Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

Criptomonedas y derecho penal: más allá del blanqueo de capitales *

Adán Nieto Martín y Beatriz García-Moreno
Universidad de Castilla-La Mancha

NIETO MARTÍN, ADÁN y GARCÍA-MORENO, BEATRIZ. Criptomonedas y derecho penal: más allá del blanqueo de capitales. *Revista Electrónica de Ciencia Penal y Criminología*. 2021, núm. 23-17, pp. 1-31. http://criminet.ugr.es/recpc/23/recpc23-17.pdf

RESUMEN: Las normas relativas al blanqueo de capitales y la financiación del terrorismo son el aspecto más conocido de la regulación penal de las criptomonedas. Sin embargo, los retos que plantean al derecho penal estas monedas virtuales son más diversos y a ellos se dedica el presente trabajo. En una primera parte, se reflexiona sobre la conveniencia de proteger desde el derecho penal el monopolio de los Estados frente a la emisión de monedas virtuales y criptomonedas. En una segunda parte se aborda la protección del usuario de criptomonedas como consumidor, analizándose tres tipos de conductas: los fraudes que tienen en lugar en el momento de la adquisición de criptomonedas o en su lanzamiento, las operaciones similares al abuso de mercado en el mercado de criptomonedas y, finalmente, la protección de las criptomonedas como medios de pago, aspecto éste del que se ocupa la reciente Directiva europea 2019/713.

PALABRAS CLAVE: Criptomonedas, fraude, delito contra los consumidores, política monetaria.

TITLE: **Cryptocurrencies and criminal law: beyond money laundering**

ABSTRACT: Money laundering and financing of terrorism regulations are the best known aspect of the criminal regulation of crypto currencies. However, the challenges posed to criminal law by these virtual currencies are more diverse and this paper focuses on them. In the first part, it reflects on the convenience of protecting through criminal law the monopoly of the States against the issuance of virtual currencies and cryptocurrencies. The second part deals with the protection of the cryptocurrencies user as consumers, analyzing three types of behaviors: frauds that take place at the moment of the acquisition of cryptocurrencies or at their launch, operations similar to market abuse in the cryptomarket, and finally, the protection of cryptocurrencies as a means of payment, an aspect that is dealt with in the recent European Directive 2019/713.

KEYWORDS: Cryptocurrencies, fraud, offences against consumers, monetary policy.

Fecha de recepción: 15 enero 2021

Fecha de publicación en RECPC: 4 octubre 2021

Contacto: Beatriz.GarciaMoreno@uclm.es

SUMARIO: I. El punto de partida: ¿Qué política legislativa y por tanto política criminal frente a las criptomonedas? II. Monedas virtuales, criptomonedas: ¿resulta necesario proteger penalmente la política monetaria? 1. La creación no autorizada de criptomonedas. 2. La "casa de papel" o la creación indebida de criptomonedas. III. Fraudes y publicidad engañosa en la emisión y oferta de criptomonedas. IV. Criptomonedas y Derecho penal del mercado de valores. V. Las criptomonedas

como medio de pago. 1. La asimilación. 2. La distinción entre delitos de lesión y ámbito previo. 3. Medios de pago materiales e inmateriales: la relevancia de la criminalidad informática. 4. ¿Cuándo existe una sustracción, apoderamiento o falsificación o posesión ilegítima de un medio de pago? 5. El derecho penal como ultima ratio y el delito de fraude (Art. 6). 6. La falsificación en un medio de pago distinto al efectivo (art. 4. b) y 5 b)). VI. Conclusiones. Bibliografía.

* Este trabajo se enmarca en el desempeño de la Dra. García-Moreno como titular de un contrato postdoctoral para la excelencia científica en el desarrollo del Plan Propio de I+D+i de la Universidad de Castilla-La Mancha, cofinanciado por el Fondo Social Europeo. También a la participación de ambos autores en el proyecto de investigación "Cryptocurrencies and Crime: EU Regulatory Needs and Enforcement Strategy (CRYPTOCRIME)"- 017/11757193, liderado por la profesora Allegrezza.

I. El punto de partida: ¿Qué política legislativa y por tanto política criminal frente a las cripto-monedas?

Las criptomonedas[1] carecen de una regulación jurídica unitaria y esta circunstancia caracteriza la relevancia penal de los comportamientos que se comenten mediante las mismas. Su régimen jurídico penal, al igual que su régimen jurídico en general, resulta discontinuo y fragmentario, lo que complica la descripción de los riesgos penales derivados de la creación y funcionamiento de las criptomonedas[2]. A esta tarea hay que añadir además otra dificultad: La variedad de monedas virtuales que tienen cabida dentro de este concepto - con diversas características y grados de control por parte de sus operadores- y la rapidez con la que aparecen otras nuevas[3].

Las normas relativas al blanqueo de capitales y la financiación del terrorismo son el aspecto más conocido de la regulación jurídico penal de las criptomonedas. Desde su aparición, la mayor preocupación es que puedan servir como medio de pago en transacciones ilícitas y como forma para introducir activos procedentes de actividades delictivas en la economía legal[4]. La Directiva (UE) 2018/843 del Parlamento europeo y del Consejo[5] tiene como finalidad, en este punto, considerar sujetos

[1] Para un estudio sobre la aparición de las criptomonedas, sus características y algunos de los retos que presenta para el derecho -más allá del derecho penal-, vid. BARROILHET DÍEZ, 2019, passim.

[2] La UE ha dado ya os primeros pasos en la regulación del mercado de los criptoactivos y en abril de 2020 la Comisión presentaba una propuesta de regulación. Vid. Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM(2020) 593 final, 2020/0265 (COD).

[3] De acuerdo con CoinMarketCap existen en la actualidad más de 10.400 criptomonedas (último acceso: 10.6.2021). CoinMarketCap (coinmarketcap.com) es una plataforma online que realiza un seguimiento de la capitalización de diferentes criptomonedas, la cantidad de operaciones que las utilizan y el precio actual convertido a monedas fiduciaria.

[4] Vid. UNITED STATES DEPARTMENT OF JUSTICE, 2020, pp. 5 y ss. Se encuentra aquí una exposición de los usos ilícitos de las criptomonedas detectados en la práctica, tanto como medio de pago en mercados ilícitos (e.g. de armas, pornografía infantil) como para la ocultación de otras actividades ilícitas, como el fraude fiscal.

[5] Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Diario Oficial de la Unión Europea L 156/43, 19 de junio de 2018.

obligados a las personas que realizan dos actividades claves en el comercio de criptomonedas, de un lado, los proveedores de servicios de cambio entre las monedas virtuales y las fiduciarias o de curso legal y, de otro, los proveedores de servicios de monedero. Estas disposiciones no suponen ninguna novedad en la estrategia de prevención del blanqueo de capitales. Se trata de asignarles la función de "vigilantes" en dos actividades clave en el tráfico de criptomonedas con el fin de que den la alarma ante las autoridades encargadas de la prevención del blanqueo cuando detecten operaciones sospechosas. Aunque nuestro trabajo dejará de lado este aspecto[6], la Directiva del 2018 contiene una definición de moneda virtual que después ha sido acogida por otras regulaciones[7].

Como ha declarado recientemente el Tribunal Supremo español las criptomonedas no son dinero de curso legal[8]. Esta afirmación implica que su posible falsificación o emisión indebida no pueda ser sancionada a través de los delitos de falsedad de moneda. La afirmación del TS coincide con el concepto de moneda contenido en la Directiva relativa a la falsificación del euro[9], que armoniza los delitos de falsedad de moneda en todos los países miembros. La Directiva sigue siendo tributaria de la Convención de Ginebra de 1924, que abarca sólo a monedas de curso legal, entendiendo

[6] Para un análisis en detalle sobre esta cuestión, vid. NAVARRO CARDOSO, 2019, pp. 18-38; HOUBEN/SNYERS, 2018 pp. 58-85; PÉREZ LÓPEZ, 2017, pp. 151 y ss; MÖSER/BÖHME/ BREUKER, 2013, pp. 1-11; NAVARRO LÉRIDA,2020, pp. 485-512; PÉREZ MEDINA, 2020, p.18 ; BROWN, 2016, pp. 1-10.

[7] La Directiva define la moneda virtual -género al que pertenecen las criptomonedas- como "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 aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos". Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. Diario Oficial de la Unión Europea L 156/43, 19 de junio de 2018.

[8] Vid. STS 20 junio 2019 (ECLI: ES:TS:2019:2109). En esta resolución el Tribunal Supremo sostiene que se trata de un activo patrimonial inmaterial de contraprestación o intercambio en aquellas transacciones bilaterales en las que los contratantes lo acepten. El Banco Central Europeo ha adoptado también esta postura, indicando con rotundidad que "las monedas virtuales no son dinero ni monedas desde una perspectiva legal". Vid. BANCO CENTRAL EUROPEO, 2015, p. 25. Menos clara, sin embargo, resulta la posición del TJUE se ha referido al bitcoin como una "divisa virtual de flujo bidireccional, que se intercambia por divisas tradicionales en las operaciones de cambio, que no tiene ninguna finalidad distinta de la de ser un medio de pago". Vid STJUE 22 octubre 2015 (ECLI:EU:C:2015:718), §24 cuestión prejudicial planteada por el *Högsta förvaltningsdomstolen*, asunto C-264/14. Las Conclusiones del Abogado General, J. Kokott, señalan además que su posesión no tiene ninguna otra utilidad que utilizarlos en cualquier momento como medio de pago y los califica, por tanto, como un medio de pago puro. En este mismo sentido se han pronunciado los tribunales estadounidenses. En EEUU, el Treasury Department ha reconocido que pueden ser similares a la moneda de curso legal pero que le faltan algunas de sus características. Por su parte, el Internal Revenue Service ha señalado que las criptonedas están sujetas a impuestos y que si se utiliza como pago, debe tratarse como moneda. Sobre el estatus legal de las criptomonedas en EEUU puede verse KETHINENI/ CAO, 2020, pp. 7-8.

[9] Art. 2 de la Directiva 2014/62/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a la protección penal del euro y otras monedas frente a la falsificación, y por la que se sustituye la Decisión marco 2000/383/JAI del Consejo. Diario Oficial de la Unión Europea L 151/1, 21 de mayo de 2014.

por tales aquellas que tienen que ser obligatoriamente admitidas como medios de pago.

Además, las criptomonedas quedan fuera del ámbito de la legislación de la UE en materia de servicios financieros y, por tanto, no están sujetas a las disposiciones relativas a la protección de los inversores y la integridad del mercado -incluidas las de manipulación de mercado- y, además, escapan a la supervisión de las autoridades bursátiles[10].

Ahora bien, aunque jurídicamente las criptomonedas no sean dinero, ni activos financieros, nada impide considerarlas como bienes de consumo. Un bien de consumo que puede utilizarse como medio de pago y en el que algunos ciudadanos deciden invertir sus ahorros. En este sentido su estatus es similar a las inversiones que se realizan en oro. El que sean un bien de consumo implica que les es aplicable el derecho que tutela a los consumidores y especialmente las disposiciones sobre publicidad engañosa que se contienen en la Directiva 2006/144/CE sobre publicidad engañosa[11].

Asimismo, para el Derecho de la UE, las criptomonedas, aunque no son dinero de curso legal, son un medio de pago. La reciente Directiva 2019/713[12] relativa a la falsedad en medios de pago distintos al efectivo las ha incluido dentro de las denominadas monedas virtuales, a las que define como "representación digital de valor que no ha sido emitida ni está garantizada por un banco central ni por una autoridad pública, no está necesariamente asociada a una moneda de curso legal ni posee la condición jurídica 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". Y es que, en efecto, las criptomonedas son una clase de monedas virtuales que se caracterizan por utilizar para su circulación una determinada tecnología: un registro de transacciones descentralizado, pero unitario, que utiliza la criptografía como mecanismo de seguridad. Esta tecnología es lo que conocemos básicamente como *blockchain* y, en lo que aquí interesa, confiere un gran protagonismo a la criminalidad informática como herramienta para realizar las diversas conductas delictivas que tienen lugar en este ámbito.

La superación de este marco regulatorio discontinuo y la fijación de una política criminal coherente en relación con las criptomonedas exigen determinar cuál va a ser

[10] Sobre la posible consideración de los criptoactivos como producto financiero y su sujeción a la normativa europea en este sentido, vid. AUTORIDAD EUROPEA DE VALORES Y MERCADOS , 2019, pp. 18 y ss.

[11] Directiva 2006/114/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, sobre publicidad engañosa y publicidad comparativa. Diario Oficial de la Unión Europea L 376/21, 27 de diciembre de 2006.

[12] Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo. Diario Oficial de la Unión Europea L 123/18, 10 de mayo de 2019.

la posición del legislador hacia las mismas[13]. Existen básicamente tres posibilidades en este punto.

La primera es adoptar una actitud favorable. Si se considerara oportuno que su uso se expanda y se parifiquen con el dinero fiduciario, lo coherente sería darles una protección penal semejante a la que éste tiene a través de los delitos de falsificación de moneda (asimilación). Para ello habría que adaptar las modalidades comisivas de estos delitos a las monedas virtuales y criptomonedas.

La segunda posición sería la neutralidad. En este escenario lo oportuno seria aplicar los tipos penales existentes en la medida que ello sea posible, sin violentar la prohibición de analogía, y reforzar el sistema penal frente a los delitos cuya comisión puede verse facilitada por las criptomonedas. Esto último, precisamente, es lo que ha ocurrido con la reciente modificación de la Directiva de blanqueo de capitales y financiación del terrorismo.

Como tercera posibilidad, cabe una posición algo más cautelosa, en el sentido de no prohibir, pero sí al menos someter a algún tipo de autorización o supervisión la emisión de criptomonedas. Es un camino que ya se ha emprendido por algunos Estados dentro de los EEUU, como es el caso de Nueva York, o dentro de la UE por países como Alemania o - con una regulación particularmente detallada - Estonia. Estas regulaciones tienen como nota común exigir algún tipo de autorización para la emisión de una criptomoneda, así como para ejercer actividades como la de intercambiador, oferente o incluso minero. La finalidad de esta normativa es la defensa del consumidor, ya sea ahorrador o inversor. No obstante, y como paso previo, es preciso preguntarse si además deben establecerse disposiciones, incluidas penales, que preserven el monopolio de los Estados frente a la emisión de monedas virtuales y criptomonedas[14].

La segunda parte del trabajo se centra en la protección del usuario – real o potencial – de criptomonedas como consumidor. En este punto se analizarán tres tipos de

[13] Un análisis sobre las distintas posiciones en la regulación del Bitcoin -en particular, analizando las adoptadas por EEUU, China y Rusia- puede leerse en JIA / ZHANG, 2018, pp. 88-108.

[14] Esta parece ser la posición de la UE respecto al tratamiento de los criptoactivos. En la propuesta de reglamento para la regulación de este mercado se muestra decidida a su impulso, admitiendo que pueden tener grandes ventajas tanto para los participantes en el mercado como para los consumidores. Así, señala que "Las emisiones de criptoactivos, al simplificar los procesos de captación de capital e intensificar la competencia, pueden suponer una forma más barata, menos gravosa y más inclusiva de financiar a las pequeñas y medianas empresas (pymes). En cuanto a las fichas de pago, cuando estas se usan como medio de pago, pueden brindar la oportunidad de realizar pagos más baratos, rápidos y eficientes, en particular a nivel transfronterizo, dado que se limita el número de intermediarios". Ahora bien, de igual modo, establece sistemas de autorización y supervisión de los proveedores de servicios de criptoactivos, los emisores de fichas referenciadas a activos y los emisores de fichas de dinero electrónico, permitiendo por ejemplo la denegación de la autorización cuando el modelo de negocio del emisor puede suponer una amenaza grave para la estabilidad financiera, la transmisión de la política monetaria o la soberanía monetaria; además incluye medidas de transparencia informativa para la protección de consumidores y medidas dirigidas a prevenir el abuso de mercado, con el fin de garantizar la integridad de los mercados de criptoactivos. Vid. Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM(2020) 593 final, 2020/0265 (COD).

conductas. La primera son los fraudes que tienen en lugar en el momento de la adquisición de criptomonedas o en su lanzamiento (III), aspecto éste que se deja de lado en la Directiva sobre falsificación de los medios de pago. El segundo grupo de conductas se centra en operaciones similares al abuso de mercado en el mercado de criptomonedas (IV). Se trata de la protección del propietario como inversor. Finalmente nos ocuparemos de la protección de las criptomonedas como medios de pago, aspecto éste sobre el que se ocupa la reciente Directiva europea 2019/713 (V).

II. **Monedas virtuales, criptomonedas: ¿resulta necesario proteger penalmente la política monetaria?**

1. ***La creación no autorizada de criptomonedas***

La moneda constituye uno de los atributos de la soberanía y por esta razón ha gozado siempre de una amplia protección penal. Como es bien conocido, las conductas delictivas sobre la moneda física fueron consideradas históricamente delitos de lesa majestad, pero además, aunque de manera menos conocida, el derecho penal también ha desempeñado un papel relevante a la hora de proteger la propia política monetaria y las normas que aseguran la supremacía de la moneda estatal dentro del territorio, frente a otras monedas extranjeras o monedas privadas, que han existido en algunos países a lo largo de la historia. Soberanía, moneda y territorio constituyeron una triada de elementos inseparables, que desde el inicio de la globalización se ha visto en parte socavada por la libre circulación de capitales. La aparición de las monedas virtuales y criptomonedas supone un paso más en esta dirección. Hasta ahora el libre mercado de monedas, que produce la libre circulación, se da entre las monedas fiduciarias de cada Estado. Las monedas virtuales y las criptomonedas conllevan una privatización, en cuanto que su aceptación supone admitir que monedas privadas compitan con las estatales[15].

Para responder a la pregunta que se plantea en el título de este epígrafe, y reflexionar sobre el posible diseño de la intervención penal, es necesario detenerse sobre el concepto de dinero. El dinero materialmente se caracteriza por cumplir tres funciones. En primer lugar, porque se admite generalizadamente como medio de pago. En segundo lugar, porque es capaz de conservar su valor en el tiempo, lo que por ejemplo nos permite ahorrar, porque sabemos que pasados los años esta cantidad de dinero depositada no disminuirá significativamente. Y, finalmente, en tercer lugar, porque el dinero sirve para medir eficazmente el valor de las cosas. Medimos con él el valor de bienes o servicios en dinero. En teoría estas funciones las puede cumplir tanto una moneda de curso legal o moneda fiduciaria como una moneda privada.[16]

[15] NISTICÒ, 2019, pp. 3 y ss. Un estudio económico sobre la competición entre monedas estatales y monedas privadas puede leerse en FERNÁNDEZ-VILLAVERDE/ SANCHES, 2016, pp. 19 y ss.

[16] Sobre la posibilidad de que las criptomonedas cumplan con estas tres funciones, vid. HE, D. /

Los Estados han tenido en su mano tradicionalmente una serie de herramientas que les han servido para garantizar una situación de monopolio de su moneda frente al resto de monedas estatales.Lo que ahora se plantea es la posibilidad de utilizarlas frente a las nuevas monedas privadas.

La primera herramienta es la declaración de la moneda estatal como moneda de curso legal, de tal forma que en su territorio sea obligatorio aceptar esta moneda como forma de pago para salvar una deuda. Más aún, algunos Estados establecen incluso que su moneda es la única admisible como medio de pago, de modo tal que no se puede saldar una deuda o hacer una compra dentro del territorio utilizando una moneda distinta. Esta manifestación de la soberanía estatal fue apoyada históricamente mediante una norma penal específica, que sancionaba la negativa a aceptar dinero de curso legal como medio de pago (vid. por ejemplo, en España, el art. 573.1 del CP español de 1973, con un precepto procedente del art. 482.7 del CP de 1848). Muy pocos son los países que han prohibido hasta el momento los pagos en monedas virtuales y criptomonedas[17].

La segunda y principal herramienta que tiene el Estado de asegurar la efectividad de su moneda son las normas de control de cambios, cuyo objetivo es establecer un control administrativo sobre la exportación o importación de la moneda, las operaciones de cambio o la tenencia de otras monedas extranjeras dentro del territorio. Con ello se restringe que los ciudadanos de un territorio utilicen como instrumento de pago monedas distintas a la estatal y además se fuerza a que ahorren en estas monedas, ya sea dentro o fuera del territorio. El derecho penal ha estado indisolublemente unido a los sistemas de control de cambios, con el fin de reforzar la vigencia de estas normas cuya finalidad era asegurar la supremacía de la moneda estatal dentro del territorio y en definitiva la soberanía estatal.

Finalmente, la tercera y principal forma de asegurar la efectividad de la moneda estatal es la política monetaria en manos de los bancos centrales, cuyo objetivo es el control de la inflación. Una moneda sana, sin inflación, no necesita ni control de cambios, ni medidas que obliguen al pago en moneda nacional. Una moneda sin inflación puede competir con ventaja dentro de su territorio con cualquier otra moneda. En realidad, el resto de instrumentos tienen hoy un carácter excepcional cuando un Estado no es capaz de mantener una moneda competitiva en el mercado. La libre

HABERMEIER, K. F. / LECKOW/ HAKSAR/ ALMEIDA/ KASHIMA/ KYRIAKOS-SAAD/ OURA/ SAADI SEDIK/ STETSENKO/ VERDUGO YEPES, 2016, pp. 10-17 Estos autores concluyen que las criptomonedas en la actualidad no satisfacen ninguna de las tres funciones del dinero. Así, entienden que su alta volatiilidad limita su función como depósito de valor, su limitada aceptación en las transacciones impide considerarlo un medio de pago y, finalmente niegan su rol como unidad de cuenta independiente pues en lugar de utilizarse para medir el valor de bienes y servicios directamente, representan el valor en moneda fiduciaria según el tipo de cambio de la criptomoneda. En el mismo sentido, BANCO CENTRAL EUROPEO, 2015, pp. 23 y ss.

[17] Argelia, Marruecos, Bolivia, Nepal, Pakistán, y Vietnam, entre otros, han prohibido cualquier transacción con criptomonedas. Vid. THE LAW LIBRARY OF CONGRESS OF THE US, GLOBAL LEGAL RESEARCH CENTER, 2018, p. 2. Vid. también JIMÉNEZ, 2020, passim.

circulación de capitales, que es uno de los fundamentos de la UE, no sólo *ad intra* sino también con terceros países, tiene como condición la existencia de una moneda fuerte, lo que se consigue con la independencia del Banco Central Europeo y su política destinada a garantizar la inflación de los precios.

Dentro de este modelo económico, la aparición de las criptomonedas lleva a hacerse dos preguntas consecutivas. La primera, tal como ya avanzábamos, si debemos admitir que las monedas virtuales y criptomonedas compitan libremente, en nuestro caso, con el euro. La respuesta que hasta ahora ha dado el Banco Central Europeo es afirmativa[18]. No hay que poner mayores restricciones a la libre circulación de las monedas virtuales que las que existen en relación con otras monedas de curso legal. En la actualidad prácticamente las únicas restricciones admitidas a la libre circulación de capitales son las procedentes de la normativa sobre blanqueo de capitales, que en cierta medida ha venido a sustituir como paradigma de control estatal a las antiguas legislaciones de control de cambios. A diferencia de lo que ocurría antaño, donde el principal peligro para la estabilidad monetaria eran las monedas de otros Estados, hoy el principal peligro para la economía y el sistema monetario es que las grandes masas procedentes de actividades delictivas ingresen en la economía legal. Igualmente, las restricciones que el blanqueo de capitales impone sirven también para el control del fraude fiscal. Se trata de un sistema de control menos incisivo que el sistema de autorizaciones característico del control de cambios y, por tanto, más acorde con el principio de proporcionalidad y la libre circulación de capitales. La Directiva 2018/843 del Parlamento europeo y del Consejo somete a las monedas virtuales y las criptomonedas al mismo régimen que al dinero estatal. Al igual que las casas de cambio son sujetos obligados por esta normativa, también lo son las entidades que realizan actividades claves en el comercio de criptomonedas, como los proveedores de servicios de cambio entre las monedas virtuales y la fiduciarias o decurso legal y los proveedores de servicios de monedero.

La segunda pregunta es si, más allá de este punto, no es necesaria una intervención del Banco Central Europeo sobre monedas virtuales y criptomonedas con el fin de alcanzar el gran objetivo de la política monetaria que es el control de la inflación y la política de estabilidad en los precios. Entiéndase que el objetivo no es intervenir para garantizar la estabilidad de las criptomonedas. Como veremos después, su volatilidad es uno de sus hándicaps principales, por lo que el objetivo es intervenir con el fin de que su creación no afecte negativamente a la estabilidad de las monedas estatales, en nuestro caso el euro.

El patrón oro aseguraba eficazmente el valor y la estabilidad de la moneda, pues esta tenía como referencia un bien naturalmente escaso. Tras su abandono, la política monetaria tiene como objetivo garantizar su escasez, y por tanto mantener su valor,

[18] Sin perjuicio de las posibles consecuencias para el control de la inflación y la estabilidad financiera si el volumen de criptomonedas emitidas aumentara, vid. BANCO CENTRAL EUROPEO, 2015, p. 26 y ss.

de manera diversa. En un primer momento, se trataba fundamentalmente de controlar las nuevas emisiones de moneda física. En la actualidad este aspecto de la política monetaria resulta residual. La moneda física se crea simplemente cuando se detecta que existe una demanda de esta[19]. En la actualidad, además de la fijación de coeficientes de solvencia a los bancos, la forma de controlar la cantidad de dinero de los bancos centrales es la política de tipos de interés. La cantidad de dinero que existe actualmente depende de los bancos privados y sus políticas de préstamos. Alrededor del 90% del dinero existente se genera de este modo. El Banco Central Europeo hace como banco de bancos prestando el dinero que los bancos necesitan, por esta razón tienen capacidad para controlar de manera indirecta la emisión de dinero que estos hacen. Si baja el tipo de interés al que vende el dinero a los bancos, estos a su vez pueden bajar los tipos que aplican a los clientes, conceder más préstamos y generar más dinero.[20]

Las criptomonedas en cuanto son adquiridas con dinero estatal y pueden ser convertidas libremente en moneda estatal podrían llevar a un aumento de la inflación semejante a la creación incontrolada de dinero a través de los bancos, si se generan sin control y se utilizan como forma de financiación. Aunque este peligro suele considerarse hoy lejano, debido a la relativamente pequeña cantidad de criptomonedas que existen en la actualidad,[21] resulta conveniente reflexionar acerca de la necesidad de establecer un control sobre su emisión e igualmente sobre la posibilidad de realizar operaciones financieras, con criptomonedas. Esto último supondría la aparición de una actividad bancaria paralela a la existente con las monedas oficiales. Los sujetos que debieran estar sometidos al control en el momento de la emisión serían los *Initial Coin Offeror,* que lógicamente tendrían que identificarse. En la actualidad esto no siempre resulta posible, pues no siempre el emisor es una persona física o jurídica

[19] Decisión del Banco Central Europeo de 6 de diciembre de 2001 sobre la emisión de billetes de banco denominados en euros. Diario Oficial de la Unión Europea L 337/52, 20 de diciembre de 2001.

[20] Desde luego, un tercer mecanismo que aquí no interesa y va a dejarse de lado es la política presupuestaria y el control de la deuda pública. El Estado crea también dinero mediante los presupuestos y la emisión de deuda pública.

[21] El volumen de transacciones realizadas con criptomonedas es todavía insignificante y la doctrina considera que, al menos por el momento, no existe riesgo de que el mercado de las criptomonedas afecte a la política monetaria. Además, se considera que algunas de sus características -como la elevada volatilidad impide que las criptomonedas desempeñen adecuadamente la función del dinero y pudieran llegar a sustituirlo. En el caso de que el volumen de transacciones aumentara muy significativamente sería posible que llegara a comprometer la eficacia de las algunas medidas de política monetaria; aparecería también un riesgo fiscal derivado de la reducción los ingresos por señoreaje y, sobre todo sería relevante en la medida en que la especulación pusiera en riesgo la estabilidad de la economía fiat. Vid. NISTICÒ, 2019, p. 3, IBOLD, 2019, p. 106 y CLAEYS/DEMERTZIS/ EFSTATHIOU, 2018, pp. 7 y ss. Así lo reconoce el propio BANCO CENTRAL EUROPEO, 2015, p. 25. Ahora bien, la aparición de las llamadas «criptomonedas estables mundiales», puede suponer un cambio de paradigma en este sentido pues "al incorporar características para estabilizar su valor y aprovechar los efectos de red derivados de las empresas que promueven estos activos, aspiran a una mayor difusión", Exposición de Motivos de la. Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM(2020) 593 final, 2020/0265 (COD), p. 2.

identificable, pero lo cierto es que la propuesta de regulación europea del mercado de criptoactivos también parece avanzar en la línea que proponemos, en tanto que solo autoriza a los emisores a ofertar públicamente estos criptoactivos o a solicitar su admisión a negociación en una plataforma de negociación de criptoactivos si están constituidos como persona jurídica[22]. En realidad, no resulta coherente que mientras que la actividad de los intercambiadores de criptomonedas y los proveedores de servicios de monedero estén sometidos a control a través de la legislación sobre blanqueo de capitales, no lo esté en modo alguno la de aquellas entidades que crean las criptomonedas.

Con el fin de establecer un hipotético sistema de control podría tomarse como modelo el § 35 de la Ley de Bancos (BankG) alemana que castiga con multa o pena privativa libertad de hasta cinco años la emisión no autorizada de dinero o de bonos al portador sin interés, aunque su valor no se fije en euros[23]. Este precepto cuya importancia práctica es hoy nula, tenía sentido cuando al lado del dinero emitido por los bancos centrales, existían bancos privados con autorización para la emisión de moneda. El §35 se refiere en exclusiva a dinero y además a dinero físico, por lo que no resultaría de aplicación a la creación no autorizada de criptomonedas, aunque éstas operen como medios de pago y estén próximas a cumplir las funciones que la moneda de curso legal tiene. No obstante, tanto el bien jurídico como la estructura del delito sería semejantes. Carece de sentido esperar una emisión de criptomonedas de tal magnitud como para poner en peligro el sistema monetario, razón por la cual resulta necesario un delito de peligro abstracto, donde baste con la emisión no autorizada.

En suma, tras cuanto acaba de indicarse, desde el punto de vista de la soberanía monetaria, las criptomonedas no plantean, de un lado, mayores problemas que las monedas procedentes de otros Estados. Por eso la regulación debe inspirarse en la libre circulación de capitales, cuyas únicas restricciones son hoy las procedentes de la normativa sobre blanqueo de capitales. Por otro lado, y desde el punto de vista del gran objetivo de la política monetaria, que es la lucha contra la inflación o garantizar la estabilidad en los precios las criptomonedas, no suponen hoy un peligro serio.

II. *La "casa de papel" o la creación indebida de criptomonedas*

Muy distinta a la puesta en circulación no autorizada por los bancos centrales de criptomonedas, es su creación indebida. En efecto, dada la naturaleza no corpórea de las criptomonedas no es posible la creación de moneda (billetes) falsos, que es la

[22] Vid. arts. 4 y 15, donde se regulan los requisitos para las autorizaciones y también art. 3 donde se contiene la definición de "emisor de criptoactivos" de la Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM(2020) 593 final, 2020/0265 (COD).

[23] Preceptos similares existen en otros ordenamientos, vid. al respecto IBOLD, 2019, p. 102; vid. también, BANCO CENTRAL EUROPEO, 1999, pp. 85 y ss.

conducta más frecuente en los delitos de falsedad de moneda, pero sí que es posible esta otra conducta, mucho menos frecuente en la moneda fiduciaria, como es la creación indebida de la misma. Se trataría de una conducta similar a la prevista en el art. 3.2 de la Directiva 2014/62 relativa a la protección del euro y otras monedas contra la falsificación, que sanciona la producción de moneda falsa haciendo uso de las instalaciones legales, de las fábricas de moneda o centros autorizados para su producción, pero infringiendo los derechos o condiciones con arreglo a los cuales las autoridades competentes pueden emitir billetes o monedas.

La necesidad de una incriminación de estas características depende de en qué medida técnicamente resulta posible crear nuevas criptomonedas en contra de la política que a este respecto se hayan establecido en los *Initial Coin Offering*. Esta conducta puede darse en el caso de criptomonedas "pre-minadas"[24], aquellas en las que los *coin offers* las acuñan antes de su lanzamiento[25]. En estos casos los oferentes suelen, al igual que ocurre con el dinero, tener la posibilidad de acuñar más monedas, si por ejemplo lo requiere la demanda, pero siempre dentro del marco autorregulatorio de cada criptomoneda. En este escenario cabría por ejemplo que un hacker entrara en el sistema y creara moneda no autorizada por el emisor o incluso que el propio emisor, contraviniendo su propia política monetaria las creara indebidamente.

Dado que las criptomonedas no son monedas de curso legal y que no pueden ser asimiladas a estas, por impedirlo a la prohibición de analogía, no resultan de aplicación los delitos de falsedad de moneda, donde esta conducta se tipificó ya por el art. 2 de la Convención de Ginebra de 1929 y como hemos visto recoge la Directiva 2014/62. La imposibilidad de aplicar estos preceptos penales no implica, sin embargo, una laguna. Más allá de la utilización de los delitos informáticos, que habrían de utilizarse necesariamente como medio, la actuación del derecho penal podría articularse a través de los delitos de falsedad documental. Los delitos de falsedad de moneda pertenecen a la familia más amplia de las falsedades documentales[26], en cuanto que la moneda no es sino un tipo de documento. Por esta razón, rechazada la aplicación del precepto más específico – la falsedad de moneda – podríamos acudir al más genérico de la falsedad documental.

La posibilidad de considerar que la criptomoneda es un documento requiere sin embargo una mayor reflexión. En principio, la criptomoneda puede considerarse un

[24] Es el caso de criptomonedas como Ripple XRP, Nxt-Nextcoin y BitShares.

[25] Las criptomonedas minadas son activos que no dependen de una autoridad centralizada y que se generan cada vez que un participante de la cadena de bloques (un minero) logra validar un bloque. Las monedas pre-minadas, por el contrario, se caracterizan porque no se generan a través de la minería, sino que son liberadas al momento de crear el bloque génesis de la blockchain y repartidas, en un porcentaje o en su totalidad, entre un grupo de personas determinado por sus desarrolladores, mediante un proceso estipulado dentro del protocolo de la moneda. Obsérvese que las criptomonedas pre-minadas sí que tienen un *coin offeror* identificable, que regula y se responsabiliza de su emisión. Vid. Definición de "faucet" en UNITED STATES SENTENCING COMMISSION, 2018, p. 1.

[26] Vid, PUPPE,2005, § 146.

documento en el sentido que contiene una declaración de voluntad que le otorga un determinado valor. Una criptomoneda creada indebidamente supone una declaración de voluntad mendaz. La mayoría de los ordenamientos han dejado atrás la necesidad de que los documentos tengan entidad física y admiten los documentos electrónicos. Lo importante para encontrarnos con un documento a efectos penales es que el soporte – físico o electrónico – sea capaz de albergar de manera duradera una declaración de voluntad, e identificar a la persona que realiza esta declaración. En aquellas criptomonedas donde como hemos visto existe un *Initial Coin Offering*, es decir, una persona u organización identificable que emite la criptomoneda ésta puede identificarse como autora de la declaración y por tanto no habría problema alguno para admitir que nos encontramos ante un documento. No parece compartir esta opinión, sin embargo, el Tribunal Supremo español que en varias sentencias ha sostenido que uno de los elementos del concepto de documento es que contenga una declaración comprensible de acuerdo a los usos sociales, afirmando que un escrito en clave o encriptado no es un documento pues se pretende con su confección todo lo contrario, que su contenido no sea comprensible para quien no esté en posesión de la correspondiente clave[27].

Más complejo es apreciar esta característica cuando la criptomoneda se emite de manera automatizada, sin que ninguna persona física tenga dominio sobre este proceso, como ocurre por ejemplo con el Bitcoin. Aunque nada impide que un documento – una declaración de voluntad - pueda ser emitido por un "no humano", lo importante es que una persona física tenga dominio efectivo sobre la declaración de voluntad. Lo anterior se ve claro con un ejemplo: el tacógrafo que llevan incorporados los camiones contiene sin duda una declaración de voluntad, que narra los tiempos de descanso y de actividad de voluntad. Ahora bien, esta declaración de voluntad es realizada de manera automática sin intervención de la voluntad humana.

Algunos ordenamientos, como singularmente el alemán (§ 268) o el portugués (§ 258), cuentan con un delito específico, denominado anotación técnica falsa, para sancionar precisamente estos casos en donde la declaración de voluntad corresponde de manera automática a una máquina y, precisamente, la intervención humana se produce para alterar esta declaración de voluntad. Un tipo penal de estas características, a mi juicio, capta correctamente la conducta típica consistente en alterar de manera indebida el proceso de creación automatizada de criptomonedas.

III. **Fraudes y publicidad engañosa en la emisión y oferta de criptomonedas**

Aunque el término fraude es un concepto lleno de ambigüedad, en lo que sigue la utilizaremos como una manifestación no veraz susceptible de ocasionar un perjuicio

[27] Esta declaración se realiza *obiter dicta*, resolviendo un posible error en la valoración de la prueba al haber considerado como documento a efectos probatorios elementos que podrían no reunir todas sus características, pero que en absoluto relacionados con las criptomonedas. STS 28 mayo 2001 (ECLI:ES:TS:2001:4426), FD 8º. Vid. también STS 13 septiembre 2002 (ECLI:ES:TS:2002:5850), FD 1º.

patrimonial a una tercera persona. A continuación, presentaremos diversos tipos de fraude que pueden darse a lo largo de la vida de la criptomoneda.

Siguiendo este orden cronológico, el primer bloque de comportamientos que debe analizarse son las conductas fraudulentas que se producen con relación a la creación y oferta de criptomonedas[28]. La creación de una nueva criptomoneda tiene un coste considerable, por esta razón no es posible ponerla en el mercado sin socios. Incluso gigantes como Facebook, que tiene previsto el lanzamiento de una nueva moneda, necesita de inversores como Visa, Paypal etc. En otros casos, los inversores se buscan en el mercado, y es precisamente en este terreno donde algunos estudios han puesto de manifiesto que alrededor del 80% de las ofertas iniciales son estafas[29]. Los supuestos lanzadores de moneda comienzan prometiendo rendimientos altos, que sólo abonan en un primer momento para después desaparecer[30]. En ocasiones, el riesgo no deriva de haber proporcionado información engañosa respecto de la oferta sino de la falta absoluta de ésta. Autoridades como la AEVM o la SEC[31] han alertado sobre el riesgo que supone la asimetría informativa en estos procesos[32] e incluso China las prohibió en 2017, declarándolas recaudación ilegal de fondos, imponiendo el reembolso de las cantidades ya pagadas a los inversores y prohibiendo a los *exchangers* el cambio de las criptomonedas procedentes de ICOs en marcha [33].

La segunda tipología de conductas, la más frecuente en la práctica, es la oferta falsa de criptomonedas. Determinadas personas se ofrecen como intermediarios, para comprar criptomonedas, con los fondos que los clientes les transmiten, sin que realmente tengan intención de realizar esta operación. De un supuesto similar se ha ocupado el Tribunal Supremo español[34]. El acusado fundó una empresa cuyo objetivo

[28] La Autoridad Europea de Valores y Mercados ha alertado de forma reiterada sobre los riesgos de invertir en ofertas iniciales de criptomonedas o tokens. Vid. AUTORIDAD EUROPEA DE VALORES Y MERCADOS, 2017, pp. 1 y 2; y del mismo autor, 2018, pp. 1 y 2. También lo han hecho numerosas autoridades nacionales, como la estadunidense SEC, vid. SECURITIES EXCHANGE COMMISSION, 2017, passim, que fue compartido por la Comisión Nacional de los Mercados y de la Competencia en nuestro país, reconociendo que, aunque los entornos normativos y de mercado español y estadounidense presenten diferencias significativas, se estima que las consideraciones, conclusiones y recomendaciones contenidas en el comunicado pueden ser una guía útil para inversores y profesionales del sector.

[29] Así lo señala el estudio elaborado por Satis Group LLC, referenciado en DÜRR/ GRIEBEL/ WELSCH/ THIESSE, 2020, p. 1. El estudio llevado a cabo por Liebau y Schueffel, sin embargo, arroja datos menos contundentes. Vid. LIEBAU/SCHUEFFEL, 2019, pp. 1-7.

[30] Vid. por ejemplo, el caso de fraude en relación con las criptomonedas Pincoin: y Plexcoin, entre otras. CONLON/ MCGEE, 2021, pp. 3 y 4.

[31] Ibidem.

[32] En este sentido resulta muy ilustrativo el estudio realizado por Zetzsche, Buckley, Arner y Föhr, que en casi el 25% de los casos analizados en el estudio, los *whitepapers* no ofrecían ninguna descripción de las circunstancias financieras del proyecto, es decir, no se incluía ninguna información sobre cómo se utilizaría el capital recaudado, en qué etapas, etc. Solo el 34.84% de de los casos, incluían información sobre la normativa aplicable. En el 57.68% de los casos, los se proporciona el nombre del lanzador. En el 42,35% de los casos, el nombre dado como autor del whitepaper es diferente del del lanzador de la ICO. Por ello, concluye, que la decisión de invertir en estas ofertas no es racional, dada la limitada información que se facilita en ellas. ZETZSCHE/BUCKLEY/ARNER/FÖHR, 2019, pp. 287-293.

[33] EUROPA PRESS, 2017, passim.

[34] STS 20 junio 2019 (ECLI: ES:TS:2019:2109).

era gestionar los bitcoins que le eran entregados en depósito por varios clientes, con el fin de reinvertir las ganancias y entregar finalmente los dividendos obtenidos. Su intención desde el primer momento era apoderarse de los bitcoins sin cumplir con sus obligaciones[35].

Una tercera tipología de fraude se asemejaría a un delito publicitario, cuyos protagonistas serían los denominados *coin offeros*. La conducta consistiría en hacer manifestaciones falsas o incorrectas sobre las propiedades esenciales de una criptomoneda o el rendimiento económico que puede obtenerse mediante la inversión. Con frecuencia, la "publicidad" no va referida tanto a las características de la moneda o de la inversión, sino a buscar que los consumidores la adquieran por el tipo de plataforma en la que aparece[36] o por las personas que dicen haberlas adquirido. En Twitter, Facebook o foros de internet, que son los lugares donde más publicidad se realiza, se han hackeado en ocasiones cuantas de personas famosas con el fin de utilizar indebidamente su nombre como medio publicitario.[37] En ocasiones han sido los propios "mineros" quienes han realizado este tipo de "publicidad" falsa. La proliferación de estas conductas llevó a Facebook, Twitter o Google a prohibir la publicidad de criptomonedas, para después volver a admitirla sometiéndola a algún tipo de control previo.

Un tipo especial de publicidad falsa es la que se inserta dentro de una estafa piramidal, de acuerdo con el "esquema Ponzi". Se trata de prometer a los adquirientes grandes beneficios (por ejemplo, del 200%) a corto plazo y bajo riesgo, satisfaciendo estos ingresos con los primeros inversores para así atraer otros nuevos[38]. En 2013 la SEC ya advirtió del riesgo de las ICOs que encubren esquemas Ponzi[39]. En España una estafa que responde a esta tipología está siendo actualmente investigada por la

[35] Un caso muy conocido con una mayor entidad es el caso BitKRX, en donde el engaño consistió en que la oferente de criptomonedas se hizo pasar por una filial de una conocida y reputada entidad financiera sur coreana: Vid. YOUNG, 2017, passim.

[36] Así, por ejemplo, se ha clonado la web de algún banco respetable, para desde allí hacer ofertas de criptomonedas

[37] En enero de 2018, una cuenta de Twitter falsa aparentaba pertenecer al gurú de la ciberseguridad y entusiasta de la criptografía John McAfee. Esta cuenta publicó un tweet apoyando a la criptomoneda GVT, nombrándola "moneda del día". Para algunos miembros de la comunidad criptográfica, esto fue razón suficiente para comprar GVT y solo cuatro minutos después de que se publicara el tweet, el precio de GVT había subido de 30 a 45 dólares y el volumen de operaciones se había duplicado. Quince minutos más tarde, el precio rondaba los 30 dólares de nuevo, después de que los primeros compradores "saliesen corriendo". En una investigación, se reveló que la cuenta de Twitter era falsa y no estaba asociada con McAfee en absoluto, vid: CHEO, 2018, passim.

[38] Un caso que responde a esta tipología, en el Reino Unido, es el de Bitconnect. Esta plataforma permitía a sus usuarios prestar dinero en forma de bitcoin durante un determinado periodo de tiempo. El atractivo eran los beneficios que prometía. Cuando un usuario finalizaba un contrato de préstamo obtenía unas ganancias del 40% sobre los fondos que había prestado, además de una bonificación del 0,2% diario. La estafa pudo llevarse a cabo de manera continuada en cuanto que respondía al tipo de estafa piramidal. Vid: PALMER, 2020, passim. También parece haber un esquema piramidal detrás de la criptomoneda PRO Currency, habiendo anunciado la SEC hace algunos meses, acciones contra sus lanzadores. Vid. SECURITIES EXCHANGE COMMISSION, 2019, passim.

[39] Vid. SECURITIES EXCHANGE COMMISSION, 2013, pp. 1-2.

Audiencia Nacional. De acuerdo con las investigaciones realizadas hasta la fecha, cerca de 22.000 inversores, de 78 países, invirtieron sus ahorros en la criptomoneda Unete, que prometía una rentabilidad anual del 275 %. La cuantía del fraude, que se llevó a cabo entre 2013 y 2015 se estima en 228 millones de euros[40].

La mayor parte de ellos pueden ser sancionados, sin demasiados problemas, a través de tipos penales como la estafa o, en su caso, el delito publicitario. No existe, por tanto, necesidad político criminal alguna de proponer nuevos tipos penales o modificaciones en los ya existentes. Si acaso y dado el mercado global y sin fronteras en el que se mueven las criptomonedas lo relevante será la mejora de las técnicas de cooperación judicial.

IV. **Criptomonedas y Derecho penal del mercado de valores**

El Derecho de la UE no considera las monedas virtuales y criptomonedas instrumentos financieros[41], por lo que no son objeto de la regulación del mercado de valores, ni tampoco objeto de la supervisión de sus autoridades. Pese a ello, en el mercado de criptomonedas se producen con frecuencia comportamientos que son similares a la manipulación de mercado[42]. Estas manipulaciones provocan alteraciones de valor, que incrementan aún más la volatilidad de este tipo de activos.

Las técnicas de manipulación que se utilizan no son nada sofisticadas. Así, por ejemplo, se ha acudido a utilizar compradores ficticios con el fin de simular un gran volumen de compras y de este modo incrementar el precio al aumentar de manera ficticia la demanda (*washing trade*)[43]. Esta conducta equivale al tipo de manipulación operativa que se recoge en el art. 5 2 b) de la Directiva sobre abuso de mercado donde se sanciona la realización de operaciones ficticias o simuladas con el fin de alterar el valor de un instrumento financiero. Un caso algo más sofisticado es la creación de monedas de apoyo al bitcoin. Con el fin de contrarrestar las fuertes bajadas de valor que experimentó esta moneda en 2013 y 2017 se crearon monedas de apoyo con el único fin de invertir en bitcoins y mantener su valor. El resultado fue tan espectacular que en la "crisis" del 2017 se consiguió un aumento de valor de 1.000 a 20.000 dólares[44].

[40] GIL, 2018, passim.

[41] Art. 4, apartado 1, punto 15, de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE Texto pertinente a efectos del EEE. Diario Oficial de la Unión Europea L 173/349, 12 de junio de 2014.

[42] Refiriéndose al Bitcoin como ecosistema, pero trasladable a la gran mayoría de monedas virtuales, vid. GANDAL/HAMRICK/MOORE/OBERMANM, 2018, p. 86.

[43] Un estudio de Bitwise señala que cerca del 95% del volumen de es falso. Vid. HOUGAN/LIN/LERNER, 2019, pp. 35 y ss. El estudio de CONG et Al. Lo señala como un problema de primer orden en los exchanges no regulados. Vid. CONG/LI/TANG/YANG, 2019, pp. 38 y ss.

[44] Un estudio de la influencia de la criptomoneda Tether en el mercado del bitcoin en el año 2017 puede verse en GRIFFIN/SHAMS, 2020, pp. 1939 y ss.

Al igual que en el delito de manipulación de mercados cualquier persona puede llevar a cabo este tipo de conductas, sin embargo, existe un fuerte incentivo para que sus autores sean los intercambiadores de moneda o incluso los propios mineros con el fin de incrementar artificialmente el valor de las monedas que poseen.

Siguiendo con los paralelismos entre el mercado de criptomonedas y los mercados de valores una conducta común a los mismos es la consistente en una administración desleal por parte de los intercambiadores. Una regla básica de comportamiento de la legislación del mercado de valores relativa a las agencias (*brokers*) es aquella que les obliga a no anteponer sus intereses a los de los clientes, ni a otorgar preferencia a las órdenes de un cliente sobre las de otro.[45] Este comportamiento constituye en muchos ordenamientos un delito de administración desleal. El anonimato de las operaciones con criptomonedas hace que esta conducta desleal de los intercambiadores sea difícil de descubrir. A diferencia de las agencias de valores sobre los intercambiadores no pesa ninguna obligación de llevar un registro público. Los datos de sus transacciones figuran únicamente en sus bases de datos[46]. A esta tipología de conducta pertenecen también los casos de *front running*. Básicamente este supuesto consiste en que el *broker*, que tiene conocimiento que un cliente va a realizar la compra de un determinado valor, se adelanta comprando este activo financiero para después vendérselo a un precio superior a su cliente[47].

Algunos ordenamientos como el alemán han sometido a supervisión algunas actividades realizadas con monedas virtuales y criptomonedas cuando se trata de actividades prototípicas del sector bancario, como la concesión de préstamos en criptomonedas y monedas virtuales o la realización de contratos de depósitos. La finalidad de esta supervisión, consistente en la necesidad de obtener una autorización, es la protección de los clientes y del propio sistema financiero[48]. No existe algo análogo en el caso del mercado de valores y ello que, en este punto, habría intereses relevantes que tutelar. La creación y el lanzamiento de una moneda virtual o criptomoneda no se somete a requisitos previos ni por el Derecho de la UE, ni por los ordenamientos estatales[49].

El problema no es en cualquier caso sólo la falta de preceptos penales específicos. En algunos Estados, como singularmente España, podrían ser de aplicación tipos penales genéricos como la administración desleal o el *aggiotagio*, aunque no lo sea el

[45] Vid. arts. 221 y ss de la Ley Mercado de Valores.

[46] La falta de transparencia se ha subsanado de algún modo a través de la Directiva antiblanqueo, que busca establecer unos estándares de transparencia en este tipo de mercado, lo cual obliga a los *crypto exchanges* y *crypto wallets* a realizar un registro de todos sus clientes, así como reportar anualmente sus movimientos.

[47] La plataforma Bancor reconoció haber tenido problemas de front-running. Vid. CHAPARRO,2019, passim.

Para un estudio de este tipo de prácticas en los exchanges descentralizados, vid DAIAN/ GOLDFEDER/ KELL/ LI/ ZHAO/ BENTOV/ BREIDENBACH/ JUELS, 2019, pp. 3 y ss.

[48] Vid., al respecto, IBOLD, 2019, p. 106.

[49] Como ya se ha puesto de manifiesto, la propuesta de regulación europea sí que establece controles.

abuso de mercado. La cuestión principal reside en la falta de eficacia de la supervisión y de control. En muchos Estados esta actividad quedará en manos de las autoridades de consumo, que tienen unos medios legales y materiales mucho más reducidos que las autoridades bancarias y de bolsa. Es prácticamente imposible, al menos en España, donde además no tienen rango estatal sino regional,que puedan hacer frente a las dificultades de supervisión y control de un mercado globalizado como es el de las criptomonedas.

V. **Las criptomonedas como medio de pago**

1. ***La asimilación***

Junto con la regulación relativa al blanqueo de capitales, la Directiva 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo, que debería haber sido transpuesta a más tardar el 31 de mayo de este año, constituye el segundo ámbito donde encontramos una mención expresa de las monedas virtuales, con una clara intención de asimilar su tutela penal[50]. La Directiva asimila las monedas virtuales, en cuanto sean medio de pago, a la moneda de curso legal en el delito de fraude (art. 6) e igualmente asimila a los monederos al resto de instrumentos de pago, de manera similar a las tarjetas de crédito o a otros medios más modernos como las aplicaciones de móvil. De este modo, les resulta de aplicación la figura de utilización fraudulenta (art. 3) y las infracciones relacionadas con esta utilización (art. 4 y 5). Pese a que la asimilación como punto de partida político-criminal resulta acercada, al menos en el caso de las criptomonedas, como subespecie dentro de las monedas virtuales, hay algunos aspectos que deben ser discutidos. La sanción penal a los fraudes realizados mediante criptomonedas plantea algunas particularidades con relación al resto de los medios de pago distintos al efectivo.

2. ***La distinción entre delitos de lesión y ámbito previo***

La característica principal de la Directiva desde el punto estrictamente penal es el adelanto de la barrera de intervención. La Directiva se compone de dos delitos de resultado: los delitos de utilización fraudulenta (art. 3) y fraude (art. 6), que requieren un perjuicio patrimonial como consecuencia de realizarse con ellos un pago no consentido en beneficio de otra persona. Estos dos tipos penales de resultado vienen precedidos del castigo de otros comportamientos delictivos donde se sancionan comportamientos previos, alejados de la causación del daño patrimonial. Estos comportamientos previos los podemos dividir en cuatro bloques distintos: (a) el apoderamiento u obtención ilícita de un medio de pago ajeno, (b) la falsificación, (c) la posesión de medios falsificados u obtenidos ilícitamente con el fin de utilizarlos y

(d) el comercio con estos medios (art. 4 y 6). Además de este conjunto de infracciones, se sanciona también la creación y el comercio con herramientas necesarias a la comisión de estos delitos.

Esta clara distinción entre comportamientos que ocasionan un resultado y delitos que sancionan comportamientos preparatorios, aunque es clara en relación con los medios de pago tradicionales, no es correcta en el caso de las criptomonedas. La mera tenencia de una tarjeta de crédito, previamente robada o falsificada, y de sus claves hace distante la aparición del perjuicio patrimonial. Su propietario, debido a la configuración de este medio de pago por las entidades emisoras, tiene grandes posibilidades de autodefensa: puede anular la tarjeta con una sola llamada telefónica. Además, de haber sido utilizada tiene muchas posibilidades de anular el pago. No ocurre lo mismo con los monederos electrónicos, donde la tenencia del monedero con sus respectivas claves, otorgan una disponibilidad similar a si alguien posee una billetera con dinero físico. Un monedero de monedas virtuales no sólo otorga la capacidad de disponer sobre activos patrimoniales, que se encuentran ubicados o custodiados en otro lugar y por una tercera persona (una entidad bancaria), sino que incorpora el valor de los activos patrimoniales, de manera semejante a una billetera tradicional[51]. Estas consideraciones afectan, al resto de comportamientos que se sitúan por la directiva en el ámbito previo. El robo, el hurto o la apropiación indebida de un monedero virtual -cuando éste se incorpora a un dispositivo físico– es similar al robo, hurto o apropiación indebida, etc. de un monedero tradicional. Por esta razón, en relación con la mayoría de las criptomonedas, y a los monederos como medios de pago, la diferencia entre ámbito previo y delitos de resultado no me parece tan relevante. El acto de disposición que realiza posteriormente la persona que ha sustraído el monedero u obtenido sus claves a través de un delito informático constituye un caso de agotamiento del delito, similar a quien después de hurtar un monedero convencional se compra con los billetes que en él se contienen unas botellas de vino. Esta circunstancia debería ser tenida bien en cuenta por los Estados miembros a la hora de transponer la Directiva.

3. *Medios de pago materiales e inmateriales: la relevancia de la criminalidad informática*

Una segunda característica de la Directiva es que está bien atenta al proceso de desmaterialización de los instrumentos de pago. Si estos en un primer momento se asociaban a un determinado soporte físico (tarjetas, cheques de viaje…), en la actualidad los pagos se han virtualizado, bastando una serie de indicadores. Por esta razón distingue entre elementos de pago materiales (art. 4) e inmateriales (art. 5). Los

[51] Ha llamado también la atención sobre estos riesgos GONZÁLEZ-MENESES, no sólo respecto al uso ilegítimo de estas claves sino respecto a la capacidad de obrar de quien realiza la transacción y la realidad del consentimiento. Vid. GONZÁLEZ-MENESES, 2015, p. 106.

monederos pueden ser medios de pago materiales o inmateriales. La principal virtualidad de esta distinción es que en relación con los primeros las conductas delictivas son las prototípicas de los delitos contra la propiedad: robo, hurto, apropiación indebida (art. 4 a); mientras que, en el caso de los medios de pago inmateriales, las conductas típicas constituyen casos de criminalidad informática (art. 5 a).

En el caso de las criptomonedas, éstas pueden estar contenidas tanto en monederos materiales, como inmateriales. Ejemplo de los primeros serían monederos de papel, donde las claves se encuentran escritas en un papel o encriptadas en un código QR, cuyos códigos se introducen cuando se desea realizar la transacción. Igualmente encontramos los denominados monederos fríos, muy similares físicamente a un pen drive, que están desvinculados de la red. En relación con estos monederos son perfectamente posibles las conductas de robo, hurto o falsificación que se describen en el art. 5 a). No obstante, en el caso de los monederos fríos una vez conectados a la red es posible obtener ilícitamente su información a través de conductas de hacking.

Los monederos más utilizados son, sin embargo, los denominados calientes, que se caracterizan por estar conectados a internet de manera constante. Entre las billeteras calientes encontramos la billetera de escritorio o de móvil, la cual es una aplicación que se descarga en un ordenador o dispositivo especifico. Incluso hay billeteras en línea que están ubicadas en una web. A este tipo de medios de pago se accede normalmente a través de conductas constitutivas ya de por sí delitos informáticos, tal como se indica en el art. 5 a) de la Directiva que menciona expresamente como formas de comisión las infracciones previstas en los art. 3 a 6 de la Directiva 2013/40 sobre delitos informáticos[52].

La forma más utilizada para acceder a las claves es el *phising*. El tipo más común de *phising* es la clonación de sitios web legítimos que puede ser desde una casa de cambio, hasta una cartera en línea, y lo propagan por distintos medios, incluyendo correo electrónico, chats y hasta anuncios de Google que pueden ser confundidos con la página original en los resultados de búsqueda. En ocasiones, los estafadores se ahorran la molestia de crear el sitio falso y simplemente se hacen pasar por el equipo de soporte de alguna plataforma legítima, incluyendo casas de cambio y carteras. De esta forma, lo único que imitan son los logos y la dirección de correo de la empresa dentro del mensaje que envían a sus víctimas para anunciarles de algún presunto inconveniente y solicitarles su información privada con el falso propósito de ayudarlos[53]. Otro de los ataques más conocidos a los monederos es el que se realiza

[52] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, Diario Oficial de la Unión Europea L 218/8, 18 de agosto de 2013.

[53] En octubre de 2017, un ataque *phishing* logró robar más de 15 mil dólares en monedas Ethereum, antes de ser descubierto. El ataque llegó mediante un correo electrónico que, aparentemente pertenecía a MyEtherWallet (MEW), y requería actualizar la información sobre el balance de las carteras con motivo de la próxima actualización. A través de un link contenido en el correo, los usuarios eran dirigidos a un sitio web que copiaba exactamente la interfaz de la página oficial de MEW, la única diferencia era una especie de coma debajo de la

mediante un *malware*. Existen diferentes tipos de *malware* a la hora de atacar los *wallets*, pero uno de los más destacados es el malware denominado *CryptoCurrency Clipboard Hijackers* (secuestradores de portapapeles)[54], el cual busca en el portapapeles de Windows las direcciones de criptomonedas y si detecta una, la intercambia, siendo su función principal la de cambiar las direcciones utilizadas para transferir criptomonedas por la de los hackers[55].

Un aspecto que debe ser discutido es la relación entre los delitos informáticos y la infracción prevista en el art. 5 a) de la Directiva. Se trata de determinar si la utilización del delito informático debe castigarse de manera independiente a la obtención ilícita de las claves o datos que permiten su utilización. A mi juicio, aunque normalmente se considera que los delitos informáticos no pierden su autonomía en cuanto que protegen un bien jurídico propio, en este caso no es fácil mantener la dualidad de bienes jurídicos en el caso específico de las criptomonedas. La afectación de la seguridad del tráfico económico en el ciberespacio es un interés que se protege de manera inmanente, junto al patrimonio, en el caso de las criptomonedas. Aunque puede haber supuestos, en que pueda realizarse por separado la afectación patrimonial y el ataque informático, al menos en el caso de las criptomonedas estos son absolutamente excepcionales. La solución más correcta sería por ello apreciar un concurso de normas, de otro modo se incurriría en un supuesto de *bis in idem*.

4. *¿Cuándo existe una sustracción, apoderamiento o falsificación o posesión ilegítima de un medio de pago?*

Los medios de pago distintos al efectivo suelen estar compuestos por razones de seguridad elementos diversos, donde además del soporte físico o virtual su utilización se condiciona a la tenencia de una serie de claves. Tal como indica el preámbulo

t, en la URL (ejem: ponían www.myetherwalleț.com en vez de www.myetherwallet.com). Los ataques de phishing a estos monederos no han cesado, vid. ALEXANDRE, 2019, passim. En otros supuestos, algunas de las billeteras falsas, aprovechan la reputación de otra compañía y simulan ser la aplicación de esa compañía famosa, como sucedió con la empresa Trezor (empresa famosa dedicada a las billeteras hardware). Un ciberdelincuente utilizó el nombre de Trezor para lanzar una billetera en la Google Store llamada "Trezor Mobile Wallet", con el único propósito de defraudar a los usuarios que introdujeran en ella sus claves. Vid. STEFANKO, 2019, passim. Otro caso también a destacar es el del intercambiador criptográfico Poloniex, que en 2017 fue el objetivo de una estafa sofisticada, donde al menos tres aplicaciones vinculadas fraudulentamente a Poloniex se pusieron en la tienda Google Play. Dos de ellas se descargaron más de 5,500 veces antes de ser eliminadas de la tienda. Estas aplicaciones pidieron a los usuarios de Poloniex que introdujeran las credenciales de sus cuentas, lo que permitió a los estafadores realizar transacciones en nombre de los usuarios e incluso bloquear a las víctimas sus propias cuentas. Vid. DE, 2017, passim.

[54] SUBERG, 2018, passim.

[55] Otra de las vías frecuentes de llevar a cabo el phishing a través de malware es el uso de extensiones en navegadores web. Vid. ZMUDZINSKI, 2020, passim. También se han advertido los riesgos del uso *de brain wallets*. Estas herramientas a priori ofrecen una mayor seguridad para almacenar bitcoins pues permiten generar direcciones de Bitcoin y claves privadas y públicas a partir de una sucesión de palabras establecida por el usuario a manera de contraseña, sin embargo, algunos estudios han revelado que el nivel de seguridad de estas contraseñas no es suficiente. Vid. VASEK/ BONNEAU/ CASTELLUCCI/ KEITH/MOORE, 2017, pp. 615 y ss.

de la Directiva la posesión o el apoderamiento ilícito del medio de pago solo se produce cuando se contiene el conjunto de elementos que permiten realizar la transferencia patrimonial. En el caso de los monederos, ya se trata de monederos materiales o inmateriales, la realización de una transferencia de criptomonedas desde el mismo, por ejemplo, ordenando un pago, requiere poseer la clave pública y, por supuesto, la clave privada. La clave pública equivale a la dirección o nombre del usuario, por ella es reconocido en las transacciones, mientras que la clave privada equivale a la firma. Por esta razón, sólo la obtención de la clave privada implica el apoderamiento o la posesión ilícita del monedero.

5. *El derecho penal como ultima ratio y el delito de fraude (Art. 6)*

Aunque como hemos indicado es posible en el caso de criptomonedas la realización de la conducta prevista en el art. 3, en el caso por ejemplo de compras en comercio que admitan como medios de pagos criptomonedas, la forma más habitual de realizar un acto de disposición no consentido será la prevista en el art. 6 de la Directiva consistente en: "la realización o causación de una transferencia de dinero, de valor monetario o de moneda virtual, con el ánimo de procurar un beneficio económico ilícito para el autor o un tercero ocasionando en consecuencia un perjuicio patrimonial ilícito a otra persona, será punible como infracción penal cuando se haya cometido intencionadamente: a) sin derecho a ello, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información; b) sin derecho a ello, introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos".

Esta infracción, como es bien conocido, tiene una estructura similar al delito de estafa (engaño, error, acto de disposición patrimonial, perjuicio patrimonial), distinguiéndose por la ausencia de los dos primeros elementos. La razón reside en que sólo de manera metafórica puede hablarse de "engañar" a una máquina. La estafa, según la concepción mayoritaria, está pensada únicamente para relaciones interpersonales. A partir de aquí, la discusión principal entorno a esta figura se ha centrado en analizar sí y en qué medida las conductas que sustituyen al "engaño", previstas en las letras a) y b) del art. 6 pueden ser consideradas desde un punto de vista valorativo similares al engaño. Una interpretación restrictiva de estos elementos daría lugar a una protección del patrimonio asimétrica, más severa y, por tanto, injustificada en el caso de las estafas interpersonales que en el caso de las estafas informáticas.

Este debate, situado en los medios de pago, tiene un trasfondo práctico y político criminal importante, que por supuesto no debe eludirse en el caso de las criptomonedas. Una interpretación estricta de las formas de "engañar" de la estafa informática obliga por ejemplo a las entidades que están tras las tarjetas de crédito (Visa, Mastercard…) a incrementar sus medidas de seguridad. La confianza en este medio de pago, antes que en el derecho penal, debe venir de la generación de medidas de

seguridad o formas de revertir el pago que impidan un perjuicio patrimonial de las personas propietarias de las tarjetas. Por el contrario, una interpretación amplia supondría poner el derecho penal al servicio de un modelo de negocio, que puede reducir sus inversiones en seguridad, confiado en que el derecho penal sancionará a aquellos que abusen de un medio de pago. Dicho en pocas palabras, la legitimidad de un precepto como el de fraude depende del desarrollo de medidas de seguridad relevantes, pues sólo en este caso el desvalor de esta conducta pueda ser equiparado al delito de estafa.

Esta cuestión de política criminal, que ha tenido una gran relevancia en la interpretación de este tipo penal en diversos países de la UE, ha afectado a la modalidad más frecuente en la práctica que consiste en la introducción de datos en el sistema informático con el fin de lograr una transferencia indebida de activos. En este punto existen interpretaciones que requieren un engaño similar al delito de estafa, según el cual el sistema informático debería necesariamente comprobar en alguno de sus procesos si la persona que introduce las claves tiene realmente autorización para ellos. En esta misma línea restrictiva, otros mantienen una "personificación de la relación" de tal forma que en lugar del computador se colocara una persona física. Existiría engaño cuando el autor tiene un deber de informar expresamente acerca de su capacidad para introducir los datos. No obstante, la interpretación mayoría entiende que lo relevante es la introducción de datos de manera contraria a la voluntad de la persona que tiene capacidad para introducirlos. La similitud con el delito de estafa reside en que se crea una apariencia de que hay una transacción querida por su titular cuando en realidad no es así.

La postura que se adopte, más o menos restrictiva, debe venir marcada por las medidas de seguridad que contengan los medios de pago distintos al efectivo, y en nuestro caso los monederos. No sería acertado que el derecho penal viniera a alimentar una desidia generalizada en la introducción de medidas de protección. En el caso de las criptomonedas, los monederos están incrementando paulatinamente sus medidas de seguridad, a través de actualizaciones constantes del software de los monederos, con el objetivo de poner nuevo y continuos obstáculos a los hackers. A veces, ofrecen la posibilidad de cifrar la clave privada para que el acceso a ella sea limitado. Otras billeteras también permiten a los usuarios añadir una capa adicional de seguridad a la billetera agregando su propia contraseña. Hay billeteras que permiten establecer la posibilidad de firmas múltiples, lo cual obliga a utilizar dos dispositivos para realizar una transacción, debiendo introducir en ambos una contraseña diferente o depender la autorización de la firma del código que se te genere en uno de los dispositivos. También existen *wallets* más sofisticados que permiten realizar transacciones a través de scanner biométrico, incluso existen algunas *wallets* calientes que permiten realizar transacciones sin internet, con el objetivo de distanciarse aún más del peligro.

El nivel de garantías exigido a los monederos tiene importancia, más allá de la delimitación del delito de estafa, para establecer la posible responsabilidad civil en los casos en que un monedero sea hackeado como consecuencia de medidas de seguridad deficientes o mal implementadas[56]. Se han dado ya supuestos de empresas que prestaban este tipo de servicios que se han declarado insolventes como consecuencias de ataques informáticos, sin restituir a los clientes los valores perdidos[57].

Un supuesto especial dentro del delito de fraude (art. 6) sería aquel en el que la propia empresa que ha suministrado el monedero la que dispone ilícitamente de las criptomonedas. Aunque esta cuestión puede depender de los distintos tipos de monederos, en realidad es difícil ver en este punto que existe una suerte de contrato de depósito entre los propietarios de criptomonedas y las empresas que suministran servicios de monedero, que nos permitiera hablar de un delito de apropiación indebida o administración desleal. La empresa que suministra el monedero proporciona un servicio o producto y su vinculación con el propietario de criptomonedas no tiene ningún componente de salvaguarda patrimonial. Por ello el acceso indebido a las claves y su posterior utilización pueden ser calificadas respectivamente dentro de los art. 4 a), 5 a) y 6.

6. *La falsificación en un medio de pago distinto al efectivo (art. 4. b) y 5 b))*

La alta fiabilidad técnica de blockchain hace que hasta ahora apenas se haya planteado la posibilidad de que puedan existir conductas ilícitas por parte de los mineros que actúan como registradores de las diversas transacciones. La conducta ilícita más importante que podría realizar el "minero" es la falsificación del registro descentralizado que supone blockchain. Por ejemplo, el minero podría intervenir para hacer un doble pago con una misma criptomoneda, modificando el asiento donde se atestigua un determinado pago realizado con un bitcoin para generar otro bloque y otra cadena diversas de pago.

Desde un punto de vista técnico, es prácticamente imposible alterar este registro, al menos en cuando actúa con criptomonedas. Cada moneda virtual que se crea genera una anotación registral, a la que se van añadiendo sucesivas inscripciones por cada vez que se transfiere. Esto es lo que literalmente significa blockchain: una cadena de bloques o inscripciones. Estas anotaciones se van realizando de manera

[56] Algunos monederos se comprometen por ejemplo a devolver el dinero si son hackeados, pero esto no suele ser normal. En Italia, en el caso Bitgrail, que afecta no a un monedero sino a un intercambiador, tuvo que responder civilmente ante sus clientes tras ser hackeado. Vid. PARTZ, 2018, passim.

[57] Concretamente en julio 2017, el CEO de la billetera digital Cryptsy, Paul Vernon, declaró su empresa en bancarrota tras un supuesto hackeo. Tras dejar desamparados a una gran cantidad de clientes, éstos decidieron demandarle, siendo declarado culpable de robar más de 11 mil Bitcoin de sus clientes en 2014 y se le condenó a pagar 8,2 millones de dólares (el valor de las criptomonedas en ese momento) en daños y perjuicios. Actualmente Vernon se encuentra huído en China y no ha devuelto la suma. Vid. HIGGINS, 2016, passim. Vid. también el caso de Mark Karpeles, CEO de Mt. Gox, EFE, 2017, passim.

sucesiva por distintos mineros. La posibilidad de hacer un doble pago, es decir, utilizar una moneda dos veces exigiría deshacer la cadena modificando las anotaciones realizadas por otros mineros.

La fiabilidad de blockchain radica, además de en la utilización de algoritmos como medios de certificación, en que en su confección interviene un número considerable de personas que además no se conocen entre sí y que se sitúan en diversas partes del mundo. Para que existiera una falsificación en el registro deberían ponerse de acuerdo tal cantidad de "registradores" que resulta básicamente inconcebible una conducta de estas características o bien desarrollar medios de computación tan potentes que fueran capaces de desentrañar el complejo sistema de encriptación en que se basan las criptomonedas[58].

Ahora bien, esta imposibilidad técnica de realizar una falsificación cambia si el número de mineros se reduce. Si por ejemplo se diera el caso que una determinada criptomoneda fuera minada por un número reducido de mineros cabria un acuerdo entre los mismos que abriera las puertas a una falsificación del registro[59]. Es lo que, al parecer, pudiera haber ocurrido en el caso una criptomoneda denominada Etherum Classic en la cual se ha constatado como una misma monea se encontraba en dos monederos a la vez. Esto fue posible porque los hackers se actuaron desde dentro una vez que se habían hecho con todo el poder computacional, controlando un mismo grupo más del 51% de las transacciones realizadas con dichas monedas. Al tener el control total de la red, realizaron transacciones de un monedero a otro para después "cancelarlas" en el monedero emisor y poseer de nuevo la cantidad previamente emitida, duplicando así una misma moneda. Concretamente los ataques, lograron bifurcar la red, incorporando una rama alternativa de la cadena de bloques con una transacción conflictiva y un número mayor de bloques confirmados, manteniendo en el monedero emisor el bitcoin pero también en el monedero de destino. De este modo, se llegaron a identificar hasta 12 transacciones duplicadas por valor de 1,1 millón de dólares[60].

Casos como el de Etherum aconsejan plantearse la responsabilidad de los mineros por este tipo de falsificaciones en el registro. Tal como hemos explicado anteriormente, los delitos de falsedades documentales han aceptado desde hace ya tiempo a los documentos informáticos como un tipo más de documentos. Otra cosa es el carácter que a este documento se le deba otorgar. Básicamente todos los ordenamientos distinguen entre documentos públicos y privados. Todo depende de si la persona que genera el documento es un funcionario público, que actúa con la obligación de decir la verdad en él, o un particular. Desde este punto de vista, no hay otra salida que considerar que blockchain como registro es un documento privado, lo que reduce su

[58] Vid. GONZÁLEZ-MENESES, 2015, pp. 40 y ss.

[59] Un análisis sobre la efectividad del blockchain frente a los llamados "ataques" del 51%" puede encontrarse en SAYEED/MARCO-GISBERT, 2018, pp. 9-14.

[60] Vid. CONTRERAS, 2019, passim; BRAMDON, 2019, passim.

ámbito de protección frente a los documentos públicos, así como las penas que se imponen como consecuencia de su falsificación. En la mayor parte de ordenamientos el delito de falsedad en documento privado carece además de autonomía una vez que el documento se instrumentaliza para cometer otro delito que es el que origina el perjuicio patrimonial.

La conducta previa del minero falsificando el registro tampoco podría ganar autonomía, considerando que conlleva la realización de las figuras delictivas previstas en los art. 4 b) y 5 b) de la Directiva, que se refieren, respectivamente, a la falsedad de medios de pago m,teriales o inmateriales. Sencillamente esto es así, porque aquí la falsedad no se produce en el medio de pago – el monedero – sino en el registro. No obstante, este tipo de comportamientos puede considerarse un caso de fraude del art. 6, en cuando que existe una alteración de los datos del sistema informático, que conlleva una transferencia indebida de activos patrimoniales, con el consiguiente perjuicio patrimonial para el titular de la moneda y el beneficio injustificado del minero o un tercero.

En cualquier caso, y aunque técnicamente no está del todo claro cómo pueden producirse conductas de falsedades en blockchain, la importancia que este registro está llamado a desempeñar en el tráfico económico hace imprescindible introducir el debate acerca de cómo sancionar la falsedad en sus acentos. El desarrollo de medios de computación cuánticos aumentaría la potencia de los ordenadores y por tanto la capacidad de descifrar los algoritmos que sirven para garantizar la seguridad registral dentro de blockchain. Igualmente, los casos de cárteles entre mineros-registradores no son pura ficción como pone de relieve el caso Ethereum. La solución sería equipara el blockchain a un registro público y por tanto a un documento público.

VI. **Conclusiones**

Las criptomonedas constituyen una innegable fuente de riesgos penales. Hasta el momento, el que mayor atención ha atraído es su posible empleo en mercados ilícitos y como forma para introducir activos procedentes de actividades delictivas en la economía legal. Sin embargo, este trabajo ha puesto de manifiesto que éstas no son las únicas actividades ilícitas -o que debieran serlo- vinculadas a la emisión y funcionamiento de las criptomonedas.

Desde el punto de vista de la soberanía monetaria, las criptomonedas no plantean mayores problemas que las monedas procedentes de otros Estados y, por eso, la regulación debería inspirarse en la libre circulación de capitales, cuyas únicas restricciones son hoy las procedentes de la normativa sobre blanqueo de capitales. Desde el punto de vista de la política monetaria, por el momento las criptomonedas no suponen un peligro para el control de la inflación y la estabilidad de los precios, debido a su reducido volumen de transacciones. Sin embargo, si se llegaran a generar sin

control y se utilizan como forma de financiación, sí que podrían causar un incremento de la inflación. En este sentido, se ha propuesto someter a control a los oferentes en el momento de la emisión y sancionar la emisión no autorizada a través de un delito de peligro abstracto. Además, respecto a las criptomonedas pre-minadas, se ha planteado su posible creación indebida por parte de un tercero -e.g. un hacker- o el propio emisor de las criptomonedas contraviniendo su propia política monetaria. A este respecto, habiendo descartado los tipos de falsedad de moneda por no tratarse de moneda de curso legal, se ha planteado la posibilidad de aplicar los delitos de falsedad documental.

Los fraudes representan en la práctica uno de los principales focos de riesgo. Se ha constatado que un elevado porcentaje de las ofertas de criptomonedas contienen información falsa o incompleta, emplean esquemas ponzi o se sirven de determinadas plataformas o de perfiles hackeados de personas conocidas para lograr la inversión en estos criptoactivos. Aquí, los delitos de estafa y publicitario parecen colmar satisfactoriamente las necesidades punitivas, aunque conviene mejorar las estrategias para la detección y persecución de estos comportamientos.

En el mercado de criptomonedas se producen con frecuencia comportamientos que son similares a la manipulación de mercado, como el uso de compradores ficticios para simular un gran volumen de ventas. De esta forma se provocan alteraciones de valor que incrementan aún más la volatilidad de este tipo de activos. Pese a ello, las criptomonedas no tienen por el momento la consideración de instrumento financiero en el derecho europeo, en consecuencia, no están sometidas a la regulación del mercado de valores ni son objeto de la supervisión de sus autoridades, que resultaría fundamental. Aunque cualquier persona puede realizar estas conductas, existe un fuerte incentivo para que sus autores sean los intercambiadores de moneda o incluso los propios mineros con el fin de incrementar artificialmente el valor de las monedas que poseen. También es posible la administración desleal por parte de los intercambiadores, a través de prácticas como el front-running. La dificultad, en estos casos, deriva del anonimato de las transacciones y, por tanto, en la dificultad para identificar a los responsables.

Finalmente, la Directiva 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo incluye una mención expresa de las monedas virtuales, con una clara intención de asimilar su tutela penal. Aunque esta asimilación es un adecuado punto de partida, las criptomonedas presentan algunas peculiaridades: (1) En primer lugar, la distinción entre infracciones que causan un resultado y aquellas otras que castigan comportamientos preparatorios no es adecuada en el caso de las criptomonedas, pues un monedero de criptomonedas no sólo otorga la capacidad de disponer sobre activos patrimoniales sino que incorpora el valor de los activos patrimoniales. (2) Puesto que los monederos pueden ser medios de pago materiales o inmateriales (monederos fríos o calientes), los tipos penales relevantes son distintos

respecto a unos y otros: en relación con los primeros las conductas delictivas son las prototípicas de los delitos contra la propiedad, mientras que, en el caso de los medios de pago inmateriales, las conductas típicas constituyen casos de criminalidad informática. En los casos en los que el objeto del delito son monederos inmateriales, se ha considerado que lo más apropiado es apreciar un concurso de normas entre el delito informático y el delito contra la propiedad para evitar incurrir en *bis in idem*. (3) El apoderamiento o posesión ilícita del monedero se produce con la obtención de la clave privada. (4) La forma más habitual de realizar un acto de disposición no consentido será la realización o causación de una transferencia de dinero obstaculizando o interfiriendo indebidamente en un sistema de información o empleando indebidamente datos informáticos. La discusión principal entorno a esta figura se ha centrado en analizar sí y en qué medida las conductas que sustituyen al "engaño", previstas en las letras a) y b) del art. 6 de la Directiva pueden ser consideradas desde un punto de vista valorativo similares al engaño (5) La conducta ilícita más importante que podría realizar el "minero" es la falsificación del registro descentralizado aunque, por el momento, resulta poco probable debido a la alta fiabilidad técnica. Esto podría cambiar si se reduce el número de mineros, ya que un acuerdo entre ellos permitiría la falsificación del registro.

Bibliografía

ALEXANDRE, A. (2019), "Los usuarios de las criptobilleteras Electrum y MyEtherWallet se enfrentan a ataques de phishing", en *CoinTelegraph*, https://es.cointelegraph.com/news/users-of-crypto-wallets-electrum-and-myetherwallet-face-phishing-attacks (fecha de consulta: 10.6.2021).

AUTORIDAD EUROPEA DE VALORES Y MERCADOS (2017), "Statement: ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)", París, https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf (fecha de consulta: 10.6.2021).

AUTORIDAD EUROPEA DE VALORES Y MERCADOS (2018), "ESMAs warn consumers of risks in buying virtual currencies", París, https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf (fecha de consulta: 10.6.2021).

AUTORIDAD EUROPEA DE VALORES Y MERCADOS (2019), "Initial Coin Offerings and Crypto-Assets", París, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (fecha de consulta: 10.6.2021).

BANCO CENTRAL EUROPEO (2015), *Virtual currency schemes: A further análisis*, Frankfurt am Main, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (fecha de consulta: 10.6.2021).

BANCO CENTRAL EUROPEO (1999), *Report on the legal protection of banknotes in the European Union member States*, Frankfurt am Main, https://www.ecb.europa.eu/pub/pdf/other/bnlegalen.pdf (fecha de consulta: 10.6.2021).

BARROILHET DÍEZ, A. (2019), "Criptomonedas, economía y derecho", *Revista chilena de derecho y tecnología*, vol.8, n. 1, pp. 29-68.

BRAMDON, R. (2019), "Why the Ethereum Classic hack is a bad omen for the blockchain", en *The Verge*, 9.1.2019, https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto (fecha de consulta: 10.6.2021).

BROWN, S. D. (2016), "Cryptocurrency and criminality: The Bitcoin opportunity", *The Police Journal: Theory, Practice and Principles,* vol. 89, n. 4, pp. 1-13.

CHAPARRO, F. (2019), "Bancor had a front-running problem, so it hired one of the manipulators to fix it", en *Yahoo Finance*, 15.5.2019, https://finance.yahoo.com/news/bancor-had-front-running-problem-183830201.html (fecha de consulta: 10.6.2021).

CHEO, J. (2018), "Fake news can make or break stock prices", en *Bank of Singapore,* 6.4.2018, https://www.bankofsingapore.com/research/Fake-news-can-make-or-break-stock-prices.html (fecha de consulta: 10.6.2021).

CLAEYS, G.; DEMERTZIS, M.; EFSTATHIOU, K., DIRECTORATE-GENERAL FOR INTERNAL POLICIES OF THE UNION- EUROPEAN PARLIAMENT (2018), *Cryptocurrencies and monetary policy, In-depth analysis: monetary dialogue*, Bruselas, pp. 1-12.

CONG, L. W.; LI, X.,TANG, K y YANG, Y. (2019), "Crypto Wash Trading", *SSRN Electronic Journal*, pp. 1-65.

CONLON, T.; MCGEE, R. (2021), "ICO Fraud and Regulation", *SSRN Electronic Journal*, pp. 1-16.

CONTRERAS, M. (2019), "Alguien ha logrado clonar criptomonedas en un ataque sin precedentes que abre muchos interrogantes", en *Business Insider*, 12.1.2019, https://www.businessinsider.es/ataque-ethereum-classic-consigue-clonar-criptomonedas-357287 (fecha de consulta: 10.6.2021).

DAIAN, P.; GOLDFEDER, S.; KELL, T.; LI, Y.; ZHAO, X.; BENTOV, I.; BREIDENBACH, L.; JUELS, A. (2019), "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges", *arXiv 1904.05234*, pp. 1-23, https://arxiv.org/abs/1904.05234 (fecha de consulta: 10.6.2021).

DE, N. (2017), "Fraudsters Post Fake Poloniex Cryptocurrency Trading Apps to Google Store", en *CoinDesk*, 25.10.2017, https://www.coindesk.com/fraudsters-post-fake-poloniex-crypto-trading-apps-google-store (fecha de consulta: 10.6.2021).

DÜRR, A.; GRIEBEL, M.; WELSCH, G.; THIESSE, F. (2020), "Predicting fraudulent initial coin offerings using information extracted from whitepapers", en AA.VV., *Proceedings of the 28th European Conference on Information Systems (ECIS)*, Marrakech, pp. 1-16.

EFE (2017), "Empieza el juicio por fraude contra el dueño de la casa de cambio de bitcoins Mt.Gox", en *La Vanguardia*, 11.7.2017, https://www.lavanguardia.com/economia/20170711/424050548110/juicio-fraude-mark-karpeles-bitcoins-mtgox-japon.html (fecha de consulta: 10.6.2021).

EUROPA PRESS (2017), "China prohíbe la emisión de monedas virtuales como método para financiarse", en *RTVE*, https://www.rtve.es/noticias/20170904/china-prohibe-emision-monedas-virtuales-como-metodo-para-financiarse/1608404.shtml (fecha de consulta: 10.6.2021).

FERNÁNDEZ-VILLAVERDE, J.; SANCHES, D. (2016), "Can currency competition work?", *National Bureau of Economic Research Working Paper Series*, n. 22157, pp. 1-43.

HE, D.; HABERMEIER, K. F.; LECKOW, L. B.; HAKSAR, V.; ALMEIDA, Y.; KASHIMA, M.; KYRIAKOS-SAAD, N.; OURA, H.; SAADI SEDIK, T.; STETSENKO, N.; VERDUGO YEPES, C. (2016), *Virtual Currencies and Beyond:*

Initial Considerations, International Monetary Fund Staff Discussion Notes 2016/003, Washington D.C.

IBOLD, V (2019), "Private Geldschöpfung durch virtuelle Währungen Strafbares Verhalten de lege lata und de lege ferenda unter besonderer Berücksichtigung der geltenden europäischen Währungsordnung", *ZIS*, n. 2, pp. 95-109.

HOUBEN, R.; SNYERS, A. (2018), *Cryptocurrency and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, Bruselas.

JIA, K.; ZHANG, F. (2018), "Between liberalization and prohibition. Prudent enthusiasm and the governance of Bitcoin/blockchain technology", en CAMPBELL-VERDUYN, M. (Ed.) Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance, RIPE Series in Global Political Economy, Routledge, Taylor & Francis Group, London, pp. 88-108.

LIEBAU, D.; SCHUEFFEL, P. (2019), "Cryptocurrencies & Initial Coin Offerings: Are they Scams? - An Empirical Study*", The Journal of The British Blockchain Association*, Vol 2, n.1, pp. 1-7.

HIGGINS, S. (2016), "Cryptsy CEO Stole Millions From Exchange, Court Receiver Alleges", en *CoinDesk*, 11.8.2016, https://www.coindesk.com/cryptsy-ceo-millions-digital-currency-steal (fecha de consulta: 10.6.2021).

HOUGAN, M; LIN, H.; LERNER, M. (2019), "Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market *For The World's First Digital Commodity, Bitwise Asset Management"*, https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf (fecha de consulta: 10.6.2021).

GANDAL, N.; HAMRICK, J.T.; MOORE, T.; OBERMAN, T. (2018), "Price Manipulation in the Bitcoin Ecosystem", *Journal of Monetary Economics*, Vol. 95, pp. 86-96.

GIL, J. (2018), "La estafa de la moneda virtual española: un botín de 228 millones", en *El País*, 21.1.2018, https://elpais.com/politica/2018/01/19/actualidad/1516402754_895017.html (fecha de consulta: 10.6.2021).

GONZÁLEZ-MENESES, M. (2015), *Entender Blockchain. Una introducción a la Tecnología de Registro Distribuido*, Thompson Reuters Aranzadi. Pamplona.

GRIFFIN, J. M; SHAMS, A. (2020), "Is Bitcoin Really Un-Tethered?", *The Journal of Finance,* vol.75, n. 4, pp. 1913-1964.

HOUGAN, M; LIN, H.; LERNER, M. (2019), "Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market For The World's First Digital Commodity, Bitwise Asset Management", https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf (fecha de consulta: 10.6.2021).

JIMÉNEZ, D. (2020), "Bolivia y Ecuador entre los países que prohíben el comercio de criptomonedas en el mundo", en *CoinTelegraph*, 29.2.2020, https://es.cointelegraph.com/news/bolivia-and-ecuador-among-countries-that-ban-cryptocurrency-trading-in-the-world (fecha de consulta: 10.6.2021).

KETHINENI, S.; CAO, Y. (2020), "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity", *International Criminal Justice Review,* Vol. 30, n. 3, pp. 1-20.

NAVARRO CARDOSO, F. (2019), "Criptomonedas (en especial, bitcóin) y blanqueo de dinero", *Revista Electrónica de Ciencia Penal y Criminología*, 21-14, pp. 1-45.

NAVARRO LÉRIDA, M. S. (2020), "Prevención del blanqueo de capitales y beneficial owners: La irrupción del blockchain en la delimitación del concepto de control empresarial", en GONZÁLEZ VÁZQUEZ, J. C./ COLINO MEDIAVILLA, J.L.(dirs.), Regulación bancaria y actividad financiera, Madrid, La Ley, pp. 485-512.

MÖSER, M.; BÖHME, R.; BREUKER, D. (2013), "An inquiry into money laundering tools

in the Bitcoin ecosystem", en AA.VV., Proceedings of the Seventh APWG eCrime Researcher's Summit, San Francisco, pp. 1-14.
NISTICÒ, S. (2019), "Criptovalute, Sovranismo e Sistema Monetario", *Working Papers Series Dipartamento di Scienze Sociali ed Economiche, Sapienza Università di Roma*, n. 8, pp. 1-14.
PALMER, D. (2020), "Alleged Promoter of BitConnect Crypto Scam Charged in Australia", en *Yahoo Finance*, 18.11.2020, https://finance.yahoo.com/news/alleged-promoter-bitconnect-crypto-scam-093346221.html (fecha de consulta: 10.6.2021).
PARTZ, H. (2018), "Las autoridades italianas confiscan el Bitcoin de las billeteras de BitGrail tras una orden de la Corte", en *CoinTelegraph*, 16.6.2018, https://es.cointelegraph.com/news/italian-authorities-seize-bitcoin-from-bitgrail-wallets-following-court-order (fecha de consulta: 10.6.2021).
PÉREZ LÓPEZ, X. (2017), "Las criptomonedas: Consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España", *Revista de Derecho Penal y Criminología*, n. 18, pp. 141-187.
PÉREZ MEDINA, D. (2020), "Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo", *Boletín criminológico*. *Edición Especial. II Encuentro de Jóvenes Investigadores en Criminología*. Artículo 10/2020_EJIC (n. 206), pp. 1-24.
PUPPE, I. (2005), «§ 146», en KINDHÄUSER, U. /NEUMANN, U. /PAEFFGEN, H. U (dirs.), *Nomos Kommentar Strafgesetzbuch*, Baden-Baden, Nomos Verlagsgesellschaft.
SAYEED, S.; MARCO-GISBERT, H. (2018), "On the effectiveness of blockchain against cryptocurrency attacks", en MONTEIRO, C. D. C.; CHATZIKOKOLAIS, K., TOLENTINO, C. H. C. (Eds.)*; The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Atenas,* pp. 9-14.
SECURITIES EXCHANGE COMMISSION (2017), "Statement on Cryptocurrencies and Initial Coin Offerings", https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (fecha de consulta: 10.6.2021).
SECURITIES EXCHANGE COMMISSION (2019), "SEC Sues Alleged Perpetrator of Fraudulent Pyramid Scheme Promising Investors Cryptocurrency Riches", https://www.sec.gov/news/press-release/2019-74 (fecha de consulta: 10.6.2021).
SECURITIES EXCHANGE COMMISSION (2013), "Investor Alerts: Ponzi Schemes Using Virtual Currencies", https://www.sec.gov/servlet/sec/investor/alerts/ia_virtualcurrencies.pdf (fecha de consulta: 10.6.2021).
SUBERG, W. (2018), "Report: 2.3 Million Bitcoin Addresses Targeted by Malware That 'Hijacks' Windows Clipboard", en *CoinTelegraph*, 2.7.2018, https://cointelegraph.com/news/report-2-3-million-bitcoin-addresses-targeted-by-malware-that-hijacks-windows-clipboard (fecha de consulta: 10.6.2021).
STEFANKO, L. (2019), "Fake cryptocurrency apps crop up on Google Play as bitcoin price rises", en *WeLiveSecurity*, 23.05.2019, https://www.welivesecurity.com/2019/05/23/fake-cryptocurrency-apps-google-play-bitcoin/ (fecha de consulta: 10.6.2021).
THE LAW LIBRARY OF CONGRESS OF THE UNITED STATES, GLOBAL LEGAL RESEARCH DIRECTORATE (2018), *Regulation of Cryptocurrency Around the World*, Washington, D.C., https://www.loc.gov/item/2018298387/ (fecha de consulta: 10.6.2021).
UNITED STATES DEPARTMENT OF JUSTICE (2020), Report of the Attorney general's Cyber Digital Task Force. Cryptocurrency. Enforcement Framework, Washington D.C.,

https://www.justice.gov/archives/ag/page/file/1326061/download (fecha de consulta: 10.6.2021).

UNITED STATES SENTENCING COMMISSION (2018), "Bitcoin Glossary: 2018 Annual National Seminar", https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (fecha de consulta: 10.6.2021)

VASEK, M.; BONNEAU, J.; CASTELLUCCI, R.; KEITH, C., MOORE, T. (2017), "The Bitcoin brain drain: a short paper on the use and abuse of bitcoin brain wallets", Lecture Notes in Computer Science, pp. 609-618.

YOUNG, J. (2017), "South Korean Government Concerned With Scams in Bitcoin Market, Fake Exchanges", en *CoinTelegraph*, 25.12.2017, https://cointelegraph.com/news/south-korean-government-concerned-with-scams-in-bitcoin-market-fake-exchanges (fecha de consulta: 10.6.2021).

ZETZSCHE, D. A.; BUCKLEY, R. P.; ARNER, D. W.; FÖHR, L. (2019), "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators", *Harvard international Law Journal*, n. 2, pp. 267-315.

ZMUDZINSKI, A. (2020), "Google elimina 49 extensiones de phishing que roban datos de criptomonedas", en *CoinTelegraph*, 15.4.2020, https://es.cointelegraph.com/news/google-removes-49-phishing-extensions-that-steal-cryptocurrency-data (fecha de consulta: 10.6.2021).