes en territorio español de personas o entidades residentes en el extranjero, que realicen ofertas iniciales de nuevas monedas virtuales, respecto de las que entreguen a cambio de aportación de otras monedas virtuales o de dinero de curso legal”.

Además, también existe la obligación de declarar las criptodivisas que se encuentran en el extranjero. Así, en la misma ley, se modifica el artículo 201.bis referente a la infracción tributaria por fabricación, producción, comercialización y tenencia de sistemas informáticos que no cumplan las especificaciones exigidas por la normativa aplicable. Se modifican los apartados 1 y 2 de la disposición adicional decimoctava para regular las criptomonedas. Así, en el apartado 1. d) se añade “información sobre las monedas virtuales situadas en el extranjero de las que se sea titular, o respecto de las cuales se tenga la condición de beneficiario o autorizado o de alguna otra forma se ostente poder de disposición, custodiadas por personas o entidades que proporcionan servicios para salvaguardar claves criptográficas privadas en nombre de terceros, para mantener, almacenar y transferir monedas virtuales”.

Sobre los impuestos, el IRPF (Impuesto sobre la Renta de las Personas Físicas) debe declararse en el caso de que las ganancias se hayan producido a través de una inversión y solamente en el caso de realizar una transacción en la que se formalice la ganancia. Si con el activo “no hago ningún movimiento de mis criptomonedas, no tributo, ya que no hay ganancia, aunque suban o bajen de valor”¹⁶. En cuanto al IVA (Impuestos sobre el Valor Añadido), no se aplica en las transacciones, pero sí en el caso de que se utilicen las criptomonedas para la compra de un bien o un servicio. Por lo que, en ese caso, se aplicará el IVA correspondiente al tipo de bien o al tipo de servicio al que se haya recurrido. En referencia al Impuesto del Patrimonio (IP), depende de cada Comunidad Autónoma la cantidad mínima aplicable. Por tanto, “a la hora de calcular el total de bienes que tenemos a final de año, habrá que valorar las criptomonedas que tenemos con el valor de 31 de diciembre y sumar dicho valor al resto de bienes que tengamos (acciones, inmuebles, cuentas corrientes, terrenos, fondos, etc.), para ver si tenemos que presentar el Impuesto de Patrimonio y pagar por él”¹⁷.

¹⁶ ACADEMY BIT2ME. *Impuestos: Hacienda y Bitcoin ¿qué declarar en España por tener criptomonedas?*

¹⁷ *Ibidem*

En el caso de obtener pérdidas se computará como que “el dinero que hayas perdido con una inversión de criptomonedas se restará a lo que has ganado con otra de otro tipo, y solo tributarás por la diferencia entre ambas”.¹⁸

¿Es suficiente esta regulación para evitar la comisión de delitos? Es evidente que, si se comete un delito de estafa, de extorsión, robo o blanqueo de capitales, existe una legislación específica que se encuentra tipificada en el Código Penal español, como se justificará posteriormente. Esta regulación permite condenar este tipo de hechos delictivos relacionados con temas económicos que se puedan cometer, pero, aunque el Bitcoin deje de ser anónimo, si lo intercambias en plataformas legalizadas por los gobiernos en las que se identifica con documentos de identidad a los inversores, los ciberdelincuentes podrían seguir utilizando otros medios para cometer ilegalidades con las que poder lucrarse de forma que se desconozca totalmente por las autoridades la procedencia de ese dinero, así como el propio destinatario.

2. Criptomonedas en Europa

La regulación de las criptomonedas en Europa está tomando dos vías distintas, por un lado, las regulaciones de la Unión Europea (UE) con tal de establecer un proyecto común al que se puedan acoger todos los países pertenecientes y, por otro lado, las consideraciones específicas sobre la regulación de las criptomonedas en los países de la UE.

En este apartado trataremos de investigar qué proyectos planea la UE para una regulación de las criptomonedas para todos los países adscritos y, por otro, como regulan o pretenden regular las criptomonedas países como Alemania, ya que el 7% de la población ha invertido en criptomonedas convirtiéndose así en uno de los que más invierte de Europa¹⁹. Pero también Reino Unido, el cual, pese a que no se encuentra dentro de la UE, es uno de los países que más utiliza Bitcoin, colocándose en el top 5 mundial²⁰. También evaluaremos otros países, como Francia, Holanda, Italia, Portugal o Irlanda, donde se mostrará como cada país tiene sus propias maneras de regular o, por contra su poca predisposición a hacerlo.

2.1. Regulaciones de la Unión Europea

La Unión Europea no tiene ninguna regulación específica sobre criptomonedas, pero sí que existe un reglamento en camino que se denomina propuesta MiCA (*markets in crypto-assets*), el cual tiene la intención de regular aquellas monedas que están respaldadas por divisas reales, como el euro o el dólar, que posiblemente verá la luz a finales del año 2021 o ya en el 2022. Esta propuesta debe ser aprobada por el Consejo y el Parlamento Europeo²¹.

El objetivo principal del reglamento MiCA es “dotar de seguridad jurídica a un mercado que ahora mismo parece carecer de ella, como han puesto de manifiesto diferentes casos de estafa en los bitcoins”²². Por tanto, esta propuesta pretende dotar de transparencia la emisión de algún criptoactivo en particular, establecer normas que protejan a los consumidores frente a los abusos del mercado, regular las ofertas públicas de criptoactivos y regular las autorizaciones y las condiciones de funcionamiento de aquellos que proveen al público de

¹⁸ *Ibidem*

¹⁹ GIL, J.A. (2021). Países que más invierten en criptomonedas. *TreceBits*

²⁰ MARTÍNEZ, D. (2021). *Ranking de los países donde más utilizan bitcoin.*

²¹ RAMÍREZ, HELENA (2021). *La regulación de criptomonedas en España.*

²² RAMÍREZ, HELENA (2021). *MiCA, la propuesta de la UE para la regulación del mercado de criptoactivos.*

criptomonedas, es decir, los *exchanges* o intercambiadores de criptomonedas. Estos últimos, por tanto, deberán, según el borrador, publicar un White Paper que “recoja toda la información relevante sobre su producto, junto a una descripción detallada de las operaciones que llevarán a cabo, cómo se planea emplear los fondos en el proyecto, las obligaciones que adquieren o los riesgos en torno a su producto”²³.

Asimismo, conviene aclarar que la UE define a las criptomonedas en la Quinta Directiva, donde introduce el punto 18 al artículo 3 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20 de mayo de 2015 (conocida como la Cuarta Directiva y hoy modificada por la Quinta Directiva). En esta Directiva se indica que las monedas virtuales son una “representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero que es aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos”.

También es importante esclarecer que las plataformas de intercambios de monedas o *exchanges* están obligados a que, todas aquellas personas que decidan registrarse en alguna de estas páginas de compra de criptomonedas, muestren su documento de identidad como se muestra y regula el 19 de junio de 2018, época en la que se aprobó la mencionada Directiva 2018/843/UE, del Parlamento Europeo y del Consejo o «Quinta Directiva», donde se modificó la Directiva (UE) 2015/849, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo o “Cuarta Directiva”, y se introdujo cambios sobre los sujetos obligados al cumplimiento de la normativa en materia de prevención del blanqueo de capitales y la financiación del terrorismo.

2.2. Consideraciones específicas sobre la regulación de las criptomonedas en los países de la UE

a) Alemania

En el caso de Alemania, nos encontramos que se está regulando a favor de la instauración de las criptomonedas, ya que, como publicaba Cointelegraph (una reconocida web de articulistas especializada en criptodivisas) “a partir del 2 de agosto de 2021, los fondos institucionales alemanes podrán tener hasta un 20% de sus activos en criptomonedas”²⁴. Ello muestra la necesidad del país alemán de regular las criptomonedas facilitando el uso de las criptodivisas como medio de cambio económico, y favorece de esta manera a los inversores de las monedas virtuales, las cuales pueden servir tanto de “reserva de valor, activo especulativo o como método de pago”²⁵.

b) Francia

El país francés, al igual que el alemán, clasificó las criptomonedas en 2020 con tres interpretaciones posibles: “como moneda, como instrumento financiero que se aplica como

²³ *Ibidem*

²⁴ BOURGI, SAM (2021). Ley alemana que permite a los fondos institucionales invertir en criptomonedas entrará en vigor el 2 de agosto. *Cointelegraph*

²⁵ ESPARRAGOZA, LUIS (2021). Más de 4000 fondos de inversión en Alemania podrán invertir en Bitcoin y criptomonedas. *Criptonoticias*

medio de intercambio entre individuos o entidades legales, y como valor en el sentido legal”²⁶

François Villeroy de Galhau, el director del Banco de Francia, considera urgente la regulación del mercado de las criptomonedas con tal de evitar lo que él mismo citó como “el riesgo de una erosión de nuestra soberanía monetaria y un potencial debilitamiento del euro”²⁷. Por ello, el Banco Francés estudia un programa piloto para crear su propia *stablecoin*, con tal de evitar que las criptomonedas afecten la soberanía monetaria de la UE. De esta forma, es el propio Gobierno de Francia el que pide a la UE que “la Autoridad Europea de Valores y Mercados, o ESMA, regule la actividad relacionada a las monedas digitales en toda la Unión Europea”²⁸.

c) Holanda

Un tribunal holandés dictaminó en 2018 que “las monedas virtuales se pueden considerar como medios de intercambio, pero no satisfacen los criterios para la moneda de curso legal”²⁹. Por ello, depende de cada inversor los riesgos que pueda sufrir por el hecho de intercambiar criptomonedas.

Pese a ello, el Gobierno holandés necesitó instaurar lo que se conoce como KYC (*Know Your Customer* o “conozca a su cliente”) para conocer la cantidad de cripto inversores residentes en Holanda. Este sistema consiste en “la práctica que realizan las compañías para verificar la identidad de sus clientes cumpliendo con las exigencias legales y las normativas y regulaciones vigentes”³⁰. Pese a ello, “el Banco Central holandés aún no sabe cuántos inversores cripto hay en los Países Bajos”³¹, como afirma Cointelegraph.

d) Italia

En Italia, este mismo verano se alertó por parte de las autoridades financieras italianas sobre los riesgos que pueden existir al operar con criptomonedas, por ello “la Comisión Nacional del Mercado de Valores de Italia (CONSOB, por sus siglas en italiano) emitió un comunicado, según el cual las empresas pertenecientes a Binance Group no tienen autorización para ofrecer servicios de inversión en el país europeo”³².

Pese a la prohibición de uno de los *exchange* más importantes del mundo, Savona, jefe de Commissione Nazionale per le Società e la Borsa (Consob), dijo que “los activos no regulados podrían usarse en el lavado de dinero, distorsionar las políticas monetarias establecidas y socavar el poder de los bancos centrales en Europa y el mundo”³³. Por lo que también instó a la UE a que se adoptara una regulación comunitaria.

²⁶ BARI, MATÍAS (2021) *Cómo avanzan las regulaciones a las criptomonedas en el mundo*.

²⁷ WRIGHT, TURNER (2021). “No nos queda mucho tiempo” para regular las criptomonedas, según el director del Banco de Francia.

²⁸ MCBRIDE, LANDON (2021). *El Gobierno francés impulsa la creación de una agencia que regule las criptomonedas en toda la UE*.

²⁹ WAGEMAKERS, BJORN (2018). *REGLAMENTO DE CRIPTOMONEDAS EN LOS PAISES BAJOS*.

³⁰ ELECTRONIC IDENTIFICATION (2021). *Qué es KYC (Know Your Customer) y su actualidad en 2021*.

³¹ AVAN-NOMAYO, OSATO (2021) *Los reguladores holandeses no conocen el número exacto de inversores en criptomonedas en los Países Bajos*.

³² IBARRA, JUAN (2021). *Binance tampoco puede operar en Italia, dice el regulador financiero italiano*.

³³ EZANIME (2021). *El regulador del mercado de valores de Italia pide una regulación sobre las criptomonedas para prevenir la actividad criminal*

e) *Portugal*

Actualmente, Portugal está considerada por la comunidad de los cripto inversores como un paraíso fiscal de criptomonedas, ya que “la Autoridad Fiscal ha considerado que los ingresos obtenidos a través de criptomonedas no forman parte de ninguna categoría imponible de ingresos. Solo considera la posibilidad de gravar tales ingresos cuando puede considerarse como ingreso profesional, es decir, se requiere una prueba de que los ingresos tienen una recurrencia regular y que constituyen la actividad profesional del cripto-inversor.”³⁴

Además, también existe en Portugal la posibilidad de obtener el Estado de Residente No Habitual, es decir que existen unas “enormes ventajas fiscales para los extranjeros que no han sido considerados residentes en Portugal en los últimos cinco años y que vienen a vivir a Portugal”³⁵.

f) *Irlanda*

En Irlanda, las empresas que se dedican a la compra y venta de criptomonedas “deberán realizar comprobaciones de diligencia debida sobre sus clientes y dar cuenta del origen y el destino de los fondos”³⁶. Para ello, deberán declarar ante el Banco Central que “mantienen políticas de lucha contra el lavado de dinero y de lucha contra la financiación del terrorismo de acuerdo con las mismas normas que se exigen a los proveedores de servicios financieros convencionales”³⁷. Por lo que ya no se permite a los cripto inversores especular con monedas digitales de manera anónima con tal de evitar la comisión de delitos como el blanqueo de capitales.

g) *Reino Unido*

No existen regulaciones estrictas en Reino Unido sobre las criptomonedas, pero sí que exige a las plataformas que dispensan criptodivisas que tomen medidas para evitar el blanqueo de capitales y la financiación del terrorismo. Actualmente, se encuentran todavía investigando la manera de obtener una mejor regulación del mercado de criptodivisas para evitar los vacíos legales que éstas tienen.

Recientemente, como muestra de la tendencia reguladora de este país para luchar contra el fraude fiscal, la FCA, el organismo de control financiero de Reino Unido, ha exigido a Binance Markets Limited que cancele todas sus actividades en Gran Bretaña para el 30 de junio de 2021, pero no que esto “no afectará a los servicios que ofrece en Binance.com, según la propia compañía”³⁸. Es decir, que solo afecta a una parte de los servicios que ofrece la plataforma Binance, uno de los *exchanges* más famosos del mundo. Por lo tanto, se denota que el Reino Unido toma decisiones reguladoras con tal de evitar el blanqueo de capitales prohibiendo a los *exchanges* alguna de sus actividades, como se ha mostrado en este ejemplo, que considera facilitadores de blanqueo de capitales.

Conviene aclarar que, pese a que Reino Unido no pertenece a la Unión Europea, se encuentra dentro de Europa y todavía mantiene relación en algunos aspectos como puede ser la

³⁴ LAMARES, CAPELA & ASOCIADOS (2021). *Portugal y las criptomonedas*.

³⁵ *ibidem*

³⁶ HAIG, SAMUEL (2021). Las cryptoempresas irlandesas impondrán controles de identificación contra el lavado de dinero a partir de abril. *Cointelegraph*

³⁷ *ibidem*

³⁸ RUS, CRISTIAN (2021). Reino Unido prohíbe algunas actividades de Binance como los contratos de futuros a partir del 30 de junio. *Xataka*

cooperación en materia antiterrorista. Es por ello que, pese a su decisión de no pertenecer a la UE, se les incluye en este apartado.

3. Criptomonedas en el resto del mundo

Si no cooperan todos los países del globo para regular las criptomonedas, ¿cómo va a ser posible evitar que se cometan delitos con ellas? Este interrogante nos muestra de forma clara que, sin una cooperación internacional en cuanto a la regulación de las criptomonedas, podría darse el caso de que los países las utilizaran en su beneficio, es decir, para blanquear dinero o para cometer otro tipo de delitos. La cooperación internacional en cuanto al traspaso de información entre países para desarticular organizaciones criminales que se pueden encontrar en cualquier parte del mundo, se hace muy necesaria para el caso de las criptomonedas.

En este apartado estudiaremos que opciones ofrecen las grandes potencias mundiales como Estados Unidos o China, y en Latinoamérica, donde, más concretamente El Salvador ha legalizado las criptomonedas como monedas de curso legal, lo que está provocando que otros países del entorno, como la República de Panamá, se esté replanteando en los parlamentos legislativos la opción de instaurar las criptodivisas como medio de pago.

a) Estados Unidos

Gary Gensler, el actual presidente de la Comisión de Bolsa y Valores (SEC), pide una regulación inminente del mercado de criptomonedas en Estados Unidos. Además, afirma también que tendrán mucha relevancia las criptomonedas en los próximos 5-10 años, pero bajo “un marco de política pública”³⁹. Todo ello tiene el objetivo de proteger a la sociedad, el mercado y a los inversores, ya que “el porcentaje de activos “altamente especulativos” dentro del mercado de cryptoactivos es del 95% y la protección de los inversores es escasa”⁴⁰, según asegura Gensler.

Estados Unidos es el país con más preparación para comenzar la regulación de las criptomonedas con 17.000 cajeros especializados en criptodivisas. Por este motivo, podría erigirse como uno de los primeros países en encontrar una regulación que permita un uso lícito del Bitcoin y el resto de criptomonedas con tal de proteger a los inversores y evitar la comisión de delitos con dichas monedas digitales por medio de Internet.

b) China

El Banco Popular de China (el Banco Central chino) definió su última postura como “no aceptar como forma de pago los tokens digitales (activos que funcionan como monedas, pero no tienen valor de curso legal)”⁴¹, lo cual provocó una disminución de los precios en el mercado de criptomonedas en ese mismo 2021.

Este mismo año, China, junto con la Asociación Nacional de Finanzas por Internet, la Asociación Bancaria y la Asociación de Pagos y Compensación de China, aprobaron prohibir

³⁹ CIVIETA, OSCAR (2021). Estados Unidos abre la puerta a la regulación de las criptomonedas. *Business Insider*

⁴⁰ DOMINGUEZ, DANIEL (2021). EEUU mueve ficha para regular las criptomonedas. *Finance*

⁴¹ ELECONOMISTA (2021). Las pretensiones de EEUU de una mayor regulación abren un horizonte de más 'bandazos' en las criptomonedas *El Economista*.

las instituciones y plataformas que ofrecían operar con criptomonedas, aunque este hecho no afectaría a los particulares.

Pese a ello, el Gobierno Chino permite a los usuarios de Alipay de Alibaba “probar la criptomoneda de ese país, el yuan digital, a través de una aplicación llamada «Digital RMB»”⁴². Por ello, sorprende que China prohíba el uso de criptodivisas, pero no el uso del Yen digital como medio de pago de curso legal.

c) Latinoamérica

Muchos países latinoamericanos comienzan también a presentar proposiciones para intentar regular las criptomonedas, como es el caso de Colombia, con tal de prevenir riesgos delictivos relacionados con las monedas digitales⁴³. Pero, no es el único país en hacerlo, Panamá, por ejemplo, el 7 de septiembre presentó un proyecto de ley que permite admitir el Bitcoin y el resto de criptomonedas como moneda de curso legal. El objetivo es “hacer que el país sea compatible con *blockchain*, los criptoactivos e Internet”⁴⁴, así como “atraer inversionistas y emprendedores que se enfoquen en la economía digital”⁴⁵, con tal de estimular la economía del país.

Esto se produce a causa de la legalización de las criptomonedas en el Salvador, que ha producido una ola regulatoria en Latinoamérica. La Asamblea Legislativa de El Salvador aprobó en junio de 2021 el uso legal de las criptomonedas como medio de pago que “obliga a los comercios y empresas a aceptar bitcoin como medio de pago”⁴⁶. Esta aprobación se realizó a pesar de la oposición, que considera que “el bitcoin es conocido por cambiar constantemente de valor, además de posibilitar el blanqueo de capitales”⁴⁷.

IV. DELITOS ECONÓMICOS

1. Tipología

Los delitos económicos son muy diversos y dinámicos, ya que se van adaptando a los nuevos tiempos, aprovechando los vacíos legales para lucrarse. Aproximadamente, desde el surgimiento de los Estados durante la industrialización y el dinero fiduciario, comenzaron los delitos económicos, los cuales se realizaban de forma física, es decir, mediante atracos a mano armada en bancos. Era la etapa conocida como la de los bandoleros, posterior a la de los piratas. Seguidamente, tras el surgimiento de las mafias y bandas organizadas para cometer delitos, se fueron perfeccionando y adaptando a los nuevos avances tecnológicos hasta el surgimiento de los *hackers* o piratas informáticos.

⁴² SANTISTEVAN, BETSSY (2021). China prohíbe a instituciones y medios de pago operar con criptomonedas. *Criptonoticias*.

⁴³ CUARTAS BÁEZ, R. Y. (2019). *Hacia una regulación de los criptoactivos en Colombia: el enfoque de los sistemas de prevención del riesgo de LA/FT*

⁴⁴ PARTS, HELEN (2021). La República de Panamá presenta un proyecto de ley para regular las criptomonedas. *Cointelegraph*

⁴⁵ FERNÁNDEZ, FROILAN (2021). En Panamá diputado presenta proyecto de ley para regular las criptomonedas. *Criptonoticias*

⁴⁶ PASTOR, JAVIER (2021). *El Salvador se convierte en el primer país del mundo en el que bitcoin se convierte en criptomoneda de curso legal, pero no sin polémica.*

⁴⁷ EL ECONOMISTA (2021). Protestas y dudas en El Salvador ante la inminente adopción del bitcoin como moneda de intercambio. *El Economista*.

Para comprender los distintos tipos de delitos económicos que se pueden cometer, es necesario establecer, previamente, una clasificación junto con una breve explicación sobre las características de cada uno de ellos. Esto nos permitirá una mejor identificación posterior de los delitos que se puedan cometer con criptomonedas. Las tipologías de delitos económicos que podemos encontrar en el Código Penal que pueden servir para nuestro objeto de estudio, se detallan a continuación.

a) Estafas

Las estafas se encuentran reguladas en el Título XIII del Código Penal, donde se regulan los delitos contra el patrimonio y contra el orden socioeconómico. Más específicamente se encuentran en el Capítulo VI, el cual versa sobre las defraudaciones (Sección 1: las estafas). Las estafas vienen definidas en el artículo 248, el cual establece en el apartado 1 que “cometen estafa los que, con ánimo de lucro, utilicen el engaño para producir error en el otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”. Además, en el apartado 2 del mismo artículo se establece que las personas como reos de estafa son los que, mediante manipulación informática o artificio semejante, consiguen “una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro (...), los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas (...) utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero”. Esta definición del apartado 2 es la técnica denominada *phishing*, con la cual los ciberdelincuentes suplantan páginas webs con la intencionalidad de que la víctima suministre sus datos personales, como pueden ser contraseñas de correos o de cuentas bancarias, para posteriormente poder lucrarse.

Por tanto, la regulación del Código Penal ya contempla la posibilidad de condenar a aquellos que cometen estafas con criptomonedas, ya que se valen de producir un error en la víctima y actúan desde el desconocimiento de ésta sobre el tema de las criptodivisas con tal de lucrarse. Asimismo, se pueden utilizar o manipular medios o programas informáticos para cometer este tipo de actos delictivos.

Además, existen agravantes dependiendo de las cantidades sustraídas, del número de personas afectadas o de si supone un grave perjuicio para la víctima o su familia, como bien se establece en el artículo 250 del Código Penal.

b) Extorsiones

En el mismo Título XIII, pero en el Capítulo III, encontramos la extorsión, la cual, como está tipificado en el artículo 243, se define como “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”. Este delito puede percibirse de forma más clara mediante los ejemplos que se explicarán en el siguiente apartado, pero si se comete, por ejemplo, un secuestro de ordenadores mediante un ataque informático en el que se exige al propietario que, para librarse de ese ataque, tenga que aportar una remuneración económica, ya podría ser extorsión por el hecho de sentirse obligado o intimidado por la violencia del ataque, pese a que éste no sea de forma física, sino virtual. En este delito, no solo se pretende proteger el patrimonio, sino también la libertad de las personas.

c) Blanqueo de capitales

La tipificación del delito de blanqueo de capitales se encuentra en el mismo Título que los anteriores, en el XIII, referente a delitos contra el patrimonio y contra el orden socioeconómico. En el artículo 301.1 se tipifica el tipo básico donde se define la acción delictiva como “el que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquier tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos”. Además, se aplicaría un agravante en el caso de que fuese realizada por una organización criminal dedicada al blanqueo de capitales como se establece en el artículo 302.1.

d) Financiación de organizaciones criminales o grupos terroristas

En este apartado se verá, por un lado, que entiende el Código Penal como organización criminal y, por otro, que entiende por terrorismo. Posteriormente, se analizará cómo se tipificaría la financiación a este tipo de organizaciones delictivas que tienen una estructura conformada exclusivamente para delinquir.

Para ello, se recurre a al Título XXII referente a los delitos contra el orden público y más específicamente al Capítulo VI para conocer los límites establecidos por el Código penal a las características que deben darse para calificar a un conjunto de personas que ha cometido una serie de delitos como organización criminal. En el artículo 570 bis, en su apartado uno, se establece que “se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido que, de manera concertada y coordinada, se repartan diversas tareas o funciones con el fin de cometer delitos”. Pero también pueden existir agravantes, como se muestra en el apartado 2 del mismo artículo, cuando “esté formada por un elevado número de personas (...), disponga de armas o instrumentos peligrosos (...) o disponga de medios tecnológicos avanzados de comunicación o transporte que por sus características resulten especialmente aptos para facilitar la ejecución de los delitos o la impunidad de los culpables”.

Asimismo, en el artículo 570 ter se establecen las penas de “quienes constituyeren, financiaren o integraren un grupo criminal”. Y, por otro lado, en el artículo 570 quarter, en el apartado 3, se aclara que las mismas penas serán aplicables a “toda organización o grupo criminal que lleve a cabo cualquier acto penalmente relevante en España, aunque se hayan constituido, estén asentados o desarrollen su actividad en el extranjero”.

En cuanto al terrorismo, se encuentra regulado también en el Título XXII referente a los delitos contra el orden público y, más concretamente, en el Capítulo VII en el que se tipifican los delitos de las organizaciones y grupos terroristas. En la Sección II de dicho capítulo, se define el terrorismo en el artículo 573 del Código Penal en su apartado 1 como “la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexual, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, de falsedad documental, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, (...) y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades: subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo; alterar gravemente la paz pública;

desestabilizar gravemente el funcionamiento de una organización internacional; o provocar un estado de terror en la población o en una parte de ella”.

Asimismo, el Código Penal, en el mismo artículo, pero en el apartado dos, también considera como terrorismo “los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior”. En el artículo 197 bis se condena al que “por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.” Mientas que, en el 197 ter se pretende juzgar a los que posean “una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.” Por otro lado, en el artículo 264, se castiga al que “por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave”.

Igualmente, estos delitos de terrorismo pueden agravarse si, como se muestra en el artículo 574, se depositaran “armas o municiones, la tenencia o depósito de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o de sus componentes, así como su fabricación, tráfico, transporte o suministro de cualquier forma, y la mera colocación o empleo de tales sustancias o de los medios o artificios adecuados”.

Es ya en el artículo 576 del Capítulo VII del Título XXII del Código penal, donde se juzga a los que “por cualquier medio, directa o indirectamente, recabe, adquiera, posea, utilice, convierta, transmita o realice cualquier otra actividad con bienes o valores de cualquier clase con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte, para cometer un acto terrorista, es decir, que en este artículo se condena la financiación del terrorismo”. En el apartado 2, se establece que se juzgaría como coautores si el dinero es empleado “para la ejecución de actos terroristas concretos”.

e) *Robo*

En cuanto a la tipificación del robo, tenemos que recurrir a los artículos 237 y 238 también en el Título XIII, pero en el Capítulo II referente a los robos. Conviene destacar que una de las principales diferencias entre el hurto y el robo es el empleo de fuerza en las cosas o en las personas. Por ello, en nuestro caso, si es sustraer una contraseña para robar una cantidad de dinero de un *Wallet* donde una persona tiene sus criptomonedas guardadas, estaríamos hablando de robo, no de hurto, ya que se ha empleado la fuerza sobre las cosas. Esto queda plasmado en el artículo 238 del Código Penal, donde se establece el uso de llaves falsas para cometer el robo.

f) *Especulación*

El artículo 284 del Código Penal impone penas de cárcel e inhabilitaciones para los que “empleando violencia, amenaza, engaño o cualquier otro artificio, alterasen los precios que hubieren de resultar de la libre concurrencia de productos, mercancías, instrumentos financieros, contratos de contado sobre materias primas relacionadas con ellos, índices de referencia, servicios o cualesquiera otras cosas muebles o inmuebles que sean objeto de contratación”. En el mismo artículo, en el apartado 2, se expresa que “de manera directa o indirecta o a través de un medio de comunicación, por medio de internet o mediante el uso de

tecnologías de la información y la comunicación, o por cualquier otro medio, difundieren noticias o rumores o transmitieren señales falsas o engañosas sobre personas o empresas, ofreciendo a sabiendas datos económicos total o parcialmente falsos con el fin de alterar o preservar el precio de cotización de un instrumento financiero o un contrato de contado sobre materias primas relacionado o de manipular el cálculo de un índice de referencia, cuando obtuvieran, para sí o para tercero, un beneficio, siempre que concurra alguna de las siguientes circunstancias: a) que dicho beneficio fuera superior a doscientos cincuenta mil euros o se causara un perjuicio de idéntica cantidad; b) que el importe de los fondos empleados fuera superior a dos millones de euros; c) que se causara un grave impacto en la integridad del mercado”. Asimismo, este artículo establece penas superiores, como se tipifica en el apartado 3, “si el responsable del hecho fuera trabajador o empleado de una empresa de servicios de inversión, entidad de crédito, autoridad supervisora o reguladora, o entidad rectora de mercados regulados o centros de negociación”.

Por tanto, la alteración de los precios de un activo está considerado un delito siempre que se realice sin el conocimiento previo de la víctima con tal de engañarla y sustraerle su capital sin que ésta sea consciente. Todo ello se contempla en el Código Penal español en el Capítulo XI, el cual hace alusión a los delitos realizados contra la propiedad intelectual e industrial. También hace mención al mercado y a los consumidores en el Título XIII (delitos contra el patrimonio y contra el orden socioeconómico). Más específicamente, en el interior del Capítulo XI, en la Sección III.

2. Ejemplos de delitos económicos cibernéticos con criptomonedas

De igual manera que sucedía con los piratas en la época del descubrimiento de América, donde atracaban aquellos barcos que conocían de ante mano que portaban armas, oro o alimentos, en la actualidad, con la evolución del tiempo y la tecnología, estos atracos ahora se cometen navegando por Internet.

En este apartado se expondrán varios ejemplos de delitos económicos con criptomonedas para ilustrar cómo se cometen los actos criminales con las actuales monedas digitales. Para ello, se seguirá la misma estructura que en el apartado anterior. Es decir, los hechos delictivos que se abordarán serán los siguientes: las estafas que se puedan producir con las criptodivisas; las extorsiones como por ejemplo secuestrar un ordenador a cambio de una remuneración con Bitcoins; el blanqueo de capitales mediante criptomonedas; la financiación de organizaciones criminales o terroristas; robos a Wallets (monederos digitales), que permite guardar el dinero virtual; y, por último, la especulación que se genera con la intención de manipular los mercados por parte de ciertos grupos que se organizan por foros de Internet.

2.1. Estafas. Arbistar 2.0 S.L., suplantación de personajes televisivos y sorteos de criptomonedas.

Las estafas que se producen por medio de anuncios que surgen en las páginas webs cuando se navega por Internet son un tipo común de delito que se puede cometer con criptomonedas. Estas estafas te prometen ganancias marcando un mínimo de inversión y prometiendo unos beneficios que deben parecer motivantes de cara al estafado, para que caiga en la trampa, invierta su dinero y posteriormente lo pierda. Este tipo de estafas las podemos encontrar en distintos ejemplos que se muestran a continuación.

La empresa Arbistar 2.0 S.L. con sede en Tenerife, se promocionaba en internet como especialistas en *trading* y análisis de mercado. A continuación, en la Ilustración 1, se puede apreciar la página web de la empresa, donde promocionaban sus productos.



Ilustración 1. La Audiencia Nacional investigará el caso Arbistar, la mayor estafa piramidal con criptomonedas. Fuente: Salces, L. y Belinchon, F. (2021).

La empresa creó el *Community bot*, un bot de arbitraje que prometía sacar un alto rendimiento y un retorno de la inversión, todo esto, mediante la compra automatizada de bitcoins. En septiembre de 2020, la compañía Arbistar decide cesar la actividad del bot, publicando una nota informativa en la prensa⁴⁸ y comunicando el cierre del producto y la consecuente pérdida en capital para los inversores. Las sospechas indican que se trata de una empresa dedicada a la estafa piramidal.

Mientras la empresa asegura que se trata de un error informático debido a una mala configuración del bot, los inversores afectados están organizándose para tomar acciones legales contra la empresa Arbistar 2.0 S.L.⁴⁹.

Según el despacho de abogados que lleva el caso de denuncia colectiva, las cifras ascienden a 800 asesorados, más de 120.000 posibles afectados y 15 millones de euros desaparecidos⁵⁰.

Este método de estafa se basa en hacer réplicas de sitios webs (usualmente se dirige tráfico a esas webs falsas) mediante el pago de anuncios o enviando correos electrónicos con los links falsos y robando los datos del usuario, cuando este intenta iniciar sesión.

En la página web de *Binance*⁵¹ podemos encontrar diferentes casos de *phishing*, que ayudan a los usuarios a prevenir dichos ataques. Podemos encontrar los ejemplos de réplicas de sitios

⁴⁸ ARBISTAR 2.0 S.L. (2020) *Nota informativa. Cierre del Community Bot*.

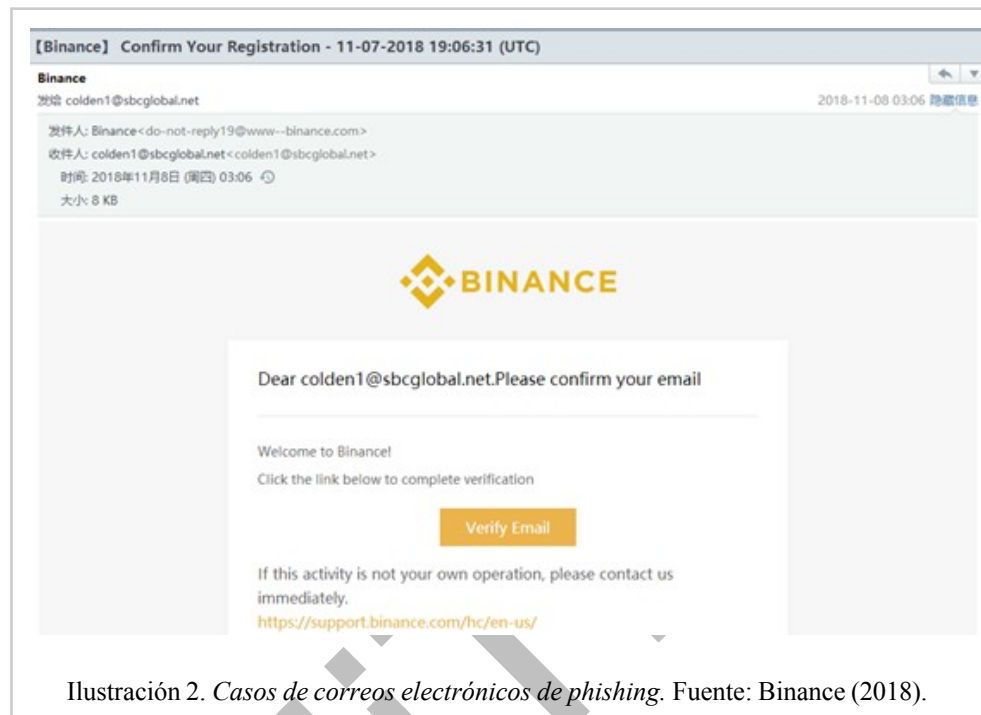
⁴⁹ DP ABOGADOS (2020) *Afectados por el incumplimiento contractual-estafa de Arbistar 2.0, Nimbus y Mind Capital*.

⁵⁰ LABE ABOGADOS (2020) *Estafa Arbistar*.

⁵¹ BINANCE (2108). *¿Qué es el Phishing?*

web⁵² que consisten en copiar con máximo detalle la página de inicio de sesión y al introducir las credenciales, el hacker roba sus datos. Al tener las credenciales, puede acceder a su cuenta y vaciarla.

Otro tipo de casos de *phishing* son los que suceden por correo electrónico. En estos ejemplos, también realizados en la página de *Binance*⁵³, se roban los datos del usuario mediante el envío de un correo falso de verificación, como el que se puede ver en la Ilustración 2.



Al pinchar con el ratón en verificar, redirige al usuario a una página donde puede introducir sus credenciales de *Binance*. Cuando las introduce y pulsa iniciar sesión, se le redirige a una página que le pide el código de autenticación en dos pasos, de *Google Authenticator*. Estos datos son más que suficientes para tener acceso a la cuenta de la víctima.

Recientemente ha habido una oleada masiva de anuncios publicitarios en internet, vinculados a estafas con criptodivisas. El típico artículo de “caso de éxito” encarnado por famosos nacionales, fácilmente reconocibles por la víctima.

El gancho es, mediante el uso del *phishing*, vender la idea de que las celebridades más conocidas del país han invertido en bitcoin y han sacado una alta rentabilidad. Por lo tanto, las formas de engaño son el uso de un señuelo (famoso conocido en el país) y una réplica de una página web conocida, también en el país. Es por eso por lo que estas estafas están enfocadas a los países donde se quiere atacar. Estos anuncios, como ya se ha mencionado, se venden con la idea de alta rentabilidad o la posibilidad de doblar el capital invertido y una vez tirado el anzuelo, se redirige al usuario a la web donde se le robarán los datos personales.

Bitcoin Revolution es un programa cuyos promotores se dedican a hacer de *brokers* para esos nuevos inversores, captados mediante noticias falsas como las mencionadas con anterioridad.

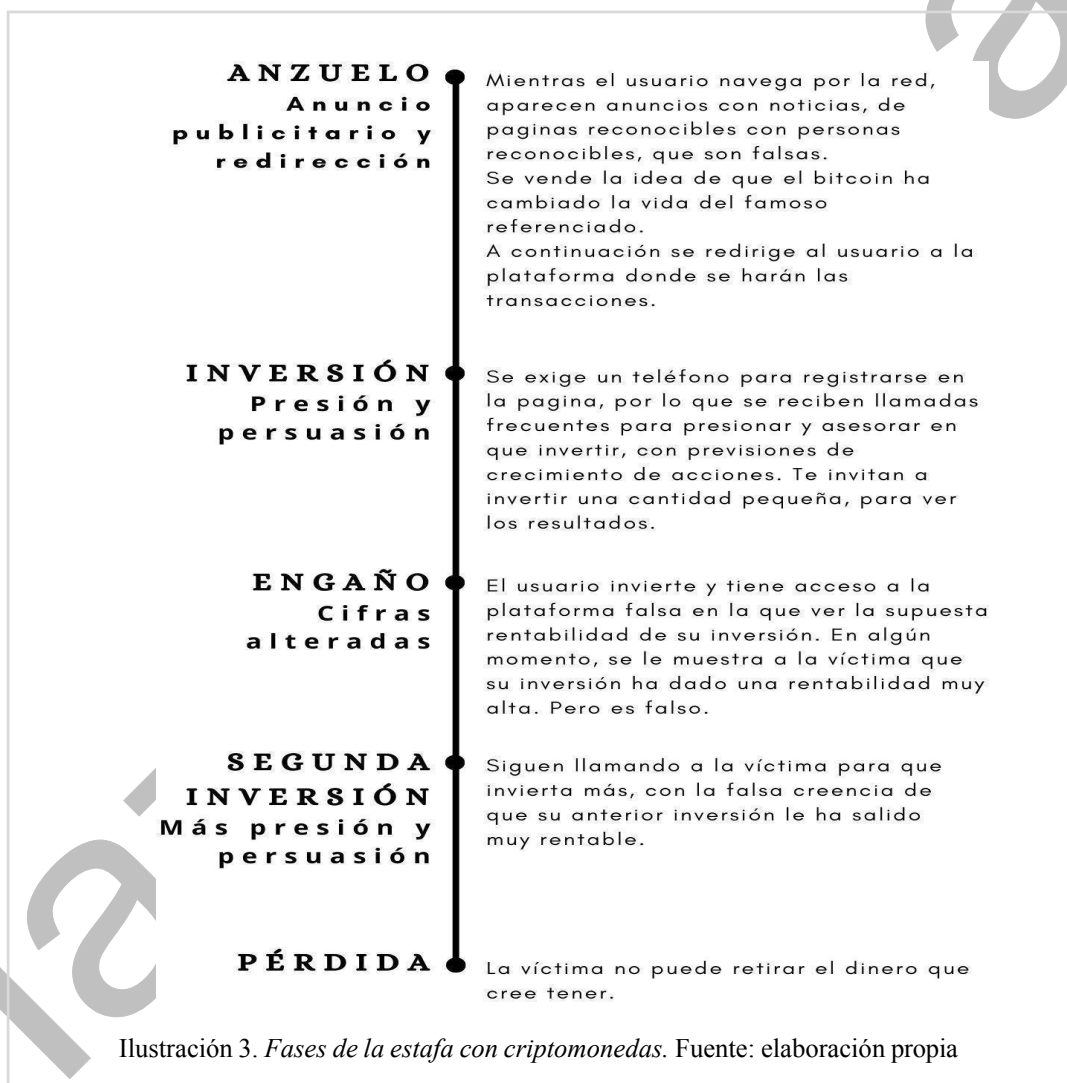
⁵² BINANCE (2018) *Casos de sitios phishing*.

⁵³ BINANCE (2018) *Casos de correos electrónicos de Phishing*.

Las altas tarifas de transacción y la inexperiencia de los inversores, puede suponer una pérdida importante de dinero, pues la inversión está sujeta a un alto riesgo.

En resumen, este tipo de estafas se dan en diferentes pasos. Primeramente, la compra de anuncios en plataformas conocidas, como *Google*, *Facebook* o *Instagram*. A continuación, hace falta esperar a que los usuarios “piquen” y accedan al anuncio. Aquellos que se interesan por el contenido son redirigidos a las páginas del grupo *Bitcoin Revolution* para asignarles un *broker*. Éste les asesorará con el fin de sacar la máxima inversión por parte del usuario que, si no se convence, se le aplicarán métodos de presión tales como llamadas telefónicas, intentando convencerle de la inversión o prospectando que ciertas acciones van a subir, para intentar conseguir sacar el máximo dinero posible.

Para entender mejor cómo funciona este proceso, se puede visualizar la Ilustración 3.



Aprovechando la gran crisis económica que agitó al mundo durante la pandemia, los delincuentes han difundido noticias falsas con el fin de lucrarse económicamente. Aparecieron multitud de anuncios (principalmente en Facebook) disfrazados de noticias bajo el nombre de algún periódico conocido.

El caso de Jordi Évole, que fue usado como imagen para una de estas campañas de estafa, redirigía a los usuarios a la web de *bitcoin revolution* o la de *bitcoin code*. Pero cabe destacar

que, a lo largo de estos últimos años, los responsables de esta estafa han ido cambiando el nombre del timo. Desde *Bitcoin Evolution* o *CryptoBoom* hasta otros como *Bitcoin Trader*, *Bitcoin Era* o *Bitcoin System*.

Su estrategia fue usar una captura de su aparición en televisión para simular que durante el programa había desvelado su secreto acerca del dinero que ganaba invirtiendo en criptomonedas. Como se puede ver en la Ilustración 4, replicaron el periódico *La Vanguardia* para captar la atención de los usuarios y dar más credibilidad. Esto tuvo que ser desmentido por el programa de televisión en el que apareció, y el propio Évole ha tomado acciones legales. Los famosos que han utilizado en esta estafa son una cantidad sorprendente. Jordi Cruz, es otro de los muchos que han usado como imagen (Ilustración 5).



Ilustración 4. *El timo de las criptomonedas usa a Jordi Évole y El Hormiguero.* Fuente: Chaves, A. (2020).



Ilustración 5. *Los 6 principales métodos de estafa de criptomonedas.* Fuente: Crypto Tips (2020).

Otro tipo de estafa son los sorteos de criptomonedas. Este método funciona mediante el uso de bots, que comentan bajo las publicaciones que hacen personas famosas en las redes sociales. Normalmente estos ataques van dirigidos a personas que están en el mundo de las criptomonedas para dar sentido a la promoción de dicho sorteo y porque les permite segmentar el público al que dirigen la estafa. El comentario contiene un mensaje con un enlace que dirige a los usuarios al sitio web donde supuestamente obtendrán sus criptomonedas gratis.

Al parecer Twitter ha podido luchar, mediante el uso de bots, contra las estafas de sorteos falsos de criptomonedas en las secciones de comentarios, pero existe otro método que les permite generar más confianza a los usuarios. Se trata del hackeo de cuentas verificadas y de empresarios influyentes, que utilizan para publicitar los sorteos de bitcoins. Pagan para que ese *tweet* se anuncie en la plataforma y así consiguen llegar a un gran número de personas.

El caso de los anuncios sigue siendo una brecha por la que los ciberdelincuentes pueden meterse y encontrar sus víctimas.

Uno de los casos más conocidos de este tipo de estafas es de la suplantación de identidad de Elon Musk vía Twitter. Los estafadores usaron una cuenta verificada de un estudio de cine inglés, pero con el nombre de Elon Musk para publicar la estafa. Promocionaron un sorteo de bitcoins con un enlace directo, usando el sistema de anuncios publicitarios de Twitter⁵⁴. En la siguiente imagen se puede ver una captura del tweet publicado por los cibercriminales. Pero Elon Musk no es el único que sufre este tipo de suplantaciones de identidad, existen muchos otros casos, como por ejemplo Bill Gates, Jeff Bezos o Warren Buffett. Todos ellos grandes empresarios, relacionados con la inversión o el mundo de las criptodivisas, tal y como se muestra en la Ilustración 6 y 7.

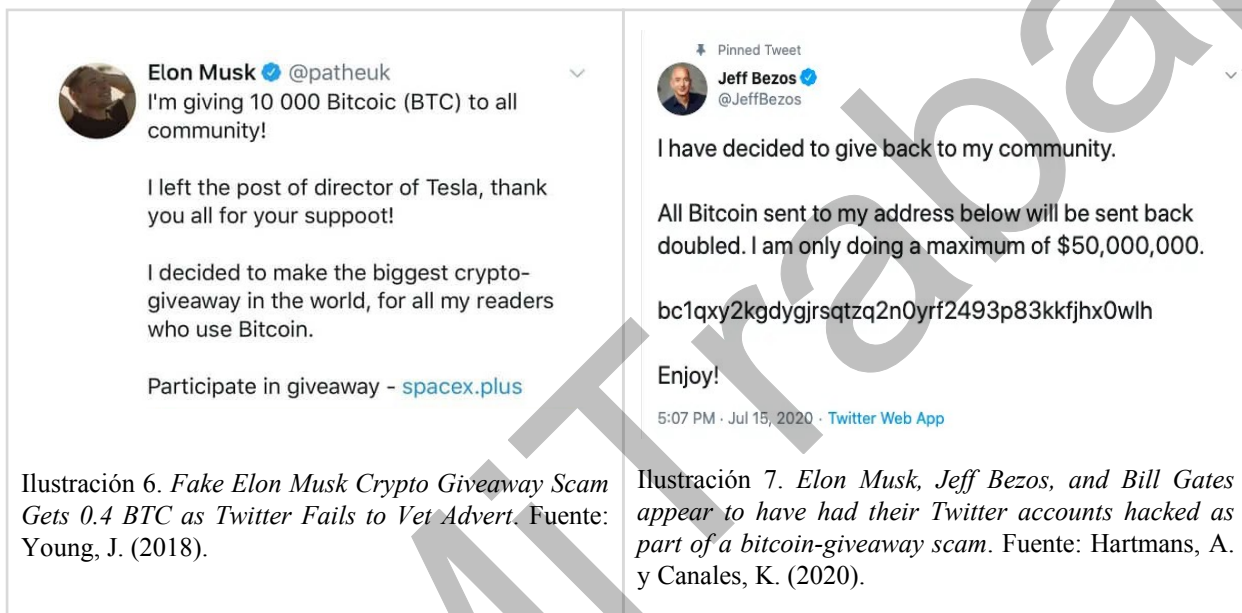


Ilustración 6. Fake Elon Musk Crypto Giveaway Scam Gets 0.4 BTC as Twitter Fails to Vet Advert. Fuente: Young, J. (2018).

Ilustración 7. Elon Musk, Jeff Bezos, and Bill Gates appear to have had their Twitter accounts hacked as part of a bitcoin-giveaway scam. Fuente: Hartmans, A. y Canales, K. (2020).

1.2. Extorsión. Secuestro de ordenadores mediante *ransomware*

Se han dado con bastante frecuencia casos en los que grupos de cibercriminales se organizan para secuestrar e inutilizar ordenadores de empresas de gran reputación, como el caso de Movistar. La única solución que brindaban para desbloquear dichos ordenadores era con el pago de Bitcoin. Este es el ejemplo más destacado que permite visualizar otra manera más de emplear las monedas criptomonedas para lucrarse ilegalmente.

En el año 2017, la empresa telefónica sufrió un ataque de *ransomware* con una versión de WannaCry. Sus datos fueron secuestrados y para recuperarlos pedían como rescate unos 300 bitcoins. En ese momento el precio del bitcoin oscilaba entre los 2.000 y los 3.000 USD, tal y como se puede ver en la Ilustración 8.

⁵⁴ JOSEPH YOUNG (2018) Fake Elon Musk Crypto Giveaway Scam Gets 0.4 BTC as Twitter Fails to Vet Advert. *CNN*



Los ciberdelincuentes estaban pidiendo una suma de entre 600.000 y 900.000 USD. Cabe destacar que en esas fechas el bitcoin empezó a subir drásticamente, llegando a alcanzar su máximo histórico para ese entonces en julio de 2017.

El secuestro de datos a Telefónica supuso una acción inmediata de la compañía, deteniendo todos los ordenadores rápidamente. Para conseguirlo, difundieron el siguiente comunicado por su intranet, el cual se muestra en la Ilustración 9.

Telefónica LA INTRANET GLOBAL

13 / 03 / 2017

ELEGIMOS TODO

URGENTE: APAGA TU ORDENADOR YA

El equipo de Seguridad ha detectado el ingreso a la red de Telefónica de un malware que afecta tus datos y ficheros. Por favor avisa a todos tus compañeros de esta situación.

Apaga el ordenador ya y no vuelvas a encenderlo **hasta nuevo aviso(*)**.

Te enviaremos un correo que podrás leer a través de tu móvil cuando la situación ya esté normalizada. Además, el martes informaremos en las entradas de los edificios sobre el acceso a la red.

Ante cualquier duda contacta con la Mesa de Ayuda (29000)

(*) Desconecta el móvil de la red WiFi pero no hace falta que lo apagues

Dirección de Seguridad

Ilustración 9. Wanna Decryptor: así funciona el ransomware que se ha usado en el ciberataque a Telefónica Fuente: Pastor, J. (2017).

Pidieron a todos los empleados que dejaran de usar los ordenadores y los apagaran de inmediato. El comunicado también dice que los teléfonos debían ser desconectados de la red wifi, pero no se solicitaba su desconexión.

Aunque el ataque a Telefónica fue del que se habló más, hubo ataques a otras empresas, según un comunicado oficial emitido por la CCN-CERT⁵⁵, uno de los organismos de seguridad más importantes del país. El ataque masivo se dirigió a diversos sistemas que usaban Windows y que no estaban actualizados o parcheados a su última versión. Microsoft emitió un boletín⁵⁶ hablando de la actualización para resolver la situación de vulnerabilidad que sufrían sus sistemas operativos Windows.

Aprovechando dicha vulnerabilidad, que permitía la manipulación de los archivos de forma remota a través de SMB (*server message block*), los atacantes usaron *EternalBlue/DoublePulsar*, que ataca a los sistemas sin actualizar y se extiende por toda la intranet, infectaron los demás sistemas Windows conectados a la misma red. Debido a esto el CCN-CERT emitió un informe oficial de buenas prácticas para protegerse del *malware*.⁵⁷

El *ransomware* es un *malware*, que una vez dentro del sistema, encripta los datos y los bloquea, por lo que no se puede acceder a ellos sin una contraseña. La forma en la que se introduce este *malware* dentro del sistema puede variar, pero una vez secuestrados los datos piden un rescate por ellos. Los datos secuestrados están perdidos, pues la clave para desbloquearlos está en el sistema de donde ha salido el *hackeo*, por lo que el pago es algo obligado, a no ser que se posea algún *backup* para poder restaurarlos.

Este tipo de malware tiene también la capacidad de extenderse por el sistema, llegando a corromper archivos compartidos, a los cuales es imposible de acceder mientras sigan secuestrados⁵⁸.

1.3. Blanqueo de capitales. Caso *Mixers* y Operación Tulipán Blanca

1.3.1. *Mixers*, servicios potenciales de lavado de dinero

Puesto que las transacciones realizadas con bitcoin y las billeteras donde se almacenan son fácilmente rastreables, el anonimato del Bitcoin se ha visto afectado. Como el Bitcoin estaba muy valorado por ese anonimato, al empezar a perderse, surgió una clara necesidad de recuperarlo. Los *mixers* o mezcladores, aparecieron para poder combatir este problema emergente.

Los *mixers*⁵⁹, son servicios de mezclado de Bitcoins que permiten perder el rastro en las transacciones, evitando obtener la dirección de Bitcoin de las operaciones. Esto permite recuperar el anonimato a los usuarios, pero también deja una brecha que los delincuentes pueden aprovechar para el blanqueo de capitales. La principal amenaza es que estos servicios no solicitan la identidad del usuario y tampoco ningún tipo de pseudónimo. Además, prometen no dejar registro de los movimientos realizados.

El funcionamiento de los *mixers*⁶⁰ es el siguiente: primero, se da una dirección para retirar la criptomoneda y se indica qué moneda será mezclada. A continuación, se da una dirección de envío, donde se recibirán los Bitcoins ya mezclados. El proceso de mezclado consiste en

⁵⁵ CCN-CERT, COMUNICADOS. (2017). *Identificado ataque de ransomware que afecta a sistemas Windows*.

⁵⁶ WINDOWS SERVER 2016 (2017). *MS17-010: Actualización de seguridad para Windows Server de SMB*.

⁵⁷ CCN-CERT (2017) *Buenas Prácticas CCN-CERT BP-04/16 Ransomware*.

⁵⁸ JAVIER PASTOR (2017) *Wanna Decryptor: así funciona el ransomware que se ha usado en el ciberataque a Telefónica*. *Xataka*

⁵⁹ BOUISSA, L., GARÍN, F., & ROSTÁN, A. (2019). *Relevamiento de técnicas de rastreo y entintado de dinero en Bitcoin*.

⁶⁰ REDACCIÓN TERRITORIO BITCOIN *¿Cómo funciona un mezclador de Bitcoin?*

cambiar los bitcoins enviados por un usuario, por los enviados por otro, haciendo que los Bitcoins que llegan a la cuenta de destino, no sean los mismos que entraron, lo que dificulta mucho la trazabilidad de las transacciones. También hay un tiempo de retraso, para que dicha transacción sea aún más difícil de rastrear. Se ofrece la opción de ajustar este tiempo y se pueden alcanzar las 24 horas de retraso.

1.3.1.1. *Mixers, el caso Helix*

Larry Dean Harmon era propietario de un servicio de mezclado de Bitcoins llamado *Helix*, a su vez, también poseía un motor de búsqueda de mercado en la *Dark Web* llamado *Grams*. Su estrategia consistió en publicitar su servicio *mixer* en la *Dark web* promocionándolo como una forma ideal para ocultar las transacciones a las autoridades, según informa el departamento de justicia de los Estados Unidos⁶¹.

Harmon, colaboró con otros mercados de la internet profunda para lavar dinero obtenido mayoritariamente de actividades ilícitas, admitiendo haber conspirado con proveedores de la *Dark Web* para lavar los Bitcoins obtenidos mediante los mercados mencionados. En total, más de 300 millones de dólares (según el valor del mercado en el momento de realizar las transacciones) fueron blanqueados para diferentes clientes del servicio. Estas colaboraciones incluían uno de los mercados más grandes del internet profundo, donde se publicaba un enlace hacía el servicio, ayudando a conectar a los delincuentes con *Helix*. Otros mercados acabaron colaborando con *Helix*, ya que Harmon adaptó la interfaz para que las transacciones fueran compatibles con todos ellos, consiguiendo así más promoción.

En este caso, y tal como se explica en la declaración de infracciones de Harmon⁶², los bitcoins que entraban al *mixer* eran transferidos a una billetera propiedad de *Helix*, entonces, el servicio transmitía bitcoins ubicados en otras carteras también propiedad de *Helix*, pero que no estaban vinculadas a la *Dark Web*, a las cuentas de los clientes que solicitaban el servicio. Esto permitió que los delincuentes rompieran el rastro de sus transacciones, puesto que los Bitcoins obtenidos finalmente no procedían de la *Dark Web*.

Larry Dean Harmon se declaró culpable de los cargos y aunque la sentencia aún no está anunciada, se enfrenta a un máximo de 20 años de cárcel.

1.3.2. *Tulipán blanca*

La operación Tulipán Blanca, realizada en 2018, desarticuló una organización criminal que blanqueaba dinero obtenido ilícitamente mediante el narcotráfico. Esta organización operaba entre España, donde se vendían las sustancias estupefacientes, y Colombia, donde se retiraba el dinero blanqueado.

Los delincuentes conseguían dinero mediante la venta de sustancias ilegales y procedían a ingresarlo en cajeros españoles. Los movimientos de efectivo eran pequeños, sin llegar a superar los 3.000 € diarios⁶³, pero contaban con 174 cuentas corrientes con las que operar. Posteriormente, optaron por aprovechar el anonimato del bitcoin para seguir lavando dinero. Con estos métodos lograron blanquear más de ocho millones de euros.

⁶¹ DEPARTMENT OF JUSTICE OFFICE OF PUBLIC AFFAIRS (2021) *Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over \$300 Million*

⁶² CHANNING D. PHILLIPS (2021) *Statement of the offense and related conduct*

⁶³ SOLUCIONES CONFIRMA (2018). *La operación del mes: Tulipán Blanca, primera contra el blanqueo con bitcoins*

En la Ilustración 10, se puede ver parte del dinero, en euros, incautado a la organización criminal durante su detención.



El blanqueo de dinero se producía mediante tarjetas de crédito sujetas a personas ajenas que prestaban su identidad con el fin de permitir a los delincuentes hacer estos movimientos bancarios. Posteriormente el dinero era retirado por miembros de la misma organización, que viajaban a Colombia para retirar el dinero en efectivo en diferentes ciudades colombianas.

Estos movimientos bancarios están atados a nombres y son fácilmente rastreables. Esto, junto a la presión de las entidades bancarias con las que operaban, hacen que la organización criminal ponga al bitcoin en el punto de mira.

Para romper el rastro del dinero negro, la organización empezó a comprar criptomonedas, en su mayor parte Bitcoins.

La guardia civil logró colaborar con las autoridades finlandesas, país en el que se encontraba la sede de la plataforma de venta de criptomonedas, quienes ayudaron a reconstruir el trayecto que habían seguido los capitales, movidos por la organización criminal.

Gracias a esto, se pudo confirmar que el dinero invertido en bitcoin procedía de España y se pudo trazar un camino hasta los delincuentes. También se descubrió que esos fondos eran usados en operaciones de compraventa hasta ser retirados desde cuentas corrientes, también en Colombia.

Según informa la Guardia Civil⁶⁴, la operación fue posible gracias a la colaboración de varias entidades, tales como el Grupo de Blanqueo de Capitales de la Unidad Central Operativa de la Guardia Civil, Europol, la unidad *Homeland Security Investigation* de EEUU y los departamentos de blanqueo de capitales de las entidades involucradas y afectadas, quienes se juntaron para efectuar una operación que se catalogó como pionera en nuestro país, puesto que la criptomoneda era uno de los métodos más nuevos para el blanqueo de capitales. El caso se cerró con 11 detenidos y 137 personas más bajo investigación policial.

⁶⁴ GUARDIA CIVIL (2018). *La Guardia Civil desarticula una organización criminal dedicada al blanqueo de capitales procedentes del narcotráfico mediante el uso de criptomonedas*

1.4. Financiación de organizaciones criminales o grupos terroristas como el ISIS

El Bitcoin ha servido durante muchos años como medio para financiar organizaciones criminales y terroristas. Se han publicado varios artículos donde se especulaba que las monedas virtuales servían para financiar este tipo de grupos con el fin de suplir gastos para poder cometer actos criminales.

Los grupos criminales se financian utilizando las nuevas tecnologías. Es habitual ver el uso de *crowdfundings*, *mecenazgos* y donaciones, tanto en el internet superficial como en la *dark web*. Se ha detectado que algunas organizaciones criminales utilizan el sistema de pago entre criminales mediante los sistemas de transacción digital, para aprovechar el anonimato que estos tienen. Tal como señala un reporte de la Europol de 2015⁶⁵, existen servicios escondidos en la *dark web* que usan bitcoin, como una de las pocas formas de pago. Esto ha sido aprovechado por las organizaciones criminales para realizar pagos, debido al anonimato que ofrecen las criptomonedas, suponiendo más del 40% de las transacciones realizadas en el momento de publicación del reporte.

Un artículo de ese mismo año⁶⁶, asegura que hay claros indicios del uso del bitcoin para la financiación de actividades criminales. Se citan algunos comentarios de *blogs* pro-ISIS de la *dark web*, que argumentan la necesidad del uso del Bitcoin como financiación. En concreto explica cómo es imposible hacer una transacción a otro combatiente de la yihad sin que el gobierno se dé cuenta de inmediato. En otro mensaje se recomienda cifrar las transacciones financieras mediante un *dark wallet*, lo cual dificulta rastrear las transacciones y evita que se apliquen impuestos a aquellas realizadas desde fuera del estado islámico. En el año 2015, se podía ver que el interés de los grupos terroristas por el Bitcoin estaba en uso y creciendo, pero no se pudo encontrar una cuenta abierta por el ISIS para aceptar donaciones directas en Bitcoin, aunque uno de los usuarios publicó un enlace a una cuenta que había logrado recaudar 5 Bitcoins por valor de 1.000\$ cada uno, en aquel entonces. Dicha cuenta fue clausurada posteriormente por el FBI.

Existe el caso de Ali Shukri Amin, un joven de 17 años que usó las redes sociales para pedir donaciones en Bitcoin para el mismo grupo terrorista, explicando cómo se podía usar la criptomoneda para enmascarar la provisión de fondos para el estado islámico⁶⁷.

También es destacable el caso de Zoobia Shahnaz, una mujer que, mediante engaños, consiguió varios créditos y tarjetas para convertirlos en Bitcoins y otras criptomonedas. La cantidad de dinero ascendía a unos 150.000 USD, que la mujer intentó enviar al estado islámico para financiar el ISIS. Finalmente fue detenida tratando, presuntamente, de viajar a Siria⁶⁸.

En la Ilustración 10 se puede ver una campaña de recaudación de fondos de Bitcoin dirigida por un grupo del Estado proislámico.

⁶⁵ EUROPOL (2015) *The Internet Organised Crime Threat Assessment (IOCTA)*. Pág.46

⁶⁶DANNA HARMAN (2015) *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*.

⁶⁷NATIONAL SECURITY DIVISION (2015) *Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL*.

⁶⁸ WILLIAM SUBERG (2017) Simpatizante del ISIS en EE. UU. fue atrapada enviando \$ 150,000 a Siria en criptomonedas lavadas. *Cointelegraph*



Ilustración 11. Los terroristas ahora se financian con Bitcoin. Fuente: Popper, N. (2019).

1.5. Robos. 2gether, Pony y Bitfinex

En el año 2020, la *startup* española *2gether* sufrió un hackeo con la intencionalidad de robar sus fondos. Los ciberdelincuentes consiguieron hacerse con la suma aproximada de 1,2 millones de euros en Bitcoin, Ethereum y otras criptodivisas⁶⁹.

Otro de los robos masivos de *wallets* más recordados es el de *Pony*⁷⁰, el nombre de un *malware* que infectaba el sistema, consiguiendo el acceso a las contraseñas de los *wallets* de los usuarios. Una vez dentro de los *wallets*, solo tenían que transferir las criptomonedas a otra cuenta.

Las credenciales comprometidas eran muchas, como se puede ver en la ilustración 11, que muestra los ordenadores infectados por *Pony*, clasificados geográficamente.

(Passwords by Countries)	
Статистика по странам	(Reports from Machines)
Страна (Country)	Количество отчетов
DE (Germany)	41177 (28.55%)
PL (Poland)	17214 (11.93%)
IT (Italy)	15672 (10.87%)
CZ (Czech Republic)	14835 (10.29%)
BG (Bulgaria)	7063 (4.90%)
FR (France)	5513 (3.82%)
HR (Croatia)	4725 (3.28%)
PE (Peru)	4616 (3.20%)
IN (India)	2761 (1.91%)
VN (Vietnam)	2234 (1.55%)

Ilustración 12. “Pony” botnet pilfers digital coins worth \$220,000 in sustained attack. Fuente: Goodin, D. (2014).

Finalmente fueron robados 85 *wallets* en total, consiguiendo diferentes criptomonedas (355 bitcoins, 280 Litecoins, 33 Primecoins y 45 Feathercoins).

⁶⁹ JAVIER PASTOR (2020) Roban 1,2 millones de euros en bitcoins en la plataforma fintech española 2gether. *Xataka*

⁷⁰ DAN GOODIN (2014) “Pony” botnet pilfers digital coins worth \$220,000 in sustained attack. *ArtsTechnica*

Por otro lado, en el año 2016, Bitfinex, una de las *exchanges* más grandes, sufrió un ataque informático debido a una brecha de seguridad, tal y como puede verse en el comunicado que emitieron⁷¹. Esto supuso el robo de 119.756 Bitcoins, más de 65 millones de dólares americanos.

No se puede saber quién tiene esos bitcoins, pero si se pueden rastrear las monedas. Por lo que hasta ahora se sabe, estos bitcoins han sido movidos en diversas ocasiones, siempre de forma intermitente. En la ilustración 12 se pueden ver las salidas de Bitcoins robados por el hacker de Bitfinex y en la 13, los destinos que han tenido.

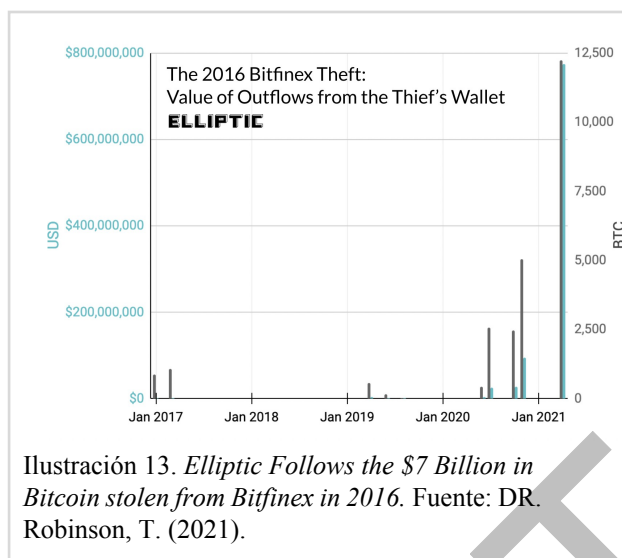


Ilustración 13. *Elliptic Follows the \$7 Billion in Bitcoin stolen from Bitfinex in 2016.* Fuente: DR. Robinson, T. (2021).

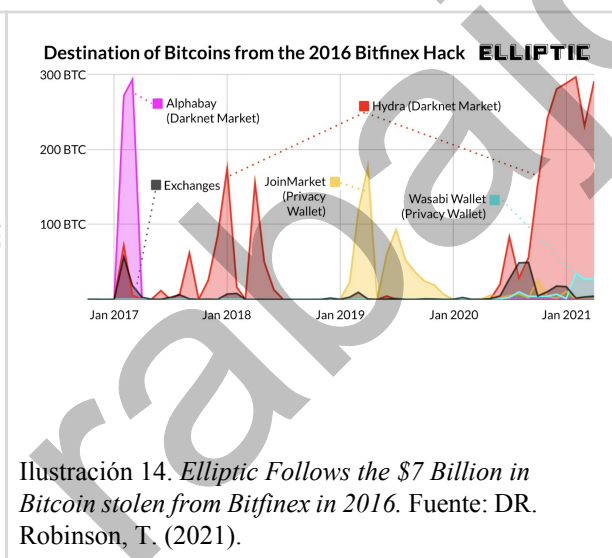


Ilustración 14. *Elliptic Follows the \$7 Billion in Bitcoin stolen from Bitfinex in 2016.* Fuente: DR. Robinson, T. (2021).

Cuatro años después del robo, se movió una cantidad mucho más grande de lo habitual, esto fue advertido por un *bot* de análisis de *blockchain*. Desde entonces, se han hecho diferentes movimientos, pero al parecer, la única vez que el *hacker* ha tenido éxito al vender parte de los Bitcoins robados fue en un mercado de la *dark web*. Algunos de ellos terminaron de nuevo en Bitfinex.

1.6. Especulación. “Pump and Dump”, Caso Tubacex y especulación por influencia

El Bitcoin es un bien, por lo que es posible que se cree una burbuja especulativa a su alrededor. Existen factores que facilitan la creación de las burbujas, algunos de ellos son⁷²:

- El almacenamiento: El almacenamiento del Bitcoin no supone un espacio excesivo, puesto que son virtuales y solo se necesitan servidores que sustenten los servicios de almacenamiento y una copia de seguridad para mantenerlos. Esto no afecta directamente al comprador, eximiéndolo de gastos adicionales de almacenaje.
- La velocidad de producción: Cuanto más despacio se produce un bien, más probabilidades de especular con él existen. Esto nos lleva a la ley de la oferta y la demanda. La oferta del Bitcoin es limitada, encontrando su tope de producción a los 21 millones, mientras su producción se ralentiza cada vez más.
- La existencia de productos sustitutos: Actualmente existen muchas criptomonedas distintas y aunque algunas de ellas se han hecho conocidas, ninguna ha conseguido posicionarse al nivel del Bitcoin ni ofrecer las mismas ventajas.

⁷¹ BITFINEX (2016) Announcements - Security Breach. *Bitfinex*.

⁷² ASTRAY RODRÍGUEZ, M. C. (2019). *Bitcoin¿ Oportunidad del siglo o burbuja especulativa?*

- **Rareza o ilegalidad:** Cuando un bien es poco común o está ilegalizado, crea una estela de desconocimiento que genera curiosidad. En este caso, la rareza la podemos encontrar en que es un bien limitado, y aunque la cantidad es elevada en número, sigue siendo escaso en comparación a lo mucho que se desea. Por otro lado, el vacío legal que implica su anonimato, permitiendo el blanqueo de capitales o la posibilidad de comprar artículos ilegales en la *Dark Web*, no hacen más que incrementar el interés en esta criptomoneda.

1.6.1. Pump and Dump: Especulación con Bitcoin

Recientemente se ha vuelto popular el uso de las influencias y los ataques en grupo para desestabilizar los mercados financieros. Este tipo de especulación genera grandes beneficios a los que organizan las acciones, pero puede llegar a causar pérdidas significativas a otros. Desde “el caso Reddit”, donde los usuarios del famoso foro elevaron las acciones de la empresa GameStop para evitar su bancarota, el *modus operandi* de la acción ha sido copiado por otros usuarios para ganar dinero especulando con el Bitcoin.

Las acciones tienen lugar en los foros de internet y más recientemente en grupos de Telegram. Uno o más usuarios se organizan para tomar la acción, deciden en qué criptomoneda van a invertir y la fecha en la cual se va a realizar dicha inversión. Los usuarios de los grupos corren la voz para aumentar la cantidad de personas que participarán y llegado el momento acordado se compra masivamente y se aumenta el precio de mercado.

Este proceso se llama “pump”. Posteriormente, el precio bajará, lo que se conoce como “dump”. El “pump and dump” es muy conocido en el mundo de la bolsa y ahora está siendo utilizado para especular con las criptomonedas.

1.6.2. Caso Tubacex

Las criptomonedas objetivo son aquellas que tienen un valor bajo. Tubacex, fue la elegida en este caso y se movió por un canal de telegram llamado WS Bets Español, según informa El País⁷³. El creador del canal informó a los usuarios del momento en el que se haría la inversión, entre todos los usuarios consiguieron dispararla hasta un 15%.



Ilustración 15. Tubacex, el fabricante de tubos sin soldadura que perdió más de 18 millones por la crisis Fuente: ABC

En la Ilustración 15 se puede ver el pico de subida de la criptomoneda de Tubacex, justo a principios de febrero, momento en el cuál desde el canal de Telegram se comunicó en qué criptomoneda invertiría el propietario.

El canal que en ese momento contaba con 6.000 seguidores, ahora cuenta con más de 9.000, lo que lo hace aún más fuerte ante futuras decisiones de inversión.

⁷³ SÁNCHEZ, ÁLVARO (2021) Imitadores de Reddit abarrotan Telegram de grupos para comprar y vender de forma coordinada. *El País*.

Economía (2021).

El mensaje fue publicado el 1 de febrero de 2021 a las 11:16 de la mañana. Un minuto después, a las 11:17, el creador del grupo publicó un *disclaimer*, avisando de que toda la información que se publica en el canal “no constituye una asesoría de inversión”, pues solo son meras opiniones. El comentario, que se encuentra fijado en el canal, tiene como objetivo evitar posibles acciones legales que puedan tomar los usuarios que pierden dinero invirtiendo.

1.6.3. Especulación por influencia

El problema con este tipo de movimientos es que la persona que hace el anuncio con el fin de lucrarse compra la criptomoneda antes de que todos los usuarios eleven su valor de mercado mediante las compras masivas, por lo que, en el momento de más valor, la vende y gana mucho dinero, sin importarle las ganancias de los otros usuarios. Este tipo de especulación se suele hacer disfrazada de consejos de inversión, pero realmente no son recomendaciones a seguir, puesto que el único que se beneficia es quien lo ha ideado. Prácticas como estas se han vuelto muy frecuentes en el nuevo mundo de los *influencers*, que al tener muchos usuarios a los que llegar, los cuáles sienten una confianza ciega en ellos, pueden idear este tipo de estrategias de engaño.

Si nos fijamos en el método de obtención de ganancias, partiendo de la base de que el que empieza la rueda de inversiones hacia una criptomoneda específica está engañando a los otros usuarios, quienes piensan que las compras se realizan masivamente en la fecha acordada, se puede comprobar cómo el cabecilla que ha realizado las compras con antelación ha utilizado el engaño para obtener sus beneficios. Aunque esta práctica no suponga la sustracción del dinero directamente a otros inversores, esos acuerdos hacen perder mucho dinero, por lo que se está coordinando una acción que perjudica a terceros con el único fin de lucrarse económicamente, sin cumplir con los acuerdos verbales.

V. MECANISMOS PARA EVITAR Y AFRONTAR DELITOS ECONÓMICOS CON CRIPTOMONEDAS

1. La legislación

¿Es suficiente la legislación y las actuaciones judiciales y policiales para hacer frente a los delitos realizados con monedas virtuales? La respuesta a esta pregunta podría ser perfectamente que no. Los Estados no están preparados todavía para hacer frente a una economía global descentralizada. Igualmente, solo tienen interés en regular las monedas que están respaldadas por alguna moneda fiduciaria como dinero de curso legal, como hemos visto anteriormente con el proyecto MiCA de la UE, mientras que el resto de criptomonedas seguirían considerándose como activos. La necesidad de los gobiernos europeos de crear una política común que regule las criptomonedas para proteger a los cripto inversores de los riesgos asociados con el uso de criptodivisas requiere de una regulación comunitaria o global para que, en circunstancias muy concretas como en el caso de que sufran un robo, una estafa o un engaño, puedan recurrir a la justicia para poder resarcir el daño causado. Asimismo, con las regulaciones también se pretende evitar el blanqueo de capitales y poder tener un mayor control por parte de las autoridades financieras de las criptodivisas que posee cada inversor.

Toda esta regulación requiere de una coordinación y planificación por parte de los gobiernos europeos. Pero lo mismo sucede con el resto de países del mundo. Estados Unidos, gran

aliado de Europa, el cual también está en proceso de legalizar las criptomonedas o, al menos, algunas de ellas, puede colaborar para prevenir este tipo de delitos comunicándose con las autoridades policiales y judiciales de los distintos países que conforman la Unión Europea.

Este tipo de regulación y de control de los cripto inversores que están identificados por los gobiernos y las autoridades financieras también sirve para evitar la financiación de grupos terroristas dado que estas monedas, al encontrarse reguladas y dejar rastros en sus transacciones, permitirían conocer mejor si se financia grupos terroristas u organizaciones criminales por medio de estas nuevas herramientas económicas que, de momento, son anónimas y pueden realizarse en cualquier parte del mundo en cuestión de minutos. Por ello, la principal cuestión de los gobiernos es que dejen de ser anónimas.

Para ello, la Unión Europea, en 2018, aprobó una directiva que considera que se debería aumentar el control de las plataformas de intercambio de criptodivisas, así como las billeteras virtuales. Aunque son muchos los países que proponen medidas que vayan más allá, hasta el momento éstas no están reguladas. No obstante, debido al decreto aprobado por la Unión Europea, algunos servicios vinculados a las criptomonedas movieron sus sedes con el fin de huir de las normativas europeas⁷⁴.

Una de las medidas para acabar con el anonimato de las criptomonedas podría ser la verificación de la cuenta por parte del usuario. Actualmente, la plataforma Binance utiliza la verificación KYC introducida recientemente⁷⁵. Las siglas KYC hacen referencia a “*know your customer*”, que significa, como ya se mencionó anteriormente, “conoce a tu cliente”. Este sistema utiliza documentos oficiales para verificar la identidad de la persona que utiliza la cuenta en Binance, lo que rompe con el anonimato y se suma a tomar medidas preventivas referentes a la identificación que ya presentaban anteriormente.

Existe la posibilidad de crear una cuenta y no verificarla, pero las funciones de ésta se verán limitadas (entre ellas los límites de depósito y las retiradas), lo cual dificulta mucho la financiación de actividades ilícitas sin una identidad.

Según Binance⁷⁶, la función de este tipo de verificación es la de recoger y verificar los datos, así como identificar al cliente y hacerle una supervisión constante. Este proceso se hace en tres pasos:

- 1º. Recogida y verificación de los datos.
- 2º. En este paso la empresa puede decidir si investigar los antecedentes del cliente, por ejemplo, este será marcado si está siendo investigado o si ha sido señalado por fraude financiero.
- 3º. Supervisión constante para detectar las transacciones sospechosas, como transacciones múltiples de cantidades significativas, lo cual puede suponer la suspensión de la cuenta y la debida notificación a las autoridades pertinentes.

Estas medidas se están haciendo cada vez más fuertes en las bolsas de criptomonedas, ya que, si no están las cuentas verificadas, los Estados pueden hacer responsables a dichas bolsas por los delitos cometidos. Cabe destacar que la KYC se introdujo en la Ley Patriótica (Ley

⁷⁴ FERRER-BONSOMS HERNÁNDEZ, IGNACIO. (2020) Entra en vigor la nueva directiva de la Unión Europea para poner cerco a las criptomonedas. *LegalToday*

⁷⁵ SARKAR, ARIJIT (2021). Todos los usuarios de Binance ahora están sujetos a la verificación inmediata de KYC. *Cointelegraph*

⁷⁶ BINANCE (2021) ¿Qué es la verificación KYC y por qué es cada vez más importante para las criptomonedas? *Binance*

Federal de Estados Unidos), en 2001, y es una parte de las prácticas anti-lavado de dinero o AML (por sus siglas en inglés), por lo que esta verificación es un pilar fundamental para la lucha contra el blanqueo de capitales.

Asimismo, Binance ya utilizaba anteriormente otros métodos de verificación para sus usuarios con tal de evitar el blanqueo de capitales o la financiación del terrorismo. Cuando un nuevo usuario decide registrarse, tiene que pasar ciertos controles para poder enviar criptomonedas a otras plataformas fuera de Binance. Entre ellas, destaca que se debe adjuntar una imagen del documento de identidad del usuario, así como permitir una identificación mediante cámara con inteligencia artificial que identifique al usuario con su documento de identidad.

Por tanto, los gobiernos europeos piden a la UE una regulación comunitaria específica para las criptomonedas que permita evitar el blanqueo de capitales y la financiación de grupos extremistas con el uso de las criptodivisas. Es la única manera de conseguir evitar que se cometan este tipo de delitos con las monedas digitales. Surgirán nuevas formas que intentarán eludir estas medidas, pero los gobiernos y la UE tienen la obligación de regular de forma específica, ofreciendo alguna garantía a aquellos *exchanges* que cumplan los requisitos de la UE para poder operar.

En definitiva, regular las plataformas que se encargan de permitir la compra o venta de criptomonedas es una garantía para los inversores, puesto que permite que operen con criptomonedas de una manera segura y sin riesgos, donde su capital puede estar salvaguardado frente a los cibercriminales.

2. Prevención: Mecanismos para evitar posibles delitos económicos con monedas digitales.

Todas las regulaciones de los países van dirigidas a prevenir el blanqueo de capitales y a proteger, en algunos casos, las inversiones de las empresas o particulares que tengan criptomonedas, pero no se dirigen a promover una mayor concienciación entre la sociedad referente a un buen uso de las criptomonedas. Por tanto, ¿Cómo podría prevenirse otro tipo de delitos como las estafas, los robos o las extorsiones? La prevención es un mecanismo fundamental para la criminología. Es necesario comprender que, para que una persona o un grupo de éstas cometa un delito, han de darse distintos factores. Desde un punto de vista sociológico, distintos autores han tratado de explicar por qué se producen los delitos económicos, lo cual permite establecer unas líneas de actuación para intentar evitar que esas facilidades sociales del entorno se reproduzcan para neutralizar las oportunidades de cometer algún tipo de delito.

Cada tipo de delito exigirá sus propios métodos preventivos. Así, en el caso de los robos o extorsiones, la única manera de prevenirlos es mediante programas de sensibilización y concienciación a la población, estableciendo unos límites seguros con ciertos certificados para comprar criptomonedas. De esta manera, se protege el capital del inversor, siendo mucho más complicado sufrir un ataque informático o una estafa. Este método se utiliza ya por parte de las autoridades policiales para evitar casos de *phishing* como las estafas que se producían suplantando al Corte Inglés⁷⁷, aunque en este caso no estén relacionadas con las criptomonedas, pero podría realizarse algún proyecto similar que pueda ser eficaz.

⁷⁷ JUSTO, DAVID (2021). "No piques": la Policía Nacional alerta sobre esta estafa que te puede llegar por WhatsApp. *Cadena Ser*

Si es el caso del secuestro de ordenadores mediante *ransomware*, como el caso analizado anteriormente de Movistar, la prevención debe recaer en la seguridad de cada ordenador y de su dueño o, si es el caso de una empresa, sobre el departamento de ciberseguridad. Este tipo de prevención es complicada, ya que, por regla general, no surgen métodos para evitar este tipo de ataques hasta que no se ha producido. Además, no se conoce el funcionamiento de dicho ataque hasta que no se produce, por lo que no puede generarse una seguridad específica frente a ese tipo de ataques.

Por otro lado, sí que existen métodos que utilizan los *exchanges*, como por ejemplo Binance, que suelen resultar bastante eficaces para evitar el blanqueo de capitales. Algunas de las recomendaciones para no caer en esta trampa es añadir a marcadores la página original, para acceder a ella con seguridad o asegurarse de que la dirección URL de la página sea la correcta. También se podría no instalar *plug-ins*, entre otras⁷⁸.

Binance, un *exchange* o intercambiador de criptoactivos que ha sido comentado anteriormente, también cuenta con mecanismos para proteger a sus usuarios de ser víctimas de ataques informáticos que puedan hacer peligrar el dinero invertido de los cripto inversores. Una forma de proteger a sus usuarios es mediante la aplicación *Google Authenticator*, la cual también se conoce como autenticación en dos pasos, que genera un código nuevo cada 30 segundos, y sin este código, independientemente de la contraseña, el usuario no podría acceder a la cuenta registrada en la plataforma⁷⁹. Igualmente, se ha detectado que las cuentas con autenticación en dos pasos también son vulnerables a veces a este tipo de estafa, puesto que los 30 segundos que dura activo el código de verificación son suficientes para que algunos delincuentes accedan a las cuentas robadas.

Es necesario también concienciar a la población de los nuevos delitos informáticos que se producen con criptomonedas con la intención de proteger tanto a empresas como a particulares de posibles estafas que se puedan realizar con criptomonedas. Pero, ¿dónde debería comenzar dicha sensibilización? La escuela es la primera institución social donde el alumnado aprende a relacionarse con sus iguales. Si se consigue que tengan actitudes prosociales en el manejo de Internet, así como evitar el uso del anonimato, se podría conseguir que utilizaran los medios digitales de manera correcta. Con ello se conseguiría eludir que en el futuro pudieran adoptar lo que se conoce como carrera criminal⁸⁰. En dichos estudios, se investiga como una persona puede volverse una persona criminal desde la adolescencia y se intenta conocer los factores de riesgo que pueden llevar a cometer un delito y que se pueden agrupar en tres fuentes de influencia⁸¹. La primera serían los factores individuales, es decir, la personalidad de cada individuo y su propia manera de desenvolverse con el entorno. La segunda consiste en los riesgos o carencias respecto al apoyo prosocial. Mientras que, por último, también influyen las oportunidades delictivas a las que se puede ver expuesto el individuo. Por esta circunstancia, no todo el mundo puede llegar a delinquir. Tampoco tienen que darse los tres simultáneamente, sino que, igual que se pueden dar de forma conjunta, también pueden producirse de manera individual. Pero, ¿Qué motivaciones presenta una persona que realiza estafas, robos o extorsiones? ¿Qué pensamientos tiene para

⁷⁸ BINANCE (2018) *Tipos de phishing - Suplantación de URL*. Disponible en:

⁷⁹ BINANCE (2020). *Cómo habilitar Google Authentication (2FA) y preguntas frecuentes*. *Binance*

⁸⁰ PIQUERO, A.; HAWKINS, D.; KAZEMIAN, L.; PETECHUK, D.; REDONDO, S. (2011). *Patrones de carrera delictiva: prevalencia, frecuencia, continuidad y desistimiento del delito*. *Revista Española de Investigación Criminológica*.

⁸¹ REDONDO, S (2008). *Individuos, sociedades y oportunidades en la explicación y prevención del delito: Modelo de Triple Riesgo Delictivo (TRD)*. *Revista Española de Investigación Criminológica*.

realizar ese tipo de actos y porque? ¿Cómo se podría evitar? La educación es una herramienta fundamental, tanto por parte de las escuelas como de los padres. En este caso, se deben fomentar los factores de protección que funcionan de barrera frente a la posible adopción de una carrera criminal y minimizar aquellos que puedan ser de riesgo.

Este método también es aplicable a otros ámbitos más concretos, puesto que las organizaciones criminales y los grupos terroristas se dedican a captar personas a cambio de una remuneración o de una vida mejor. Ello nos llevaría a suplir las carencias económicas o las expectativas sociales que, individualmente, tiene cada persona. Esta circunstancia es muy difícil que no se produzca, ya que siempre habrá personas que no se conforman con su estatus social o quieren mantenerse en él y, por tanto, intentarán utilizar medios no convencionales para ello. Si estos nuevos medios no convencionales evolucionan con el tiempo, tendrán que adaptarse, como muy bien hemos visto, evaluando el caso de la llegada de las criptomonedas al mundo.

Para que puedan darse estos programas de concienciación y sensibilización tanto en la escuela como en otros medios (como puede ser la publicidad), ya sean convencionales o digitales, como en los medios de comunicación, el gobierno ha de destinar recursos económicos para que la sociedad adquiera, con el tiempo, seguridad en las criptomonedas para comenzar a utilizarlas como medio de pago. Pero para ello, primero, ha de existir una regulación que garantice esa seguridad y que estas medidas sean efectivas frente a lo que realmente se quiere proteger. Lo que se pretende evitar más concretamente es que las personas que invierten su dinero o deciden comprar Bitcoins o cualquier otra criptomoneda para usarlas como medio de pago, no sufra ninguna estafa como las que hemos visto en apartados anteriores, ni tampoco ningún robo de criptomonedas en sus *wallets*.

Por último, también conviene señalar como medida preventiva formar a los nuevos estudiantes tantos de economía como de criminología en las nuevas formas de pago digitales con criptomonedas que se puedan instaurar en el futuro debido al auge de estas. Da la sensación de que cada vez los gobiernos están más decididos a regular las monedas digitales y, por ende, es necesario que la población esté familiarizada con ellas y se tengan el sentimiento de seguridad, que ahora mismo no pueden ofrecer, para poder utilizarlas de forma que no peligre el capital de ningún usuario. Para ello, no solo se ha de formar a los estudiantes, ya sea cursando un grado o un máster específico en criptomonedas o en delitos realizados con éstas, sino que también las autoridades policiales han de contar con los recursos necesarios para hacer frente a los delitos que se puedan cometer con criptomonedas tanto a nivel nacional como internacional. Este último requiere de la colaboración y cooperación con otros países, ya sea de la UE, como de otros países del resto del mundo. De esta forma, la sociedad estará más preparada no solo para su uso, sino para poder hacer frente de manera eficaz y rápida a la criminalidad que pueda estar asociada al Bitcoin y al resto de criptomonedas.

VI. CONCLUSIONES

Para finalizar esta investigación, se indicarán algunos de los aspectos más importantes tratados durante su desarrollo y se aludirá al cumplimiento de los objetivos propuestos inicialmente. También se concretarán las limitaciones y líneas de investigación futuras.

Tras definir y diferenciar los distintos tipos de criptomonedas en el Capítulo 2, se puede establecer que la más atractiva del mercado es el Bitcoin, pero que también pueden surgir

otras, las stablecoins, como Tether, que están respaldadas por el dólar. Se descubre, por tanto, que estas últimas son las más seguras para los gobiernos que intentan instaurar las criptomonedas en la sociedad, ya que no tienen la volatilidad que posee el Bitcoin o el resto de criptomonedas.

Asimismo, se puede apreciar que cada país está tomando medidas distintas centradas en la regulación de las criptomonedas, no solo para evitar la posible comisión de delitos económicos con ellas, como hemos visto anteriormente en el Capítulo 3, sino también para implantarlas en la sociedad como monedas de curso legal que permitan la compra y venta de bienes e inmuebles. Parece que todos los países están dispuestos a regular, pero no hay consenso, al menos dentro de la Unión Europea, sobre las medidas que puedan ser más eficaces. Por ello, también se deja cierta libertad a que cada gobierno tome las medidas que considere más oportunas. Con ello también se consigue evaluar qué regulaciones son más efectivas en ciertos países para que el resto las puedan imitar y, en todo caso, llegar a mejorarlas, con tal de construir un futuro con criptomonedas que sea seguro para toda la sociedad.

Por otro lado, y una vez evaluada la tipología de delitos económicos e informáticos realizados con criptomonedas (Capítulo 4), se percibe que es relativamente sencillo cometer delitos por el hecho de que las transacciones realizadas con Bitcoins pueden llegar a ser anónimas sin una regulación, pero ¿es realmente anónimo el Bitcoin? ¿Qué medidas se pueden tomar para que realmente dejen de ser anónimas las transacciones que se realizan con cualquier tipo de criptomoneda? Es posible contestar a estas cuestiones, aunque conviene dejar claro que los cibercriminales siempre buscan nuevas maneras para poder continuar lucrándose por cualquier medio. La contestación a estas preguntas se ha llevado a cabo durante el desarrollo del capítulo 4, lo que nos permite ahora resumir los aspectos clave en las siguientes ideas, que se centran en:

- Identificación de todos aquellos usuarios que tengan cualquier tipo de moneda digital, ya sea en un *Wallet* privado o lo contengan en un *Exchange*.
- Obligación por parte de los *Wallets* y *Exchanges* de aportar información a las autoridades sobre sus usuarios con tal de evitar el blanqueo de capitales o la financiación del terrorismo.
- Cooperación y organización entre las plataformas que ofrecen criptomonedas y los gobiernos.

Estas medidas pueden ser eficaces, pero no evitan que se siga utilizando el anonimato si se realiza de particular a particular. Esta circunstancia sería un dato interesante para investigar en el futuro: ¿cómo evitar tanto el blanqueo de capitales como la financiación de grupos u organizaciones criminales?.

Toda la legislación de los distintos países va dirigida a penalizar al blanqueo de capitales y nada a la concienciación de la ciudadanía para evitar las estafas, robos o las extorsiones que se puedan realizar con criptomonedas. De hecho, el mercado de las criptomonedas es muy inestable, aparte de que es una novedad histórica, no está centralizada ni respaldada por ningún gobierno y ello provoca inseguridades en los inversores. Con lo cual la manipulación del mercado, en cuanto la especulación, es mayor y las fluctuaciones en el precio de las criptomonedas también lo es, ya que lo mismo en un día se multiplican por dos, que se vuelen a dividir entre dos. Por ello, descubrimos que la concienciación ciudadana sobre el uso de las criptomonedas puede ser clave para la prevención, ya que la población puede protegerse

mediante el uso de *wallets* y *exchanges* que sean seguros y estén avalados por los gobiernos. Esto se ve durante el Capítulo 5.

Otro punto importante dirigido a la prevención es la actuación de las autoridades policiales, que deben estar formadas por buenos equipos de informáticos especializados en delitos con criptomonedas con tal de que puedan aprender a detectar la posible comisión de delitos con criptomonedas o disponer de buenos medios que permitan perseguir infracciones relacionados con las monedas digitales. Para ello, lo principal, además de una formación especializada en esta nueva tecnología, es dotar de mayores recursos que permitan con mayor facilidad favorecer las investigaciones que realizan.

Como se ha podido comprobar, y gracias a toda la información recopilada en esta investigación, se han podido alcanzar los objetivos propuestos inicialmente (tanto el general como los específicos).

En cuanto a las limitaciones de este estudio, caben destacar varias. Por ejemplo, no se ha podido profundizar, por cuestiones de espacio, en la importancia y las utilidades sociales que puede aportar la tecnología Blockchain, que es la que permite que el Bitcoin y el resto de criptomonedas funcionen a otros ámbitos independientes al de la economía, como pueden ser al de la seguridad, la salud, el sistema judicial o policial, ya que esta tecnología permite y favorece la transmisión de información inmediatamente de particular a particular sin intermediarios. Otra limitación se encuentra en la dificultad de acceso a cierta información sobre el tema, debido a que no existen muchos documentos académicos que traten aspectos relacionados con las criptomonedas (se considera un tema relativamente novedoso).

Asimismo, surgen nuevos interrogantes sobre el futuro de las criptomonedas y su uso en una sociedad cada vez más globalizada e interconectada. ¿Podría ser que en el futuro no existieran las monedas por países si no las monedas por empresas? ¿de qué manera se gestionaría la emisión de criptodivisas si este fuera el caso?, ¿por la propia empresa? ¿Qué criterios podrían utilizarse para establecer este método como legal?

Otra línea de investigación futura que se podría proponer iría encaminada a evitar que ciertas entidades blanqueen su capital obtenido de forma ilegal por medio de las criptomonedas. Para ello, se podría evaluar y establecer criterios de quien puede o no ejercer el control sobre un *exchange*. ¿Pueden hacer algo los *exchanges* para evitar el blanqueo de capitales? ¿Estas mismas plataformas de compra y venta de criptomonedas, pueden ser empresas dedicadas a blanquear su propio capital? La respuesta a la primera pregunta es que sí, ya que tienen la obligación impuesta por la UE de implantar mecanismos para prevenir este delito, pero ¿son suficientes? La respuesta es simple y es que no, ya que todavía existen mecanismos para enviar criptomonedas desde plataformas que no están legalizadas ni controladas. En cuanto a la segunda pregunta, la respuesta es que podría darse que alguna de las plataformas o, incluso, los creadores de alguna moneda, pudieran haberlas creado con dicha finalidad, la de blanquear capitales conseguidos por medios ilícitos, pero ¿cómo se podría regular esta circunstancia? ¿Un control de los propietarios de los *exchanges*? ¿Qué los creadores de nuevas monedas digitales tuvieran que pasar ciertos controles para que su criptodivisa fuera legalizada por las autoridades competentes? Convendría analizar y profundizar más en este tema para establecer unos límites o pautas que permitan, mediante herramientas útiles, que se utilizaran de manera lícita los *exchanges* y las creaciones de nuevas monedas digitales.

VII. BIBLIOGRAFÍA

- ACADEMY BIT2ME. *Impuestos: Hacienda y Bitcoin ¿qué declarar en España por tener criptomonedas?*. Disponible en:
- AGENCIA EFE (2021). *Las criptomonedas han llegado para quedarse, según los economistas*. Disponible en:
- ÁLVARO SANCHEZ (2021) *Imitadores de Reddit abarrotan Telegram de grupos para comprar y vender de forma coordinada*. Disponible en:
- ARÁNGUEZ SÁNCHEZ, C. (2020). *El bitcoin como instrumento y objeto de delitos. El bitcoin como instrumento y objeto de delitos*, 75-103.
- ARBISTAR 2.0 S.L. (2020) *Nota informativa. Cierre del Community Bot*. Disponible en:
- ASTRAY RODRÍGUEZ, M. C. (2019). *Bitcoin, ¿Oportunidad del siglo o burbuja especulativa?* Disponible en:
- AVAN-NOMAYO, OSATO (2021) *Los reguladores holandeses no conocen el número exacto de inversores en criptomonedas en los Países Bajos*. Disponible en:
- BARI, MATÍAS (2021) *Cómo avanzan las regulaciones a las criptomonedas en el mundo*. Infotechnology. Disponible en:
- BINANCE (2018) *Tipos de phishing - Suplantación de URL*. Disponible en:
- BINANCE (2018) *Casos de sitios phishing*. Disponible en :
- BINANCE (2018) *Casos de correos electrónicos de Phishing*. Disponible en:
- BINANCE (2021) *Fuente: ¿Qué es la verificación KYC y por qué es cada vez más importante para las criptomonedas?* Disponible en:
- BINANCE (2020). *Cómo habilitar Google Authentication (2FA) y preguntas frecuentes*. Disponible en:

- BITFINEX (2016) *Announcements - Security Breach*. Disponible en:
- BOUISSA, L., GARÍN, F., & ROSTÁN, A. (2019). *Relevamiento de técnicas de rastreo y entintado de dinero en Bitcoin*. Disponible en:
- BOURGI, SAM (2021). *Ley alemana que permite a los fondos institucionales invertir en criptomonedas entrará en vigor el 2 de agosto*. Disponible en:
- CCN-CERT, COMUNICADOS. (12/05/2017). *Identificado ataque de ransomware que afecta a sistemas Windows*. Disponible en:
- CCN-CERT, COMUNICADOS. (2017). *Identificado ataque de ransomware que afecta a sistemas Windows*. Disponible en:
- CHANNING D. PHILLIPS (2021) *Statement of the offense and related conduct* Disponible en:
- CIVIETA, OSCAR (2021). *Estados Unidos abre la puerta a la regulación de las criptomonedas*. Disponible en:
- CORREDOR HIGUERA, J. A., & DÍAZ GUZMÁN, D. (2018). Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina. *Derecho pupc*, (81), 405-439.
- CUARTAS BÁEZ, R. Y. (2019). *Hacia una regulación de los cryptoactivos en Colombia: el enfoque de los sistemas de prevención del riesgo de LA/FT* (Doctoral dissertation, Bogotá: Universidad Externado de Colombia, 2019.).
- DAN GOODIN (2014) *“Pony” botnet pilfers digital coins worth \$220,000 in sustained attack*. Disponible en:
- DANNA HARMAN (2015) *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*. Disponible en:
- DEPARTMENT OF JUSTICE OFFICE OF PUBLIC AFFAIRS (2021) *Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin ‘Mixer’ That Laundered Over \$300 Million* Disponible en:

DOMINGUEZ, DANIEL (2021). EEUU mueve ficha para regular las criptomonedas. Disponible en:

DP ABOGADOS (2020) *Afectados por el incumplimiento contractual-estafa de Arbistar 2.0, Nimbus y Mind Capital.*

ELECONOMISTA (2021). Las pretensiones de EEUU de una mayor regulación abren un horizonte de más 'bandazos' en las criptomonedas. Disponible en:

ELECONOMISTA (2021). Rogoff, sobre el bitcoin y las criptomonedas: "Las autoridades tienen que despertar antes de que sea tarde". Disponible en:

ELECONOMISTA (2021). La stablecoin de Facebook (Diem) que iba a cambiarlo todo se desinfla antes de nacer. Disponible en:

EL ECONOMISTA (2021). *Protestas y dudas en El Salvador ante la inminente adopción del bitcoin como moneda de intercambio.* Disponible en:

ELECTRONIC IDENTIFICATION (2021). Qué es KYC (Know Your Customer) y su actualidad en 2021. Disponible en:

EUROPEAN CENTRAL BANK (2012). *European Central Bank (Banco Central Europeo)-EuroSystem.*

EUROPOL (2015) The Internet Organised Crime Threat Assessment (IOCTA). Pág.46 Disponible en:

ESPARRAGOZA, LUIS (2021). Más de 4000 fondos de inversión en Alemania podrán invertir en Bitcoin y criptomonedas. Disponible en:

EZANIME (2021). El regulador del mercado de valores de Italia pide una regulación sobre las criptomonedas para prevenir la actividad criminal. Disponible en:

FERNÁNDEZ, FROILAN (2021). En Panamá diputado presenta proyecto de ley para regular las criptomonedas. Disponible en:

FERRER-BONSOMS HERNÁNDEZ, IGNACIO. (2020) Fuente: Entra en vigor la nueva directiva de la Unión Europea para poner cerco a las criptomonedas. Disponible en:

GIL, J.A. (2021). *Países que más invierten en criptomonedas*. Disponible en:

GRUPO ÁTICO 34. (2021). *La regulación de criptomonedas en España*. Disponible en:

GUARDIA CIVIL (2018) La Guardia Civil desarticula una organización criminal dedicada al blanqueo de capitales procedentes del narcotráfico mediante el uso de criptomonedas Disponible en:

HAIG, SAMUEL (2021). Las cryptoempresas irlandesas impondrán controles de identificación contra el lavado de dinero a partir de abril. Disponible en:

IBARRA, JUAN (2021). Binance tampoco puede operar en Italia, dice el regulador financiero italiano. Disponible en:

JAVIER PASTOR (2020) Roban 1,2 millones de euros en bitcoins en la plataforma fintech española 2gether. Disponible en:

JAVIER PASTOR (2017) Wanna Decryptor: así funciona el ransomware que se ha usado en el ciberataque a Telefónica. Disponible en:

JIMÉNEZ, M. N. P. (2016). Criptodivisas: del bitcoin al MUF6. El potencial de la tecnología blockchain. Revista Cesco de derecho de consumo, (19), 6-15.)

JOSEPH YOUNG (2018) Fake Elon Musk Crypto Giveaway Scam Gets 0.4 BTC as Twitter Fails to Vet Advert. Disponible en:

JUSTO, DAVID (2021). "No piques": la Policía Nacional alerta sobre esta estafa que te puede llegar por WhatsApp. Disponible en:

LABE ABOGADOS (2020) Estafa Arbistar. Disponible en:

LAMARES, CAPELA & ASOCIADOS (2021). Portugal y las criptomonedas. Disponible en:

- MARTÍNEZ, D. (2021). *Ranking de los países donde más utilizan bitcoin*. Disponible en:
- MCBRIDE, LANDON (2021). El Gobierno francés impulsa la creación de una agencia que regule las criptomonedas en toda la UE. Disponible en:
- MEDINA, D. P. (2020). Artículo 10/2020_EJIC (nº 206) Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. *Boletín Criminológico*, 1(197-206).
- MUÑOZ ESTEBAN, M. (2017). *La moneda digital: El bitcoin*.
- NATIONAL SECURITY DIVISION (2015) Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL. Disponible en:
- OLIVA LEÓN, RICARDO (2021). Regulación legal del bitcoin y de otras criptomonedas en España. Disponible en:
- OLVERA RODRÍGUEZ, PATRICIA (2016). Término CRIMIPEDIA: Web profunda, darknet y Tor. CRIMINA, centro para el estudio y prevención de la delincuencia.
- ORDINAS, MIRIAM (2017). Las criptomonedas, ¿Oportunidad o burbuja?. Informe mensual de estrategia BancaMarch.
- PASTOR, JAVIER (2021). *El Salvador se convierte en el primer país del mundo en el que bitcoin se convierte en criptomoneda de curso legal, pero no sin polémica*.
- PIQUERO, A.; HAWKINS, D.; KAZEMIAN, L.; PETECHUK, D.; REDONDO, S. (2011). Patrones de carrera delictiva: prevalencia, frecuencia, continuidad y desistimiento del delito. *Revista Española de Investigación Criminológica*, nº9.
- PARTS, HELEN (2021). *La República de Panamá presenta un proyecto de ley para regular las criptomonedas*. Disponible en:
- RAMIREZ, HELENA (2021). MiCA, la propuesta de la UE para la regulación del mercado de cryptoactivos. Disponible en:
- RAMÍREZ, HELENA (2021). MiCA, la propuesta de la UE para la regulación del mercado de cryptoactivos. Disponible en:
- REDACCIÓN TERRITORIO BITCOIN ¿Cómo funciona un mezclador de Bitcoin? Disponible en:
- REDONDO, S (2008). Individuos, sociedades y oportunidades en la explicación y prevención del delito: Modelo de Triple Riesgo Delictivo (TRD). *Revista Española de Investigación Criminológica*. Artículo 7, N. 6.

RUS, CRISTIAN (2021). *Reino Unido prohíbe algunas actividades de Binance como los contratos de futuros a partir del 30 de junio*. Disponible en:

SANTISTEVAN, BETSSY (2021). China prohíbe a instituciones y medios de pago operar con criptomonedas. Disponible en:

SARKAR, ARIJIT (2021). Todos los usuarios de Binance ahora están sujetos a la verificación inmediata de KYC. Disponible en:

SOLUCIONES CONFIRMA (2018) La operación del mes: Tulipán Blanca, primera contra el blanqueo con bitcoins Disponible en:

TENA PLATA, A. (2019). Las criptodivisas y el blanqueo de capitales.

TORRES MACIAS, E. M. (2015). Reflexiones respecto a las ventajas y desventajas del uso del Bitcoin.

WAGEMAKERS, BJORN (2018). Reglamento de criptomonedas en Países Bajos. Disponible en:

WILLIAM SUBERG (2017) Simpatizante del ISIS en EE. UU. fue atrapada enviando \$ 150,000 a Siria en criptomonedas lavadas. Disponible en:

WINDOWS SERVER 2016 (2017). MS17-010: Actualización de seguridad para Windows Server de SMB. Disponible en:

WINDOWS SERVER 2016 (2017). MS17-010: Actualización de seguridad para Windows Server de SMB. Disponible en:

WRIGHT, TURNER (2021). "No nos queda mucho tiempo" para regular las criptomonedas, según el director del Banco de Francia. Disponible en: