



Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo

DÉVIKA PÉREZ MEDINA
UNIVERSIDAD DE CÁDIZ

Title: Blockchain, cryptocurrencies and criminal phenomena: between crime and development

Abstract: Blockchain is a technology used to stock data that grow rapidly. This is the technology mostly used to create and host another recent phenomenon, cryptocurrencies. Criminal organizations also took advantage of the cryptocurrency for carrying out and financing illegal activities. Even though the operation of the blockchain is based on the clarity and transparency of its blocks, research shows that they are also linked to crimes such as money laundering, terrorist financing, or the purchase of illicit services. The objective of this study is to analyze the Spanish criminal jurisprudence on blockchain and cryptocurrencies, putting it in relation to the criminal domains highlighted by the doctrine and the administrative and legislative authorities of Spain and the European Union. In this regard, our findings show that there is a clear difference between both doctrines and courts. Whilst the doctrinal, legislative and administrative sphere focus on the use of blockchain technology and cryptocurrencies related to money laundering, terrorist financing and the purchase of illegal material, the cases that have reached the Spanish Courts have been mostly for fraud.

Keywords: cyberspace; legal analysis; Bitcoin; crimes.

Resumen: Blockchain es una tecnología utilizada para el almacenamiento de datos que crece de forma acelerada. Esta es la tecnología mayoritariamente utilizada para crear y albergar otro fenómeno reciente, las criptomonedas. En las criptomonedas han visto la oportunidad organizaciones criminales para realizar y financiar actividades ilícitas. A pesar de que el funcionamiento del blockchain se basa en la claridad y transparencia de sus bloques, los estudios muestran evidencias de su vinculación con delitos como el blanqueo de capitales, la financiación del terrorismo o la compra de servicios ilícitos. El objetivo de este estudio es analizar la jurisprudencia penal española en materia de blockchain y criptomonedas, poniéndola en relación con los fenómenos delictivos destacados por la doctrina y las autoridades administrativas y legislativas de España y la Unión Europea. A este respecto el resultado del estudio muestra que existe una diferencia clara entre ambos ámbitos. Así, mientras que en el ámbito doctrinal, legislativo y administrativo los principales focos de interés en cuanto a la utilización de la tecnología blockchain y las criptomonedas han estado relacionados con el blanqueo de capitales, las evasiones fiscales, la financiación del terrorismo y la compra de material ilícito, los casos que han llegado a los tribunales españoles han sido mayoritariamente delitos contra el patrimonio.

Palabras clave: ciberespacio; análisis jurídico; Bitcoin; delitos

Recepción del original: 16 de marzo de 2020

Fecha de aceptación: 10 de septiembre de 2020

Contacto con la autora: devika.perezmedina@gmail.com

Sobre la autora: Dévika Pérez Medina es doctoranda en el área de Derecho penal y Criminología. Su tesis doctoral investiga las implicaciones jurídicas y criminológicas de la tecnología *blockchain* y las criptomonedas. Es graduada en Derecho y Máster en Sistema Penal y Criminalidad por la Universidad de Cádiz. ORCID: <https://orcid.org/0000-0003-3141-3951>

Cómo citar este artículo: PÉREZ MEDINA, Dévika, "Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo", en Boletín Criminológico, artículo 10/2020_EJIC (nº 206)



Sumario: 1. Introducción. 2. Tecnología blockchain y criptomonedas: definición, funcionamiento y usos. 2.1. Tecnología blockchain. 2.2. Criptomonedas. 3. Metodología. 3.1 Recolección de datos. 3.2. Análisis de datos. 3.3. Estudio de la jurisprudencia española. 4. Resultados. 4.1. Análisis doctrinal y normativo comparado sobre las criptomonedas. 4.2. Tipologías delictivas de la jurisprudencia española. 4.2.1. Delitos contra el patrimonio: la estafa. 4.2.1.1 Las criptomonedas como objeto material del delito. 4.2.1.2. La criptomoneda como instrumento para la comisión del delito de estafa. 4.2.2. Delito contra la salud pública. 4.2.3. Delito de blanqueo de capitales. 5. Discusión y conclusiones. 6. Referencias.

1. Introducción

Blockchain, o cadena de bloques, ha supuesto una revolución no solo en el mundo tecnológico sino también en el mundo financiero (González-Meneses, 2019). Esta vinculación entre ambos ámbitos es natural dado que la aparición en 2009 de la cadena de bloques estuvo ligada a las criptomonedas. Por primera vez se le brindó a un objeto inmaterial la posibilidad de ser una alternativa a las transferencias tradicionales de dinero (Naranjo, 2019). La introducción del blockchain y las criptomonedas ha generado una gran preocupación por su potencial criminógeno ya que han sido utilizados en actividades ilícitas, tanto como instrumento para la comisión de delitos como siendo objeto material de los mismos. El objetivo de este artículo es contrastar si los delitos cometidos utilizando las criptomonedas que generan más preocupación en la doctrina y en las autoridades legislativas y administrativas elegidas en nuestro estudio coinciden con los delitos relacionados con las criptomonedas a los que se están enfrentando los tribunales penales españoles. El fenómeno de las criptomonedas plantea retos normativos y policiales. Antes de afrontar los mismos se debe reflexionar sobre los riesgos de las criptomonedas que se plasman en la realidad. Y para ello, una de las opciones más adecuadas es revisar y analizar a qué casos se están enfrentando los tribunales penales españoles.

Para ello, este artículo está estructurado en tres bloques. En primer lugar, se ha realizado una explicación y descripción previa de los conceptos de blockchain y criptomoneda. Estas son necesarias para entender esta tecnología y las características que la hace tan atractiva para los delincuentes. Asimismo, se realiza un estudio sobre la doctrina especializada en criptomonedas y crimen y de la apreciación por parte de diversos



estados (Rusia, China, Estados Unidos y España), entidades internacionales (Grupo Acción Financiera Internacional) y supranacionales (Unión Europea) de este fenómeno. Por último, se comprueba mediante un análisis jurisprudencial de los tribunales penales españoles si estos crímenes que se consideran los más relevantes en relación con las criptomonedas y la tecnología blockchain están ocurriendo en este territorio.

2. Tecnología blockchain y criptomonedas: definición, funcionamiento y usos

2.1. Tecnología blockchain

Blockchain, o cadena de bloques, es la tecnología en la que se albergan las criptomonedas (Houben & Snyers, 2018). Su nacimiento tuvo lugar con la criptomoneda más conocida, el Bitcoin. En 2008, en un contexto de crisis económica, Satoshi Nakamoto publicó un artículo “Bitcoin: A Peer-to-peer Electronic Cash System” (Nakamoto, 2008) con el que revolucionaría el sistema centralizado tradicional con el que funcionan las transacciones económicas. Además, la investigación en esta tecnología ha avanzado significativamente, de tal modo que su uso ya no se restringe exclusivamente a transacciones económicas (Cordero, 2019). Desde su creación, podemos clasificar la tecnología blockchain en tres categorías: Blockchain 1.0, que acoge las transferencias de criptomonedas y pagos digitales. Blockchain 2.0, que hace referencia a la inclusión de los contratos –conocidos como *smart contracts*– y, por último, Blockchain 3.0: en este último avance, la tecnología puede aplicarse a distintos ámbitos más allá del financiero o los contratos, como la medicina (Swan, 2015).

Para entender su funcionamiento hay que acudir al sistema en el que está basado su tecnología; el sistema de registros distribuidos (sistema DLT). Cuando se hace referencia al blockchain como antítesis del sistema centralizado tradicional se debe al modo de operar del sistema DLT, tecnología de almacenaje de datos de la que existen múltiples copias idénticas distribuidas (nodos) entre aquellas personas que participan en la red (Romero, 2018). Los nodos son la base del sistema. Estos pueden llegar a ser millones y se encuentran distribuidos en todo el mundo. Lo interesante de este sistema es que cada componente tiene la misma posición y valor que los demás, por tanto, nadie ostenta un cargo superior en la red, siendo lo que se conoce como un sistema “*Peer-to-peer*” (Romero, 2018).



Aunque blockchain es un tipo de sistema DLT, no todos los sistemas DLT son blockchain. Incluso dentro del propio blockchain, cada criptomoneda puede tener sus particularidades. Las diferencias entre unos tipos de blockchain y otros pueden ser desde los algoritmos que emplean para el método de consenso entre los nodos, la ratio por el que las nuevas monedas son creadas o las capacidades que tiene cada bloque. Estas diferencias están relacionadas con la aparición de nuevos usos de esta tecnología que, además, recientemente ha recibido el apoyo de gobiernos para su difusión y aplicación en distintos ámbitos. Incluso los propios bancos están desarrollando una adaptación de estas tecnologías para la emisión de monedas digitales con el objetivo de reducir costes y aumentar la seguridad (Abuhayar et al., 2018). Es el caso del Banco de España, que ha realizado recientemente un informe estudiando la posibilidad de emitir monedas digitales. En el documento se exponen los beneficios y los aspectos negativos de implementar una moneda digital estable en un futuro (Ayuso & Conesa, 2020).

Un aspecto fundamental para entender el funcionamiento de esta tecnología es su ecosistema, esto es, el conjunto de sujetos que hace posible su funcionamiento e intervienen en mayor o menor medida en el sistema (Homoliak et al., 2019). Blockchain es una base de datos que conserva no solo el estado final del registro, sino el historial completo de transacciones realizadas. Cada blockchain tiene su propio ecosistema dependiendo del método de consenso que utilice la red. Un método de consenso de algoritmos es la herramienta de seguridad empleada por los nodos para evitar que puedan realizarse cambios unilaterales en la red. Si un nodo intenta introducir cambios en un blockchain, el resto de los nodos detectarán la incongruencia y desestimarán la copia inválida de la cadena, aislándola de la red (Luján, 2017).

En el estudio de este artículo nos centraremos en el utilizado por Bitcoin y sus variaciones, el algoritmo de consenso basado en el *Proof-of-Work* (PoW) (Zheng et al., 2017). En este método para agregar un nuevo bloque a la cadena se resuelve un problema criptográfico a través de ordenadores con capacidad y potencia suficiente para estar en funcionamiento por un gran periodo de tiempo. Los usuarios que poseen estos ordenadores y que ejecutan la labor de cierre de bloques son los conocidos como “mineros o nodos validadores” (Riasanow et al., 2018). Cuando se llena la capacidad de un bloque, el sistema genera la prueba de trabajo con un enigma criptográfico. El primer minero que resuelva a través de sus ordenadores el problema, cerrará el bloque y ganará una re-

compensa, en forma de una cantidad definida de Bitcoins a cambio (Ibañez, 2018). Estos nodos de consenso no son los únicos que mantienen las copias de los bloques que dan lugar a este sistema distribuido. Existen también los nodos validadores, que a diferencia de los mineros solo pueden leer el contenido de la cadena de bloques, pero no escribir en ella. Su función es dar soporte al sistema, siendo una parte más de estas copias distribuidas y comprobar el correcto funcionamiento de la red (Homoliak et al., 2019).

Asimismo, es necesario hacer referencia a los usuarios del sistema, que serán los emisores y receptores del mensaje o transacción. Estos usuarios poseen una clave pública y una privada. La clave privada es una clave secreta que solo conoce su poseedor. A su vez, la clave pública es la que se muestra al exterior como una dirección a la que enviar el mensaje y a la que solo se puede acceder con la clave privada (IEEE Computer Society, 2000). El mensaje –o transacción– que envían se encripta en la red para mantener su privacidad y solo puede acceder al contenido el receptor que posee la clave privada asociada a esa clave pública. Las claves se generan con programas específicos a partir de un número aleatorio y es prácticamente imposible deducir cuál es la clave privada a partir de la clave pública (Conesa, 2019). Por tanto, dentro de la cadena de bloques hay tres tipos de sujetos relevantes: i) los nodos validadores, ii) los nodos de consenso o mineros y iii) los usuarios.

Las propiedades que han hecho a esta tecnología tan atractiva son el anonimato, la inmutabilidad del sistema, su transparencia, ausencia de terceros y el ahorro de costes. Mediante la criptografía han conseguido un sistema que, como mínimo, es pseudoanónimo y en la mayoría de los casos anónimo, gracias a la práctica de claves y mensajes cifrados que se ha visto anteriormente (Bedecarratz, 2018; Dolader et al., 2017). En la medida en que las criptomonedas pretenden funcionar como dinero efectivo, no importa la identidad personal del transmitente mientras la transacción correspondiente sea efectivamente registrada (Gonzalez-Meneses, 2019). Aunque pueda parecer que este anonimato se contraponga con la transparencia del sistema, estas características son compatibles. El libro de registro que contiene las transacciones está a la vista de todo aquel que quiera revisarlo. Los bloques, su historial y la información son transparentes y trazables. Sin embargo, no es trivial conocer la identidad de un usuario ya que la clave pública del monedero es la única necesaria para realizar la transacción. Por ello, anonimato del usuario y transparencia de la red son posibles.



Al ser una red “*peer to peer*” no es necesario un intermediario que garantice la fiabilidad de la transacción o el negocio. Por tanto, hay un ahorro en costes significativo y se evita correr el riesgo de que el intermediario pueda cometer errores y poner en peligro el sistema (Norfer et al., 2017). Además, la naturaleza encadenada de los bloques y su cierre hace imposible su modificación, haciendo un sistema inmutable.

Blockchain es una alternativa revolucionaria para el envío de datos. Su naturaleza y características han interesado a los Estados y las entidades supranacionales, como en el caso de la Unión Europea, con la creación del Observatorio de Blockchain (Comisión Europea, 1 de febrero de 2018), o de China, que recientemente ha hecho una gran inversión en la investigación de esta tecnología para usos más allá del económico (Backer, 2020).

Esta tecnología alberga el elemento en el que se centra este trabajo y que está siendo de gran interés para los criminales: las criptomonedas (Walton & Dhillon, 2017). El sistema blockchain dota a esta nueva forma de transacción de un anonimato –o pseudo-anonimato– que está provocando la asociación de este fenómeno con la comisión de crímenes.

2.2. Criptomonedas

Según la plataforma de análisis financiero *TradingView*, en diciembre de 2020 la capitalización del mercado asciende a 554 mil millones de dólares en todo el mundo (TradingView, 2020). A pesar de esta elevada cantidad, la mayoría de los Estados no tienen una extensa regulación sobre la materia. Como señala Navarro Cardoso (2019), la definición de criptomoneda ha ido avanzando con el tiempo y se mantiene en un constante cambio. En el ámbito europeo, la primera definición que ofreció el Banco Central Europeo (BCE) en 2012 afirmaba que una criptomoneda era un tipo de dinero digital no regulado, que era emitido y generalmente controlado por sus desarrolladores, y utilizado y aceptado entre los miembros de una comunidad virtual específica. Sin embargo, la definición más reciente de esta entidad señalaba a la criptomoneda como “una unidad digital de valor, no emitida por ninguna autoridad bancaria central o institución, que, en ciertas ocasiones puede ser utilizada como medio de pago alternativo al dinero” (Banco Central Europeo, 2018).

Respecto al ámbito nacional, la única definición que poseemos es la otorgada por el Tribunal Supremo en su Sentencia de 20 de junio de 2019 que señaló que el Bitcoin no es un objeto material ni tiene la consideración legal de dinero. Para el Tribunal Supremo la criptomoneda es un activo patrimonial inmaterial (STS, N.º de resolución 326/2019). Sin embargo, atendiendo a la interpretación que ha tenido lugar en otros países, podría no existir una única definición de la criptomoneda. El congresista estadounidense Paul Gosar presentó un posible proyecto de Ley (Ley de Criptomonedas de 2020) ante el Congreso de Estados Unidos en marzo de 2020 (*The Cryptocurrency Act of 2020 is “dead on arrival”*, Coindesk, marzo 2020). En esta propuesta se hace una división de tres categorías: método de pago, bienes en propiedad y un depósito de valor. Esta clasificación muestra la realidad de que no todas las criptomonedas tienen el mismo uso y será un dato relevante a la hora de regular la prevención de ciertos crímenes.

Una postura firme que parecen adoptar las potencias económicas es que las criptomonedas no emanadas por el Estado no son moneda de curso legal o dinero en metálico. Tanto en Estados Unidos como en Rusia la única posibilidad de considerarlas un método de pago equivalente al dinero ha sido crear ellos su propia criptomoneda, como propone el gobierno ruso, un rublo digital (Chudinovskikh, 2019).

Con las criptomonedas, se han introducido dos sujetos además de los ya considerados del propio ecosistema de blockchain. Estos son, las casas de cambio de criptomonedas y las empresas emisoras de monederos digitales que han sido el principal foco de regulación para la prevención del crimen.

3. Metodología

3.1. Recolección de los datos

El presente artículo es un estudio principalmente jurídico y, por tanto, de carácter cualitativo. Se ha diseñado sobre los tres pilares habituales de cualquier estudio jurídico: la normativa, la jurisprudencia y la doctrina especializada (Terradillos, 2014). A este respecto, el análisis de la normativa se ha planteado tanto en la legislación a nivel nacional como comparado y las recomendaciones realizadas por los órganos internacionales que se han pronunciado sobre la cuestión. En materia jurisprudencial, el ámbito



de referencia ha sido la jurisdicción penal española. Por su parte, el estudio doctrinal se ha focalizado en las obras publicadas, esencialmente en el ámbito jurídico, aunque también se han incorporado estudios desde un punto de vista técnico. Asimismo, se han incorporado revisiones de escritos criminológicos.

Tanto para la definición y el desarrollo de los conceptos a tratar como para la revisión de la doctrina en material penal y revisión de escritos criminológicos se ha utilizado los buscadores académicos *Google Scholar*, *Academia.edu*, *Dialnet* y *World Wide Science*. Blockchain y las criptomonedas son fenómenos recientes en materia jurídica. Igualmente, esta tecnología está en crecimiento y por ello se ha optado por limitar la búsqueda a publicaciones posteriores a 2017 en los buscadores académicos mencionados con la excepción de los documentos que dan origen al fenómeno en su aspecto técnico (Nakamoto, 2008).

La mayoría de los estudios utilizados en este trabajo provienen de los encontrados en *Google Scholar* y *Dialnet* por la facilidad para acceder directamente a los documentos. Por otro lado, los buscadores de *Academia.edu* y *World Wide Science* disponían de un contenido limitado de la relación penal criminal con los conceptos aquí estudiados. En *World Wide Science* los enlaces a los artículos que se encontraban redireccionaban, en la mayoría de los casos, a bases de datos que eran de acceso restringido.

3.2. Análisis de datos

Dado que el análisis principal es un análisis de contenido de la jurisprudencia penal española, se han priorizado aquellas aportaciones de la doctrina española sobre la materia. Asimismo, se ha realizado una revisión normativa de la que se deriva la única norma aplicable en España a este respecto: la Directiva (UE)2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 que entró en vigor en enero de 2019.

Ante la falta de normativa emanada directamente de los poderes nacionales, se ha añadido un análisis de las distintas intervenciones en el Congreso de los Diputados y el Senado para mostrar si el elemento de criminalidad dentro de las criptomonedas y el blockchain se contempla en las propuestas legislativas. Para analizar las intervenciones

se ha accedido a los diarios de sesiones de las Cortes Generales a través de las herramientas de búsqueda de las que dispone su página web. La búsqueda se ha realizado desde 2017 hasta la actualidad con la delimitación de los términos “Bitcoin, criptomoneda y blockchain” obteniendo como resultado final sesenta documentos.

Además de la normativa emanada por la Unión Europea, se ha decidido estudiar las tendencias delictivas que se han considerado en Estados relevantes en la economía mundial como son Estados Unidos, Rusia y China. Para ello se ha acudido tanto a fuentes públicas como a fuentes periodísticas. Por último, se ha añadido al estudio las recomendaciones de no obligado cumplimiento *–soft law–* emanadas del Grupo de Acción Financiera Internacional (GAFI) en su publicación “Las directrices para un enfoque basado en riesgo de las monedas virtuales” (2015).

3.3. Estudio de la jurisprudencia española

Para el análisis de la jurisprudencia se ha utilizado el motor de búsqueda del Consejo General del Poder Judicial (CENDOJ). Esta plataforma publica sistemáticamente las decisiones dictadas por los órganos judiciales superiores (de la Audiencia Provincial en adelante). La publicación de las decisiones de los órganos judiciales inferiores como los juzgados de instrucción o los juzgados de lo penal es esporádica. Por tanto, esta base de datos cuenta con limitaciones para el análisis.

Para la búsqueda en la plataforma se han utilizado los filtros de jurisdicción *–penal–* y búsqueda de texto libre en el que se ha incluido los términos: “criptomoneda”, “blockchain”, “Bitcoin” y “criptodivisa”. En la búsqueda se encontraron 24 resultados de distintos órganos. El listado de estas resoluciones se incorpora en la Tabla 1. En la Tabla 1 se distinguen elementos identificativos propios de la decisión tales como la fecha de la misma y el órgano del que emana. A su vez se han añadido otros elementos útiles para el análisis de estas decisiones. Por una parte, con el título de “casos” se ha añadido una columna en la que se hace referencia al procedimiento originario del que proviene la decisión. De esta forma, pueden agruparse aquellas resoluciones que, pese a ser dictadas por distintos órganos, tienen su origen en los mismos hechos delictivos (lo que ocurre en cinco ocasiones). Igualmente se ha añadido una columna en relación con



los delitos a los que se refiere cada una de las decisiones. Los datos se han incorporado a esta columna de manera acrítica, simplemente añadiendo la referencia específica que contiene la resolución.

Las decisiones referidas en la Tabla 1 han dado lugar al análisis jurisprudencial que se incorpora en el mismo apartado. No obstante, algunas de estas decisiones no han sido estudiadas. Se han descartado aquellas que hacen referencia a extradiciones y cuestiones de competencia dado que su contenido no desarrolla el sustento fáctico del caso. Asimismo, aquellas decisiones que tratan sobre delitos en los que la criptomoneda, aunque se incluya en los hechos del caso, no tienen una relación directa con el fenómeno delictivo, como son aquellas que incluyen la criptomoneda como método de pago de bienes y objetos lícitos, también se han descartado.

La propia metodología utilizada genera un sesgo evidente en la investigación, pues se tomaron en consideración únicamente aquellos casos que han llegado a los tribunales españoles. De estos, solo los que los tribunales han emitido algún tipo de documento en el que se hace referencia al término criptomoneda o blockchain, de los cuales, solo aquellos publicados en CENDOJ. Eso hace que los casos que se están publicando en los tribunales no sea una visión completa sino condicionada por las limitaciones que aquí se indican.

4. Resultados

4.1. *Análisis doctrinal y normativo comparado sobre las criptomonedas*

La doctrina más relevante especializada en blockchain y criptomonedas relacionada con la criminalidad ha señalado que los principales crímenes que se han vinculado con este fenómeno son la financiación del terrorismo (v.g. Dion-Schwarz et al., 2019), el blanqueo de capitales (v.g. Navarro, 2019), las evasiones fiscales (v.g. Mera et al., 2018) y la compra de material o servicios ilícitos (v.g. García Sigman, 2017). En cierto modo, como ya apuntaban los autores Miró-Llinares y Moneva (2019) el traslado del crimen al ciberespacio no supone una modificación absoluta de las conductas delictivas sino una transformación en los modos de realización de las mismas. Así, para autores como Navarro (2019) la criptomoneda se considera una excelente vía para el blanqueo de capitales. El autor señala que, de acuerdo con algunos estudios, la subida en el mercado

Tabla 1. Características de las sentencias analizadas

Fecha	Caso	Decisión	Órgano	Delito
23/03/2017	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial Vigo	Delito de Blanqueo de capitales y propiedad intelectual
30/06/2017	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial Vigo	Delito de Blanqueo de capitales y propiedad intelectual
07/07/2017	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial Vigo	Delito de Blanqueo de capitales y propiedad intelectual
14/07/2017	DP 247/2016 Juzgado de Instrucción I de Lleida	Sentencia	Audiencia Provincial de Lleida	Delito de estafa
03/10/2017	PA 18/2017 Juzgado Central de Instrucción nº3	Auto	Audiencia Nacional	Delito de estafa informática (Extradición)
10/11/2017	DP 1197/2016 Juzgado de Instrucción nº6 de Castellón de la Plana	Auto	Audiencia Provincial Castellón	Delito de estafa y delito de descubrimiento y revelación de secretos
29/01/2018	PA 2451/2016 Juzgado de Instrucción nº2 San Cristóbal de la Laguna	Sentencia	Audiencia Provincial Tenerife	Delito de tráfico de drogas
07/03/2018	DP 828/2015 Juzgado de Instrucción nº17 de Madrid	Sentencia	Audiencia Provincial Madrid	Delito de estafa continuada y apropiación indebida
20/03/2018	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial Vigo	Delito blanqueo de capitales y propiedad intelectual
15/06/2018	DP 51/2017 Juzgado de Instrucción nº3 de Ávila	Auto	Audiencia Provincial Ávila	Delito de estafa
23/07/2018	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial de Vigo	Delito de blanqueo de capitales y propiedad intelectual
28/09/2018	PA 2451/2016 Juzgado de Instrucción nº2 San Cristóbal de la Laguna	Sentencia	Tribunal Superior de Justicia Las Palmas	Delito de tráfico de drogas
03/10/2018	PA 480/2017 Juzgado de Instrucción nº2 San Cristóbal de la Laguna	Sentencia	Audiencia Provincial Tenerife	Delito de tráfico de drogas
31/10/2018	DP 74/2011 Juzgado de Instrucción nº2 de Redondela	Auto	Audiencia Provincial Vigo	Delito de blanqueo de capitales y propiedad intelectual
11/12/2018	DP desconocida Juzgado de Instrucción nº3 de Santander	Auto	Audiencia Provincial Santander	Delito de estafa
21/02/2019	DP 607/2017 Juzgado de Instrucción nº3 de Zaragoza	Sentencia	Audiencia Provincial Zaragoza	Delito de falsificación de moneda
11/04/2019	DP 584/2018 Juzgado Mixto nº5 de Madrid	Auto	Audiencia Provincial Madrid	Delitos de estafa informática agravada, blanqueo de capitales, descubrimiento y revelación de secretos, contra la propiedad industrial y pertenencia a una organización criminal
20/06/2019	DP 584/2018 Juzgado Mixto nº5 de Madrid	Auto	Audiencia Provincial Madrid	Delitos de estafa informática agravada, blanqueo de capitales, descubrimiento y revelación de secretos, contra la propiedad industrial y pertenencia a una organización criminal
20/06/2019	DP 828/2015 Juzgado de Instrucción nº17 de Madrid	Sentencia	Tribunal Supremo	Delito continuado de estafa y apropiación indebida
10/10/2019	DP 584/2018 Juzgado Mixto nº5 de Madrid	Auto	Audiencia Provincial Madrid	Delitos de estafa informática agravada, blanqueo de capitales, descubrimiento y revelación de secretos, contra la propiedad industrial y pertenencia a una organización criminal
22/10/2019	DP desconocida Juzgado de Instrucción nº3 de Pamplona	Sentencia	Audiencia Provincial Pamplona	Delito leve de estafa
24/10/2019	DP 19/2019 Juzgado de Instrucción nº27 de Madrid	Auto	Tribunal Supremo	Delito de estafa (cuestión de competencia)
29/10/2018	DP 373/2019 Audiencia Provincial de Málaga	Sentencia	Audiencia Provincial Málaga	Delito de defraudación de fluido eléctrico o análogos
10/12/2019	DP desconocida Juzgado de Instrucción nº3 de Pamplona	Sentencia	Audiencia Provincial Pamplona	Delito leve de estafa
20/02/2020	PA 51/2019 Juzgado de Instrucción nº6 de Tarragona	Auto	Audiencia Provincial Tarragona	Delito de estafa



de diciembre de 2017 se debió a un movimiento especulativo producto de un lavado de dinero a gran escala (Navarro, 2019). Del mismo modo, Saldaña (2017) señala a los Bitcoin como protagonistas en el blanqueo de dinero mediante la compra de criptomonedas con dinero obtenido de ganancias ilícitas. Como indican Walton y Dhillon (2019) el anonimato no es la única característica que beneficia el uso de este método de transacción. La rapidez de los pagos y el bajo coste de los *exchanges* son dos cualidades de las criptomonedas muy valoradas para este tipo de delito (Walton & Dhillon, 2019).

Estudios doctrinales (Mounteney et al., 2017; Xie, 2019) ponen de relieve que, además del blanqueo de capitales, es muy común el uso de las criptomonedas para las transacciones de bienes y servicios ilícitos. El método más usual, para la compra de estupefacientes, armas o consumo de pornografía infantil es a través de la *Dark Web*¹. García Sigman (2017) señala que las criptomonedas facilitan la compra de estupefacientes en el Internet oscuro al por mayor. Como muestra parte de la doctrina, uno de los delitos que mayor preocupación ha generado a las instituciones son las evasiones fiscales. Dos características facilitan la comisión de este crimen: el anonimato y la ausencia de intermediarios financieros que controlan los movimientos como ocurre con el caso de los bancos (Mera et al., 2018).

Por otra parte, los grupos terroristas han encontrado en las criptomonedas una vía de financiación. Así lo señala Dion-Schwarz et al. (2019) en su estudio sobre el uso de las criptomonedas en el terrorismo. El autor resalta el uso de esta nueva tecnología para la financiación de grupos terroristas, y además pone de relieve las criptomonedas alternativas al Bitcoin que más se usan para estas transacciones como Blackcoin o Monero² (Dion-Schwarz et al., 2019).

Las cifras expuestas por la doctrina explican la preocupación por la utilización de este fenómeno en actividades de origen ilícito. Según Foley et al. (2018, pp. 2 y 3),

1. La *Dark Web* o internet oscuro es un subgénero de un ecosistema más amplio de mercados ilícitos a través de internet. Los vendedores se registran en esta plataforma para vender las mercancías ilícitas a cambio de una comisión que se quedan los administradores. Estos últimos garantizan la infraestructura necesaria en el mercado para el anonimato de la compraventa (Martin et al., 2020).

2. Se puede considerar Bitcoin como una criptomoneda, más que anónima, pseudanónima. Es relativamente sencillo conectar las identidades de las direcciones Bitcoin. Sin embargo, existen criptomonedas que han trabajado como objetivo principal reforzar su anonimato a través de sus protocolos de ecosistema. Es el caso de Monero, Blackcoin, Darkcoin o Zerocoin (Antonopoulos, 2015)



“al menos un 44% de las transacciones realizadas en criptomonedas están asociadas a actividades ilícitas, casi la mitad de las operaciones”. El estudio realizado por Dyson et al. (2019) muestra cómo el anonimato es la característica principal de las criptomonedas que las hace atractivas para su uso en estos actos. Estos autores proponen como solución un sistema que centre los controles en el tránsito de la criptomoneda del marco del blockchain al cambio por dinero de curso legal (Dyson et al., 2019).

Esta preocupación no se ha reflejado en la introducción de cambios legislativos. De hecho, en el caso de España, no existe normativa específica sobre la materia. Sin embargo, tras un análisis de los diarios de sesiones del Congreso y el Senado, se tiene presente este fenómeno. En febrero de 2018 el Grupo Parlamentario del Partido Popular puso de manifiesto la importancia que están teniendo estos cryptoactivos en el mercado e instó al Gobierno a estudiar los aspectos fiscales del uso de la criptomoneda para evitar cualquier tipo de evasión, así como los aspectos relacionados con la prevención del blanqueo de capitales (Boletín Oficial de las Cortes Generales, de los días 7 y 8 de febrero de 2018). Asimismo, tanto el Grupo Parlamentario del Partido Popular como el Grupo Parlamentario Vasco trajeron a colación la importancia de una regulación supranacional y se señaló la importancia del anonimato como característica clave para el favorecimiento de la comisión de hechos delictivos como la financiación del terrorismo, blanqueo de capitales y tráfico de divisas (Boletín Oficial de las Cortes Generales, de los días 7 y 8 de febrero de 2018). Además, en octubre de 2018 se propuso en el Congreso el debate en la Comisión de Economía y Empresa sobre la posición que debe tomar España respecto al uso y regulación de la criptomoneda y la necesidad de establecer un marco legal para prevenir la financiación del terrorismo o el tráfico de estupefacientes (Boletín Oficial de las Cortes Generales, de 30 de octubre de 2018).

Hasta el momento el Estado Español no ha aprobado ninguna normativa relacionada con esta cuestión. De hecho, la única norma relevante aplicable en España es la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 que entró en vigor en enero de 2019. Su objetivo era modificar la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo. Esta nueva incorporación considera que el anonimato de las monedas virtuales permite su uso indebido con fines delicti-



vos. Para ello, establece que es necesario un control por parte de los proveedores de servicios *exchanges* (casas de cambio de monedas virtuales) y de los proveedores de servicios de custodia de monederos electrónicos. Las herramientas para este control deberán disponerlas las Unidades de Inteligencia Financiera nacionales, que tienen que obtener información que les permita asociar las direcciones de monedas virtuales a la identidad del propietario de la misma.

La Directiva (UE) 2018/843 marca la tendencia en el interés del legislador europeo en relación con las criptomonedas y la criminalidad. Los legisladores de otros Estados fuera de la UE que han tomado en consideración la cuestión de la criptomoneda se han posicionado en sentido similar. Rusia ha sido uno de los Estados que también ha perseguido el blanqueo de capitales a través de este fenómeno. La Federación Rusa aún no ha adoptado la ley que regula la circulación de las criptomonedas que tiene como objetivo combatir el blanqueo de capitales y las evasiones fiscales (Chudinovskikh & Servrygin, 2019). En Estados Unidos se han tomado iniciativas para un mayor control de los *exchanges* como ha ocurrido en el seno de la Unión Europea con la intención de controlar el blanqueo de capitales y las evasiones fiscales (Edwards et al., 2019). Por su parte, China ha experimentado prohibiciones y permisiones a lo largo de los años del uso de la criptomoneda para pagos dentro del país (Xie, 2019). Por último, GAFI publicó unas directrices sobre las políticas necesarias para proteger el sistema financiero contra el lavado de activos y la financiación del terrorismo entre las que se incluían el control de las casas de cambio (GAFI, 2019). Estas directrices que se han ido actualizando desde 2015 han sido la base para las corrientes legislativas que se ha señalado.

4.2. Tipologías delictivas en la jurisprudencia española

Aunque existe una ausencia de regulación en el Estado Español sobre las criptomonedas, esto no ha impedido que lleguen casos a los Juzgados y Tribunales penales españoles en los que se encuentra este fenómeno. Con este análisis se quiere dar a conocer cuáles son los casos que están llegando a la jurisprudencia española.

4.2.1. Delitos contra el patrimonio: la estafa

En el estudio de estas decisiones se ha encontrado la presencia mayoritaria de delitos de estafa, considerando a la criptomoneda tanto su instrumento para la comisión del delito como su objeto material.

4.2.1.1. Las criptomonedas como objeto material del delito

En el análisis de dos casos en los que la criptomoneda aparece como objeto material del delito de estafa se observa que, a pesar de la similitud entre ambos, existen disparidades en su interpretación. De esta manera, cuando el Bitcoin era objeto del delito las causas fueron sobreseídas por resultar imposible identificar a los responsables, como ocurrió en la Audiencia Provincial de Ávila en el año 2018 (AAP de Ávila, N.º Resolución 150/2018, 15 de junio de 2018). Los hechos del caso recogían un presunto delito de estafa puesto que el perjudicado invirtió Bitcoins en una empresa y no los logró recuperar. En su momento el Juzgado de Instrucción sobreseyó el caso fundamentando que no se pudo identificar a los autores. A pesar de algunos indicios para la posible identificación de las personas responsables a través de sus dominios en internet, la Audiencia Provincial no modificó el sobreseimiento. La inadmisión de la querrela fue justificada por diversos argumentos que manifestaban un conocimiento escaso sobre las criptomonedas y una permanente identificación con el riesgo.

Al ser difícil la identificación de los autores por las características que imbuyen al sistema blockchain, la Audiencia Provincial optó por rechazar, ante el desconocimiento de su funcionamiento, las investigaciones. En primer lugar, se rechazaron las informaciones policiales sobre la titularidad de los datos de dominio de la empresa INVESTFOND.EU recogidos en el informe, sin ser tenidos en cuenta como indicios de una posible autoría (AAP de Ávila, N.º Resolución 150/2018, 15 de junio de 2018, RJ segundo). El Tribunal lo fundamentó en la no regulación que rodea a la criptomoneda y al sistema descentralizado de blockchain. Al no existir una centralización de los flujos, consideraban que su control es más complicado y, por consiguiente, era muy difícil determinar la autoría. En este punto se refleja una incomprensión del sistema y del anonimato, ya que parece que identifica a los posibles autores de un delito de estafa con los mineros o nodos. Como ya se ha destacado en este trabajo, la red descentralizada está formada por miles o millones de



mineros cuya función es inscribir mediante ordenadores y algoritmos automáticos las transacciones en la cadena de bloques (Sempere, 2017). Es por ello que la relación entre la descentralización de la red en diversos usuarios y la difícil determinación de la autoría de un delito de estafa carece de sentido.

Por otro lado, para reforzar su posición, el tribunal se basó en la advertencia realizada por la Comisión Nacional del Mercado de Valores (CNMV) sobre los elevados riesgos que podría tener la inversión a través de estos sitios y que la falta de diligencia es del denunciante al iniciarse en negocios considerados de alto riesgo. De hecho, la Audiencia responsabilizó al propio denunciante al considerar que había carecido de la diligencia debida. Esta valoración sobre las inversiones de alto riesgo y el deber de diligencia por parte del afectado se ha visto contrariada por el segundo caso que encontramos: la Sentencia de la Audiencia Provincial de Madrid de 7 de marzo de 2018 (SAP de Madrid, N° de resolución 185/2018, 7 de marzo de 2018). En este caso, la narración de los hechos muestra una situación similar a la expuesta anteriormente. Varios poseedores de Bitcoins hacen un contrato con una empresa para que invierta en el mercado con la intención de obtener beneficios a cambio de entregar una comisión. Con el tiempo, el intermediario de las inversiones informa de la pérdida de los Bitcoins en la inversión y los inversores denuncian un delito de estafa. En esta ocasión, la Audiencia Provincial de Madrid sí consideró que existía un delito de estafa y que la pérdida de Bitcoin no recaía en la diligencia de los inversores, sino en la voluntad de enriquecimiento ilícito del intermediario. Esta posición tomada por parte del tribunal disiente de lo resaltado en la resolución 150/2018 de la Audiencia Provincial de Ávila analizada anteriormente y las advertencias realizadas por la CNMV no se sacan a relucir en esta sentencia. La Audiencia Provincial de Madrid basó su argumentación en que el riesgo de pérdidas o posible fraude fue utilizado por el acusado actuando dolosamente para aprovecharse de esta volatilidad y respaldar las pérdidas. Como prueba, se estudió el valor del Bitcoin durante el periodo contractual y su fluctuación fue estable.

A raíz de la rápida identificación del presunto autor de los hechos, los argumentos esgrimidos en anteriores ocasiones sobre la complejidad del funcionamiento del blockchain, el riesgo de las inversiones y las altas probabilidades de fraude no fueron invocados. La sentencia de la Audiencia Provincial de Madrid fue recurrida

en casación ante el Tribunal Supremo (TS) lo que permitió que este se pronunciara, por primera vez, sobre la naturaleza jurídica de la criptomoneda el 20 de junio de 2019 como se ha señalado en apartados anteriores (STS, N.º de resolución 326/2019, 20 de junio de 2019).

4.2.1.2. La criptomoneda como instrumento para la comisión del delito de estafa
Por otro lado, en relación con los delitos de estafa en los que la criptomoneda es el instrumento del delito nos encontramos ante un delito del 248.2 CP también conocido como delito de *phishing*. La Audiencia Provincial de Madrid en su resolución (AAP de Madrid, 704/2019, 2019) recoge los hechos de un grupo criminal que fue condenado por estafa. Los condenados obtenían claves bancarias de terceros y las cantidades obtenidas se transformaban posteriormente en la moneda virtual Bitcoin. Asimismo, la decisión redactada por la Audiencia Provincial de Santander en diciembre de 2018 muestra un caso en el que el acusado aceptó una oferta de trabajo por la cual se comprometía a recibir ingresos en su cuenta y transferirlos posteriormente a través de la moneda Bitcoin a los monederos virtuales que se le indicaba (AAP Santander, 520/2018, 2018). El tribunal señaló que el uso de la moneda Bitcoin denotaba que el investigado tenía conocimiento de que se podía estar desarrollando una actividad ilícita ya que borraba el rastro del destino del dinero al usar las criptomonedas.

Por otro lado, La Audiencia Provincial de Lleida condenó por un delito continuado de estafa del 250 del CP en el que el Bitcoin se usó para la compra de tarjetas que no eran de su propiedad y que posteriormente se emplearon para la compra de productos por Internet (Sentencia de la Audiencia Provincial de Lleida, 208/2017, 2017).

Distintos de esos supuestos, aunque también en el ámbito defraudatorio, se encuentra el caso de la SAP de Málaga 373/2019 de 25 de octubre de 2019. En la misma se condena al individuo en aplicación del artículo 256.1 del CP por utilización de un equipo de telecomunicación, sin consentimiento de su titular ya que el condenado minó criptomonedas utilizando los equipos informáticos de la empresa en la que trabajaba.



4.2.2. Delito contra la salud pública

En el caso del delito contra la salud pública, solo se han encontrado dos casos relacionados. El acceso a los criptomercados para la compra de estupefacientes va ligado al pago en criptomonedas en este ámbito (Barratt & Aldridge, 2020). En ambos casos de la Audiencia Provincial de Santa Cruz de Tenerife (SAP de Santa Cruz de Tenerife, N° de resolución 294/2018, 3 de octubre de 2018) y el Tribunal Superior de Justicia de Canarias (STSJ de Canarias, N° de la resolución 39/2018, 28 de septiembre de 2018) se muestra cómo los acusados recibían el dinero en efectivo en las cuentas y posteriormente compraban Bitcoins y con estas, las sustancias estupefacientes.

4.2.3. Delito de blanqueo de capitales

Por último, en lo referente al delito de blanqueo de capitales, aunque aparecieron seis decisiones en relación con este crimen, eran todas pertenecientes al mismo caso. Hay que tener en cuenta que en esta situación el sujeto investigado no ha realizado acciones directamente vinculadas al blanqueo de capitales. El acusado se dedica a la validación de bloques o minería Bitcoin, labor que no tiene relación directa con las transacciones ni la compra de criptoactivos. La unidad de policía y el Ministerio Fiscal consideraron que la maquinaria utilizada para la validación de bloques podía estar vinculada a actos ilícitos relacionados con el blanqueo de capitales. Su principal fundamento era la relación del apelante con otro hombre que era miembro principal de una organización dedicada a la venta de descodificadores de señal digital, cuyos beneficios ilícitos se canalizaban a través de letras de cambio y pagarés, apoyados en la inversión en centros de minería *Bitcoin* que luego se intercambiaba con dinero en metálico. Su relación, según el autor, proviene de la venta de una página web y unas conversaciones telefónicas sobre la transformación del dinero virtual en dinero de curso legal (AAP de Vigo, 537/2017, 2017, RJ cuarto). Por ello, relacionan el material utilizado para la minería *Bitcoin* con las actividades de blanqueo de dinero.

5. Discusión y conclusiones

En este artículo se han comparado los ámbitos en los que, según la doctrina y las autoridades españolas e internacionales, las criptomonedas están vinculadas a la criminalidad

frente a los casos que resuelven los tribunales españoles en relación a las criptomonedas. Los resultados sugieren que existe una notable diferencia entre ambas realidades. La doctrina ha identificado una serie de categorías como las más propicias y habituales en la utilización criminal de las criptomonedas. Estos delitos, como se ha indicado anteriormente, son el blanqueo de capitales, la financiación del terrorismo, la evasión fiscal y la compra de servicios y materiales de origen ilícito. También se ha explicitado que estos crímenes coinciden parcialmente con aquellos en los que han focalizado su interés los diferentes Estados, entidades supranacionales e internacionales.

Sin embargo, el análisis de las resoluciones judiciales de los tribunales penales españoles que acaba de exponerse muestra que no son estos los delitos cometidos mediante las criptomonedas que están siendo investigados y sentenciados por el poder judicial español. De hecho, de los casos expuestos la mayoría están relacionados con delitos patrimoniales, concretamente el delito de estafa. De las situaciones estudiadas solo en una aparece como único delito investigado el blanqueo de capitales. No obstante, los elementos que se han podido extraer de este caso evidencian que el papel de las criptomonedas no ha sido el de vehículo para la comisión del blanqueo de capitales. Más bien, la actividad de minería por parte del sujeto ha sido tomada como indicio para vincular al acusado con la comisión de este delito. Parece que no se trata de una situación propia de blanqueo de capitales sino de una interpretación errónea de la labor de un nodo validador que no tiene relación directa con la compra de criptomonedas.

Esta disensión interna entre las cuestiones destacadas por la doctrina y las autoridades legislativas y administrativas de las regiones más relevantes del mundo, por un lado, y, por otro lado, los casos de los tribunales españoles, requeriría un análisis más profundo. Como punto de partida de este posible futuro análisis podemos esbozar dos hipótesis. La primera considera que realmente en el territorio español no se están cometiendo delitos de blanqueo de capitales y financiación del terrorismo mediante las criptomonedas. Esta hipótesis supone que los delitos más referidos por la doctrina y que más preocupan a las autoridades administrativas y reguladoras apenas tienen presencia en España. La segunda hipótesis plantea que estos casos no están llegando a los tribunales. Esta hipótesis presenta a su vez dos posibilidades alternativas. La primera alternativa es que la utilización de la criptomoneda en este tipo de delitos sea tan reciente que aún no se encuentran resoluciones judiciales sobre la materia. La segunda



es que las características propias de las criptomonedas, esencialmente el anonimato y la ausencia de intermediarios controladores, determinan que la comisión de estos delitos no esté siendo respondida adecuadamente por las autoridades policiales y judiciales.

Cabe también plantearse la dotación de medios y conocimientos sobre criptomonedas con la que cuenta la policía y los jueces en España. El escaso conocimiento de un fenómeno tan complejo también puede ser causa para la limitada presencia de este tipo de casos ante los tribunales españoles. El desequilibrio entre jurisprudencia y normativa, y otros problemas en las sentencias –como las expuestas en este artículo– no se deben a que blockchain nos confronte con dificultades no contempladas en el orden jurídico, sino a que la falta de conocimiento técnico en estos organismos impide la aplicación del derecho existente en los casos en los que esta tecnología está involucrada.

Por otro lado, habría que valorar por qué solo son foco de atención aquellos crímenes cometidos a través de las criptomonedas y si la propia tecnología blockchain no sería también un instrumento efectivo para la comisión de otros delitos, como puede ser la tenencia de pornografía infantil utilizando este recurso y valiéndose de las características que dificultan su persecución.

El sistema blockchain y las criptomonedas no suponen una tecnología negativa para su uso. La posibilidad de tener una base de datos pública e inmutable muestra una robustez frente a la manipulación y fomenta la transparencia. Los usos de estas tecnologías son inmensos y por ello se considera como una de las revoluciones digitales con mayor potencial disruptivo de los últimos años gracias a su novedad, crecimiento y ejercer un impacto considerable en el ámbito socioeconómico.

Las criptomonedas han propiciado su desarrollo en ámbitos criminales por algunas de sus características como son el anonimato y la inexistencia de un intermediario de control. Lo que apunta Miró-Llinares (2011) en términos generales de la cibercriminalidad sirve también en el ámbito específico de las criptomonedas. Conforme se incrementa su uso, la delincuencia a través de las criptomonedas aumentará, será mayor el número de casos que se encuentren en los tribunales y, posiblemente, se amplíen los tipos delictivos. No obstante, en este momento, mientras que la doctrina y las autoridades centran su atención en los delitos de blanqueo de capitales, financiación del

terrorismo, evasiones fiscales y la compra de servicios o material de origen ilícito, a los tribunales llega otra realidad. Los delitos patrimoniales han tenido una gran presencia en los casos recogidos en la jurisprudencia española hasta el momento. El trabajo presenta distintas hipótesis y alternativas sobre por qué se presenta esta disparidad.

Las limitaciones implícitas a la metodología utilizada en este estudio generan cierta problemática en cuanto al acceso a los datos. Es por ello que entendemos que esta investigación podría reproducirse en los próximos años. De esta forma se valoraría una de las variables que se ha introducido: la relativa al tiempo necesario para que otros hechos delictivos relacionados con las criptomonedas lleguen a los tribunales españoles. Junto a esto, también sería conveniente la realización de investigaciones que sirvieran para analizar los medios y el conocimiento en relación a las criptomonedas con los que cuentan los distintos estamentos de investigación de estas conductas criminales.

6. Referencias

- Antonopoulos, A.M. (2015). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media.
- Ayuso, J. & Conesa, C., (2020). *Una Introducción al debate actual sobre la moneda digital del Banco Central*, Banco de España.
- Baker, P. (2020) *The Chinese government has earmarked additional funding for a blockchain-based trade finance platform developed and led by the country's central bank*, Disponible en: <https://www.coindesk.com/china-injects-4-7m-into-central-banks-blockchain-trade-finance-platform> (Fecha de consulta: 9 de junio de 2020)
- Barratt, M.J., Aldriedge, J. (2020), No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions, *International Journal of Drug Policy*, <https://doi.org/10.1016/j.drugpo.2020.102894>
- Bedecarratz Cholz, F. (2018). Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista Chilena de Derecho y Tecnología*, (7)1, 79-105, <http://dx.doi.org/10.5354/0719-2584.2018.48515>.
- Chudinovskikh, M., Sevryugin, V. (2019). Cryptocurrency regulation in the BRICS Countries and the Eurasian Economic Union, *BRICS Law Journal*, 6(1), 64-81. Doi: 10.21684/2412-2343-2018-6-1-63-81.
- Código Penal Español, Ley Orgánica 10/1995, de 23 de noviembre de 1995.



- Conesa, C. (2019). *Bitcoin: ¿Una solución para los sistemas de pago o una solución en busca de problema?*, Banco de España.
- Comisión Nacional del Mercado de Valores, www.cnmv.es (Fecha de la consulta 9 de junio de 2020)
- Cordero Valdavida, M. (2019). Blockchain en el sector público, una perspectiva internacional. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, 16, 16-34.
- Dion-Schwarz, C., Manheim, D. & Johnston, P.B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers*, RAND Corporation.
- Dolader Retamal, C., Bel Roig, J. & Muñoz Rapia, J.L. (2017), La blockchain, fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial*, 405, 33-40.
- Dyson, S., Buchanan, W., Bell, L., (2018), The Challenges of Investigation Cryptocurrencies and Blockchain Related Crime. *The Journal of The British Blockchain Association*, 2(1), 1-6. Doi: 10.31585/jbba-1-2-(8)2018
- Edwards, F.R, Hanley, K., Litan, R. & Weil, R.L., (2019), Crypto Assets Require Better Regulation: Statement of the Financial Economists Roundtable on Crypto Assets, *Financial Analysts Journal*, 14-19. Doi: <https://doi.org/10.1080/0015198X.2019.1593766>
- Foley S., Karslen, J. R., Putnins T. J. (2019). Sex, Drugs, and bitcoin: How Much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, 32(5), 1798–1853. <https://doi.org/10.1093/rfs/hhz015>
- GAFI, Monedas virtuales: Directrices para un enfoque basado en riesgo (actualización 2019), Disponible en : www.cfatf-gafic.org , (Fecha de consulta 30 de mayo de 2020) .
- García Sigman, L.I. (2017). Narcotráfico en la Darkweb: los criptomercados. *Revista Latinoamericana de Estudios de Seguridad*, 21, 191-206. <http://dx.doi.org/10.17141/urvio.21.2017.2824>
- González-Meneses, M. (2019), *Entender Blockchain. Una introducción a la tecnología de registro distribuido*, Aranzadi.
- Homoliak, I., Venugolapan, S., Hum, Q., Reijsberg, D., Schumi, R. & Szalachowski, P., (2019). The Security Reference Architecture for blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats and Defenses, arXiv preprint arXiv:1910.09775.
- Houben, R., Snyers, A., (2018), *Cryptocurrency and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament.
- Ibañez Jiménez, J. W., (2018), *Blockchain: Primeras cuestiones en el ordenamiento español*, Dykinson.

- Kuhn, D., *The Cryptocurrency Act of 2020 is Dead on Arrival*, Disponible en: <https://www.coindesk.com/the-cryptocurrency-act-of-2020-is-dead-on-arrival-washington-dc-tells-sponsors> (Fecha de consulta: 9 de junio de 2020).
- Luján Villareal, G., (2018). *Blockchain. No todo lo que brilla es Bitcoin*, Instituto de Relaciones Internacionales, Universidad Nacional de la Plata.
- Martin, J., Munksgaard, R., Coomber, R., Demant, J. & Barratt, M.J. (2020), Selling drugs on Darkweb cryptomarkets: differentiated pathways, risks and rewards, *British Journal of Criminology*, 60, 559-578. <https://doi.org/10.1093/bjc/azz075>
- Mera, A., Jafari, A., Vo-Huu, T., Jabiyev, B. & Mirzazade, R. (2018). Cryptocurrency: A challenge to legal system, *SSRN Electronic Journal*, 1-22. <http://dx.doi.org/10.2139/ssrn.3172489>
- Microprocessor and MS Committee. (2000). IEEE Standard Specifications for Public-Key Cryptography. *IEEE Computer Society*, 1-226.
- Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?”. *Crime Science*, 8(1), 12. <https://doi.org/10.1186/s40163-019-0107-y>
- Miró-Llinares, F. (2011). La oportunidad criminal en el ciberespacio, *Revista Electrónica de Ciencia Penal y Criminología*, 7, 1-07.
- Mitre Abuhayar, C., Alonso-Allende, J., Escauriaza, M., Gonzalo, J., Márquez, R. & Moreno, F.J. (2018). Descifrando la blockchain, *Nuevas Tendencias*, 100, Universidad de Navarra.
- Mounteney, J., et al. (2017). The Internet and drugs markets. *European Monitoring Centre for Drugs and Drug Addiction*, Publications Office of the European Union. <https://doi.org/10.1159/000018959>
- Nakamoto, N., *Bitcoin: A Peer-to-Peer Electronic Cash System*, Disponible en: <https://Bitcoin.org/Bitcoin.pdf> (Fecha de consulta: 9 de junio de 2020)
- Naranjo Valencia, S. (2019). Desafíos jurídicos que implica el pacto de criptomonedas como medio de pago en la celebración de un contrato de compraventa civil. Una mirada desde el neoinstitucionalismo, *Revista Con-Texto*, 50, 99-114.
- Navarro Cardoso, F. (2019). Criptomonedas (en especial, bitcóin) y blanqueo de dinero, *Revista Electrónica de Ciencia Penal y Criminología*, 21(14), 1-45.
- Norfer, M., Gomber, P., Hinz, O. & Schierek, D. (2017), Blockchain. *Business and Information System Engineering*, 59(3), 183-187. DOI 10.1007/s12599-017-0467-3
- Pastor Sempere, M.C (2017), Criptodivisas: ¿Una Disrupción Jurídica en la Eurozona? *Revista de Estudios Europeos*, 70, 284-318.
- Riasanow, T., Burckhardt, F., Soto Setzke, D., Böhm, M. & Krcmar, H. (2018), The Generic blockchain Ecosystem and its Strategic Implications. *Twenty-fourth Americas Conference on Information Systems*.



- Romero Ugarte, J.L. (2018), Tecnología de Registros Distribuidos (DLT): una introducción. *Boletín económico 4/2018*, Banco de España.
- Saldaña Taboada, P. (2017), ¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado. *El Criminalista Digital. Papeles de Criminología*, 6, 1-41.
- Swan, M. (2015), *Blockchain. Blueprint for a new economy*, O'Reilly.
- Terradillos Basoco, J.M. (2014), *Lineamientos metodológicos para la investigación jurídica*, PUCP.
- Unión Europea. Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018.
- Walton, J.B., Dhillon, G. (2017). Understanding Digital Crime, Trust, and Control in Blockchain Technologies, *Twenty-third Americas Conference on Information Systems*, 1-10.
- Xie, R. (2019). Why China had to “Ban” Cryptocurrency but the U.S. did not: A Comparative Analysis of Regulations on Crypto-Markets Between the U.S. and China. *Washington University Global Studies Law*, 18(2), 457-492 .