FACULTAD DE DERECHO

CRIPTOMONEDAS Y CRIMINALIDAD: UN MEDIO Y UN OBJETO PARA LA DELINCUENCIA ORGANIZADA

Autor: Sergio Gato Carmona

5º E-3 B

Derecho Penal

Tutor: Alberto Rodríguez-Mourullo Otero

Madrid

Junio de 2022

"You follow drugs, you get drug addicts and drug dealers. But you start to follow the money, and you don't know where it's gonna take you."

-Detective Lester Freamon, The Wire, T1 Episodio 9

Resumen

La aparición de los criptoactivos en el mercado, junto con el resto de las aplicaciones basadas en *blockchain,* está provocando una revolución en el mundo financiero. Las criptomonedas constituyen un depósito de valor que no cuenta con un titular registrado y no emitido por una entidad central que permite hacer transferencias cuasi instantáneas y transfronterizas, de forma garantizada.

A su vez, el modus operandi de las organizaciones criminales ha ido aumentando su complejidad en la última década por el aumento del tamaño de las redes, el número de jurisdicciones en las que operan y el volumen de beneficios procedentes de actividades ilícitas. En los últimos años, numerosos grupos criminales han diversificado sus operaciones y se han adentrado en el lucrativo mundo del cibercrimen, estando algunos de estos grupos apoyados por actores estatales.

Por tanto, la existencia de las criptomonedas facilita la obtención de beneficios de las organizaciones criminales debido a su inmediatez y universalidad, así como la distribución y ocultación de los activos procedentes del delito. Un factor clave es la falta de centralización que dificulta la actuación de las autoridades a la hora de identificar a los titulares de los beneficios, siendo imposible acudir a una entidad que mantenga un registro de titularidad los activos y sus movimientos.

En este trabajo se ha pretendido analizar el uso delictivo de las criptomonedas, las características que las hacen idóneas para la comisión de ilícitos y su relación con el delito de blanqueo de capitales del Código Penal español. A lo largo de este trabajo, se analizan las herramientas jurídicas y técnicas con las que cuentan las autoridades para identificar y decomisar criptoactivos de origen ilícito y, por otro lado, las herramientas utilizadas por los criminales para evitar ser aprehendidos.

Palabras clave: criptomonedas, criptoactivos, blanqueo de capitales, crimen organizado, cadena de bloques, carteras digitales.

Abstract

The appearance of crypto assets in the market together with other blockchain based applications is causing a revolution in the financial world. Cryptocurrencies are an asset without a registered owner and not issued by a central entity that allows guaranteed cross border and almost instant transactions.

At the same time, the modus operandi of criminal organizations has increased its complexity in the last decade due to the increase in the size of criminal networks, the number of jurisdictions where they operate and the volume of illegal profits. In the past few years, some criminal groups have diversified their activities by starting their cybercrime operations, of which some are state backed.

Therefore, the existence of cryptocurrencies makes easier for criminal organizations to obtain profits due to its immediacy and universality, as well as facilitating the distribution and the obfuscation of the assets originated from crime. One key factor is the lack of centralization that makes difficult for the authorities to identify the owners of the assets, because it is impossible to obtain for the information from an entity that keeps track of ownership and asset movements.

The goal of this thesis is to analyze the criminal use of cryptocurrencies, the characteristics that make them an idoneal asset for criminal activities and their relation to the crime of money laundering from the Spanish Criminal Code. Throughout this thesis, the legal procedures, and technical tools at the disposal of the Spanish authorities to identify and confiscate crypto assets of illegal origin will be analyzed as well as the tools used by the criminals to avoid being apprehended.

Keywords: *cryptocurrencies, crypto assets, money laundering, organized crime, blockchain, digital wallets.*

ÍNDICE

I. INTRODUCCIÓN

Una persona con el pseudónimo de Satoshi Nakamoto publicaba en el año 2009 el *whitepaper* de, y desde entonces la importancia de los criptoactivos y el *blockchain* no ha dejado de aumentar, especialmente durante los últimos 5 años en los que su valor se ha multiplicado. Nakamoto, define bitcoin como "una versión *peer-to-peer* de dinero electrónico que permitiría enviar pagos online de una parte a otra sin la necesidad de pasar por una institución financiera".[1] 13 años después, nuevas monedas, tokens, métodos de pago, plataformas y productos desarrollados utilizando *blockchain* se han materializado y su número no deja de crecer cada día a un ritmo cada vez más rápido. El bitcoin es la criptomoneda más popular por ser la primera y por sus grandes subidas y bajadas de precio desde el año 2017 en adelante. Las criptomonedas han sido presentadas al público en un primer momento, como el "dinero de las redes criminales" para comprar armas y drogas, pero se han terminado popularizando como un instrumento de inversión que ha atraído a pequeños inversores y posteriormente a las grandes instituciones financieras de todo el mundo. A la vez que la revolución financiera está impactando a la sociedad, las redes criminales han adaptado su modus operandi para aprovechar las ventajas que un medio de pago descentralizado, anónimo y que funciona a través de internet puede aportar para continuar sus actividades y facilitando nuevas actividades criminales como los ataques de *ransomware*.

1. OBJETIVOS

El objetivo de ese trabajo es poner en contexto los usos criminales de las criptomonedas como objeto material y como instrumento para la comisión de diversos delitos, pasando a realizar posteriormente un análisis de los medios jurídicos para investigar y decomisar criptomonedas en el ámbito del proceso penal. Por otro lado, en una segunda parte del trabajo se incidirá en el blanqueo de capitales con criptoactivos analizando sus características con las acciones típicas de este delito y diferentes medios empleados por las redes de blanqueo para su comisión que serán comentados en torno al modelo de tres fases del blanqueo de capitales definido por el GAFI.

[1] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009, (disponible en https://bitcoin.org/bitcoin.pdf)

2. METODOLOGÍA

La metodología de este trabajo ha variado en función del capítulo del trabajo, aunque de forma común a todos los apartados se ha realizado una revisión de documentación técnica relacionada con la tecnología y las características en una primera fase en la localización de sentencias y autos procedentes de la jurisdicción penal relacionados con criptomonedas. Para la localización de estos documentos se han realizado búsquedas en el buscador del CENDOJ, la base de datos NEO de Lefebvre, Aranzadi de Thomson Reuters y Tirant Online Premium de Tirant lo Blanch utilizando términos de búsqueda como criptomonedas, bitcoin, minería y *blockchain* combinados con los distintos filtros que ofrecen estos servicios para delimitar los resultados. Una vez obtenida la documentación de interés se ha procedido a estudiarla y analizar en conjunto con noticias de prensa relacionadas e informes de la Fiscalía y del Ministerio del Interior para seleccionar los delitos en los que el uso de criptodivisas es más relevante. Para el siguiente capítulo de esta tesis se han estudiado las medidas incluidas en la Ley de Enjuiciamiento Criminal en vigor junto con doctrina de la Fiscalía General del Estado y manuales jurídicos especializados en investigación informática para redactar el apartado de medios de investigación. Este apartado del trabajo requiere un entendimiento básico del funcionamiento tecnológico de las criptodivisas para poder poner en contexto las medidas de investigación y decomiso disponibles en el ordenamiento jurídico que no hace menciones explícitas a temas relacionados con criptomonedas. En el último apartado del trabajo se estudia en profundidad el delito de blanqueo de capitales y su relación con las criptomonedas, haciendo un estudio pormenorizado de sus características en relación con los procesos de blanqueo de capitales, obteniendo gran parte de la información de documentos especializados y de conceptos desarrollados previamente en otros epígrafes del trabajo. Durante este apartado se utilizan las fases de blanqueo de capitales definidas por el GAFI y se relacionan con diferentes medios empleados que son explicados a través de informes de instituciones como Europol, consultoras especializadas en criptomonedas y notas de prensa de operaciones de la Guardia Civil y Policía Nacional en las que se han desarticulado organizaciones dedicadas al blanqueo de capitales con criptomonedas.

3. CONCEPTOS TÉCNICOS

Antes de comenzar a estudiar las cuestiones planteadas en el trabajo de investigación, es importante conocer la base de las claves a estudiar.

3.1. Criptomonedas

Las criptomonedas son medios de intercambio y de depósito de valor digitales cuya propiedad y transacciones están registradas por un libro mayor basado en la tecnología *blockchain*, lo que permite que no haya un tercero que controle todo el libro. La primera criptomoneda, creada en 2009 por Satoshi Nakamoto, es el Bitcoin y es la más conocida, siendo la segunda más conocida y usada el Ether, creada en 2013[2]. La propiedad de las criptomonedas se atribuye al poseedor de las claves de la cartera digital a las que están asociadas, que es simplemente una dirección dentro de la cadena de bloques.

3.2. *Blockchain* / cadena de bloques

Es una base de datos conectada, única y descentralizada que puede contener información de diferente tipo, y que se almacenada en todos los nodos de la cadena, es decir, no se almacena en un lugar centralizado, sino que hay una copia en cada uno de los terminales que existen y cada cambio se almacena en todos ellos. Los nodos de la cadena verifican y añaden nuevos datos, que se replican en todos los terminales, conservando una referencia al bloque previo, lo que permite mantener y garantizar el orden. Dentro de la cadena de bloques nos encontramos 3 elementos principales: claves criptográficas, contando cada uno de los usuarios de la red cuenta con una clave pública y otra privada, enlazadas entre si, permitiendo mediante la aplicación de estas, la determinación de que un mensaje o archivo han sido encriptados por el titular. Otro de los elementos principales, son los *hashes*, que son el resultado de aplicar un algoritmo matemático a un archivo y que permite de forma sencilla determinar si un archivo ha sido manipulado o no, sin mostrar el contenido de este, es decir garantiza la integridad e inalterabilidad[3]. Para entender el proceso de añadido de los bloques de la cadena, es importante mencionar el *proof of work*[4], que es el sistema de consenso descentralizado en el que la red

[2] Buterin, V., "Ethereum Whitepaper", 2014 (disponible en https://ethereum.org/en/whitepaper/; última consulta 25 de abril de 2022).
[3] Legerén-Molina, A., "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain", *Revista de Derecho Civil,* vol. VI, núm. 1, 2019, pp. 177-237.
[4] Ethereum.org, "Proof-of-work (POW)", 2022 (disponible en https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/; última consulta 3 de marzo de 2022).

procesa y confirma las transacciones, generando el hash y añadiendo un bloque a la cadena, lo que evita ataques y manipulaciones. Este sistema de consenso se ayuda de un sello temporal (*time stamping*) con la información del momento exacto en la que se ha minado el bloque. Por participar en este proceso, unos usuarios de la red que compiten entre ellos para llevarlo a cabo, llamados mineros, reciben una recompensa por el consumo de recursos informáticos. Otras cadenas de bloques utilizan como mecanismo de consenso el *proof of stake*[5], que funciona mediante un mecanismo formado por validadores conectados a la red que no compiten entre ellos, y que realizan procesos que requieren menor potencia computacional.

3.3. Bitcoin

Dinero electrónico desarrollado por Satoshi Nakamoto en 2009[6] cuyo objetivo es evitar el uso de un tercero verificador, mediante el uso de pruebas criptográficas en lugar de la confianza. Las transacciones son imposibles de revertir y el sistema se basa en una red de nodos con capacidad computacional, que verifican las transacciones. Para el funcionamiento de la red existe un sistema que incentiva la participación de los nodos, muy similar al de los mineros de oro, que tratan de obtener el mineral para ponerlo a circular en el mercado. Para el ámbito del trabajo es importante centrarse en la privacidad del sistema, que en lugar de limitar el acceso a la información como haría un banco tradicional, en el que las transacciones entre cuentas son secretas para terceros, la información sobre las transacciones es pública; se sabe que se ha hecho una transacción de cierta cantidad de una persona a otra, pero no se puede asociar la transacciones con una identidad específica.

3.4. Ethereum

Es un protocolo enfocado en la construcción de aplicaciones descentralizadas mediante el uso de una cadena de bloques con su propio lenguaje de programación que permite desarrollar programas informáticos con sus propias normas de propiedad y transacciones. La red Ethereum permite 3 tipos de aplicaciones: aplicaciones financieras, semi-financieras y de gobierno descentralizado y voto. La red Ethereum incluye su propia criptomoneda llamada Ether, aunque la red permite su uso para crear otras criptomonedas, que establece un mecanismo para el pago

[5] Ethereum.org, "Proof-of-stake (POS)", 2022 (disponible en https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/; última consulta 3 de marzo de 2022)
[6] Nakamoto, S, op. cit.

de las comisiones de las transacciones y para aportar liquidez a la red[7]. Las transacciones realizadas son públicas, pero las identidades de los dueños de las carteras son anónimas.

3.5. Finanzas descentralizadas (DeFi)

"DeFi, también referidas como "finanzas abiertas", es un conjunto de servicios financieros y aplicaciones basados en *blockchain*/sistema de registros distribuidos cuya intención es aumentar o reemplazar los servicios financieros actuales, a los que se suele referir como finanzas centralizadas"[8].

Las finanzas descentralizadas permiten el uso de distintos instrumentos financieros tradicionales como préstamos y depósitos o intercambio de activos, pero también productos financieros menos tradicionales, como criptomonedas asociadas al valor de un activo, denominadas *stable coins.*

II. USOS DELICTIVOS DE LAS CRIPTOMONEDAS

1. CONSIDERACIONES GENERALES

Las criptomonedas permiten la ejecución de transacciones monetarias en un entorno no regulado ni controlado por organismos de vigilancia como pueden ser las autoridades fiscales y los organismos de prevención de blanqueo de capitales. Las transacciones son cuasi inmediatas en la mayoría de los casos, irreversibles y es complicada la identificación de los titulares de las carteras, ya que como he explicado en el apartado de conceptos técnicos, las transacciones son públicamente verificables en el "libro mayor" pero los titulares de las "cuentas" no están identificados ante una autoridad como si ocurre con una cuenta bancaria tradicional. A su vez, facilitan transferir cantidades de dinero entre países sin enfrentarse a procesos burocráticos o a esperas ya que las carteras no se encuentran en un país determinado, sino que residen únicamente en la *blockchain*.

[7] Buterin, V., Op. cit.
[8] Andrei-Dragoș, P., "Decentralized Finance (DEFI) – The LEGO of finance", *Social Sciences and Educational Research Review,* 2020, p. 323 (disponible en https://sserr.ro/wp-content/uploads/2020/07/SSERR_2020_7_1_321_349.pdf)

Las criptomonedas podrían considerarse una alternativa mejorada al dinero en efectivo desde el prisma de facilitar de la comisión de ilícitos, ya que sus transacciones al igual que con el papel moneda no están sujetas al control de las autoridades y permiten operar de forma anónima sin tener que hacer intercambios físicos y no pueden ser decomisadas, como se puede hacer con el efectivo, permitiendo también hacer transacciones transfronterizas sin necesidad de ocultar grandes cantidades de efectivo y transportarlo. En cualquier caso, realizar transacciones anónimas con criptomonedas presenta ciertas dificultades y no es tan sencillo como acudir a una página web que ofrezca servicios de intercambio de criptomonedas, adquirirlas con nuestra tarjeta de crédito y comenzar a operar usando nuestras recién adquiridas monedas virtuales, ya que las principales plataformas cumplen con las normativas anti-blanqueo y requieren verificar la identidad del usuario para poder operar con ellas. Por esta razón al igual que con el dinero en efectivo existen personas que cooperan a la hora de ingresar y transferir dinero procedente de actividades ilícitas, en el mundo de las criptomonedas también existen las mulas.

Para ilustrar el papel de las criptomonedas en la comisión de diversos delitos de diferente tipología, se comentarán brevemente distintas sentencias en los siguientes epígrafes.

1.1. Delito de estafa

Las criptomonedas, por su dificultad de comprensión y falta de regulación, facilitan notablemente la comisión del delito de estafa que según el artículo 248.1 del Código Penal es: *Cometen estafa los que, con ánimo de lucro, utilizaren engañado bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.*

Tras la lectura y el estudio de diversas sentencias publicadas en relación con criptomonedas se pueden distinguir uso de las criptomonedas como objeto material del delito y como instrumento para la comisión del delito de estafa.

Para ilustrar un supuesto de estafa del artículo 248 del Código Penal en el que las criptodivisas han sido el objeto material del delito, utilizaremos una sentencia de la Audiencia Provincial de

Madrid[9] en la que se condena a un ciudadanos español que en 2014 había constituido una compañía en Londres que ofrecía servicios de *trading* de alta frecuencia, que consisten en realizar inversiones con algoritmos informáticos que implementan estrategias de inversión de corta duración y en gran cantidad, con la criptomoneda Bitcoin y según se indica en la sentencia movido por un ánimo de enriquecimiento ilícito y aparentando solvencia. Esta persona suscribió contratos con al menos 5 personas que le transfirieron un total de 35,35 *bitcoins* por un valor en ese momento de unos 11.820 euros, acordando reinvertir los beneficios y entregar las ganancias al vencimiento del contrato a cambio de una comisión. Esta persona según queda probado en la sentencia, y en el posterior recurso ante el Tribunal Supremo, no ejecuta ninguna de las operaciones de negociación ni reintegra los bitcoins recibidos, alegando la pérdida total de la inversión e incluso una generación de comisiones más elevadas que el capital invertido y en su escrito de defensa remite al juzgado unos informes quincenales con el rendimiento de las inversiones, que según la Sala en su fundamento jurídico segundo no fueron enviados en ningún momento a los contratantes y que contaban con numerosas contradicciones. Además, el órgano juzgador remarca que los informes carecen de valor probatorio ya que no se identifica ninguna de las transacciones de forma individual, lo que permitiría probar de forma inequívoca las operaciones realizadas, ya que una de las características del Bitcoin es la posibilidad de auditar todas las transacciones realizadas en su red. La Sala reprocha al condenado no haber puesto a disposición sus claves para probar que realizó las operaciones. Por estos hechos se le impone una condena de dos años por un delito continuado de estafa ya que se considera que ninguna de las explicaciones aportadas por el acusado resulta creíble.

Por otro lado, se puede observar el uso de criptomonedas en el marco de una transacción habitual como puede ser una venta de segunda mano por internet que nunca se llega a completar. Para ilustrar este tipo de supuestos hemos seleccionado una sentencia dictada por el Juzgado de Instrucción nº4 de Cartagena, con fecha de 27 de diciembre de 2019[10] en la que se condena a una persona que ofertaba en un sitio web de compraventa de segunda mano un componente de ordenador. Este individuo acuerda con otro usuario de la plataforma, la venta del componente previo pago de 1,2343 bitcoins, que se depositan en una cartera de criptomonedas de la plataforma Coinbase. El vendedor nunca envía el producto ni reintegra el

[9] Sentencia de la Audiencia Provincial de Madrid sección 3ª núm. 2779/2018, de 7 de marzo, ECLI:ES:APM:2018:2779. Fecha de la última consulta: 3 de marzo de 2022.
[10] Extraída de la sentencia de la Audiencia Provincial de Cartagena sección 5ª núm. 1308/2020, de 14 de julio, ECLI:ES:APMU:2020:1308. Fecha de la última consulta: 3 de marzo de 2022.

precio abonado. Se condena al vendedor por un delito leve de estafa a una pena de multa y a reintegrar 1,2434 bitcoins al perjudicado. En este supuesto, lo que ha variado con respecto a cualquier otra estafa de este tipo, es el medio de pago, ya que el reo ha utilizado las criptomonedas para hacer atractiva la oferta, pero este engaño se podría haber realizado con otro una transferencia bancaria, por ejemplo.

2. CIBERDELITOS

A la hora de definir los cibercrímenes, podemos tomar como referencia la Instrucción 2/2011 de 11 de octubre de la Fiscalía General del Estado y la Circular 3/2017, de 21 de septiembre, que establecen la competencia de los Fiscales de Sala de Criminalidad Informática en los siguientes delitos:

- Delitos en los que la actividad criminal son los propios sistemas informáticos
    - Delitos de daños y sabotaje informático.
    - Delitos de acceso sin autorización a datos, programas o sistemas informáticos.
    - Delitos de descubrimiento y revelación de secretos cometidos a través de las TIC o almacenados en soportes informáticos.
    - Delitos de descubrimiento y revelación de secretos de empresa a través de las TIC o almacenados en soportes informáticos.
    - Delitos contra los servicios de radiodifusión e interactivos
- Delitos en los que la actividad criminal de sirve de la informática para su ejecución
    - Delitos de estafa informática
    - Delitos de acoso a menores de 16 años
    - Delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil
    - Delitos contra la propiedad intelectual
- Delitos en los que la actividad criminal se aprovecha de la informática y entraña especial complejidad en su investigación

Según el Informe de Criminalidad Informática presentado por el Ministerio del Interior para el año 2020, que evalúa las denuncias presentadas ante las Fuerzas y Cuerpos de Seguridad del Estado, el 16,3% de las infracciones penales denunciadas en nuestro país eran cibercrímenes.

Este último dato crece cada año, ya que en el año 2016 estos delitos solo representaban un 4,6% de los delitos denunciados.

2.1. Delito de estafa informática

Esta modalidad del delito de estafa tiene una especial relevancia ya que representa el 89,6%[11] de los hechos conocidos por las FCSE en el ámbito de los ciber delitos. En este tipo del delito de estafa, se sustituye el engaño por un programa informático malicioso. Estos delitos cada día más comunes por la penetración de la tecnología en todas las esferas de la sociedad tienen un impacto importante y sus autores suelen utilizar las criptomonedas para canalizar los beneficios obtenidos. Un caso para destacar por su relevancia internacional y porque fue enjuiciado por en nuestro país por la Sección 1ª de la Audiencia Nacional es el del grupo de hackers conocido como Carnabak[12]. Esta organización se dedicaba a infectar sistemas informáticos con técnicas de *phishing* de correo electrónico a bancos de todo el mundo para poder controlar sus cajeros permitiendo a la organización enviar órdenes de retirada de efectivo de forma remota. El dinero era recogido por personas encargadas de ello por la organización. El líder de la organización operaba desde España y recibía de las "mulas" el dinero obtenido en criptomonedas, que posteriormente convertía en dinero de curso legal que utilizaba para recargar tarjetas prepago o para adquirir vehículos y propiedades, introduciendo este dinero obtenido ilícitamente en el circuito legal. En la sentencia[13] se identifican activos por un valor total de 3,9 millones de euros entre vehículos, joyas, motos y dinero en cuentas bancarias, aunque según fuentes periodísticas la organización podría haber retirado hasta 10.000 millones de euros.

2.2. Delito de daños informáticos

[11] D.G. de Coordinación y Estudio de la Secretaría de Estado de Seguridad - Ministerio del Interior, "Estudio sobre la cibercriminalidad en España - 2020", 2021, p.41 (disponible en http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3; última consulta 4 de marzo de 2022).

[12] Herraiz, P., "Cae en España el 'hacker' de los 10.000 millones, el ciber ladrón más importante del mundo: Carbanak", *El Mundo*, 27 de marzo de 2018 (disponible en https://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html; última consulta el 4 de abril de 2022).

[13] Sentencia de la Audiencia Nacional sección 1ª núm. 2959/2021 de 5 de julio, CENDOJ: SAN 2959/2021. Fecha de la última consulta: 4 de abril de 2022.

El delito de daños informáticos contemplados en el artículo 264 y ss. del Código Penal castiga a la persona que sin autorización y de manera grave borre, altere, suprima, o haga inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos. Uno de los tipos de ataque informático que más relevancia ha tomado en los últimos años, son los ataques de *ransomware*, que son un tipo de software malicioso que encripta los archivos de un dispositivo o una red de equipos, dejándolos inservibles y pidiendo el actor malicioso un "rescate" para desbloquear los equipos[14]. Un caso paradigmático de *ransomware* en España es el sufrido por el Servicio Público Estatal de Empleo en el mes de marzo del año 2021, que bloqueó la totalidad de sus equipos y sistemas de comunicación, paralizando la actividad normal de la entidad durante más de mes y medio[15]. El caso del SEPE no ha sido enjuiciado de momento y se desconoce la identidad de sus responsables, pero en la base de datos del CENDOJ se encuentra la sentencia otro uno de los casos de *ransomware* más conocidos de España, que fue el del virus de la Policía, un ataque informático realizado a gran escala en todo el mundo y que bloqueaba los ordenadores infectados haciéndose pasar por la Policía Nacional y cobrando una multa falsa de 100 euros, que se abonaba a través de pasarelas de tarjetas prepago online como Paysafecard o Ukash y se retiraban en efectivo por una red de mulas que trabajaba para la organización. Según la sentencia de la Audiencia Nacional[16], en la causa estaban personadas unas 933 víctimas en España y los responsables fueron condenados a un delito de estafa en concurso medial con el delito de daños informáticos. Durante la investigación, se detectó el uso de criptomonedas por parte de la organización para ocultar sus ganancias. En los últimos años, el uso de criptomonedas para solicitar los rescates se ha popularizado porque dificultan la labor de los investigadores y su adquisición es sencilla para cualquier usuario de internet. Según la consultora de análisis de datos de *blockchain*, Chainanalysis, en el año 2020 se recibieron pagos por rescates de ataques de *ransomware* en criptomonedas por un valor aproximado de 350 millones de dólares, un incremento del 311% con respecto a los datos de 2019[17].

[14] Gobierno de EE. UU., "Ransomware 101", *StopRansomware* (disponible en https://www.cisa.gov/stopransomware/ransomware-101; última consulta 5 de abril de 2022).
[15] Aguiar, A. R., "El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el 'ransomware'", *Business Insider*, 2 de diciembre de 2021 (disponible en https://www.businessinsider.es/vivio-ciberataque-sepe-dentro-19000-horas-extra-973861; última consulta el 5 de abril de 2022)
[16] Sentencia de la Audiencia Nacional sección 4ª núm. 704/2016, de 3 de marzo, CENDOJ: ECLI:ES:AN:2016:704. Fecha de la última consulta: 5 de abril de 2022.
[17] Chainanalysis, "The 2021 Crypto Crime Report", 16 de febrero de 2021, p.26.

3. OTROS DELITOS

3.1. Delitos de defraudación de fluido eléctrico y análogas

Como se ha comentado en el epígrafe de conceptos técnicos, algunas redes de *blockchain* requieren para validar las cadenas y crear nuevos bloques, procesos también conocidos como minar, una gran capacidad de procesamiento informático que va aparejada de un elevado consumo eléctrico. No hemos podido localizar sentencias en repositorios públicos, pero según una nota de prensa de la Policía Nacional[18] se ha intervenido recientemente una granja de minado de criptomonedas en la provincia de Toledo que se servía de una acometida ilegal para alimentar los equipos necesarios para el minado. Los mineros obtienen una recompensa en criptomonedas por sus labores por lo que al no hacer frente a los gastos de electricidad obtendrían una mayor rentabilidad en sus actividades.

3.2. Delitos contra la salud pública

Las criptomonedas como ya se ha comentado antes permiten realizar pagos por internet fuera del sistema bancario tradicional por lo que en ocasiones se utilizan para adquirir productos ilícitos en internet como pueden ser drogas ilícitas. Hemos recopilado una sentencia de la Sección 2ª de la Audiencia Provincial de Tenerife[19] en la que se condena por conformidad a una persona que adquiría anfetaminas y MDMA por internet con el objetivo de ponerlas a la venta, y realizaba el pago en la criptomoneda Bitcoin con el objetivo de evitar ser detectado. Las compras las realizaba utilizando la red TOR que es un protocolo de internet cuya principal característica es la de preservar la privacidad de sus usuarios[20] y que cuenta con sus propios sitios web únicamente accesibles desde la red entre los que se encuentran tiendas de internet que ofertan productos ilícitos y que en el caso que nos ocupa, donde se adquirieron las drogas por parte del acusado y que posteriormente se enviaban por correo postal.

[18] Dirección General de la Policía, "La Policía Nacional desmantela una "granja" ilegal de "minería" de criptomonedas en un chalet de Toledo", 2021, (disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=9583; última consulta 5 de abril de 2022).
[19] Sentencia de la Audiencia Provincial de Tenerife sección 2ª núm. 1900/2018, de 3 de octubre, ECLI:ES:APTF:2018:1900. Fecha de la última consulta: 6 de abril de 2022.
[20] Skerrit, B., "How does Tor *really* work?", *Medium*, 28 de enero de 2018 (disponible en https://medium.com/hackernoon/how-does-tor-really-work-c3242844e11f; última consulta 6 de abril de 2022).

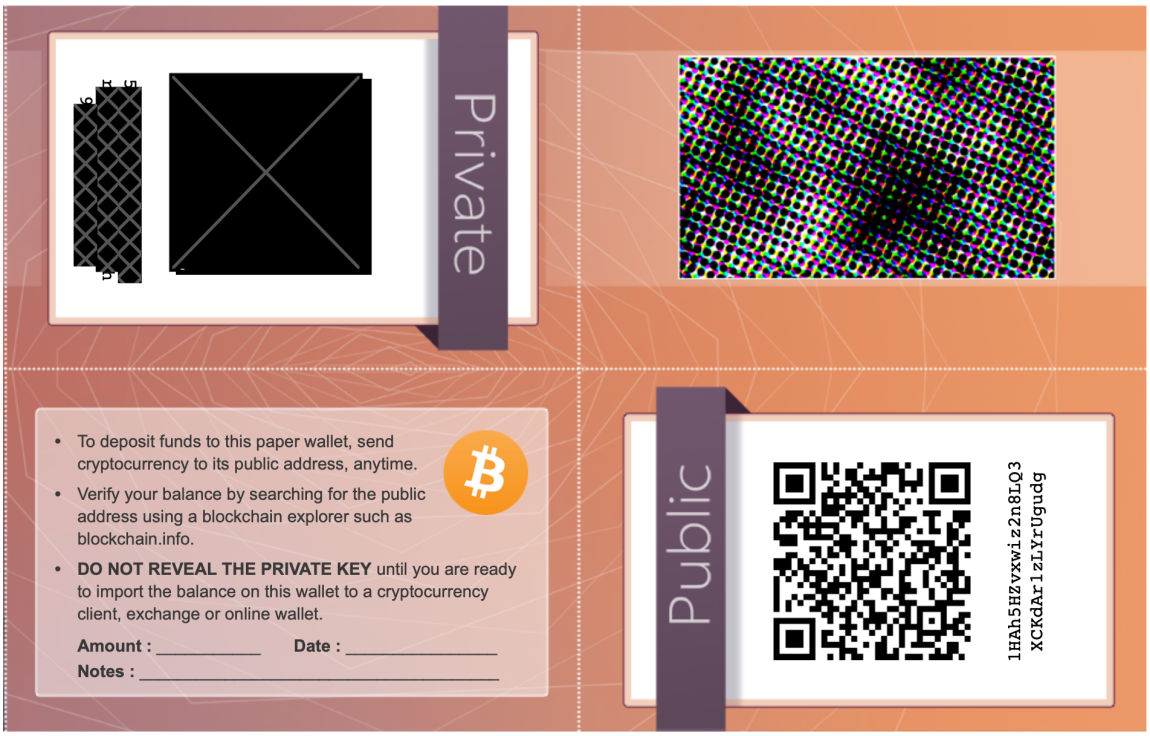
III. MEDIOS PARA LA INVESTIGACIÓN Y ENJUICIAMIENTO

Como se ha explicado en el apartado de conceptos técnicos de este trabajo las finanzas descentralizadas y la cadena de bloques se caracterizan por una falta de regulador central como puede ser el Banco de España en el ámbito bancario español o el registro de la propiedad en el caso de bienes. Esta característica dificulta las labores de indagación ya que no existe una autoridad central a la que acudir para solicitar los datos sobre titularidad. Antes de comenzar a analizar las medidas para la investigación establecidos en la Ley de Enjuiciamiento Criminal, es conveniente describir de forma resumida las diferentes formas para ser propietario de criptomonedas, ya que las medidas a adoptar para perseguir el delito pueden variar.

En primer lugar, una descripción de una cartera de criptomonedas es "el equivalente a una cartera física en la *blockchain*. La cartera contiene tus claves privadas que te permiten utilizar tus monedas en la red."[21]. Las carteras se pueden clasificar por su método de funcionamiento, en calientes o frías, o por el soporte físico de las misma, de *hardware, software,* web o papel. Las carteras "calientes" son aquellas que están conectadas a internet y su principal característica es que facilitan la operativa con criptomonedas y en ocasiones incluyen servicios adicionales[22]. Este tipo de carteras son ofertadas por compañías prestadoras de servicios de custodia de criptoactivos y de intercambio de moneda virtual y para utilizarlas es necesario una cuenta y una conexión a internet. Por otro lado, las carteras frías no están conectadas a internet y suelen ser un medio físico en el que quedan almacenadas la clave pública, necesaria para recibir transacciones, y la privada, para poder operar con la cartera. Normalmente este tipo de carteras son de *hardware*, es decir, dispositivos físicos, conocidos como *ledgers,* que cuentan con un generador aleatorio de claves que quedan almacenadas en el mismo y para operar con ellos, hay que conectarse con un dispositivo electrónico. Por otro lado, existen las carteras de *software*, que consisten en un programa informático instalado en el ordenador y permiten al usuario tener un control de sus propias claves, a diferencia de las carteras calientes, en las que la gestión de claves es realizada por el prestador de servicios. Por último y de forma residual, existen las carteras de papel, que son de tipo frío, y que consisten en una hoja de papel que incluye la clave pública y clave privada de una cartera, siendo una característica de estas la

[21] Bitcoin.org, "Vocabulary – Bitcoin" (disponible en https://bitcoin.org/en/vocabulary#wallet; última consulta 22 de marzo de 2022).
[22] Binance, "What is a crypto wallet?", 18 de junio de 2019 (disponible en https://academy.binance.com/en/articles/crypto-wallet-types-explained; última consulta 22 de marzo de 2022).

imposibilidad de realizar transacciones con ellas de forma directa, ya que es necesario utilizar un cliente para ello. A modo de curiosidad se ha creado una cartera de Bitcoin específica para este trabajo que nos permitirá explicar su funcionamiento.



La clave pública de la cartera es 1HAh5HZvxwiz2n8LQ3XCKdAr1zLYrUgudg y con esta dirección cualquiera puede enviar Bitcoin por lo que podría decirse que es el equivalente al número IBAN de una cuenta bancaria. La clave privada, se puede asimilar a las claves de banca online, y ha sido censurada porque permitiría a cualquiera importar el balance de la cartera a un cliente para poder operar con ella. Si otro usuario de la red decide transferir 1 Bitcoin a la dirección arriba indicada, siempre y cuando cuente con suficientes fondos en una cartera de la que conoce la clave privada, la transacción se ejecutará y quedará registrada en la cadena de bloques tras un proceso de validación. A diferencia de un mensaje de texto o de una transferencia de archivos por correo electrónico, el receptor de la transferencia no tiene que estar conectado a la red porque en el "libro contable" de la red, queda registrado el "asiento" que establece que a la cartera con clave 1HAh5HZvxwiz2n8LQ3XCKdAr1zLYrUgudg, le pertenece el Bitcoin transferido y podrá operar con él en el futuro, siendo este registro inalterable.

En resumen, nos encontramos con un activo digital con valor dinerario que permite realizar transacciones, no tiene un soporte físico determinado, no está regulado por una autoridad centralizada y cuyos titulares no están claramente identificados.

1. DIFICULTAD PARA IDENTIFICAR A LOS TITULARES

Como se ha demostrado anteriormente, la creación de carteras de criptodivisas es un procedimiento no regulado, que deriva de una serie de operaciones matemáticas y es completamente diferente a la apertura de una cuenta bancaria con un número IBAN en la que poder recibir transferencias, que exige acudir a una entidad bancaria autorizada por el Banco de España y aportar la documentación necesaria que suele consistir como mínimo en un documento de identidad oficial. Para el análisis de las cuestiones presentadas en este epígrafe se realizará un enfoque principal en torno al Bitcoin para simplificar las explicaciones, aunque lo explicado en este apartado es de aplicación para la gran mayoría de criptoactivos.

El anonimato del Bitcoin reside en que no hay un titular oficial registrado de las direcciones, de hecho, una persona podría controlar tantas direcciones como desee. Además, en el caso de las carteras no custodiadas o frías no es posible eliminarlas, pero en el caso de las cuentas en servicios de custodia o carteras calientes es posible cancelar la cuenta[23]. La cuestión a estudio sobre las dificultades para identificar a los titulares varía en función del origen del Bitcoin perteneciente a las direcciones y si está almacenado en un servicio de custodia o no. Para simplificar, el Bitcoin se puede obtener participando en la cadena de bloques, adquiriéndolo en una casa de cambio o cajero de Bitcoin o recibiéndolo de otra cartera. En función del origen del Bitcoin la posibilidad de identificar al titular será más o menos sencilla.

1.1. Procedente de actividades de minado

Como se ha explicado en el apartado de conceptos técnicos los mineros son personas que participan en la cadena de bloque aportando capacidad de procesado por verificar y procesar las transacciones de la cadena de bloques mediante operaciones matemáticas que son muy complicadas de generar, pero muy sencillas de verificar para el resto de los nodos de la red,

[23] Kohler, C., "Can you delete a bitcoin wallet?", *The Bitcoin Manual,* 1 de diciembre de 2021 (disponible en https://thebitcoinmanual.com/articles/delete-btc-wallet/; última consulta 28 de marzo de 2022).

este proceso se conoce como *proof-of-work*. A cambio reciben de la red las comisiones de transacciones y una recompensa de nuevos bitcoins, actualmente es de 6,25 bitcoins por bloque generado, que va reduciéndose aproximadamente cada 4 años[24]. Los nuevos Bitcoin son entregados por la red a los mineros en una transacción especial denominada *coinbase*[25] y al no intervenir terceras personas, no se conoce la identidad de los mineros, que en ocasiones trabajan de forma agrupada combinando su capacidad de procesado, ya que la red prioriza las operaciones de aquellos mineros que son capaces de realizar las operaciones matemáticas de forma más rápida. En un epígrafe posterior del trabajo, se analizará como una forma de blanquear capitales a través de la inversión de los ingresos procedentes de operaciones ilícitas en equipos de minado de Bitcoin que generan beneficios ya que el bitcoin obtenido se puede vender por dinero FIAT o intercambiar.

En el caso de que posteriormente el minero traslade sus Bitcoin a una cartera custodiada, se podrían aplicar las medidas del siguiente epígrafe.

1.2. Adquirido y/o custodiado en servicios online

Existen numerosas empresas que prestan servicios de intercambio de moneda fiduciaria por monedas virtuales y es la forma más popular de adquirir Bitcoin y otras criptodivisas. Estas compañías pueden estar domiciliadas en cualquier país del mundo y habitualmente aceptan pagos a través de tarjetas bancarias como VISA y MasterCard, transferencia bancaria y PayPal, que son métodos de pago que generalmente requieren de identificación del usuario para poder utilizarse. Por otro lado, un gran porcentaje de los prestadores de servicio de intercambio y de custodia están sujetos a diversas normativas de blanqueo de capitales y recopilan datos de los usuarios que utilizan sus servicios para cumplir con estas obligaciones. Los medios y procedimientos disponibles para obtener la identidad de los usuarios variarán en función de si la plataforma se encuentra en España o en el extranjero.

[24] bit2me academy, "¿Qué es el halving Bitcoin y qué función tiene? "(disponible en https://academy.bit2me.com/que-es-halving-bitcoin/; última consulta el 28 de marzo de 2022).

[25] Gjermundrød, H., Chalkias, K. y Dionysiou, I., "Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems", 2016 (disponible en https://www.researchgate.net/publication/313345971_Going_Beyond_the_Coinbase_Transaction_Fee_Alternative_Reward_Schemes_for_Miners_in_Blockchain_Systems; última consulta 30 de marzo de 2022).

2.1.1 Servicios domiciliados en España

Los servicios con sede en España están sujetos a la última modificación de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo que realiza una serie de definiciones interesantes para este epígrafe del trabajo y los siguientes. Por un lado, la Ley define en el artículo 1 apartado 5 las **monedas virtuales** como "aquella representación digital de valor no emitida ni garantizada por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente". En el apartado 6 del mismo artículo **el cambio de moneda virtual por moneda fiduciaria** "la compra y venta de monedas virtuales mediante la entrega o recepción de euros o cualquier otra moneda extranjera de curso legal o dinero electrónico aceptado como medio de pago en el país en el que haya sido emitido". El artículo 2 apartado 1 z) de esta misma Ley, establece que serán sujetos obligados los servicios de cambio de moneda virtual por moneda fiduciaria. Las obligaciones establecidas por la Ley de Blanqueo de Capitales son extensas y no son objeto de estudio de este trabajo, pero se puede destacar la obligación de los servicios de intercambio de identificar a los titulares, el establecimiento de requisitos para poder comenzar las relaciones de negocio y la obligación para las casas de cambio de notificar cualquier hecho u operación que pueda estar relacionada con el blanqueo de capitales o la financiación del terrorismo. La Ley además establece en su disposición adicional segunda que "Las personas físicas o jurídicas que, cualquiera que sea su nacionalidad, ofrezcan o provean en España servicios de los descritos en los apartados 6 y 7 del artículo 1 de la ley, deberán estar inscritas en el registro constituido al efecto en el Banco de España"[26] y se establecen sanciones por la prestación de servicios por parte de entidades no registradas. A fecha 31 de marzo de 2022 constan inscritos en el registro[27] 7 servicios de cambio de moneda virtual por moneda fiduciaria, de los cuales 5 cuentan con establecimiento permanente en España. Por tanto, los servicios con sede o que operen en España deben contar

[26] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. (BOE núm. 103 de 29/04/2010), última actualización publicada del 28 de abril de 2021.

[27] Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónico del Banco de España (disponible en https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html).

con información de sus usuarios que deberán proporcionar bajo petición motivada, concreta y específica al Ministerio Fiscal o la Policía Judicial según establece el artículo 7 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales,[28] no estando incluidos en el ámbito de aplicación de este artículo aquellos datos que requieren de autorización judicial por su afectación a los derechos fundamentales, por lo que en principio la titularidad de criptomonedas podría ser información solicitable al amparo de esta disposición.

2.2.1 Servicios domiciliados en el extranjero

Los servicios con sede en el extranjero pueden presentar dificultades para las autoridades responsables de la investigación a la hora de obtener acceso a los datos de los usuarios ya que los medios para obtener la información variarán en función de la jurisdicción en la que se encuentren las plataformas. Por otro lado, pese a que la mayoría de los servicios de intercambio están sujetos a normativas de prevención de blanqueo de capitales y llevan a cabo procesos de KYC[29], por lo que las identidades de los clientes suelen ser recabadas, existen servicios de intercambio calificados como de alto riesgo[30] que no realizan las verificaciones de identidad, no responden a solicitudes de información de las autoridades y se encuentran en países que se caracterizan por contar normativas de secreto bancario y cuyas jurisdicciones no cooperan en materia de blanqueo de capitales. Estas jurisdicciones se encuentran en las listas "negras" y "grises" publicadas por el GAFI[31].

[28] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. (BOE núm. 126, de 27 de mayo de 2021).
[29] KYC: siglas en inglés de *Know Your Customer* que son procesos que realizan las entidades que están sujetas a normativas de prevención de blanqueo de capitales para verificar la identidad de sus clientes (**fuente**: Estudillo, M., "¿Qué es Know Your Customer (KYC) y qué implica?", *Signaturit Blog*, 1 de febrero de 2021 (disponible en https://blog.signaturit.com/es/que-es-know-your-customer-kyc-sector-financiero; última consulta 12 de abril de 2022).
[30] Hudson Intelligence, "High-risk exchange" (disponible en https://www.fraudinvestigation.net/cryptocurrency/tracing/high-risk-exchange; última consulta 13 de abril de 2022).
[31] Grupo de Acción Financiera Internacional: institución intergubernamental dedica a la vigilancia del blanqueo de capitales y la financiación del terrorismo a nivel global.

a. Servicios domiciliados en la UE

Si interesa solicitar información sobre posibles cuentas en servicios de criptomonedas con sede en la Unión Europea, será necesario que la autoridad competente para investigar los solicite mediante los siguientes mecanismos establecidos.

Orden Europea de Investigación

"Es una resolución judicial, emitida o validada por una autoridad judicial de un Estado miembro con vistas a obtener pruebas"[32] y que emana de una Directiva[33] de la Unión que es transpuesta al ordenamiento español en la Ley 3/2018[34]. La Directiva incluye en sus artículos 26 y 27 las consideraciones con respecto a la información bancaria y financiera, quedando regulado en el artículo 26 a la obtención de información sobre cuentas que puedan pertenecer al sujeto pasivo del procedimiento y el artículo 27 regula la modalidad investigación para obtener información sobre las operaciones una cuenta específica. La directiva no introduce los servicios de intercambio de criptomonedas, aunque sí que recoge las cuentas en entidades distintas de un banco en el considerando 28. Según la transposición de la directiva, en el artículo 186 apartado 5 letra a) de la Ley 3/2018 se considerará entidad financiera aquella que se ajuste a la definición establecida por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo y si acudimos a la última modificación de la Ley 10/2010[35], que los servicios de intercambio de moneda virtual son sujetos obligados, por lo que entendemos que la Orden Europea de Investigación permitiría solicitar asistencia a otras jurisdicciones europeas.

b. Servicios domiciliados fuera de la UE

En estos supuestos el Juzgado responsable de la investigación deberá acudir a los procesos de auxilio judicial internacional como las comisiones rogatorias, que son comunicaciones que se dirigen a un juez extranjero para obtener información de una personan investigada en otro país, y en el caso que nos ocupa, información sobre posibles cuentas en servicios de custodia o intercambio de criptomonedas a nombre de la persona investigada. En España el Consejo

[32] Rodríguez-Medel Nieto, C., *TESIS DOCTORAL: Prueba penal transfronteriza: su obtención y admisibilidad en España,* Madrid, 2017, p. 305.
[33] Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal.
[34] Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación
[35] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

General del Poder Judicial cuenta con un Servicio de Relaciones Internacionales que apoya a los jueces en la preparación de solicitudes de auxilio judicial internacional[36]. En función del país destinatario de la comisión rogatoria se aplicarán tratados bilaterales entre España y el tercer estado o el principio de reciprocidad.

Por otro lado, algunos servicios de intercambio y custodia de criptomonedas cuentan con sus propios procedimientos para responder a solicitudes de las autoridades sin necesidad de recurrir a instrumentos de auxilio judicial. Por ejemplo, Binance, el principal servicio de custodia e intercambio del mundo[37], y cuyo domicilio social no queda claramente identificado, tiene a disposición de las autoridades judiciales y policiales un buzón web[38] para remitir solicitudes de información sobre usuarios del servicio.

1.3. Intercambio entre particulares

Una opción menos conocida es el intercambio directo entre las partes, también denominado intercambio *peer-to-peer*. Al realizarse la transacción sin el uso de un proveedor de servicios de intermediación, como sería el caso de una transferencia entre dos carteras no custodiadas, se permite evitar las medidas de identificación y prevención de blanqueo de capitales a las que suelen estar obligados los proveedores de servicio[39]. Como desventaja, existe un elevado riesgo de fraude ya que las transacciones no están protegidas[40] por un tercero. Hay plataformas que facilitan a las personas interesadas ponerse en contacto y cuentan con sistemas de valoraciones para conocer el historial de operaciones de la contraparte, pero el riesgo de impago o de no recibir los criptoactivos sigue existiendo. Por otro lado, se pueden encontrar numerosos anuncios de intercambio de criptomonedas en tablones de segunda mano online. Con una simple búsqueda en la página de segunda mano Milanuncios, es posible constatar la existencia

[36] Poder Judicial de España, "Auxilio judicial Internacional" (disponible en https://www.poderjudicial.es/cgpj/es/Temas/Relaciones-internacionales/Auxilio-judicial-internacional/Informacion-general/; última consulta 10 de abril de 2022).
[37] de Best, R., "Largest cryptocurrency exchanges based on 24h volume in the world on May 2, 2022", *Statista,* mayo de 2022 (disponible en https://www.statista.com/statistics/864738/leading-cryptocurrency-exchanges-traders/; última consulta 15 de abril de 2022).
[38] Binance, "Binance Law Enforcemente Guidelines" (disponible en https://www.binance.com/en/support/law-enforcement/guidelines; última consulta 16 de abril de 2022).
[39] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* FATF, Paris, 2021, p.20, disponible en www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
[40] Europol, *Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2021, p.9.

de numerosos vendedores que ofrecen este servicio, muy probablemente sin cumplir con ninguna de las medidas establecidas por la Ley de Prevención de Blanqueo de Capitales.

Además, siempre es posible encontrar personas dispuestas a aceptar criptomonedas por cualquier tipo de bien, incluyendo inmuebles. En el caso de los bienes que requieren de escritura pública, aunque la operación se llevara a cabo con carteras no custodiadas cuyos activos fueran difíciles de localizar, los notarios en España cuentan con el Índice Único Normatizado Notarial[41], una base de datos que contiene información de las operaciones que realizan a diario los notarios, y que comprueba el Órgano Centralizado de Prevención del Blanqueo de Capitales que es responsable de analizar la información y en caso de indicios de blanqueo de capitales derivar la información al SEPBLAC[42].

Generalmente, los intercambios entre particulares no permiten el blanqueo a gran escala y añaden riesgo de fraude a las operaciones, por lo que las redes de blanqueo utilizan otro tipo de servicios y prácticas, que se analizarán en epígrafes posteriores del trabajo.

2. DIFICULTAD PARA SU DECOMISO

Las criptomonedas pueden ser ocupadas como evidencia física de la comisión del delito, como instrumento del delito, y como pieza de convicción. La Ley de Enjuiciamiento Criminal[43] en su artículo 334 establece que "El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquier clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida." Asimismo, en los artículos 127 y siguientes del Código Penal se establece como pena accesoria de los delitos dolosos el decomiso de los bienes, medios o instrumentos con que se haya preparado o ejecutado el delito y en para ciertos delitos las ganancias, incluso

[41] Consejo General del Notariado, "La colaboración de los notarios en la prevención del blanqueo de capitales, de la financiación del terrorismo y el fraude fiscal", p. 5 (disponible en https://www.notariado.org/portal/documents/176535/0/Los+m%C3%A1s+de+2.800+notarios+espa%C3%B1oles%2C+desde+sus+notar%C3%ADas%2C+se+han+convertido+en+aliados+cada+vez+m%C3%A1s+imprescindibles+del+Estado+para+luchar+contra+estos+delitos.+Para+intensificar+y+canalizar+esta+labor%2C+el+Minister.pdf/49cb4054-4417-935e-9993-cfc45d3a51fa?t=1565770020482; última consulta 18 de abril de 2022).
[42] Consejo General del Notariado, "Prevención del blanqueo de capitales" (disponible en https://www.notariado.org/portal/prevenci%C3%B3n-del-blanqueo-de-capitales; última consulta 18 de abril de 2022).
[43] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (Última actualización de 2 de julio de 2021).

transferidas a terceros, siempre y cuando se cumplan ciertos presupuestos. En el artículo 127 octies del CP se establece que estos bienes podrán ser puestos en depósito desde las primeras diligencias y se podrán realizar de forma anticipada. Cabe destacar la función del Ministerio Fiscal para el aseguramiento de la responsabilidad civil *ex delicto* en delitos que producen un menoscabo en la esfera jurídico-patrimonial tal y como se desarrolla en la Circular 4/2010 de la Fiscalía General del Estado[44].

De forma más específica en el caso de las criptomonedas, los medios para decomisarlas variarían en función del soporte en el que se custodien las claves, en el caso de carteras frías, o si están en algún servicio de custodia online, es decir, una cartera caliente.

2.1. Intervención de criptoactivos en carteras frías

En el caso de este tipo de carteras las custodia de los criptoactivos no está delegada a un tercero y por tanto el investigado almacena sus propias claves en algún soporte de los mencionados anteriormente. Para poder decomisar estos activos será necesaria la clave privada.

Si las claves se encuentran de forma legible en una pieza de papel o similar, los agentes de Policía Judicial en el marco de una orden de entrada y registro acordada por la autoridad judicial podrán, al amparo del artículo 574 de la LECrim, recoger los papeles que contengan las claves, en el caso de que estos monederos fueran necesarios para el resultado del sumario.

En el caso de que las claves se encuentren almacenadas en un dispositivo de almacenamiento masivo, como puede ser el disco de un ordenador, memoria de un teléfono, memoria externa USB o una cartera de hardware, habría que atenerse a las medidas de investigación tecnológica introducidas por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[45].

[44] Circular 4/2010, de 30 de diciembre, sobre las funciones del Fiscal en la investigación patrimonial en el ámbito del proceso penal.
[45] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE núm. 239 de 6 de octubre de 2015).

Las medidas contenidas en el capítulo IV de la LECrim requieren de una autorización judicial que podrá ser acordada de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. El auto motivado deberá contener el hecho punible de investigación y la calificación jurídica, identidad de los investigados, la extensión, unidad de PJ que intervendrá, duración, forma y finalidad entre otros. En el caso de una simple aprehensión de dispositivos electrónicos no será suficiente con la autorización de entrada y registro en el domicilio del investigado, que en ningún caso permitirá el registro de los datos contenidos en los mismos sin perjuicio de una posterior autorización judicial solicitando el registro del dispositivo[46].

Para la ocupación de las claves de las criptomonedas que puedan estar relacionadas con la comisión de ilícitos, las unidades de PJ que intervengan bajo el amparo de un auto motivado del Juzgado de Instrucción competente se pueden encontrar con el supuesto en que las claves o el software utilizado para gestionarlas no esté protegido con contraseña, lo que facilitará la obtención de las claves, debiendo obtenerse un volcado[47] de los sistemas del investigado, ya que según el apartado 2 del artículo 588 sexies c. de la LECrim se evitará la incautación de los soportes físicos excepto que existan otras razones que lo justifiquen.

En el caso de que se encuentren protegidas las carteras que contienen las claves de los criptoactivos con algún tipo de contraseña, el dispositivo de almacenamiento en su totalidad o en un dispositivo de hardware seguro específico para almacenar estas claves como pueden ser los *ledgers*, cabe solicitar la colaboración voluntaria del investigado o intentar acceder rompiendo o evitando el sistema de protección. Se debe acudir al apartado 5 del artículo 588 sexies c. de la LECrim que establece que "Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia" excluyéndose al propio investigado, porque atentaría contra su derecho a no declarar contra sí mismo y a no confesarse culpable, y a las personas dispensadas de la

[46] Delgado Martín, J., *Investigación Tecnológica y prueba digital en todas las jurisdicciones,* Wolters Kluwers, Madrid, 2016, página 369.
[47] **Volcado:** consiste en la realización de una copia espejo o copia bit a bit de la información original según la Circular de la Fiscalía General del Estado 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos.

obligación de declarar por relación de parentesco o por secreto profesional. En relación con el deber de colaboración, la Fiscalía General del Estado en su circular 5/2019 entiende que el ámbito del mismo será únicamente la facilitación de información, bien de las claves de acceso o bien información sobre el sistema ateniéndose al tenor literal del artículo, en cambio, según ZARAGOZA TEJADA el precepto debe ser interpretado conjuntamente con el artículo 588 septies b), sobre el registro remoto, y sobre el que más adelante hablaré, que contempla un deber de colaboración más allá del suministro de información y puede alcanzar "la colaboración precisa para la práctica de la medida y el acceso al sistema, dentro de lo que desde luego cabe, la elaboración y aportación a las autoridades de un software de desbloqueo"[48]. Por otro lado, parece lógico que el artículo anterior incluye entre estos terceros a las unidades especializadas en delitos informáticos de la Policía Nacional y de la Guardia Civil, que no constituiría una colaboración de un tercero si son las unidades designadas para realizar el registro por el auto dictado por el Juez de Instrucción en funciones de Policía Judicial.

Con la tecnología actual de encriptación el desbloqueo de un dispositivo o programa puede resultar especialmente complejo incluso para expertos en la materia y esta complejidad aumenta cuando se utilizan "carteras" de hardware específicas, conocidos como *ledger*, cuyo diseño está centrado en torno a la protección de las claves con complejos sistemas de seguridad y encriptación[49]. El dispositivo más vendido de este tipo es el Ledger Nano S fabricado por la compañía Trezor, con un precio de unos 60€ y está disponible en numerosas tiendas de electrónica especializadas, por lo que es un dispositivo muy accesible para proteger las claves privadas de los criptoactivos y que puede presentar problemas a la hora de solicitar a terceros su desbloqueo.

En el caso de que durante la investigación se prevea que las personas investigadas no van a colaborar con las autoridades y existan indicios de que se han tomado medidas para proteger las claves contra métodos conocidos de desbloqueo, se puede optar por otra de las medidas de investigación tecnológica introducidas por la Ley Orgánica 13/2015, que permite el registro remoto de equipos informáticos y se regula en los artículos 588 septies a y septies b de la

[48] Zaragoza Tejada, J. I., Bermúdez González, J. A., & Madrigal Martínez-Pereda, C. *Investigación tecnológica y derechos fundamentales. : Comentarios a las modificaciones introducidas por la Ley 13/2015*. Thomson Reuters Aranzadi, 2017, pp. 445-447.

[49] Trezor, "Why is Ledger Nano so secure?", 14 de enero de 2021 (disponible en https://www.ledger.com/academy/basic-basics/ledgers-bit-of-it/ledger-nano-security-made-easy; última consulta 20 de abril de 2022).

LECrim. Esta medida es invasiva del derecho a la intimidad y al secreto de las comunicaciones, ya que al contarse con acceso remoto al dispositivo las comunicaciones recibidas podrán ser interceptadas, y por tanto requiere autorización judicial del Juez Competente y el legislador ha establecido en el artículo 588 septies b de la LECrim, que la medida se podrá conceder por el tiempo máximo de un mes siendo prorrogable hasta un máximo de tres meses y se ha establecido una serie de delitos graves *numerus clausus* que se podrán perseguir usando esta medida según el artículo 588 septies a apartado 1: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

La medida consiste en el acceso mediante código o datos de identificación, sin realizar instalación de programas informáticos en los equipos investigado, o bien a través de la instalación de un *software* que permita el escaneo de los archivos del dispositivo o la captación de las contraseñas del investigado a través de un *keylogger*[50] e incluso dar órdenes remotas al ordenador. Estas actuaciones pueden facilitar a los investigadores la obtención de la información necesaria para decomisar las criptomonedas de forma remota o en el momento del acceso físico al dispositivo ya que el investigado puede ser monitorizado mientras hace uso del *software* con el que gestiona las carteras o de los *ledgers* en los que almacena las claves. La medida podrá autorizarse para cualquier tipo de dispositivo electrónico incluyendo teléfonos inteligentes o tabletas. Esta medida, al igual que en el registro de dispositivos de almacenamiento masivo, tiene establecida en el artículo 588 septies b de la LECrim una obligación de colaborar para los prestadores de servicio[51], titulares del sistema informático y terceros a los que las autoridades soliciten información y/o colaboración para la práctica de la medida, estando obligados a guardar secreto acerca de estos requerimientos.

[50] ***Keylogger***: programa malicioso que registra lo que tecleas, fuente: INCIBE, *La jerga de la seguridad: ¿de qué hablamos cuando decimos…?*, 2016 (disponible en https://www.incibe.es/en/node/2943).

[51] El concepto de prestador de servicio queda definido en el Anexo de Definiciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico: persona física o jurídica que proporciona un servicio de la sociedad de la información. En la misma Ley se definen los servicios de la sociedad de la información como: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

Esta medida presenta desventajas técnicas ya que los dispositivos tecnológicos modernos cada vez integran más medidas para garantizar la seguridad de los datos y en ocasiones los propios fabricantes no tienen capacidad para facilitar el acceso a los datos sin contar con la contraseña. Por otro lado, el tipo de delitos perseguibles con la medida de acceso remoto son terrorismo, los cometidos en el seno de una organización criminal y los cometidos a través de medios informáticos, y por tanto, nos encontramos ante tipos penales de cuyos autores se puede presumir un grado elevado de conocimientos informáticos o el uso de prácticas tendentes a proteger sus sistemas contra intrusiones ajenas en mayor medida que lo que se espera de un usuario medio, lo que dificultaría la medida de registro remoto. Por último, esta medida resulta más compleja que el registro de un dispositivo al que se tiene acceso directo, ya que requiere de una preparación avanzada por parte de las autoridades responsables de ejecutar la medida en cuanto al tipo de sistemas a atacar y las técnicas a utilizar, aparte de que en caso de detectarse la intrusión por las personas investigadas puede provocar comportamientos dirigidos a encubrir la actividad criminal y que podrían frustrar las diligencias de investigación.

Una vez obtenida la clave privada de las carteras a intervenir, se podrá custodiar la clave por el Juzgado, pero se corre el riesgo de que otra persona conocedora de la clave o el propio investigado trasladen los criptoactivos, por lo que el Juez podrá autorizar la transferencia a un tercero que custodie las criptomonedas en una cartera diferente tal y como se realizó en el Auto de 22 de diciembre de 2017 del Juzgado de 1ª Instancia e Instrucción N.º 2 de Redondela.[52]

2.2. Intervención de criptoactivos almacenados en carteras calientes

La principal diferencia de estos tipos de cartera es que la persona titular de los criptoactivos no custodia las claves privadas y por tanto no existen claves privadas como tal, ya que las criptomonedas son custodiadas por un tercero. En la última modificación de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo se define a los **proveedores de servicios de custodia de monederos electrónicos** como "aquellas personas físicas o entidades que prestan servicios de salvaguardia o custodia de claves

[52] Velasco, E., "Sobre el Blockchain y su aplicación a las criptomonedas", *El Derecho*, disponible en https://elderecho.com/sobre-el-blockchain-y-su-aplicacion-a-las-criptomonedas; última consulta del 2 de abril de 2022.

criptográficas privadas en nombre de sus clientes para la tenencia, el almacenamiento y la transferencia de monedas virtuales".

Si un investigado almacena sus criptomonedas en un servicio de custodia, la única forma posible para tomar el control de los criptoactivos es bien acceder a la cuenta del investigado y cambiar las claves, transferir las monedas a otra cartera que no esté gestionada por el investigado o solicitar al servicio de custodia que embargue el contenido de las cuentas del investigado. El principal escollo es que la mayoría de los servicios están localizados fuera de España y no constan en el registro habilitado para tal efecto en el Banco de España. A fecha 31 de marzo de 2022 constan 3 servicios de custodia de los cuáles 2 de ellos cuentan con un establecimiento permanente en España[53].

En el caso de servicios de custodia con sede en España o sujetos a la normativa española la autoridad judicial competente podrá realizar un requerimiento judicial a las entidades para que embargue las criptodivisas de determinados usuarios.

El caso de los servicios de custodia extranjeros se podrá recurrir a las Oficinas de Recuperación de Activos si el servicio se encuentra en otro Estado Miembro de la Unión Europea. Estos oficinas "colaboran en la localización de patrimonios y cuentan con los medios técnicos y jurídicos precisos para la gestión y realización de los bienes incautados".[54] En el caso de que el servicio de custodia se encuentre domiciliado fuera de la Unión Europea la autoridad investigadora deberá remitir una solicitud de asistencia judicial internacional, cuyo éxito dependerá de la existencia de Tratados o Acuerdos con el país de destino, así como la existencia de una relación de reciprocidad con España.

[53] Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónico del Banco de España (disponible en https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html).

[54] Circular 4/2010, de 30 de diciembre, sobre las funciones del Fiscal en la investigación patrimonial en el ámbito del proceso penal.

Por otro lado, una práctica ya realizada en España, según un artículo de prensa[55] que narra como una unidad de Policía Judicial decomisó en 2013 criptomonedas mediante la aprehensión del equipo informático del investigado encendido y con la sesión iniciada en los servicios de custodia de criptomonedas, por lo que no requirieron de sus claves. Mediante una autorización judicial el equipo interviniente de PJ transfirió los criptoactivos del investigado a unas carteras gestionadas por la policía que se pusieron a disposición del Juzgado. Para realizar el decomiso por este método, se requiere una labor de investigación avanzada, un conocimiento de los hábitos del investigado para realizar la entrada y registro en el momento adecuado y con la rapidez suficiente.

2.3. Realización de valor de las criptomonedas incautadas

La LECrim contempla en el Capítulo II bis, Título V del Libro II la realización anticipada de efectos judiciales en los artículos 367 quáter y 367 quinquies. Los bienes podrán ser realizados siempre y cuando se traten de bienes de lícito comercio, no sean piezas de convicción y sean perecederos, sus gastos de conservación sean superiores al valor o se deprecien por el transcurso del tiempo. En el caso de las criptodivisas son bienes de lícito comercio, no constituyen piezas de convicción ya que por sí mismos no convencen al juzgador acerca del ilícito, es más, son bienes intangibles. Resulta factible entender que las criptodivisas se pueden depreciar con el transcurso del tiempo, aunque es cierto que también se pueden apreciar, resulta lógico realizar el valor del bien para evitar una posible pérdida de su valor en el futuro.

La realización de los efectos con valor se podrá realizar bien por subasta pública o por medio de persona o entidad especializada, siendo la última opción probablemente la más adecuada para criptoactivos, acudiendo a compañías especializadas en intercambio de criptoactivos. Además, no podrá realizarse si está pendiente el recurso interpuesto contra el embargo de los bienes. El juez puede acordar de oficio o a instancia del Ministerio Fiscal la realización de los efectos judiciales.

La realización anticipada de criptodivisas como una práctica ya realizada por los tribunales españoles es constatable revisando resoluciones en bases de datos jurídicas, por ejemplo, se observa en un Auto de la Audiencia Provincial de Pontevedra que desestima el recurso de una

[55] Romero, P., "Así se incauta la Policía de bitcoins", *El País,* 1 de noviembre de 2013, (disponible en https://www.elmundo.es/tecnologia/2013/11/01/5270d45363fd3da7618b4576.html; última consulta el 25 de marzo).

persona a la que se le habían intervenido criptomonedas, concretamente bitcoin como efecto del delito, en el que se realizaba por parte del Juzgado Instructor una propuesta para vender el bitcoin, que fue rechazada por las partes por tener que hacerse en diferentes casas de intercambio y distintos días.[56]

IV. BLANQUEO DE CAPITALES CON CRIPTODIVISAS

1. EL DELITO DE BLANQUEO DE CAPITALES: INTRODUCCIÓN AL TIPO PENAL

El delito de blanqueo de capitales está tipificado en el derecho penal español en el artículo 301 del Código Penal y sanciona la "realización de ciertos actos que tienen como finalidad ocultar o encubrir su origen ilícito o ayudar a la persona que haya participado en la infracción a eludir las consecuencias legales de sus actos"[57]. El objeto material del delito son las ganancias obtenidas de una actividad delictiva previa, pudiendo tratarse de bienes de cualquier tipo que cuenten con un valor económico y puedan ser incluidos en el tráfico mercantil, por lo que las criptodivisas estarían incluidas dentro del tipo. Además, el apartado 2 del artículo 301 del CP tipifica el blanqueo sucesivo recayendo la conducta sobre el blanqueo de un bien ya "blanqueado" con el objetivo de ocultar o encubrir su verdadero origen y que tal y como ha establecido la jurisprudencia posibilita una autoría independiente del delito en el caso de que interviniesen diferentes personas en las distintas fases de proceso[58]. Por tanto, el acto de convertir dinero en efectivo procedente de un ilícito en criptoactivos con el fin de ocultar su origen inicial constituiría una conducta típica del delito de blanqueo de capitales según nuestro ordenamiento penal.

2. CARACTERÍSTICAS DE LAS CRIPTODIVISAS EN RELACIÓN CON LAS FASES DEL BLANQUEO DE CAPITALES

Las criptodivisas tienen unas características que se han mencionado a lo largo de este trabajo que las hacen atractivas como medio material para el blanqueo de capitales.

---

[56] Auto de la Audiencia Provincial de Pontevedra sección 5ª núm. 527/2018, de 31 de octubre. Base de datos Lefebvre EDJ 2018/659954. Fecha de la última consulta: 14 de abril de 2022. FD 1º.
[57] Gutiérrez Rodríguez, M., "El delito de blanqueo de capitales y otras conductas afines", Liñán Lafuente, A., (coord.), Derecho Económicos y Empresariales, Dykinson, Madrid, 2020, pp. 362-377.
[58] Sentencia del Tribunal Supremo Sala Segunda, de lo Penal, núm. 266/2005, de 1 de marzo. ECLI: ES:TS:2005:1267.

2.1. Cuasi anonimato.

El "libro público" característico de la *blockchain* en el que todas las transacciones se van registrando y son visibles por cualquiera, incluye la dirección de origen y de destino, así como cantidades entre otros datos, pero la identidad de los titulares de las direcciones no es una información presente en la cadena de bloques y teóricamente no se puede asociar a un individuo. Si se opta por las anteriormente mencionadas carteras custodiadas, lo habitual es que el prestador de servicios requiera la información del titular de la cuenta para cumplir con las normativas de prevención de blanqueo de capitales. Por tanto, el uso de criptodivisas es similar al del efectivo en el sentido de que el papel moneda no cuenta con una inscripción del propietario de los billetes, pero a su vez, las transacciones en la mayoría de las redes *blockchain* dejan un rastro público e imborrable, con excepción de algunas criptodivisas específicas que se comentarán posteriormente.

2.2. Descentralización: transferencias internacionales sin intermediarios.

Como se ha mencionado anteriormente, las transacciones se ejecutan a través de un procedimiento informático que garantiza que los activos lleguen de una dirección a otra. Tradicionalmente el lavado de dinero transfronterizo se realiza a través de una red de bancos especializados en transacciones transfronterizas[59], pero en el caso de las criptodivisas no es necesaria su intermediación, en primer lugar, porque dentro de la *blockchain* las carteras no tienen domicilio a diferencia de las cuentas bancarias, y, en segundo lugar, el proceso informático sustituye a los bancos intermediarios que hacen llegar las transacciones de una cuenta a otra. Aunque teóricamente no sean necesarios los intermediarios, más adelante veremos como existen servicios que realizan operaciones intermedias para dificultar el trazado de las transacciones.

2.3. Rapidez en las operaciones

59 Campbell-Verduyn, M., Bitcoin, crypto-coins and global anti-money laundering governance, Crime Law and Social Change, 2018, p.4., disponible en https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance

Otra de las características de las criptomonedas que resulta de interés para el blanqueo de capitales es la velocidad en la que se ejecutan las transacciones. En el epígrafe anterior se ha mencionado la posibilidad de hacer transacciones transfronterizas sin necesidad de intermediarios, pero además una transferencia en la mayoría de las redes es infinitamente más rápida que entre cuentas bancarias. Las transferencias en la *blockchain* requieren de un procesado por parte de los validadores o mineros. Este tiempo varía en función de las comisiones que se paguen y de si la red utiliza sistemas de tipo *proof-of-work*, más lentos, o *proof-of-stake,* más rápidos, por lo que por ejemplo una transacción en Bitcoin tarda una media de 40 minutos, pero una en la criptodivisa Cardano (ADA) sería prácticamente inmediata[60]. En cambio, las transferencias bancarias SEPA, dentro de la zona euro, tardan un máximo de 2 días laborables en ejecutarse[61] y las internacionales con el sistema SWIFT hasta un máximo de 4 días laborables[62].

2.4. Irreversibilidad de las transacciones: seguridad en los pagos

Cuando Satoshi Nakamoto crea el Bitcoin establece como uno de sus principios básicos la irreversibilidad de las transacciones para reducir los costes de intermediación, por lo que una vez una transferencia ha sido confirmada y se ha registrado en la *blockchain*, esa transferencia no se puede deshacer porque el siguiente bloque de la cadena incluirá información sobre esa transacción[63]. Las diferentes redes de *blockchain* cuentan con procesos de validación de transacciones basados en algoritmos matemáticos en lugar de en la confianza en una institución bancaria, permitiendo a los blanqueadores de capitales proteger sus activos de embargos e intervenciones de órganos estatales que no podrán o interceptar las transferencias.

2.5. Medio de intercambio y activo financiero a la misma vez

[60] de Best, R., "Average transaction speed of 66 cryptocurrencies with the highest market cap as of March 2022"*, Statista*, 2022 (disponible en https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/; última consulta 19 de abril de 2022).
[61] N26, "How long does a transfer take?", 15 de febrero de 2022 (disponible en https://n26.com/en-eu/blog/how-long-does-a-bank-transfer-take; última consulta 20 de abril de 2022).
[62] Smith, M., "SWIFT transfers explained (how they work, how long they take & what they cost)" (disponible en https://www.keycurrency.co.uk/swift-transfer/; última consulta 20 de abril de 2022).
[63] Conesa, C., *Bitcoin: ¿una solución para los sistemas de pago o una solución en busca de problema?*, Banco de España, Documentos Ocasionales nº1901, 2019, disponible en https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/19/Fich/do1901.pdf

Los criptoactivos cuentan con un valor en el mercado y se pueden comprar y adquirir en mercados cuya operativa es similar a los mercados de divisas[64] y a su vez, se pueden asimilar a un producto financiero. No existe un precio oficial de las criptomonedas, aunque en general todos los servicios de intercambio cuentan con precios prácticamente idénticos ya que en el caso de diferencias de precio habrá inversores que las aprovechen para realizar operaciones de arbitraje[65] y los precios se corregirían automáticamente. Hay criptoactivos que se caracterizan por su volatilidad y sus rendimientos como el Bitcoin que en 2021 aumentó un 70% su valor y superó el beneficio del índice S&P 500, que sigue a 500 compañías cotizadas de EE. UU., cuyo retorno fue del 28%[66] y, por otro lado, criptodivisas cuyo valor se mantiene estable porque están respaldadas por dinero FIAT, otras criptomonedas o bienes como el oro[67]. Además, existen productos financieros que permiten obtener rendimientos financieros invirtiendo criptomonedas como por ejemplo el *staking*[68]*,* préstamos y depósitos. Por otro lado, las criptomonedas también sirven como un medio de pago, ya que, a diferencia de una acción o un bono, existe mayor facilidad para intercambiarlas bien por otras criptomonedas directamente o como medio de pago por productos y servicios. Por ejemplo, la compañía de automóviles Tesla ha aceptado Bitcoin como método de pago en algunos países.[69]

3. FASES DEL BLANQUEO DE CAPITALES

El proceso de blanqueo de capitales suele ser representado usando modelos que simplifican las fases que se llevan a cabo durante la comisión del ilícito. Algunos de los modelos más

---

[64] España Alba, V. M., *Secreto bancario y paraísos fiscales: la ingeniería fiscal al servicio del blanqueo de capitales*, Sepín, Madrid, 2017, p. 104.
[65] Arbitraje: Consiste en aprovechar la diferencia de precio entre diferentes mercados sobre un mismo activo. Fuente: elEconomista, "Arbitraje financiero" (disponible en https://www.eleconomista.es/diccionario-de-economia/arbitraje-financiero; última consulta 1 de mayo de 2022).
[66] Bizouati-Kennedy, Y., "Bitcoin Returns Reach Over 70% in 2021, Outperform Gold and Stock Market for Third Straight Year", *Yahoo Finance,* 30 de diciembre de 2021 (disponible en https://finance.yahoo.com/news/bitcoin-returns-reach-over-70-205650585.html?guccounter=1; última consulta 1 de mayo de 2022).
[67] BBVA, "¿Qué son las 'stablecoins' y para qué sirven?", 28 de enero de 2019 (disponible en https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/; última consulta 1 de mayo de 2022).
[68] *Staking*: Algunas criptodivisas utilizan el modelo *proof-of-stake,* como por ejemplo las de la red Ethereum, y pueden utilizarse en el proceso de *staking* que consiste en comprometer una serie de criptoactivos para que participen en el proceso de validado de bloques de transacciones de la cadena con los recursos de su ordenador o colaborando a con otros usuarios través de un agregador. Al realizar *staking* se recibe de la red una recompensa que se asemeja a los intereses que paga un depósito bancario. Fuente: Coinbase, "What is staking?" (disponible en https://www.coinbase.com/learn/crypto-basics/what-is-staking; última consulta 1 de mayo de 2022).
[69] Tesla, "What You Need To Know If You Use Bitcoin" (disponible en https://www.tesla.com/assets/pdf/BTC_What_You_Need_To_Know_en_US.pdf; última consulta 1 de mayo de 2022).

utilizados son el Modelo Bernasconi, Modelo de Zünd, Modelo de Ackerman y el Modelo de tres fases del GAFI[70]. La jurisprudencia española también se ha pronunciado sobre las fases del proceso de blanqueo, manifestando la STS 156/2011, de 21 de marzo que "el delito de blanqueo de capitales se vertebra en tres fases sucesivas"[71] mencionado una primera fase de colocación de los bienes, de distracción para disimular su origen y de reintegración en la que el dinero blanqueado vuelve a su titular, coincidiendo estas con las fases que establece el FATF[72].

3.1. Fase de colocación

En esta fase los beneficios del delito se introducen en el sistema financiero mediante la separación en cantidades más pequeñas de efectivo que se utilizan para bien realizar depósitos en entidades bancarias o para adquirir instrumentos financieros como títulos al portador. En el caso de las criptomonedas si el beneficio del delito se ha obtenido en criptomonedas, por ejemplo, si son criptodivisas procedentes del pago de un "rescate" de un ataque de *ransomware* o de una estafa online, el proceso de colocación consistirá principalmente en desligar de la cartera inicial las transferencias recibidas. Por otro lado, si el beneficio del delito se ha obtenido en efectivo, se deberán realizar procedimientos para convertirlo en criptodivisas. La cuasi anonimidad de las criptomonedas facilita esta fase por la facilidad de crear direcciones en las que recibir los activos, así como las transacciones en tiempo real, que permiten transferir los beneficios del delito a gran velocidad. Además, que exista una alta negociabilidad y disponibilidad de los criptoactivos en el mercado, permite a las redes criminales utilizar diferentes plataformas y servicios para transferir y negociar con criptodivisas en cantidades que no llamen la atención de las autoridades de prevención de blanqueo[73].

3.2. Fase de estratificación

En esta fase del proceso de blanqueo se produce el encubrimiento del origen de los beneficios. Tradicionalmente se realizan transacciones y movimientos mediante la adquisición de activos financieros, el traspaso entre numerosas cuentas bancarias internacionales a través de

[70] España Alba V. M., *op. cit*., p. 28.
[71] STS núm. 156/2011, de 21 de marzo [versión electrónica – base de datos Vlex https://vlex.es/vid/-272355247]. Fecha de la última consulta 2 de abril de 2022. FJ 1.
[72] FATF, "How is money laundered?" (disponible en https://www.fatf-gafi.org/faq/moneylaundering/; última consulta el 18 de abril de 2022).
[73] Raymond Choo, K., "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?" en Kuo Chen, D. L., *Handbook of Digital Currency*, Elsevier, 2015, pp. 283-307.

jurisdicciones que no cooperan en operaciones internacionales contra el blanqueo de capitales y el uso sociedades pantalla gestionadas por testaferros entre otros métodos. En el caso de las criptomonedas se transfieren de unas carteras a otras utilizando herramientas y servicios que permiten ofuscar el destino de las transacciones, se convierten en criptoactivos con funcionalidades específicas para la privacidad o se simulan compraventas de productos o prestación de servicios ficticios para dar un aspecto de legalidad a las transacciones. Además, otra opción para las redes de blanqueo de capitales es constituir sociedades pantalla o utilizar a testaferros para adquirir o intercambiar criptomonedas.

3.3. Fase de integración

Es la última fase del proceso de blanqueo de capitales en la que "los bienes están a disposición del autor del delito en la corriente monetaria con una apariencia legítima"[74] y se han realizado los procesos previos para complicar la identificación del origen real de los beneficios. En el caso de las criptomonedas se pueden mantener como inversión, utilizar para adquirir participaciones de compañías cotizadas, adquirir bienes muebles o inmuebles y recargar tarjetas de débito prepago para utilizar en diversos establecimientos. Una de las ventajas de los criptoactivos es que el autor del delito puede recibir en una cartera fría de su posesión los criptoactivos ya alejados del origen delictivo sin necesidad de someterse a procesos de identificación orientados a la prevención del blanqueo de capitales, pudiendo además transferirlos de forma rápida a sus colaboradores.

4. MEDIOS EMPLEADOS

En este epígrafe del trabajo se va a identificar algunos de los medios utilizados por las organizaciones criminales para blanquear capitales mediante criptodivisas

4.1. Cajeros automáticos

España es uno de los países del mundo con mayor número de cajeros de criptomonedas y según el sitio web Coin ATM Radar[75] existen 229 cajeros operativos. En estos cajeros se puede

[74] España Alba V. M., *op. cit*., p. 30.
[75] Coin ATM Radar, "Bitcoin ATMSs in Spain" (disponible en https://coinatmradar.com/country/199/bitcoin-atm-spain/; última consulta 9 de mayo de 2022).

comprar y vender distintas criptomonedas usando dinero en efectivo y/o tarjeta y según las comprobaciones realizadas en los sitios web de varios proveedores[76], la mayoría de los proveedores no exige identificarse para operaciones en efectivo con importes inferiores a 1.000 euros para residentes y 9.990€ para no residentes. Además, en otras jurisdicciones se considera que las transacciones en cajeros automáticos son ocasionales y por tanto no se exigen a los prestadores de servicio que lleven a cabo procedimientos de verificación de identidad[77]. Esta falta de procedimientos de KYC permite a las redes intercambiar dinero en efectivo procedente de actividades ilícitas por criptomonedas de forma anónima, encuadrándose este proceso en la fase de colocación del delito de blanqueo de capitales, mediante el uso de "mulas" de dinero que realizan transacciones por debajo del límite que exige identificación, que es suficientemente alto como para permitir convertir miles de euros al día. Las comisiones de estos cajeros están en torno al 10% de la operación, pero las organizaciones las asumen como un coste razonable por su facilidad de uso y rapidez. En mayo de 2019 la Guardia Civil desarticuló en la operación "Kampuzo" a una organización dedicada al blanqueo de capitales en Madrid que convertía en criptoactivos más de 100.000 euros al día utilizando cajeros ubicados en Madrid junto con una red de sociedades constituidas con documentación falsa[78].

Por otro lado, la posibilidad que ofrecen algunos de estos cajeros de recibir criptodivisas en una dirección y entregar una cantidad de efectivo, lo que se asimilaría a una retirada de efectivo tradicional y se encuadraría dentro de la fase de integración, posibilitan la conversión de criptomonedas en efectivo con apariencia legítima y que suele ser complicada de trazar, si se han realizado adecuadamente las fases de colocación y estratificación.

4.2. Mezcladores de criptomonedas

Son servicios que permiten ofuscar el origen y destino de criptomonedas como Bitcoin, cuyas transacciones son públicas y accesibles para cualquier persona, con el objetivo de mejorar la privacidad de los usuarios. Este tipo de servicios que cobran una comisión de en torno al 1 y

[76] Con fecha de 3 de abril de 2022, en el sitio web de la operadora de cajeros Shitcoins.club se indica que el límite para transacciones en efectivo es de 990€ para residentes y 9990€ para no residentes. En la web de otro proveedor BitBase, se establece el mismo límite para operaciones sin identificación en el enlace https://bitbase.es/cajeros-bitcoin.

[77] FATF, op. cit. p. 49

[78] Gabinete de prensa de la Guardia Civil, "La Guardia Civil desarticula una organización criminal autónoma de blanqueadores de dinero a través de la compraventa de criptomoneda", 8 de mayo de 2019 (disponible en https://www.guardiacivil.es/es/prensa/noticias/6975.html; última consulta 18 de abril de 2022).

3%[79] son claves para la fase de estratificación del dinero porque encubren el origen de los criptoactivos. Estos servicios generalmente requieren el depósito progresivo de las criptodivisas en las direcciones del servicio, mezclando las transacciones de varios usuarios en la misma cartera, y posteriormente transfieren cantidades diferentes en una o varias transacciones a una o varias direcciones, sin que coincidan las transacciones iniciales con las de salida. Según la consultora especializada Chainanalysis[80] en el año 2020 el 55% de los fondos que se enviaban a servicios de mezclado provenían de mercados de la *darknet*, un 20% provenía de estafas, un 10% de rescates procedentes de ataques de *ransomware* y un 10% de fondos robados en ataques informáticos y se está produciendo un aumento significativo de los fondos enviados usando servicios de mezclado en los últimos dos años.

4.3. Criptodivisas especializadas

Existen monedas alternativas como Monero (XMR) y Zcash (ZEC) que están centradas en la privacidad desde su concepción. En el caso de Monero[81], pese a ser una criptomoneda, los importes de las transacciones no son públicos y se crea automáticamente una cartera para cada transacción. Zcash[82] permite la creación de carteras privadas que son interoperables con las carteras públicas, similares a las de Bitcoin. Estas monedas son menos populares que Bitcoin o Ethereum porque los principales servicios de intercambio no las aceptan debido a presiones regulatorias y, por tanto, son menos líquidas a la hora de convertirlas en efectivo o intercambiarlas por otras monedas virtuales[83]. Estas monedas se suelen utilizar en la fase de colocación y de estratificación del delito de blanqueo de capitales ya que permiten introducir los beneficios en el sistema y ocultando su verdadero origen.

4.4. Tarjetas prepago y regalo

Existen compañías que permiten adquirir tarjetas prepago físicas de las principales redes utilizando criptomonedas con las que acudir a un cajero automático tradicional y realizar

[79] BitcoinWiki, "Bitcoin Fog" (disponible en https://en.bitcoinwiki.org/wiki/Bitcoin_Fog; última consulta 18 de abril de 2022).
[80] Chainalysis, op. cit. p. 10.
[81] Monero, "Moneropedia" (disponible en https://www.getmonero.org/resources/moneropedia/; última consulta 21 de abril de 2022).
[82] Zcash, "How it works" (disponible en https://z.cash/technology/; última consulta 21 de abril de 2022).
[83] Europol, op. cit. p. 7.

retiradas de efectivo o bien realizar compras en establecimientos físicos u online. También es posible adquirir tarjetas regalo de servicios online mediante criptodivisas. En la fase de integración del delito de blanqueo de capitales estas tarjetas son utilizadas por los criminales para gastar los activos previamente blanqueados como se ha visto en la sentencia de la Audiencia Nacional núm. 704, del 3 de marzo de 2016, que juzga a los responsables del "virus de la Policía" que utilizaban tarjetas prepago previamente adquiridas por internet para realizar retiradas de efectivo anónimas.

4.5. Servicios de intercambio de alto riesgo

Existen servicios de intercambio de criptomonedas que se localizan en jurisdicciones de alto riesgo como se ha mencionado en epígrafes anteriores y que operan de forma encubierta en la *Darkweb*[84] sin cumplir con las preceptivas obligaciones de KYC y, por otro lado, los servicios de intercambio anidados (*nested exchanges*) que utilizan otras plataformas de intercambio para ofrecer sus productos. En el caso de estos servicios existe un grupo importante que cumple con sus obligaciones de prevención de blanqueo de capitales mientras que otros ofrecen servicios directamente enfocados hacia el cibercrimen.[85]

4.6. Adquisición de equipos de minado de criptomonedas

Algunas organizaciones criminales adquieren con los beneficios procedentes del delito equipos de minado de criptomonedas, que participan verificando transacciones en de la *blockchain* a cambio de una recompensa en criptoactivos, lo que les permite obtener criptomonedas muy complicadas de trazar como se ha explicado anteriormente. Generalmente el minado de criptomonedas se realiza con equipos informáticos destinados a tareas informáticas de alto rendimiento como videojuegos, aunque en función de la criptodivisa a minar puede llegar a ser necesario el uso de equipos informáticos específicamente diseñados para estas tareas.[86] El uso de ganancias ilícitas para adquirir equipos de minado de criptodivisas o la contratación de servicios de minado a terceros, se encuadraría dentro de la fase de estratificación, ya que con

[84] Contenido en internet que no está indexado en motores de búsqueda y requiere de un software o configuraciones específicas para acceder. Fuente: Avast, "What is the dark web?" (disponible en https://www.avast.com/c-dark-web#topic-1; última consulta 22 de abril de 2022).
[85] Chainanalysis, op. cit. p.13.
[86] Bit2me academy, "What is a mining rig?" (disponible en https://academy.bit2me.com/en/que-es-rig-de-mineria/; última consulta 22 de abril de 2022).

estas inversiones se trata de encubrir el origen ilícito del dinero. En España un Juzgado de Instrucción de Redondela decomisó en 2017, 36 equipos de minado de criptomonedas como objeto material del delito de blanqueo de capitales en el marco de una causa contra una organización criminal.[87] Además, la Policía Nacional ha publicado comunicados relacionados con operaciones realizadas contra organizaciones criminales que presuntamente cometían delitos contra la Seguridad Social y a la que se había intervenido una granja de criptomonedas, que utilizaban para blanquear las ganancias obtenidas, así como dinero en criptoactivos.[88] Las organizaciones suelen utilizar enganches ilegales a la luz sancionados por el delito de defraudación de fluido eléctrico del artículo 255 del Código Penal para reducir los costes de operar los equipos de minado y obtener una mayor rentabilidad.

4.7. Uso como instrumentos financieros y/o como depósito de valor

Algunas criptomonedas como Bitcoin son conocidas por el público general por su alta volatilidad y las altas rentabilidades obtenidas por los primeros inversores. Además de existir miles de criptodivisas diferentes, con características variadas y con distintos enfoques, es posible operar con futuros de criptomonedas y otros instrumentos financieros para obtener una rentabilidad. Este tipo de productos que se encuentran en constante desarrollo bajo el nombre de DeFi (finanzas descentralizadas) permiten a las redes de blanqueo por un lado diversificar el destino de las criptodivisas para encubrir su origen ilícito y, posteriormente, en la fase de integración, invertir los criptoactivos ya blanqueados y aumentar sus rentabilidades, en lugar de adquirir acciones de una compañía o comprar bonos.

Un producto relacionado con las criptodivisas que ha tenido un impacto mediático son los NFT (tokens no fungibles) que son ítems únicos e individualizados, almacenados en la cadena de bloques, de los que se obtiene un certificación de propiedad inalterable y que pueden consistir en archivos digitales como imágenes, objetos en videojuegos, música o películas y que llegan a alcanzar un elevado valor en el mercado.[89] Durante el año 2021 se enviaron 44,2 billones de dólares americanos a direcciones relacionadas con NFTs y se han detectado ventas ficticias

[87] Auto de la Audiencia Provincial de Pontevedra sec. 5ª, núm. 483/2017 del 30 de junio, [versión electrónica base de datos ELDERECHO EDJ 2017/17696]. Fecha de la última consulta 15 de abril de 2022.
[88] Policia Nacional, "Desarticulada una organización criminal que creaba empresas para regularizar migrantes y defraudar a la Seguridad Social", 26 de abril de 2022 (disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=11983; última consulta 28 de abril de 2022).
[89] Europol, op. cit. p. 10.

para aumentar el valor de algunos de estos tokens, en las que el vendedor se vende el NFT a si mismo por un precio superior, así como un incremento del uso de fondos ilícitos para adquirir los tokens, que por ahora representa una parte muy pequeña del volumen de actividades ilícitas realizadas con criptoactivos a nivel global[90]. Los tokens son utilizados en la fase estratificación para encubrir el verdadero origen ilícito de los criptoactivos mediante operaciones de compraventa ficticias cuyo objetivo es ofuscar el origen inicial de los beneficios.

V. CONCLUSIONES

1.- El uso delictivo de las criptomonedas es un hecho constatable a través de los numerosos artículos de prensa que mencionan la presencia de criptomonedas en entramados criminales y un número cada vez más importante de causas judiciales en las que las criptomonedas son utilizadas para la comisión del ilícito penal o para ocultar beneficios derivados del mismo. El fenómeno de los criptoactivos dificulta la investigación e intervención de los beneficios del delito, por su característica descentralización, que impide a las autoridades acudir a un organismo central para indagar sobre ciertos activos y embargarlos si necesario, y complica aún más una tarea que ya de por si era complicada previo a la popularización de las criptodivisas por la existencia de complejos entramados societarios orquestados por organizaciones criminales con altos niveles de especialización en materia de blanqueo de capitales y comisión de ilícitos. Asimismo, el aumento de la popularidad para el público general está permitiendo a los cibercriminales estafar y realizar ataques informáticos muy sofisticados en los que obtienen beneficios directamente a través de criptomonedas.

2.- La persecución de estos delitos exige a los jueces de instrucción, Ministerio Fiscal y a las Fuerzas y Cuerpos de Seguridad del Estado un conocimiento sobre tecnologías en constante desarrollo y evolución, y que en ocasiones limita mucho la actuación de las autoridades en cuanto a la complejidad de investigar delitos de criptomonedas si no se cuenta con la colaboración de las personas investigadas, ya que los sistemas de protección en torno a las criptomonedas pueden llegar a ser extremadamente robustos y sobrepasarlos puede resultar una tarea prácticamente imposible para las autoridades.

[90] Chainanalysis, "The 2022 Crypto Crime Report", febrero de 2022, p.30 (disponible en https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf).

3.- Por otro lado, la posibilidad de hacer transferencias transfronterizas sin ningún tipo de diferencia con una doméstica y que los servicios de criptomonedas se encuentren domiciliados en el extranjero, dificultan y ralentizan las actuaciones y su éxito puede depender de las relaciones bilaterales entre las autoridades de los diferentes países.

4.- Además, la existencia de un registro público e inalterable de las transacciones en la mayoría de las criptodivisas resulta de interés a la hora de enjuiciar los hechos, ya que no cabe ninguna duda de que una transacción se ha ejecutado si existe en la cadena de bloques. La existencia de este registro es un contrapeso a la anonimidad de las carteras de criptomonedas, pero tal y como se ha demostrado en este trabajo no resulta sencillo obtener criptomonedas sin que se registren los datos del titular y de forma más o menos compleja puede ser posible localizar a los compradores en ocasiones.

5.- El éxito de la lucha contra la delincuencia económica que utiliza criptoactivos dependerá de que se dote a las autoridades de los medios materiales y humanos necesarios, el desarrollo de relaciones de colaboración internacional entre autoridades y un interés de las entidades privadas que participan en el ecosistema de los criptoactivos en colaborar y participar en la lucha contra el crimen de forma diligente.

VI. BIBLIOGRAFÍA

Legislación

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. (BOE núm. 103 de 29/04/2010), última actualización publicada del 28 de abril de 2021.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. (BOE núm. 126, de 27 de mayo de 2021).

Directiva 2014/41/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (Última actualización de 2 de julio de 2021).

Circular 4/2010, de 30 de diciembre, sobre las funciones del Fiscal en la investigación patrimonial en el ámbito del proceso penal.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE núm. 239 de 6 de octubre de 2015).

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Circular 4/2010, de 30 de diciembre, sobre las funciones del Fiscal en la investigación patrimonial en el ámbito del proceso penal.

Jurisprudencia

Sentencia de la Audiencia Provincial de Madrid sección 3ª núm. 2779/2018, de 7 de marzo, ECLI:ES:APM:2018:2779. Fecha de la última consulta: 3 de marzo de 2022.

Sentencia de la Audiencia Provincial de Cartagena sección 5ª núm. 1308/2020, de 14 de julio, ECLI:ES:APMU:2020:1308. Fecha de la última consulta: 3 de marzo de 2022.

Sentencia de la Audiencia Nacional sección 1ª núm. 2959/2021 de 5 de julio, CENDOJ: SAN 2959/2021. Fecha de la última consulta: 4 de abril de 2022.

Sentencia de la Audiencia Nacional sección 4ª núm. 704/2016, de 3 de marzo, CENDOJ: ECLI:ES:AN:2016:704. Fecha de la última consulta: 5 de abril de 2022.

Sentencia de la Audiencia Provincial de Tenerife sección 2ª núm. 1900/2018, de 3 de octubre, ECLI:ES:APTF:2018:1900. Fecha de la última consulta: 6 de abril de 2022.

Auto de la Audiencia Provincial de Pontevedra sección 5ª núm. 527/2018, de 31 de octubre. Base de datos Lefebvre EDJ 2018/659954. Fecha de la última consulta: 14 de abril de 2022. FD 1º.

Sentencia del Tribunal Supremo Sala Segunda, de lo Penal, núm. 266/2005, de 1 de marzo. ECLI: ES:TS:2005:1267.

STS núm. 156/2011, de 21 de marzo [versión electrónica – base de datos Vlex https://vlex.es/vid/-272355247]. Fecha de la última consulta 2 de abril de 2022. FJ 1.

Auto de la Audiencia Provincial de Pontevedra sec. 5ª, núm. 483/2017 del 30 de junio, [versión electrónica base de datos ELDERECHO EDJ 2017/17696]. Fecha de la última consulta 15 de abril de 2022.

Obras doctrinales

Buterin, V., "Ethereum Whitepaper", 2014 (disponible en https://ethereum.org/en/whitepaper/; última consulta 25 de abril de 2022).

Legerén-Molina, A., "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain", *Revista de Derecho Civil,* vol. VI, núm. 1, 2019, pp. 177-237.

Andrei-Dragoş, P., "Decentralized Finance (DEFI) – The LEGO of finance", *Social Sciences and Educational Research Review,* 2020, p. 323 (disponible en https://sserr.ro/wp-content/uploads/2020/07/SSERR_2020_7_1_321_349.pdf)

Gjermundrød, H., Chalkias, K. y Dionysiou, I., "Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems", 2016 (disponible en https://www.researchgate.net/publication/313345971_Going_Beyond_the_Coinbase_Transaction_Fee_Alternative_Reward_Schemes_for_Miners_in_Blockchain_Systems; última consulta 30 de marzo de 2022).

Rodríguez-Medel Nieto, C., *TESIS DOCTORAL: Prueba penal transfronteriza: su obtención y admisibilidad en España,* Madrid, 2017, p. 305.

Delgado Martín, J., *Investigación Tecnológica y prueba digital en todas las jurisdicciones,* Wolters Kluwers, Madrid, 2016, página 369.

Zaragoza Tejada, J. I., Bermúdez González, J. A., & Madrigal Martínez-Pereda, C. *Investigación tecnológica y derechos fundamentales. : Comentarios a las modificaciones introducidas por la Ley 13/2015*. Thomson Reuters Aranzadi, 2017, pp. 445-447.

Gutiérrez Rodríguez, M., "El delito de blanqueo de capitales y otras conductas afines", Liñán Lafuente, A., (coord.), Derecho Económicos y Empresariales, Dykinson, Madrid, 2020, pp. 362-377.

Campbell-Verduyn, M., Bitcoin, crypto-coins and global anti-money laundering governance, Crime Law and Social Change, 2018, p.4., disponible en https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance

España Alba, V. M., *Secreto bancario y paraísos fiscales: la ingeniería fiscal al servicio del blanqueo de capitales*, Sepín, Madrid, 2017, p. 104.

Raymond Choo, K., "Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?" en Kuo Chen, D. L., *Handbook of Digital Currency*, Elsevier, 2015, pp. 283-307.

Referencias de internet

Ethereum.org, "Proof-of-work (POW)", 2022 (disponible en https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/; última consulta 3 de marzo de 2022).

Ethereum.org, "Proof-of-stake (POS)", 2022 (disponible en https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/; última consulta 3 de marzo de 2022)

D.G. de Coordinación y Estudio de la Secretaría de Estado de Seguridad - Ministerio del Interior, "Estudio sobre la cibercriminalidad en España - 2020", 2021, p.41 (disponible en http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3; última consulta 4 de marzo de 2022).

Herraiz, P., "Cae en España el 'hacker' de los 10.000 millones, el ciber ladrón más importante del mundo: Carbanak", *El Mundo*, 27 de marzo de 2018 (disponible en https://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html; última consulta el 4 de abril de 2022).

Gobierno de EE. UU., "Ransomware 101", *StopRansomware* (disponible en https://www.cisa.gov/stopransomware/ransomware-101; última consulta 5 de abril de 2022).

Aguiar, A. R., "El ciberataque al SEPE provocó que sus técnicos trabajaran 19.000 horas extras en jornadas maratonianas y festivos: así levantaron una barricada contra el 'ransomware'", *Business Insider*, 2 de diciembre de 2021 (disponible en

https://www.businessinsider.es/vivio-ciberataque-sepe-dentro-19000-horas-extra-973861; última consulta el 5 de abril de 2022).

Chainanalysis, "The 2021 Crypto Crime Report", 16 de febrero de 2021, p.26.

Dirección General de la Policía, "La Policía Nacional desmantela una "granja" ilegal de "minería" de criptomonedas en un chalet de Toledo", 2021, (disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=9583; última consulta 5 de abril de 2022).

Skerrit, B., "How does Tor *really* work?", *Medium*, 28 de enero de 2018 (disponible en https://medium.com/hackernoon/how-does-tor-really-work-c3242844e11f; última consulta 6 de abril de 2022).

Bitcoin.org, "Vocabulary – Bitcoin" (disponible en https://bitcoin.org/en/vocabulary#wallet; última consulta 22 de marzo de 2022).

Binance, "What is a crypto wallet?", 18 de junio de 2019 (disponible en https://academy.binance.com/en/articles/crypto-wallet-types-explained; última consulta 22 de marzo de 2022).

Kohler, C., "Can you delete a bitcoin wallet?", *The Bitcoin Manual,* 1 de diciembre de 2021 (disponible en https://thebitcoinmanual.com/articles/delete-btc-wallet/; última consulta 28 de marzo de 2022).

bit2me academy, "¿Qué es el halving Bitcoin y qué función tiene? "(disponible en https://academy.bit2me.com/que-es-halving-bitcoin/; última consulta el 28 de marzo de 2022).

Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónico del Banco de España (disponible en https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-

electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html).

Estudillo, M., "¿Qué es Know Your Customer (KYC) y qué implica?", *Signaturit Blog*, 1 de febrero de 2021 (disponible en https://blog.signaturit.com/es/que-es-know-your-customer-kyc-sector-financiero; última consulta 12 de abril de 2022).

Hudson Intelligence, "High-risk exchange" (disponible en https://www.fraudinvestigation.net/cryptocurrency/tracing/high-risk-exchange; última consulta 13 de abril de 2022).

Poder Judicial de España, "Auxilio judicial Internacional" (disponible en https://www.poderjudicial.es/cgpj/es/Temas/Relaciones-internacionales/Auxilio-judicial-internacional/Informacion-general/; última consulta 10 de abril de 2022).

de Best, R., "Largest cryptocurrency exchanges based on 24h volume in the world on May 2, 2022", Statista, mayo de 2022 (disponible en https://www.statista.com/statistics/864738/leading-cryptocurrency-exchanges-traders/; última consulta 15 de abril de 2022).

Binance, "Binance Law Enforcemente Guidelines" (disponible en https://www.binance.com/en/support/law-enforcement/guidelines; última consulta 16 de abril de 2022).

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* FATF, Paris, 2021, p.20, disponible en www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

Europol, *Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2021, p.9.

Consejo General del Notariado, "La colaboración de los notarios en la prevención del blanqueo de capitales, de la financiación del terrorismo y el fraude fiscal", p. 5 (disponible en

https://www.notariado.org/portal/documents/176535/0/Los+m%C3%A1s+de+2.800+notarios+espa%C3%B1oles%2C+desde+sus+notar%C3%ADas%2C+se+han+convertido+en+aliados+cada+vez+m%C3%A1s+imprescindibles+del+Estado+para+luchar+contra+estos+delitos.+Para+intensificar+y+canalizar+esta+labor%2C+el+Minister.pdf/49cb4054-4417-935e-9993-cfc45d3a51fa?t=1565770020482; última consulta 18 de abril de 2022).

Consejo General del Notariado, "Prevención del blanqueo de capitales" (disponible en https://www.notariado.org/portal/prevenci%C3%B3n-del-blanqueo-de-capitales; última consulta 18 de abril de 2022).

Trezor, "Why is Ledger Nano so secure?", 14 de enero de 2021 (disponible en https://www.ledger.com/academy/basic-basics/ledgers-bit-of-it/ledger-nano-security-made-easy; última consulta 20 de abril de 2022).

INCIBE, *La jerga de la seguridad: ¿de qué hablamos cuando decimos…?*, 2016 (disponible en https://www.incibe.es/en/node/2943).

Velasco, E., "Sobre el Blockchain y su aplicación a las criptomonedas", *El Derecho*, disponible en https://elderecho.com/sobre-el-blockchain-y-su-aplicacion-a-las-criptomonedas; última consulta del 2 de abril de 2022.

Registro de proveedores de servicios de cambio de moneda virtual por moneda fiduciaria y de custodia de monederos electrónico del Banco de España (disponible en https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos/registro-de-proveedores-de-servicios-de-cambio-de-moneda-virtual-por-moneda-fiduciaria-y-de-custodia-de-monederos-electronicos.html).

Romero, P., "Así se incauta la Policía de bitcoins", *El País,* 1 de noviembre de 2013, (disponible en https://www.elmundo.es/tecnologia/2013/11/01/5270d45363fd3da7618b4576.html; última consulta el 25 de marzo).

de Best, R., "Average transaction speed of 66 cryptocurrencies with the highest market cap as of March 2022"*, Statista*, 2022 (disponible en https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/; última consulta 19 de abril de 2022).

N26, "How long does a transfer take?", 15 de febrero de 2022 (disponible en https://n26.com/en-eu/blog/how-long-does-a-bank-transfer-take; última consulta 20 de abril de 2022).

Smith, M., "SWIFT transfers explained (how they work, how long they take & what they cost)" (disponible en https://www.keycurrency.co.uk/swift-transfer/; última consulta 20 de abril de 2022).

Conesa, C., *Bitcoin: ¿una solución para los sistemas de pago o una solución en busca de problema?*, Banco de España, Documentos Ocasionales nº1901, 2019, disponible en https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/19/Fich/do1901.pdf

Bizouati-Kennedy, Y., "Bitcoin Returns Reach Over 70% in 2021, Outperform Gold and Stock Market for Third Straight Year", *Yahoo Finance,* 30 de diciembre de 2021 (disponible en https://finance.yahoo.com/news/bitcoin-returns-reach-over-70-205650585.html?guccounter=1; última consulta 1 de mayo de 2022).

BBVA, "¿Qué son las 'stablecoins' y para qué sirven?", 28 de enero de 2019 (disponible en https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/; última consulta 1 de mayo de 2022).
Coinbase, "What is staking?" (disponible en https://www.coinbase.com/learn/crypto-basics/what-is-staking; última consulta 1 de mayo de 2022).

Tesla, "What You Need To Know If You Use Bitcoin" (disponible en https://www.tesla.com/assets/pdf/BTC_What_You_Need_To_Know_en_US.pdf; última consulta 1 de mayo de 2022).

FATF, “How is money laundered?” (disponible en https://www.fatf-gafi.org/faq/moneylaundering/; última consulta el 18 de abril de 2022).

Coin ATM Radar, “Bitcoin ATMSs in Spain” (disponible en https://coinatmradar.com/country/199/bitcoin-atm-spain/; última consulta 9 de mayo de 2022).

Gabinete de prensa de la Guardia Civil, “La Guardia Civil desarticula una organización criminal autónoma de blanqueadores de dinero a través de la compraventa de criptomoneda”, 8 de mayo de 2019 (disponible en https://www.guardiacivil.es/es/prensa/noticias/6975.html; última consulta 18 de abril de 2022).

BitcoinWiki, “Bitcoin Fog” (disponible en https://en.bitcoinwiki.org/wiki/Bitcoin_Fog; última consulta 18 de abril de 2022).

Monero, “Moneropedia” (disponible en https://www.getmonero.org/resources/moneropedia/; última consulta 21 de abril de 2022).

Zcash, “How it works” (disponible en https://z.cash/technology/; última consulta 21 de abril de 2022).

Avast, “What is the dark web?” (disponible en https://www.avast.com/c-dark-web#topic-1; última consulta 22 de abril de 2022).

Bit2me academy, “What is a mining rig?” (disponible en https://academy.bit2me.com/en/que-es-rig-de-mineria/; última consulta 22 de abril de 2022).

Policia Nacional, “Desarticulada una organización criminal que creaba empresas para regularizar migrantes y defraudar a la Seguridad Social”, 26 de abril de 2022 (disponible en https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=11983; última consulta 28 de abril de 2022).

Chainanalysis, “The 2022 Crypto Crime Report”, febrero de 2022, p.30 (disponible en https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf).