

LA UTILIZACIÓN DE LA BLOCKCHAIN EN LA CIBERDELINCUENCIA

Análisis de la ocultación de la actividad delictiva en internet

Ana Antelo Castelo

Máster en Ciberdelincuencia

Director: Tobias Gretenkort

M5.258 - Trabajo Final de Máster

Curso académico: 2022-2023

15/06/2023

UOC

RESUMEN

La tecnología Blockchain es un fenómeno muy estudiado en los últimos tiempos debido a su potencial criminógeno y su relación con la ocultación delictiva en el ciberespacio. Este estudio se centra en investigar el fenómeno desde una perspectiva técnica, analizando casos reales dentro de la literatura jurídica que ayuden a aportar claridad acerca del uso que los ciberdelincuentes hacen de la Blockchain y de las criptomonedas y su presumible relación con la ocultación de delictiva. A la hora de investigar acerca de sus características y funcionamiento, se encuentran muchas dificultades para encontrar información detallada, siendo el blanqueo de capitales el delito más relacionado con la Blockchain y las criptomonedas. Como resultado, el análisis de los casos muestra cierta relación con la ocultación delictiva debido a la pseudoanonimidad y baja rastreabilidad que caracteriza a este tipo de tecnología, pero concluye con una presencia mucho más elevada como herramienta de ayuda en la propia comisión delictiva, y por tanto, como un nuevo complemento para la aplicación de la delincuencia tradicional en el ciberespacio.

Palabras clave: Blockchain, criptomonedas, Bitcoin, cibercriminalidad, ocultación delictiva, análisis criminológico, criptografía, blanqueo de capitales, estafa.

ABSTRACT

"Blockchain technology has garnered significant attention in recent times due to its criminogenic potential and its association with criminal concealment in cyberspace. This study investigates its use by cybercriminals and the link to criminal concealment through real cases in legal literature. When researching their characteristics and functionality, numerous difficulties arise in finding detailed information on their operation, with money laundering being the most associated crime with blockchain and cryptocurrencies in the literature. As a result, the analysis reveals a connection to criminal concealment due to the technology's pseudoanonymity and low traceability. However, it concludes with a much higher presence as a facilitation tool in the actual commission of crimes, and therefore, as a new complement to the perpetration of traditional criminal activities in cyberspace."

Key words: Blockchain, cryptocurrency, Bitcoin, cybercrime, criminal concealment, criminological analysis, cryptography, money laundering, scam.

SUMARIO

1. INTRODUCCIÓN.....	4
1.1. La Blockchain como nueva oportunidad delictiva.....	4
1.2. La Blockchain como medio de ocultación de la identidad del delincuente.....	5
2. MARCO TEÓRICO	6
2.1. Definiciones	6
2.1.1. Sistema de Registro Distribuido y Blockchain	8
2.1.2. Criptomonedas y Bitcoin.....	10
2.2 Relación con la cibercriminalidad	11
2.2.1. Principales delitos relacionados con la Blockchain y las criptomonedas	11
2.2.2. Características de la Blockchain en relación con el blanqueo de capitales...	12
2.2.3. Centralización, descentralización o distribución.....	13
2.2.4. Público, anónimo o pseudoanónimo	14
2.2.5. Rastreabilidad.....	15
2.2.6. Seguridad.....	16
2.3. Puntos clave	16
2.4. Pregunta de investigación e hipótesis	17
3. METODOLOGÍA	18
4. ANÁLISIS DE LA OPORTUNIDAD CIBERDELICTIVA	18
3.1. Procedimiento de búsqueda y datos obtenidos	19
3.2. Las estafas, apropiación indebida y falsificación de moneda.....	22
3.3. Delitos contra la salud pública: Trafico de drogas.....	24
3.4. El blanqueo de capitales.....	25
3.4 Otros datos de interés.....	26
5. DISCUSIÓN.....	28
5.1. La Blockchain y su relación con la ocultación delictiva.....	28
5.2. Las características de la Blockchain y su relación con la ocultación delictiva....	29
5.3. El blanqueo de capitales y su relación con las criptomonedas y el Bitcoin.....	31
5.4. Limitaciones.....	32
6. CONCLUSIONES	32
7. BIBLIOGRAFÍA.....	33

1. INTRODUCCIÓN

El avance tecnológico ha proporcionado a la humanidad innumerables beneficios en diversas áreas como la medicina, la automoción, la educación o la comunicación, mejorando las condiciones de vida y las formas de socialización a lo largo del tiempo. Como bien expresa Ávila (2013), el desarrollo tecnológico, la información y la comunicación son la fuente básica de la revolución en las actividades humanas, y esto se ve representado en la renovación de los paradigmas sociales, económicos, culturales y políticos a lo largo del tiempo. Sin embargo, este progreso también ha traído consigo una serie de desafíos y ciertos dilemas éticos que generan grandes debates a día de hoy, como puede ser el derecho a mantener la privacidad de los datos que circulan por la red, la dependencia tecnológica, la creación de normativa legal que regule el ciberespacio, la gestión de la ciberseguridad o la ciberdelincuencia, siendo estos dos últimos puntos las claves principales sobre las que versará el presente trabajo.

1.1. La Blockchain como nueva oportunidad delictiva.

El uso de las TIC ha traído consigo el riesgo de exponerse a nuevos métodos que permiten realizar delitos tradicionales desde una nueva perspectiva, y además, la introducción de nuevas formas de criminalidad que antes difícilmente se podían realizar de la forma usual. En criminología, la ciberdelincuencia es un camino paralelo al de la delincuencia tradicional, ya que esta abarca un nuevo ámbito de actuación propio, el denominado comúnmente como ciberespacio (Miró, 2012). Conjuntamente, ciertos acontecimientos sociales de los últimos años han desencadenado un rápido proceso de tecnificación en diversas áreas muy relacionadas con la socialización humana, como podría ser el caso de la COVID19, la cual facilitó el proceso del desplazamiento de las oportunidades delictivas que ya se estaba expandiendo paulatinamente en la sociedad gracias al desarrollo de las TIC (Miró, 2021).

Partiendo de esto, podemos observar, y por tanto afirmar, que la ciberdelincuencia está desarrollándose con extrema rapidez. Si analizamos brevemente los escasos datos sobre cibercriminalidad en España, la comparativa entre la cibercriminalidad comprendida entre 2017 y 2021 nos muestra que, mientras que en 2017 la ciberdelincuencia correspondía a un 5,7% de la delincuencia total, en 2021 el dato sube hasta situarse en un 15,6%. Además, es importante destacar que dentro de ese 15,6%, el cual corresponde a un total de 305.477 ciberdelitos, un 87,4% son fraudes informáticos

(Informe sobre la cibercriminalidad en España, 2021). Este hecho sitúa a los delitos económicos como el punto principal de acción para los ciberdelincuentes, y por consiguiente, en una área de estudio muy significativa a analizar.

Como bien explica Miró (2012), los ciberdelitos económicos engloban todas las acciones criminales llevadas a cabo con la finalidad de obtener un beneficio patrimonial directo o indirecto, y el ciberespacio, al ofrecer una esfera anónima, rápida y global, es el lugar ideal donde replicar este comportamiento. Dentro de esta área, en los últimos tiempos, destacan enormemente los delitos económicos que han ido surgiendo a raíz del desarrollo de las TIC, sobresaliendo el uso de la tecnología Blockchain y la creación de las criptomonedas como una herramienta potencialmente útil para los ciberdelincuentes.

Aun así, a pesar del interés que se ha creado alrededor de estos nuevos conceptos y de la preocupación por su potencial criminógeno (Pérez, 2020) se trata de una área muy poco explorada en el campo de la criminología. Si observamos la literatura criminológica sobre Blockchain, veremos que no existen análisis técnicos que estudien las causas concretas de la preocupación acerca de la Blockchain como nueva oportunidad delictiva, pero si podemos encontrarnos con un consenso general en la motivación. Todos los autores coinciden en que la oportunidad delictiva reside en la relación entre la Blockchain y las criptomonedas, siendo estas la herramienta principal que utilizan los ciberdelincuentes porque supone una gran oportunidad para blanquear dinero obtenido a partir de actividades delictivas, dificultando así su posible persecución (Navarro, 2019; Pérez, 2017; Gabela, 2019; Zárata, 2022, Nieto et al., 2021; Criado, 2020; Saldaña, 2017). Esta concepción se basa en las características que la literatura considera esenciales, como el anonimato o la descentralización (Gabela, 2019; Navarro, 2019), concepciones que si bien es cierto que facilitan la actividad delictiva, no se basan en un análisis técnico de la realidad, si no en una idea teórica del posible uso de las criptomonedas.

1.2. La Blockchain como medio de ocultación de la identidad del delincuente.

Basándome en lo mencionado anteriormente, resulta evidente que el empleo de la Blockchain como una herramienta para ocultar la identidad del delincuente es una afirmación respaldada por diversos estudios (Saldaña, 2017; Navarro, 2019; Zárata, 2022), y el foco en el que se centran todas las áreas de conocimiento que estudian este fenómeno. En este contexto, resulta relevante resaltar los estudios desde la perspectiva jurídica, dado que todas las propuestas de regulación y reforma relacionadas con la

Blockchain se fundamentan en este conocimiento teórico y en un aspecto técnico ciertamente superficial sobre el tema. Podemos observar esta premisa en consideraciones legales como los debates acerca de legalizar las criptomonedas en forma de moneda de curso legal para eliminar esa anonimidad (Pérez, 2017) o la necesidad de gestionar la responsabilidad penal de los proveedores de servicios (Nieto et al, 2021) de la misma forma en la que se responsabilizan actualmente en los delitos informáticos. Debido a todo ello, es indispensable dar a conocer la vinculación entre la tecnología Blockchain y su capacidad delictiva desde una forma más técnica y criminológica, así como desmitificar los conceptos erróneos que se han generado alrededor de estos conceptos y mostrar la realidad del efecto de esta nueva tecnología en el panorama judicial español.

2. MARCO TEÓRICO

El primer paso indispensable para poder analizar el fenómeno a estudiar es instaurar las definiciones de los términos clave, su funcionamiento y la relación que mantienen con el tema a tratar. Esto implica poder comprender como estos operan y se relacionan entre sí, permitiéndonos establecer los motivos detrás de los cuales estas nuevas tecnológicas son un elemento clave en delitos como el blanqueo de capitales o la compraventa de sustancias ilícitas.

2.1. Definiciones

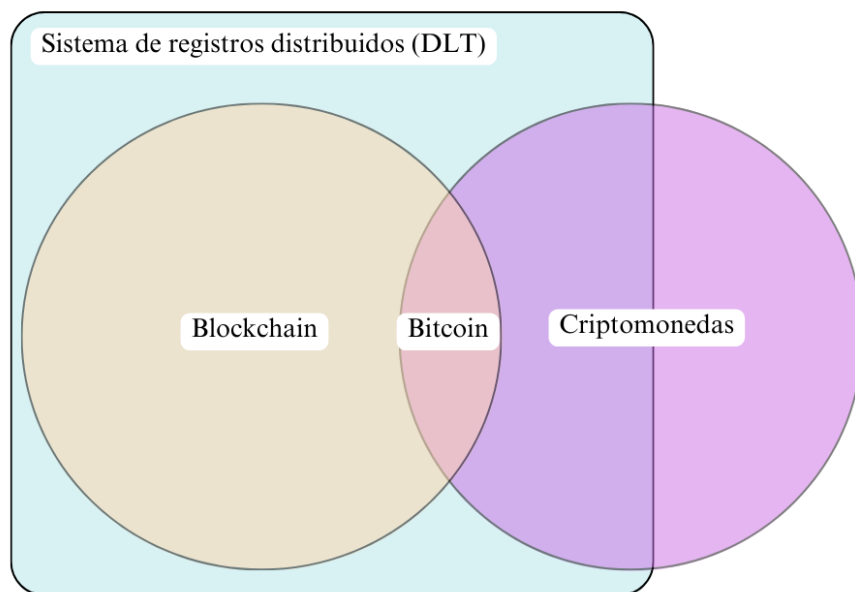
Los términos “Blockchain” y “Criptomonedas” son conceptos en cierta medida novedosos, que difícilmente se utilizan en el día a día y que pueden generar dudas o inducir a errores debido a la poca teoría existente dentro de las ciencias sociales. Además, como bien indica Pérez (2020), la mayoría de los estados no tienen una extensa regulación sobre esta materia, destacando la sola existencia de una definición en referencia a las criptomonedas en el ámbito nacional por parte del Tribunal Supremo, considerándolas un activo patrimonial inmaterial. Como podemos ver, se trata de una definición que se ciñe al concepto de evitar la anonimidad que mencionaba anteriormente y no en la comprensión del su utilidad y funcionamiento.

Si acudimos a la literatura, nos podemos encontrar con bastantes definiciones que ligan ambos conceptos, como podría ser la de Zárate (2022), donde nos indica que la Blockchain se trata del libro mayor público descentralizado de la criptomoneda, un libro donde se registran todas las transacciones de una criptomoneda, la de Navarro (2019), donde nos dice que la cadena de bloques es el ecosistema de las criptomonedas, o la de

Cerna et al. (2018) que define las criptomonedas como aquellas monedas virtuales que basan su funcionamiento en la tecnología Blockchain. Por otra parte, también existen definiciones que consideran que la Blockchain y las criptomonedas se pueden ver como sinónimos: “Monedas como Blockchain prueban que este tipo de divisas pueden adherirse a la economía tradicional y convertirse en un verdadero sistema financiero.”. (Gutiérrez, 2019, p. 5) o “En la actualidad, existen diferentes monedas de este tipo, v.g., Bitcoin, Ethereum, Litecoin, Tether o Blockchain”. (Gutiérrez, 2019, p. 3). La realidad detrás de estas definiciones es que presentan discrepancias con la evidencia disponible, puesto que los conceptos “Blockchain”, “Criptomonedas” o incluso “Bitcoin” deben ser analizados de forma separada para comprender realmente su función y relación.

Por tanto, es necesario, teniendo en cuenta la cantidad de definiciones confusas que se contradicen entre ellas, establecer un esquema que represente la jerarquía y las relaciones entre estos conceptos, incluyendo aquellos que son indispensables para la comprensión de dicha diferenciación y suelen pasar desapercibidos cuando se analiza el estado de la cuestión. El siguiente diagrama de Venn, elaborado a partir del trabajo de Gretenkort (en prensa) representa de forma visual la explicación que se seguirá en los sucesivos apartados.

Figura 1. Diagrama de Venn de la relación entre DLT, Blockchain, Criptomonedas y Bitcoin



Fuente: Adaptado en Gretenkort (en prensa)

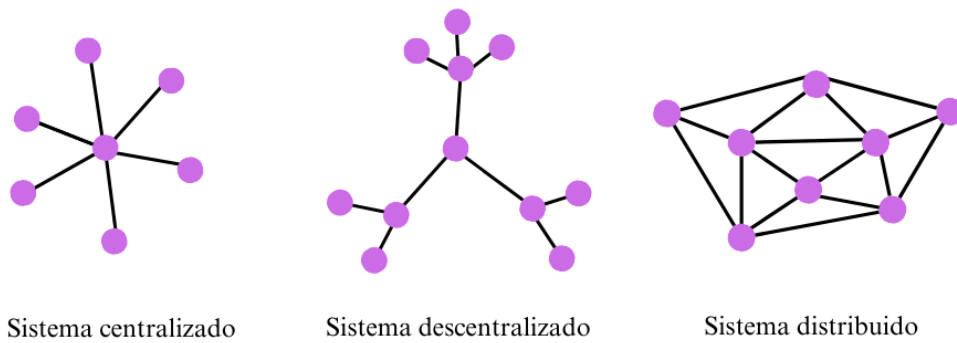
2.1.1. Sistema de Registro Distribuido y Blockchain

El primer punto que es necesario destacar es que la tecnología Blockchain está basada en un sistema de registros distribuidos, también conocido como sistema DLT (Pérez, 2020), apenas mencionado en los estudios acerca de la tecnología Blockchain (Navarro, 2019; Zárate, 2022; Grigera del Campillo, 2021; Saldaña, 2017; Gabela, 2019; Domínguez et al., 2018; Wicab, 2018), pero que es de vital importancia para entender su funcionamiento y su relación con las criptomonedas. El sistema DLT se encarga del almacenamiento de información con la finalidad de mantener un registro, es decir, su funcionamiento consiste en archivar una nueva entrada de forma cronológica en un registro, sin borrar ni editar la información anterior (Gretenkort, en prensa). El más claro ejemplo relacionado con este sistema es una cuenta bancaria tradicional, donde nos encontramos con una lista interminable de sumas y restas al saldo inicial (Gretenkort, en prensa), registrando de esta forma todas las veces que se aporta dinero nuevo o se gasta, pero nunca eliminando ni modificando los datos anteriores. Esto permite poder observar cada gasto y suma que se ha ido realizando, evitando de esta manera que pueda haber alguna modificación no deseada por el dueño de la cuenta.

La característica principal que debemos destacar de este sistema es que, como su nombre indica, se trata de un sistema distribuido, es decir, se caracteriza por realizar múltiples copias idénticas, distribuidas entre las personas que participan en la red de forma independiente (Pérez, 2020), y esto implica que no debe existir una jerarquía dentro del sistema. Esta concepción también genera cierta confusión entre la literatura mayoritaria porque existe una malinterpretación entre sistema distribuido y descentralizado. Si echamos un vistazo a las definiciones de los conceptos clave, podemos ver que la gran mayoría consideran que la tecnología Blockchain, y por tanto todas las criptomonedas al ser conceptos sinónimos, parten de un sistema descentralizado. Saldaña et al (2017) destaca como característica principal de las criptomonedas su capacidad de descentralización, Wicab (2018) incluye en su definición de Blockchain y criptomonedas el concepto de sistema privado y descentralizado, y Grigera de Campillo (2021) considera que la Blockchain, al ser un sistema distribuido, aumenta la transparencia, lo que permite una mejor trazabilidad de las transacciones.

Para poder explicar mejor la diferencia entre estas dos conceptualizaciones, se partirá de lo expuesto en la figura 2, donde se representa de forma visual las diferencias entre los tres tipos principales de sistemas.

Figura 2. Diferencias entre sistema centralizado descentralizado y distribuido



Fuente: Elaboración propia a partir de Gretenkort (en prensa)

Como se puede ver en la imagen, tanto el sistema descentralizado como el sistema distribuido parten de una descentralización, puesto que en ninguno de los dos casos los puntos o nodos llegan a estar conectados al nodo central, hecho que si se hace evidente en el sistema centralizado, el cual si se caracteriza por esa dependencia. Si se observa detalladamente la figura 2, se puede ver que dentro del sistema descentralizado también existe cierta centralización, ya que no todos los nodos están interconectados entre sí, y por tanto, este factor genera desigualdad entre ellos y dependencia del nodo central. En cambio, el sistema distribuido si cumpliría completamente esa condición, ya que no se puede observar un nodo central del que dependan realmente los demás, y aunque técnicamente haya algún nodo más central que otro, si se suprimiera cualquiera de ellos, la información seguiría siendo accesible gracias a dicha interconexión (Gretenkort, en prensa).

En cuanto a la Blockchain, esta tecnología es una forma concreta de organizar un sistema DLT. Se sustenta en un sistema peer-to-peer, donde cada componente tiene la misma posición que los demás, y esto permite que exista un mayor grado de seguridad a la hora de mantener los registros (Pérez, 2020). La clave principal reside su funcionamiento. La Blockchain presenta una cadena de bloques de transacciones enlazados que permiten la revisión constante de cada una de dichas transacciones. Esto se debe al uso de hashes criptográficos, los cuales permiten convertir la información almacenada en un conjunto alfanumérico fijo que le servirá de representación, y de esta manera, cada nueva pieza que se incorpora a los bloques quedará enlazada junto a la información anterior (Pérez, 2020). La tecnología Blockchain no es inmutable o permanente como suele mencionarse en la literatura (Navarro, 2019; Saldaña, 2017; Cerna et al., 2018), esta se puede llegar a modificar o incluso se pueden borrar partes,

pero debido a su forma de funcionamiento, los hashes criptográficos que mantienen una copia de la información anteriormente almacenada, detectan enseguida esa modificación (Gretenkort, en prensa). Es por ello por lo que se considera que la Blockchain no se puede modificar, aunque no sea un concepto técnicamente correcto. La relación entre la Blockchain y las criptomonedas nace precisamente de la utilidad de esta tecnología en la creación de monedas virtuales, ya que las características mencionadas anteriormente, como la alta seguridad y la capacidad de registrar todas las transacciones, resulta fundamental para asegurar estas nuevas formas de crear formas de pago.

2.1.2. Criptomonedas y Bitcoin

Las criptomonedas son el siguiente nivel que podemos observar en la figura 1., y son consideradas por la gran mayoría de autores, como por ejemplo Cerna et al. (2018) o Pérez (2017), como una moneda de cambio virtual. El concepto de moneda de cambio no es como tal una concepción moderna, ya que esta forma de pago ya existía en la edad media con la utilización de tarjetas, es decir, palos partidos en dos partes que se utilizaban para simbolizar una transacción. Esta ruptura del palo era tan específica que solo esas dos mitades podían juntarse y formar la figura completa (Gretenkort, en prensa). Las formas modernas de moneda de cambio, las criptomonedas, utilizan sistemas DLT para simular esa forma de garantizar la transacción (Gretenkort, en prensa), y como bien se indicaba en el apartado anterior, la Blockchain es un sistema DLT que a menudo se utiliza en la creación de criptomonedas.

Concretamente, la unión de estos dos conceptos surge de la creación del Bitcoin, una de las criptomonedas más utilizadas y dada a conocer por Shatoshi Nakamoto en 2008 en su artículo “Bitcoin: A Peer-to-peer Electronic Cash System”, donde podemos ver en la explicación de su funcionamiento que utiliza la tecnología Blockchain. Su sistema de seguridad concreto se representa mediante una firma digital, como la tarjeta mencionada en el apartado anterior. Esta firma se representa concretamente mediante una clave pública (pk) y una clave privada o secreta (sk). La clave privada, como su nombre indica, es la clave que se mantiene oculta y es diferente en cada transacción que realices, y por tanto, única cada vez (3Blue1Brown, 2018, 4:04). El conjunto del mensaje y la clave privada representa la firma digital. En cuanto a la clave pública, es la que nos permite verificar si la firma digital es verdadera o falsa. Esto se debe a que la clave pública está enlazada a la privada (3Blue1Brown, 2018, 5:18).

Aun así, es importante entender que no todas las criptomonedas utilizan este sistema de Blockchain, este es otro error común. Podemos verlo en artículos como el de Grigera del Campillo (2021), artículo que se centra en ejemplificar diferentes formas en las que se puede utilizar la Blockchain y las criptomonedas para la realización de delitos, uno de ejemplos que podemos encontrarnos versa sobre la utilización de la criptomoneda Iota para realizar Phishing. Si investigamos el sistema DLT que utiliza la moneda Iota, nos encontramos con el sistema Tangle, un sistema DLT diferente que no guarda relación con el Blockchain (Conti et al., 2022).

Por tanto, es indispensable concluir que, si bien la Blockchain es un sistema de registros distribuidos y las criptomonedas se crean a partir de estos sistemas, no todos los sistemas distribuidos son Blockchain, y a su vez, no todas las criptomonedas modernas que existen utilizan el sistema de tecnología Blockchain, pero si un sistema DLT.

2.2 Relación con la cibercriminalidad

Una vez aclarados los puntos más importantes para diferenciar correctamente los conceptos principales, es fundamental explicar la relación entre Blockchain, criptomonedas y el tema principal que se pretende abordar a lo largo de este trabajo: La ocultación de la actividad criminal en la red.

Antes de empezar, es necesario indicar que, teniendo en cuenta que el Bitcoin es la criptomoneda más utilizada que emplea Blockchain y sobre la que más información y documentación, tanto legal como técnica, se elabora, se ha acotado el análisis a esta criptomoneda. Sin embargo, es importante tener en cuenta que existe muchas otras criptomonedas con diferentes características que no tienen por qué responder o funcionar de esta misma manera.

2.2.1. Principales delitos relacionados con la Blockchain y las criptomonedas

El primer punto y el más importante para empezar a asentar esta relación es establecer los principales delitos que la literatura relaciona con el uso de la Blockchain y 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). (Pérez, 2020, p. 10)

Como podemos ver, la Blockchain y las criptomonedas se relacionan principalmente con aquellos delitos donde la acción principal consiste en la ocultación económica, ya sea esa su finalidad o el medio vital para llegar al resultado esperado. Principalmente, destaca el blanqueo de dinero, ya que es el delito más mencionado en la literatura (Navarro, 2019; Saldaña, 2017; Gabela, 2019; Nieto et al., 2021; Pérez, 2017) y el que más se correlaciona con las características de la blockchain mencionadas en la literatura. Si examinamos los hallazgos presentados en Crypto Crime Report (2023) durante el año 2022 se blanquearon 23.8 billones de dólares en criptomonedas producto de actos ilícitos, pero es la parte que arroja cierta luz acerca de cómo se blanquea ese dinero la que indica algo contradictorio, según Crypto Crime Report (2023) las criptomonedas son utilizadas como un medio de paso. Esto facilita al ciberdelincuente la ocultación, pero nos muestra que no son utilizadas como un lugar permanente donde mantener el dinero ilícito ni como un medio único a utilizar para blanquear dinero donde la criptomoneda se utilice como un medio de pago, ya que se presupone que vuelve a reintroducirse en el mercado tradicional, y es en este donde se procede a realizar el blanqueo. Esta información revela un patrón mediante el cual las criptomonedas son empleadas temporalmente por los ciberdelincuentes, sirviendo como un instrumento que les permite encubrir momentáneamente la procedencia de sus fondos ilícitos, pero no como un medio completo de blanqueo.

Debido a esto, es importante en este caso tener en cuenta las discrepancias que nos hemos encontrado lo largo del desarrollo de esta literatura. Las diferencias en cuanto a definiciones y a la falta de literatura técnica sobre esta temática generan cierta incertidumbre acerca de la verdadera relación entre la ocultación delictiva en forma de blanqueo de capitales y la Blockchain, y por lo tanto, resulta conveniente analizar las características de la Blockchain y las criptomonedas que la literatura más relaciona con este delito.

2.2.2. Características de la Blockchain en relación con el blanqueo de capitales

Partiendo de lo expuesto por Pérez (2020) y Saldaña (2023), las propiedades que han hecho a esta tecnología tan atractiva para los ciberdelincuentes son el anonimato, la inmutabilidad del sistema, la seguridad, su transparencia y trazabilidad, la ausencia de terceros y el ahorro de costes. De todos estos puntos, y en relación con el blanqueo de capitales, es necesario destacar su capacidad de anonimidad, ya que es la característica

más relacionada según la mayoría de autores (Navarro, 2019; Saldaña, 2017; Álvarez, 2022; Cerna, 2018) la rastreabilidad, ya que es un componente clave que no se tiene muy en cuenta, pero que es imprescindible para comprender su funcionamiento, y por último, la seguridad (Saldaña, 2023), porque es una característica imprescindible para un sistema implicado en transferencias económicas.

Debido a la importancia de estas particularidades, es conveniente analizarlas más concretamente teniendo en cuenta las contradicciones encontradas en la literatura.

2.2.3. Centralización, descentralización o distribución

Es importante indicar que el principal punto a partir del que surgen todas las características descritas por la literatura residen en su capacidad descentralizadora (Navarro, 2019; Zárate, 2022; Saldaña, 2017) y por tanto, es necesario incidir más concretamente en ello. La descentralización es una capacidad que, como bien se ha examinado en la literatura ya expuesta, no es del todo correcta en relación a la Blockchain y las criptomonedas.

La Blockchain es una tecnología que surge a raíz de un sistema DLT, y por tanto es distribuida, por lo que su sistema, por norma general, funciona como se indica en el esquema de la figura 2, donde podemos ver que los nodos están conectados entre si sin restricciones, sin un nodo más central que otro (Gretenkort, en prensa), en cambio, en el caso de la descentralización, podemos observar que a pesar de que no todos los nodos están vinculados al nodo central, si presenta cierta jerarquía al tener nodos más centrales que otros (Gretenkort, en prensa). Si atendemos a las argumentaciones de la literatura acerca de la descentralización, podremos ver que se ajustan más a la distribución que a la descentralización “Utilizan un sistema de transacciones descentralizados conocido como blockchain... El intercambio de estas se da de forma directa entre usuario a usuario lo que las hace no depender de instituciones financieras o gubernamentales como intermediarios” (Gabela, 2019, p. 1), por lo que se puede intuir que se trata de una mala interpretación del concepto descentralización más que de una confusión con el funcionamiento real de la Blockchain.

Por otra parte, es importante incidir en el caso concreto del Bitcoin, ya que es la criptomoneda que más se relaciona con la cibercriminalidad (Navarro, 2019; Gutiérrez, 2019), esta tiene características concretas que necesariamente se deben tener en cuenta. Siguiendo lo expuesto por Saldaña (2023) el Bitcoin presenta dificultades para soportar

todas las transacciones que los usuarios desean realizar, y esto se debe precisamente al sistema que utiliza para validar las transacciones y que genera en los usuarios que realizan dichas transacciones con bitcoin una motivación para hacer funcionar los nodos (Gretenkort, en prensa), se trata del método conocido como “Proof-of-work” abreviado a PoW. Este se basa en la utilización de un nonce, un número aleatorio que solo se utiliza una sola vez (Roy et al., 2004) y que está destinado a validar la transferencia de datos a un fragmento de información, en este caso, al bloque de transacciones (Gretenkort, en prensa). Debido a que el nonce no se puede calcular de manera significativa, se prueban diferentes nonces hasta que el correcto es elegido. Esto se realiza mediante un sistema de fuerza bruta que concede al primer nodo que logra encontrar el nonce el derecho de verificar el bloque, y a su vez, se le otorga una recompensa de una cantidad de Bitcoin por realizar el proceso (Gretenkort, en prensa), si tenemos en cuenta las altas cantidades de energía que se utilizan para poder realizar esta verificación y la competencia que este sistema genera, podemos comprender que la minería de Bitcoin ha surgido debido a la utilización de este método (Gretenkort, en prensa) y de esto se deriva, por una parte, una desigualdad entre nodos, ya que serán aquellos que puedan invertir esta cantidad de energía los que se encontrarán en una posición de poder frente a los demás, y por otra parte, la consideración del Bitcoin como un sistema más descentralizado que distribuido.

Es por todo ello que, a pesar de que la literatura mayoritaria considere a la Blockchain y a las criptomonedas, independientemente del término utilizado, como sistemas donde se realizan intercambios directos entre usuarios donde no existen sistemas de poder (Gabela, 2019), el Bitcoin y su forma concreta de verificar los bloques responde a un sistema creado por y para la competencia entre usuarios, y esto puede afectar a las consideraciones que se hacen acerca de su papel en la cibercriminalidad, y más concretamente, sobre el blanqueo de capitales, ya que la dificultad para realizar transacciones con esta criptomoneda dificulta su posible uso como una herramienta de blanqueo.

2.2.4. Público, anónimo o pseudoanónimo

En lo referente a la anonimidad, como se explicaba anteriormente, las criptomonedas utilizan sistemas DLT porque son sistemas distribuidos. Esto implica que se benefician de la falta de dependencia de un organismo de poder controlar las transacciones (Pérez, 2020), lo que nos lleva a esa ausencia de terceros ya conocida. Debido a ello, son consideradas anónimas por la mayoría de los autores, como Navarro (2019) que resume las características de las criptomonedas como seguras,

descentralizadas y anónimas. No obstante, es importante destacar que las criptomonedas son en realidad pseudoanónimas (Pérez, 2020), ya que generan cierta información que puede ser rastreada. Como bien indica Saldaña (2023), aunque las transacciones realizadas se pueden llegar a considerar anónimas al no contener datos que las relacionen con la persona que las realiza, tampoco son del todo privadas, ya que la información queda registrada de forma cronológica, irreversible y pública en la Blockchain, y cualquier persona puede acceder y comprobar la cantidad transferida, el día o la hora de cada transacción. Esta característica, como se ha indicado anteriormente, es la más relacionada con el blanqueo de capitales debido a que la utilización de criptomonedas permite realizar transacciones sin tener que identificar a la persona que realiza dicha transacción (Saldaña, 2023), y si tenemos en cuenta que el blanqueo de capitales se basa en la ocultación del capital ilícito, esta característica facilita el trabajo y convierte a las criptomonedas en una herramienta potencial.

Esto último está muy relacionado con el concepto de rastreabilidad, ya que algo anónimo, o pseudoanónimo en este caso, dificultaría la rastreabilidad de la transacción.

2.2.5. Rastreabilidad

En general, se suele entender que la anonimidad implica la imposibilidad total de rastreo. Sin embargo, al considerar los conceptos discutidos anteriormente, como es el caso de la tecnología Blockchain y las criptomonedas, particularmente Bitcoin, se encuentran elementos que combinan ambas características. Aunque la identidad del usuario sigue siendo desconocida, es posible examinar ciertos aspectos de su actividad (Saldaña, 2023). En consecuencia, las criptomonedas pueden considerarse parcialmente rastreables, ya que, como se mencionó en el apartado previo, se pueden obtener ciertos datos, como la fecha y la cantidad transferida, sin que esto implique necesariamente una identidad completa del usuario. Esto guarda relación con el primer concepto analizado, es decir, con su capacidad de distribución y su funcionamiento como un libro de registros público (Gretenkort, en prensa).

Al igual que en el caso de la pseudoanonimidad, su baja capacidad para ser rastreable representa más facilidad para ocultar un capital ilícito frente a otros medios tradicionales, exceptuando el cobro en efectivo, puesto en este último caso no hay manera de saber quien o quienes estuvieron en posición de ese dinero anteriormente (Navarro, 2019)

2.2.6. Seguridad

Finalmente, la última característica importante a tener en cuenta y que se puede relacionar con el blanqueo de capitales es la Seguridad. Como bien indica Saldaña (2023), la seguridad está ligada al propio funcionamiento de la Blockchain, concretamente, se relaciona con la inmutabilidad de la cadena, gracias a las firmas digitales encadenadas y a los números hashes que se generan en cada bloque, y con la irreversibilidad en las operaciones, es decir, se refiere a su capacidad de detectar cualquier tipo de intrusión gracias a la capacidad de cada nodo de poder disponer de una copia completa de toda la información presente en la cadena (Saldaña, 2023; Gretenkort, en prensa).

Si el Blockchain no fuese un sistema tan relacionado con la seguridad, no existiría un claro interés en su utilización para realizar transacciones de carácter económico. Esto lo podemos ver precisamente en el caso de las criptomonedas, y especialmente el Bitcoin, ya que el uso de la criptografía para las firmas en las transacciones permite asegurar dicha transacción realizada entre las partes sin tener que identificarse aportando datos personales (Saldaña, 2023). De nuevo, podemos ver que todo está ligado al concepto de pseudoaninimidad y su gran influencia como posible facilitador del blanqueo de capitales.

2.3. Puntos clave

A modo conclusivo de esta introducción al tema, se puntualizarán las ideas principales extraídas de la literatura, ya que permitirán comprender mejor los planteamientos sobre los que versará el trabajo, y que a su vez, se deberán tener en cuenta para analizar los futuros resultados:

- I. La Blockchain se relaciona directamente con las criptomonedas a un nivel tan estrecho que produce ciertas confusiones teóricas a la hora de definirlas (Zárate 2022, Gutiérrez 2019; Gabela, 2019; Cerna et al., 2018; Domínguez et al., 2018), llegando a considerarse sinónimos en algunos casos (Gutiérrez, 2019), y dificultando así la posibilidad de comprender su funcionamiento.
- II. Las características principales que señala la literatura acerca de la Blockchain y las criptomonedas son la seguridad, el anonimato y la descentralización (Saldaña 2017; Navarro, 2019; Gabela, 2019). Teniendo en cuenta las confusiones teóricas ya señaladas, en el primer caso se hace referencia a la propia tecnología Blockchain y su sistema de hashes criptográficos, en el segundo caso, el anonimato, más técnicamente conocido como pseudoanonimato (Pérez, 2020), representa el hecho de que no es

necesario ceder datos personales para crear carteras de criptomonedas ni realizar transacciones, por lo que la identidad de las personas que realizan transacciones con criptomonedas es un dato que se desconoce, y en lo referente a la descentralización, o distribución (Gretenkort, en prensa), ya que es terminológicamente más acercado, también está relacionado con la propia tecnología Blockchain, ya que se conoce como una tecnología que carece de entidad central que controle el sistema.

- III. La literatura considera que el blanqueo de capitales es el delito más frecuente donde los ciberdelincuentes utilizan las criptomonedas para ocultar el origen de los beneficios obtenidos a través de otras actividades ilícitas (Navarro, 2019; Saldaña, 2017; Gabela, 2019; Nieto et al., 2021; Pérez, 2017), esto se debe a las características ya mencionadas de pseudoanonimidad y distribución, y además, la concepción de que es un sistema seguro puede favorecer la idea del ciberdelincuente de utilizar este nuevo sistema para sus intereses (Saldaña, 2023).
- IV. El bitcoin es la criptomoneda más relacionada con la actividad y ocultación delictiva y la más estudiada en la literatura actual. (Navarro, 2019; Gabela, 2019; Saldaña 2017, Saldaña 2023; Pérez, 2020).

2.4. Pregunta de investigación e hipótesis

Por tanto, la pregunta principal que surge a partir de las dudas planteadas en la literatura (Navarro 2019; Zárata 2022; Gabela 2019; Grigera del Campillo, 2021; Saldaña, 2017; Pérez, 2017; Gutiérrez, 2019), y que se pretende responder durante la investigación, se sintetiza en:

- ¿Utilizan realmente los ciberdelincuentes la tecnología Blockchain para ocultar sus actividades delictivas en la red?

A su vez, las hipótesis que surgen a raíz de esta pregunta, y que deberán ser respondidas a lo largo del desarrollo de este trabajo, corresponderían a:

1. Los ciberdelincuentes utilizan la tecnología Blockchain para ocultar sus actividades delictivas debido a su capacidad para proporcionar un mayor anonimato y seguridad. (Navarro, 2019)
2. La naturaleza descentralizada y la anonimidad de la Blockchain representa la mayor dificultad a la hora de combatir este fenómeno. (Gabela, 2019)

3. Los ciberdelincuentes utilizan la tecnología Blockchain principalmente para realizar blanqueo de capitales y para la compra y venta de material ilícito (Gabela, 2019; Navarro, 2019)

3. METODOLOGÍA

Con el fin de abordar las interrogantes y preocupaciones surgidas a raíz de la revisión bibliográfica sobre la tecnología Blockchain, las criptomonedas, la ocultación delictiva y su vínculo con el blanqueo de capitales, se llevará a cabo una evaluación jurídica en el contexto del marco legal español. Este enfoque permitirá examinar la realidad de los casos reales y contrastarla con la información recopilada. Con ese propósito, se ha seguido el siguiente procedimiento:

1. Se ha seleccionado el buscador jurídico del Centro de Documentación Judicial (CENDOJ) para realizar la búsqueda de material jurídico debido a que es el órgano técnico del Consejo General del Poder Judicial que se encarga de la publicación oficial de la jurisprudencia española (Poder Judicial, s.f.)
2. Para ello se han seleccionado las palabras clave: “Blockchain”, “Criptomonedas” y “Bitcoin” debido a que son los tres conceptos clave más relacionados y relevantes en la literatura (Navarro, 2019; Saldaña 2017; Gabela, 2019; Wicab, 2018; Pérez, 2020). Además, se han considerado solo aquellas sentencias que guardan relación con el ámbito penal, ya que el enfoque específico de este trabajo se centra en la cibercriminalidad.
3. Tras realizar la búsqueda, se ha elaborado un gráfico que facilita la visualización de la frecuencia con la que se mencionan dichos términos, lo cual permite analizar si la confusión terminológica también está presente en la literatura jurídica.
4. A continuación, se llevará a cabo un análisis del papel desempeñado tanto por la tecnología Blockchain como por las criptomonedas en los casos identificados.
5. Por último, se discutirán los resultados obtenidos en relación con la literatura expuesta en el marco teórico, con el objetivo de dar respuesta a los planteamientos iniciales y extraer conclusiones relevantes.

4. ANÁLISIS DE LA OPORTUNIDAD CIBERDELICTIVA

Como bien se indica en la metodología, para poder dar respuesta a las dudas planteadas, se procede a analizar los casos probados en la justicia española referentes a la

Blockchain y las criptomonedas, especialmente el Bitcoin, ya que es la manera más práctica de conocer la situación actual y los casos que más se repiten en la sociedad.

3.1. Procedimiento de búsqueda y datos obtenidos

El proceso de búsqueda pretende integrar la problemática respecto a la conceptualización errónea entre Blockchain y criptomonedas, por lo que primero se ha realizado una búsqueda de sentencias relacionadas con la Blockchain, después una búsqueda relacionada solo con las criptomonedas y finalmente una búsqueda concreta relacionada con el bitcoin, al ser la moneda más conocida, y a su vez, la más relacionada con la actividad delictiva en internet. Una vez realizadas las búsquedas, se han puesto en común el conjunto de términos para examinar más de cerca la terminología más utilizada en el lenguaje jurídico.

El primer término examinado corresponde a la Blockchain, donde podemos encontrar un único resultado, la STS 2109/2019 (Figura 3). Esta sentencia hace referencia a un delito reiterado de estafa y apropiación indebida mediante el uso de bitcoin. La Blockchain es mencionada de forma explicativa para entender el funcionamiento de las criptomonedas: “El bitcoin no es sino una unidad de cuenta de la red del mismo nombre. A partir de un libro de cuentas público y distribuido, donde se almacenan todas las transacciones de manera permanente en una base de datos denominada Blockchain” (STS 2109/2019, p. 6), A su vez, también define el bitcoin como “Un activo patrimonial inmaterial” (STS 2109/2019, p. 6). Siendo estas la únicas definiciones que nos podemos encontrar en lo referente a la tecnología Blockchain y su uso en criptomonedas dentro de la jurisprudencia, como ya había mencionado anteriormente acerca de la explicación de Pérez (2020).

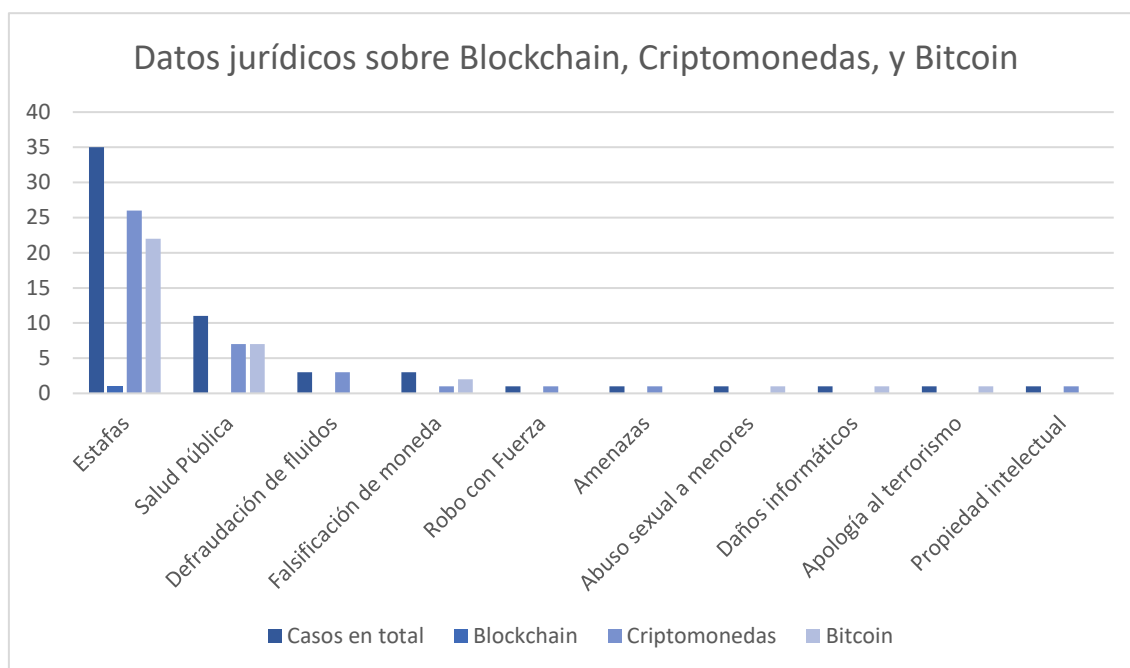
El segundo término examinado, “Criptomonedas”, es considerablemente más frecuente en los resultados. En total, se encontraron 40 casos (Figura 3) que mencionan criptomonedas, incluyendo el caso de la sentencia anterior. Estos se distribuyen de la siguiente manera: 26 corresponden a estafas, 7 casos se relacionan con delitos contra la salud pública, 3 casos están relacionados con defraudación de fluido eléctrico, y en menor medida, nos encontramos un único caso de robo con fuerza en las cosas, otro de falsificación de moneda, de amenazas y finalmente, un último caso contra la propiedad intelectual. (Figura 3)

Como podemos ver, destacan los casos de utilización de criptomonedas en estafas (SAP CC 19/2023; SAP O 1539/2022; SAP LE 43/2022; SAP PO 2387/2021; SAP Z 2056/2022; SAN 3186/2022; SAP NA 2273/2021; SAP M 7649/2022; SAP S 1593/2021; SAP IB 2322/2021) y en algunos de ellos las acciones delictivas se combinan con otras, como falsificación de moneda o apropiación indebida. El siguiente caso más recurrente es el de delitos contra la salud pública, concretamente, aquellos vinculados con la compra y venta de drogas (SAP LE 1632/2022; SAP PO 2615/2022; STSJ BAL 870/2021; SAP M 5466/2023; SAP NA 700/2022; SAP CA 3073/2021; SAP IB 919/2021), y en menor medida, también se observan delitos económicos relacionados con las criptomonedas, como la falsificación de moneda sin estafa como acompañante (SAP Z 739/2021) o la defraudación de fluido eléctrico (SAP B 1845/2022; SAP S 842/2022; SAP MA 2156/2019) debido a la minería de criptomonedas.

Es importante destacar que de estos 40 resultados, en 20 se especifica que la criptomoneda utilizada o simplemente mencionada en el caso es Bitcoin. Si realizamos una búsqueda centrada solo en Bitcoin, se obtienen 18 nuevos resultados que suprimen el término criptomoneda y mencionan directamente el Bitcoin (Figura 3). Los casos obtenidos corresponden a 9 estafas (SAP SG 411/2022; SAP LO 359/2022; SAP BA 428/2021; SJP 905/2020; SAP S 843/2020; SAP B 16826/2019; SJP 817/2019; SAP M 2779/2018; SAP L 465/2017) cuatro delitos contra la salud pública (SAP B 7133/2020; SAP TF 1900/2018; STSJ ICAN 1961/2018), dos casos de falsificación de moneda (SAP M 10579/2020; SAP Z 2107/2019), un caso de daños informáticos (SJP 2106/2019), un caso de apología al terrorismo (SAN 3185/2022) y uno de pornografía infantil (SAP MA 2072/2021), término no aceptado por la criminología debido a la falta de consentimiento en dicho acto, siendo más recomendable denominarlo como abuso sexual de menores (Interpol, s.f.), pero muy utilizado en el lenguaje jurídico.

Si observamos los datos en conjunto, podemos ver que hay un total de 58 sentencias relacionadas con la Blockchain, las criptomonedas y el Bitcoin (Figura 3). Para una visualización más simplificada y concisa de esta información, se presenta la figura 3, la cual resume los datos estadísticos recopilados en función de los términos empleados en las sentencias. En este contexto, la tabla proporciona únicamente el recuento de la frecuencia con la que cada término aparece, brindando una representación visual de su incidencia.

Figura 3: Datos jurídicos sobre Blockchain, Criptomonedas y Bitcoin.



Fuente: Elaboración propia a partir de CENDOJ.

La tabla evidencia que las criptomonedas son el término más frecuentemente utilizado en el ámbito jurídico. Esta constatación se destaca particularmente en el contexto de las estafas, donde se puede identificar una única sentencia, la STS 2109/2019, que menciona los tres términos: Blockchain, Criptomonedas y Bitcoin. Además, de las 35 sentencias relacionadas, 26 hacen uso del término "criptomonedas" en su totalidad, y dentro de estas 26, se encuentran 22 sentencias que incluyen referencias específicas al Bitcoin. Siguiendo a las estafas, como se evidenciaba en anteriormente, los delitos contra la salud pública referentes a tráfico de drogas serían los siguientes casos con más incidencia junto a la defraudación de fluidos por minería y la falsificación de moneda.

Por tanto, podemos ver que en la práctica jurídica también nos encontramos con una relación estrecha entre los términos "Blockchain", "Criptomonedas" y "Bitcoin", donde no se definen concretamente las diferencias entre ellos y se utilizan indistintamente de estas diferencias significativas, ya sean las tres a la vez, o solo el término más específico "Bitcoin", ya que en bastantes sentencias se menciona como vocablo único sin explicar su procedencia (SAP SG 411/2022; SAP LO 359/2022) o definiéndolo vagamente como moneda virtual y no como criptomoneda (SAP MA 2072/2021).

3.2. Las estafas, apropiación indebida y falsificación de moneda

Se expondrán los resultados de las estafas junto a la apropiación indebida y la falsificación de moneda a pesar de ser delitos diferentes. Esta decisión se basa en la frecuente coincidencia encontrada en la literatura jurídica estudiada, ya que se observa que los casos de estafa a menudo involucran la comisión de estas acciones.

El primer punto importante a destacar es que, en ciertos casos, las criptomonedas no han sido el objeto principal de la estafa ni han estado realmente implicadas en las acciones tipificadas, como puede ser el caso de STSJ M 1713/2023, SAP PO 2821/2022 o incluso SAP SG 411/2022. En estos casos las criptomonedas solo representan datos de la economía del acusado o del particular, como en el caso SAP PO 2821/2022 donde se menciona que el dinero que el acusado utilizaba para pagar procedía de la venta de criptomonedas, o en el caso SAP SG 411/2022, donde el dinero estafado se invirtió en criptomonedas “En los razonamientos de la sentencia, que no en los hechos probados, se habla de otros movimientos, operaciones complicadas de bizum, de bitcoin, etc. No se concretan esas operaciones, ni han sido objeto de acusación ni enjuiciamiento” (SAP SG 411/2022, p. 5). Como podemos ver, este tipo de referencias económicas no son parte de los actos que se están enjuiciando.

Una vez aclarado este punto, se procede a resumir los resultados obtenidos en lo referente a la utilización de las criptomonedas en la realización de estafas. La situación típica que se da en este tipo de casos procede de empresas que se dedican al mundo de las criptomonedas (SAP Z 2056/2022; STSJ PV 1044/2021) o particulares (SAP O 1539/2022; SAP SG 411/2022; SAP NA 2273/2021; SAP BA 428/2021) que se sirven de diferentes estrategias ilegales para la obtención de criptomonedas. Las dos estrategias principales, que suelen darse en conjunto, consisten en, por una parte, la utilización de phishing, un tipo de estafa tradicional penado en el art. 248 del Código penal, que consiste en un engaño a los usuarios para que proporcionen al atacante, o phisher, información valiosa sobre la base de alguna falsa amenaza (Myers, 2006; citado en Balcells, 2019). Por otra parte, los ciberdelincuentes proceden a utilizar las tarjetas de crédito de las víctimas para la adquisición de criptomonedas, siendo esto una estafa informática penada en el art. 249 del Código Penal y que suele conocerse como carding, y como se indicaba, consiste en el robo de datos de tarjetas bancarias y su posterior utilización ilícita (Ballcells, 2019).

Por tanto, el proceso que se lleva a cabo, descrito en las sentencias, sigue los siguientes pasos: Los ciberdelincuentes averiguan subrepticamente los datos bancarios de las víctimas, mayoritariamente mediante phishing, donde engañan a la víctima para obtener sus credenciales, y una vez obtenidos, registran los datos en páginas de compraventa de criptomonedas donde realizan varias compras sin el consentimiento del titular de la tarjeta (SAP CC 19/2023). En estos casos, la persona acusada suele considerarse cooperador necesario de la empresa o el particular que obtiene el beneficio “Se declara expresamente que, en las sucesivas fechas de 6 y 7 de diciembre de 2019, la acusada, Magdalena, cuyas demás circunstancias ya constan, cooperó hasta en tres operaciones de compra fraudulenta de criptomonedas” (SAP CC 19/2023, p. 2), esto se debe a la existencia de un engaño o acuerdo previo con las personas que se dedican a la compraventa de criptomonedas “Personas que adquieren criptomonedas engañan a terceras personas para que realicen los pagos al vendedor, de modo que así resulta cooperador involuntario del delito.” (SAP NA 2273/2021, p. 2). Dentro de estas acciones, también podemos encontrarnos con acciones más burdas, como ofertas de servicios falsos “Serafina respondiendo a un anuncio de Internet relativo a la venta de un cachorro de perro... remitió por transferencia a la cuenta... la suma de 140 euros, sin que a fecha de hoy los denunciados, hayan entregado el perro, ni devuelto el dinero.” (SAP NA 1104/2019, p. 1) para posteriormente invertir ese dinero en criptomonedas “Engaña a la denunciante diciéndole que le va a mandar un perro, para lo que consigue que le ingrese en la cuenta del apelante denunciado los 140€, y para que éste se los transfiera en criptomoneda.” (SAP NA 1104/2019, p. 2)

A su vez, como indicaba al inicio, la apropiación indebida y la falsificación de moneda suele darse conjuntamente debido a la naturaleza del tipo de estafa descrito. La apropiación indebida del patrimonio de la víctima suele verse en varias de las estafas mencionadas, como (STSJ PV 1044/2021) “Está claro que era la obtención de un lucro disponiendo el patrimonio ajeno, apropiándose de las monedas de su cliente” refiriéndose en esta caso a la apropiación de las criptomonedas de la víctima, pero también podemos encontrarnos con la apropiación del patrimonio de la víctima para la compra de criptomonedas “En consecuencia el denunciado a pesar de tener conocimiento de que había recibido una cantidad de forma indebida, decidió apropiársela enriqueciéndose en detrimento de la denunciante.” (SAP BU 343/2021, p. 3) ya que es el caso más frecuente. En lo referente a la falsificación de moneda, se falsifica dinero con la intención de invertir

financieramente en criptomonedas, concretamente en Bitcoin “Dicho acusado era el que tenía la capacidad, conocimientos y material necesarios para poder llevar a cabo esta actividad, tratándose de una persona con conocimientos informáticos y buen conocedor del manejo de Internet, llevando a cabo sus compras mediante pagos con monedas virtuales (bitcoin).” (SAP Z 2107/2019, p. 3)

3.3. Delitos contra la salud pública: Trafico de drogas

En lo referente a los delitos contra la salud pública, se trata del siguiente caso más frecuente en la literatura jurídica, y se puede observar una clara relación entre las criptomonedas y la compraventa de drogas.

Es importante destacar que las criptomonedas no son la acción principal o uno de los elementos principales que componen la acción. En estos casos, suelen ser mencionadas como un negocio externo de los acusados o para explicar el nivel económico de los acusados. “También ha recibido la herencia de su padre, que ha invertido en criptomonedas y que da clases de entrenamientos personales” (SAP LE 1632/2022, p. 15), por lo que puede considerarse como una posible excusa argumental “Por otro lado, el acusado aunque dice que se dedica a la minería de criptomonedas, no aporta prueba alguna al respecto, y es menos creíble aún que afirme que le toca de manera habitual premios en las máquinas recreativas.” (SAP CA 3073/2021, p. 5). Por otra parte, también puede encontrarse pruebas que relacionen al acusado o acusados con las criptomonedas “Se hallaron... una máquina de contar dinero, varios datafonos, seis tarjetas prepago, dos tarjetas de criptomonedas; una bolsa con MDMA” (SAP M 5466/2023, p. 5) refiriéndose a los objetos obtenidos en una entrada y registro, pero sin guardar relación directa, o al menos, sin que se mencione relación directa con el caso.

Aun así, aunque menos frecuente, también es importante resaltar el uso de criptomonedas para la compra y venta de drogas “Para la compra de las citadas sustancias estupefacientes se utilizaba la moneda virtual denominada Bitcoin y una cuenta corriente para ingresos en efectivo y posterior compra de las denominadas Bitcoin a través del acceso TOR” (SAP TF 1900/2018, p. 2) “Compraba la moneda "bitcoin" y con éstas, las sustancias estupefacientes a través de la denominada red Tor” (SAP TF 284/2018, p.2). Como podemos ver, es común como medio de pago para la compraventa de drogas online a través de la dark web.

Otro punto importante a destacar, pero que será analizado más en profundidad en el siguiente apartado, es la posibilidad de que en este tipo de delitos se utilicen las criptomonedas como una forma de ocultar las grandes sumas económicas obtenidas del tráfico de drogas.

3.4. El blanqueo de capitales

En relación al delito de blanqueo o lavado de dinero, ampliamente destacado en la literatura científica, se encontraron escasas menciones específicas en la literatura examinada. Estas menciones se encontraron en las siguientes sentencias: SAN 2959/2021, que se refiere a un caso de estafa informática continuada por parte de un grupo criminal y STSJ BAL 870/2021 y SAP IB 919/2021, relacionadas con casos de compraventa de drogas.

Partiendo de la información que estas sentencias nos brindan, podemos observar que el blanqueo de dinero se lleva a cabo principalmente de manera tradicional (STSJ BAL 870/2021), combinándose con el uso de criptomonedas “El Sr. Severino habría transformado los beneficios obtenidos a través de su actividad criminal, que se obtenían principalmente en efectivo, utilizando diferentes servicios de cambio de divisa a dinero virtual, principalmente a criptodivisas.” (SAN 2959/2021, p. 4-5) Hasta este punto, podemos observar que el ciberdelincuente efectivamente utilizó las criptomonedas como un lugar donde almacenar el dinero obtenido de forma ilícita, pero según indica la sentencia “Luego volvería a transformar en dinero de curso legal para cargar tarjetas prepago” (SAN 2959/2021, p. 5), por lo que fueron utilizadas como un método de borrar sus huellas o de despistar a los cuerpos de seguridad y no como un método de blanqueo.

En el caso de SAP IB 919/2021 no se relaciona, o al menos no se menciona, directamente el hecho de que el ciberdelincuente se dedicase a la inversión en criptomonedas con el delito de blanqueo de capitales “Sobre el delito de blanqueo de capitales con el que acusó a Rubén , y que el acusado reconoció, se dan los requisitos legales para dicha subsunción en el art.301 CP.” (SAP IB 919/2021, p. 108) “Las conversaciones en las que es intervenido acreditan que se dedica, o conoce bien, la compra de criptomonedas, pero ello no resulta incompatible con la integración en un grupo dedicado al tráfico de drogas” (SAP IB 919/2021, p. 45), como podemos ver, no hay suficiente información que relacione ambas acciones, sobre todo si tenemos en cuenta que relacionan el blanqueo de capitales principalmente con actividades inmobiliarias

“Reconoció que con Esteban llevaba temas inmobiliarios y que, ante la incipiente venta de un hotel, estuvieron hablando de invertir en Bitcoins, pero nunca le llegó a dar el dinero Esteban; de igual manera corroboró el tema de la churrería de Esteban como tema inmobiliario.” (SAP IB 919/2021, p. 47).

Por último, en el caso STSJ BAL 870/2021, nos encontramos en una situación parecida al caso anterior, donde convergen las actividades inmobiliarias y la inversión en criptomonedas “Y desde luego la dedicación del recurrente a las operaciones inmobiliarias y a las criptomonedas ha sido completamente establecida por los agentes de policía que llevaron a cabo las investigaciones” (SAP IB 919/2021, p. 78), podemos en este caso ver un patrón en las declaraciones de los acusados, donde las actividades inmobiliarias son pertinentes a la hora de justificar sus múltiples viajes “Considera imposible descartar que los viajes de Luis Manuel pudieran ser para transportar dinero y no drogas, tal y como fue admitido en juicio por el agente de policía interrogado sobre este extremo.” (SAP IB 919/2021, p. 78) pero no en el caso de las criptomonedas, donde solo se menciona la existencia de una relación con el asesoramiento de bitcoins por parte del acusado “Se dedica a la compraventa hotelera y al asesoramiento de bitcoins.” (STSJ BAL 870/2021, p. 77)

Como podemos ver, en la práctica jurídica no se menciona habitualmente una relación entre el blanqueo de dinero y las criptomonedas, y en aquellos casos donde las relacionan, se trata de situaciones donde las utilizan como una herramienta de ocultación que no directamente termina en blanqueo de capitales. También es importante tener en cuenta que, en aquellos casos donde no se relacionan puede deberse a la falta de pruebas, puesto que lo que si tienen en común es que se trata de delitos de compraventa de drogas, acción que se caracteriza por la obtención de grandes beneficios económicos, donde la inversión en criptomonedas, que no el blanqueo de capitales, puede suponer otra forma de obtener más dinero “Así, como ya dijimos en el caso de Esteban , tanto la actividad inmobiliaria como la de inversión en criptomonedas son compatibles” (SAP IB 919/2021, p. 47).

3.4 Otros datos de interés

Finalmente, es importante mencionar los resultados acerca de aquellas sentencias donde nos encontramos con delitos minoritarios, como la defraudación de fluidos, las amenazas, daños informáticos, delito contra la propiedad intelectual o el abuso sexual

infantil, ya que pueden aportar nueva información sobre la actividad delictiva de las criptomonedas.

La defraudación de fluidos es otra actividad delictiva diferente, relacionada con las criptomonedas, pero que no consiste en su uso, si no en las acciones ilegales que pueden llevarse a cabo para mantener su funcionamiento.

Se constata una instalación de equipos informáticos destinada al "minado" de criptomonedas, consistiendo dicha actividad en el empleo de ordenadores y tarjetas gráficas dispuestas con el fin exclusivo del procesamiento de los cálculos matemáticos necesarios para la realización de transacciones de monedas virtuales o criptomonedas basadas en tecnología descentralizada tales como bitcoin. (SAP S 842/2022, p. 1)

Como podemos observar, la actividad delictiva reside en el empleo de la energía eléctrica, evitando el pago de la misma con la intención de poder realizar las transacciones de criptomonedas que los acusados pretenden realizar. Este tipo de delitos se basan en el hecho de que el nivel de energía que requiere realizar estas transacciones es muy elevado, y a su vez, el coste eléctrico también es muy elevado “La actividad en si no es ilícita, pero lo que se ha constatado en el caso enjuiciado y dado el elevado precio del consumo eléctrico en nuestro país, es el uso de una conexión fraudulenta a la red eléctrica”. (SAP S 842/2022, p. 2)

En el caso del abuso sexual a menores (SAP MA 2072/2021) o de apología al terrorismo (SAN 3185/2022), el uso de criptomonedas está relacionado con el pago o financiación ilícita. En el primer caso, encontraron en el registro del móvil del acusado una billetera Bitcoin con la que realizaba transacciones económicas (SAN 3185/2022), en el segundo caso, el Bitcoin sirve de moneda de entrada a webs de contenido sexual de menores “El acceso a esta página web requería que sus usuarios paguen, mediante la moneda virtual "bitcoin", o que suban archivos de pornografía infantil.” (SAP MA 2072/2021, p. 2)

Los casos restantes no tienen el uso de criptomonedas como elemento principal. Por ejemplo, en el caso de amenazas, los acusados amenazaron a la víctima por un intento de estafa con criptomonedas “Se explica que la aquí denunciante intentó estafarle mediante criptomonedas transmitiendo que era una profesional de la materia.” (SAP M 1026/2022, p. 2), algo similar podemos observar en el caso de robo con fuerza, donde el acusado, al entrar a robar en la casa de la víctima, se apoderó de 7 unidades de ordenadores para minería de criptomonedas (SAP PO 3073/2022, p. 2).

5. DISCUSIÓN

A continuación, se llevará a cabo un análisis detallado de los resultados obtenidos y se establecerá su relación con la teoría examinada para poder responder a los planteamientos iniciales del trabajo. Para ello, se tendrán en cuenta las ideas principales extraídas del marco teórico y se compararán con los datos expuestos en los resultados, los cuales han surgido a partir del análisis de los casos relacionados con la Blockchain y las criptomonedas en el ámbito jurídico español.

Como se planteaba inicialmente, el objetivo detrás de este estudio consiste en exponer el papel de la Blockchain en la actividad ciberdelictiva actual, y más específicamente, su participación en la ocultación de la actividad delictiva en la red. La motivación detrás de esta elección reside en que este tema ha despertado una preocupación reciente en la literatura debido al creciente interés público en las criptomonedas y las potenciales oportunidades que esta nueva tecnología puede brindar a los ciberdelincuentes.

Para poder ofrecer una lectura óptima, se dividirán los planteamientos iniciales en los siguientes apartados.

5.1. La Blockchain y su relación con la ocultación delictiva

La pregunta principal sobre la que versa este trabajo plantea la duda de si la Blockchain es utilizada por los ciberdelincuentes primariamente como una herramienta de ocultación delictiva, la motivación detrás de esta pregunta reside en las características que la literatura describe, como el anonimato o la seguridad que dicho sistema garantiza (Navarro 2019; Saldaña, 2017; Zárate, 2022; Domínguez et al., 2018) y que serán examinadas en el siguiente apartado de forma más extensa puesto que una de las hipótesis se basa más concretamente en dichas características.

La respuesta en relación a la pregunta principal es afirmativa, la blockchain si tiene cierta relación con la posibilidad de ocultar actos ilícitos concretos, pero su utilización mayoritaria en la ciberdelincuencia no es dicha ocultación. Como hemos podido observar en el análisis de los resultados, la amplia mayoría de casos donde más abunda la utilización de criptomonedas son las estafas (Figura 3) donde la acción típica no se basa en la ocultación delictiva, si no en la obtención de un beneficio económico (STSJ M 1713/2023; SAP PO 2821/2022; SAP SG 411/2022), y este es el uso mayoritario que los ciberdelincuentes dan a las criptomonedas, replicando las acciones tradicionales de estafa

en el ciberespacio (Miró, 2012). Aun así, esto no implica que no exista un uso ocultativo, como se menciona mayoritariamente en la literatura, podemos observarlo en el caso SAN 2959/2021 en relación con el blanqueo de capitales, donde se utilizaban como un medio de ocultación temporal para posteriormente poder introducir el dinero en la economía tradicional (SAN 2959/2021), esto se relaciona con lo expresado en Crypto Crime Report (2023), donde se indica que se blanquearon en el año 2022 un total de 23.8 billones en criptomonedas, sin embargo, en las especificaciones se aclara que el uso de las criptomonedas es temporal, es decir, se emplean como un lugar donde depositar o almacenar el dinero antes de utilizarlo nuevamente en la economía tradicional. Por lo tanto, teniendo esto en cuenta, se interpreta que gran parte de esos billones fueron transferidos a criptomonedas como una forma de ocultación delictiva más que como un medio de blanqueo típico, donde se busca convertir dicho capital en una fuente económica legítima.

5.2. Las características de la Blockchain y su relación con la ocultación delictiva

Para entender más en detalle la relación entre la Blockchain y la ocultación delictiva, es imprescindible comprender como sus características y funcionamiento pueden ser facilitadores de dicha ocultación, o por el contrario, suponer una dificultad. Según se planteaba en la hipótesis inicial, basada en la literatura mayoritaria, la anonimidad y su naturaleza descentralizada son facilitadores a la hora de ocultar la acción delictiva, por lo que estas características suponen la mayor dificultad para combatir este fenómeno. Según lo encontrado en los resultados, las características de la Blockchain y las criptomonedas facilitan generalmente la actividad delictiva, y concretamente la ocultación delictiva en menor medida.

Como hemos observado a lo largo de toda la revisión bibliográfica, existe cierta confusión en relación con las características de la Blockchain, como puede ser el caso de los errores respecto a su capacidad distributiva o descentralizada (Gabela, 2019; Saldaña, 2017; Gutiérrez, 2018; Grigera del Campillo, 2021), el caso de la anonimidad (Gabela, 2019; Zárate, 2022), que realmente se considera como pseudoanonimidad debido al funcionamiento concreto de la Blockchain (Pérez, 2020), o el de la rastreabilidad (Pérez, 2020), no muy mencionado por la literatura pero de gran importancia respecto a la ocultación delictiva. Aun así, se han consensuado en el marco teórico las definiciones

técnicas de estas características, siendo estas las que se tendrán en cuenta para responder a las hipótesis.

Como ya se ha mencionado en el apartado anterior, el delito donde más presencia tiene el uso de criptomonedas es la estafa. La acción típica consiste en engañar a las víctimas para obtener su información bancaria y utilizar su dinero para invertir en criptomonedas (SAP SG 411/2022). También se emplean tácticas más rudimentarias, como engañar a las víctimas mediante compras fraudulentas que solo buscan obtener fondos para financiar la adquisición de criptomonedas (SAP CC 19/2023). Destaca el phishing como la principal forma de estafa, mediante el uso de páginas web fraudulentas que capturan los datos personales de las víctimas. El objetivo principal es recaudar dinero que posteriormente será invertido principalmente en bitcoin (SAP NA 1104/2019). Como podemos ver, la anonimidad o pseudoanonimidad y la rastreabilidad tienen gran relevancia para este tipo de estafas (SAP SG 411/2022), ya que al transferir el dinero robado a criptomonedas es más difícil de localizar a la hora de investigarlo debido a la ausencia de la necesidad de utilizar identidades. Esto plantea una forma adicional de ocultación delictiva.

Otro uso claramente destacado en los resultados y mencionado en las hipótesis corresponde al uso de las criptomonedas como un medio de pago. En este caso si nos encontramos con diversos resultados que corroboran esta afirmación, todos ellos relacionados con la compraventa de drogas (SAP B 7133/2020; SAP TF 1900/2018; STSJ ICAN 1961/2018) y en un único caso, la compra de material fotográfico producido como resultado del abuso sexual a menores (SAP MA 2072/2021). De nuevo, destaca principalmente su capacidad de pseudoanonimidad y rastreabilidad como potenciales favorecedores de su utilización. Esto se debe a que la compraventa de cualquier material de origen ilícito siempre ha planteado un desafío para los delincuentes, ya que los medios de pago tradicionales están sujetos a instituciones que controlan dichas transacciones y la obligación de identificarse, por lo que las criptomonedas suponen una herramienta clave.

Además, es importante destacar que la Blockchain y las criptomonedas son una tecnología relativamente nueva, un hecho que no solo explica las dificultades a la hora de establecer el marco teórico, si no que también se ve reflejado en la práctica, donde la blockchain y las criptomonedas sirven a los ciberdelincuentes como un método de engaño suficiente para estafar dinero, haciendo creer a las víctimas que este irá destinado a la compra de criptomonedas (SAP CC 19/2023) o la utilización de la estafa tradicional para

obtener dinero que cubra deudas producidas por las propias criptomonedas (SAP NA 1104/2019)

5.3. El blanqueo de capitales y su relación con las criptomonedas y el Bitcoin

La principal problemática encontrada durante el análisis reside en la relación mayoritaria de la literatura respecto al blanqueo de capitales, la Blockchain y las Criptomonedas. Como ya se ha indicado, el blanqueo de capitales no está realmente presente en los casos jurídicos analizados acerca de la Blockchain y las criptomonedas. Las únicas menciones que podemos hallar se encuentran en casos de compraventa de drogas (STSJ BAL 870/2021; SAP IB 919/2021) debido a que es una acción típica a la hora de intentar encubrir las grandes cantidades de dinero que se obtienen de este negocio ilícito. Esto nos indica que hasta cierto punto la Blockchain y las criptomonedas si pueden utilizarse como una forma de ocultación delictiva, pero no completamente como un instrumento de blanqueo de dinero.

Los motivos detrás de esta contradicción residen en la tecnología y funcionamiento del Bitcoin, la moneda más vinculada con la actividad delictiva (Navarro, 2019; Saldaña, 2017) y el blanqueo de capitales (Cypto Crime Report, 2023). Como se indicaba anteriormente, el Bitcoin presenta dificultades a la hora de soportar todas las transacciones que los usuarios quieran realizar debido al sistema “Proof-of-Work” un sistema donde se requiere la utilización de grandes cantidades de energía para llevar a cabo la verificación de la transacción. De este hecho se derivan dos consideraciones que representan los motivos de la imposibilidad de utilizar el bitcoin como un sistema de blanqueo de capitales: El Bitcoin favorece la competencia entre usuarios al recompensar con bitcoins a todo aquel que logra verificar una transferencia (Gretenkort, en prensa) lo que genera una desigualdad entre los nodos al posicionar más favorablemente a ciertos usuarios que si disponen de la capacidad de verificar dichas transacciones (Gretenkort, en prensa), y por tanto, atendiendo a las características de la Blockchain, lo convierte en un sistema más descentralizado que distribuido.

Esta desigualdad y dificultad a la hora de poder verificar una transacción entorpece enormemente la posibilidad de blanquear dinero mediante Bitcoin, un tipo de delito que necesita del constante movimiento de dinero, y que debido a la dificultad para realizar la transacción, limita enormemente sus posibilidades.

5.4. Limitaciones

Como último punto en la discusión, es crucial destacar las limitaciones identificadas durante el desarrollo de la investigación, con el fin de comprender plenamente el contexto en el que se ha llevado a cabo el estudio y las áreas que podrían ser examinadas con mayor detalle en futuras investigaciones.

1. La falta de un consenso respecto a las definiciones y al funcionamiento de la Blockchain, las criptomonedas o el bitcoin en la literatura, y por tanto, en las sentencias analizadas, dificulta el desarrollo de las interpretaciones en la parte práctica al no existir explicaciones elaboradas de su presencia en dichos casos.
2. El análisis de la oportunidad delictiva en los casos prácticos se basan solamente en hechos esclarecidos, por lo que es importante tener en cuenta que esto no representa el total de casos existentes donde se utilice Blockchain y criptomonedas, ya que la cifra negra es inherente a todas las formas de criminalidad.
3. Con respecto a este último punto, también es necesario mencionar que el estudio de estos casos prácticos está limitado concretamente al CENDOJ, y por ello, los casos analizados son solo aquellos que los tribunales españoles han hecho públicos.

6. CONCLUSIONES

Para finalizar, se expondrán las conclusiones en relación con la temática analizada.

En primer lugar, es importante señalar la falta de consenso en la literatura respecto a la definición de la Blockchain y las criptomonedas, no existen definiciones aceptadas por la normativa más allá de la escueta definición del Tribunal Supremo, y esto genera confusión y dificultad a la hora de comprender los conceptos y su funcionamiento. A raíz del análisis realizado, se ha concluido que la Blockchain, las criptomonedas y el bitcoin, aunque son conceptos relacionados, también son conceptos diferentes. El Blockchain es un tipo de sistema DLT que permite registrar información mediante la utilización de hashes criptográficos, de esta manera se garantiza que dicho proceso se realice de forma segura. Las criptomonedas, que pueden o no utilizar Blockchain para realizar transacciones, son monedas de cambio virtuales, y el Bitcoin, es un tipo de criptomoneda que si utiliza Blockchain para realizar las transacciones.

Por otra parte, las características que convierten a la Blockchain y las criptomonedas en herramientas para la ocultación delictiva también se ven afectadas por la confusión existente en la literatura. Aunque la pseudoanonimidad, la capacidad distributiva y la rastreabilidad favorecen la actividad delictiva, no necesariamente su uso está limitado a la ocultación. Como hemos visto a lo largo del trabajo, su utilidad como moneda de pago para comerciar con material ilícito y su utilidad como instrumento de engaño en las estafas está más presente en los casos jurisprudenciales que el blanqueo de capitales, delito que la literatura indicaba inicialmente como el más destacable. Por tanto, podemos concluir que, actualmente, la Blockchain y las criptomonedas representan un nuevo complemento para la aplicación de la delincuencia tradicional en el ciberespacio, donde destaca el Bitcoin como la criptomoneda más vinculada a la actividad delictiva, y por tanto, donde se debe centrar el estudio de este fenómeno.

En síntesis, este trabajo surge de la necesidad de desarrollar material científico más específico y técnico sobre este nuevo fenómeno que cada vez está más presente en la actividad delictiva, aportando a la literatura científica una revisión sistemática y criminológica acerca del consenso actual sobre la Blockchain, y por consiguiente, sobre las criptomonedas al delimitarlo dentro de la cibercriminalidad y del marco jurídico español. Esta investigación sintetiza y compara información conocida con conocimientos técnicos sobre la Blockchain y las criptomonedas, analizando las preocupaciones actuales más relevantes relacionadas con delitos que involucran la ocultación de actividades criminales mediante el uso de criptomonedas gracias a la información de casos reales expuestos en el buscador jurídico del Centro de Documentación Judicial. Esta idea pretende promover la investigación de esta nueva tecnología desde una perspectiva más técnica y específica, con la finalidad de elaborar normativas y marcos legales que tengan en cuenta la situación real de la Blockchain en la cibercriminalidad.

7. BIBLIOGRAFÍA

- 3Blue1Brown (2017, Julio 7) *Have you ever wondered how Bitcoin (and other cryptocurrencies) really work?*. [video].
<https://www.youtube.com/watch?v=bBC-nXj3Ng4>
- Ávila, W. (2013). Hacia una reflexión histórica de las TIC. *Hallazgos*, 10(19), 213-233.
<https://www.redalyc.org/articulo.oa?id=413835217013>

- Cerna, J., Díaz, J. y Melquiades, M. (2018). *El uso de las criptomonedas como medio para la impunidad del delito de lavado de activos*. Repositorio Digital Institucional de la Universidad César Vallejo. <https://hdl.handle.net/20.500.12692/36934>
- Conti, M., Kumar, G., Nerurkar, P., Saha, R. y Vigneri, L. (2022). A survey on security challenges and solutions in the IOTA. *Journal of Network and Computer Applications*, 103383. <https://doi.org/10.1016/j.jnca.2022.103383>
- Chainalysis. (2023). *The 2023 Crypto Crime Report: Everything you need to know about cryptocurrency-based crime*. [Informe]. <https://go.chainalysis.com/2023-crypto-crime-report.html>
- Domínguez, J. M., García, R. (2018). Blockchain y las criptomonedas: el caso bitcoin. *Oikonomics: Revista de economía, empresa y Sociedad*, (10). https://oikonomics.uoc.edu/divulgacio/oikonomics/_recursos/documents/10/5_Dominguez-Garcia Oikonomics 10 a4 cast.pdf
- Gabela, R. (2019). *Criptomonedas como medios comisarios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas*. [Tesis abogacía, Universidad San Francisco de Quito]. Repositorio Digital USFQ. <http://repositorio.usfq.edu.ec/handle/23000/8401>
- Gretenkort, T. (in press) *The Semiotics of Consensus - Impact of Network Topology on Communication Strategies in Spanish Language Interaction Networks*. (Tesis doctoral, RWTH Aquisgrán) Hamburgo: Peter Lang.
- Grigera, S. (2021r). Ciberseguridad y Blockchain. *Revista Blockchain E Inteligencia Artificial*, (3). [https://doi.org/10.22529/rbia.2021\(3\)05](https://doi.org/10.22529/rbia.2021(3)05)
- Gutiérrez, J. (2019). El lavado de activos en la época de las criptomonedas. *Primera línea*, 39. <http://www.mpapenalcorporativo.com/wp-content/uploads/2019/02/Entre-lineas-6.pdf>
- Balcells, M. (2019). *Comprender el delito cibernético y los delitos económicos*, UOC [Apuntes académicos]. MoodleUOC.

- Criado, J. (2020). Blockchain: Criptomonedas y tokenización de activos inmobiliarios. Efectos en el ámbito registral. *Revista de Derecho, Empresa y Sociedad (REDS)*, (16), p. 253-277. <https://dialnet.unirioja.es/servlet/articulo?codigo=7631171>
- Interpol (s.f). *Terminología apropiada*. <https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada>
- Ministerio del Interior. (2021). Informe sobre la Cibercriminalidad en España 2021. [Informe]. <https://www.interior.gob.es/opencms/pdf/prensa/balances-einformes/2021/Informe-Cibercriminalidad-2021.pdf>
- Miró, F. (2012). *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons Ediciones Jurídicas y Sociales.
- Miró, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política*, (32). <https://www.raco.cat/index.php/IDP/article/view/373815>
- Nakamoto, N. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://Bitcoin.org/Bitcoin.pdf>
- Navarro, F. (2019). Criptomonedas (en especial, bitc oin) y blanqueo de dinero. *Revista electr onica de ciencia penal y criminolog a*, 21 (14). <http://hdl.handle.net/10553/74463>
- Nieto, A., Garc a-Moreno, B. (2021). Criptomonedas y derecho penal: m s all  del blanqueo de capitales. *Revista Electr nica de Ciencia Penal y Criminolog a*, 23 (17). <http://criminnet.ugr.es/recpc/23/recpc23-17.pdf>
- P rez, D. (2020). Blockchain, criptomonedas y los fen menos delictivos: entre el crimen y el desarrollo. *Bolet n Criminol gico*, 27. <https://doi.org/10.24310/Boletin-criminologico.2020.v27i.11283>
- P rez, X. (2017). Las criptomonedas: Consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la uni n europea y en Espa a. *Revista De Derecho Penal Y Criminolog a*, (18), 141–187. <https://revistas.uned.es/index.php/RDPC/article/view/24454>

Poder Judicial (s.f). Centro de Documentación Judicial (CENDOJ).
<https://www.poderjudicial.es/cgpj/es/Temas/Centro-de-Documentacion-Judicial-CENDOJ-/#:~:text=El%20Centro%20de%20Documentaci%C3%B3n%20Judicial,servicios%20de%20gesti%C3%B3n%20del%20conocimiento>

Saldaña, P. (2023). *Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes*. [Tesis doctoral, Universidad de Granada]. Digibug.
<https://digibug.ugr.es/handle/10481/81413>

Saldaña, P. (2017). ¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado. *El Criminalista Digital. Papeles de Criminología*, (7).
<https://revistaseug.ugr.es/index.php/cridi/article/download/20883/20268>

Sentencia del Tribunal Supremo 2109/2019, del 20 de junio de 2019.

Sentencia de la Audiencia Provincial de Cáceres 19/2023, del 26 de enero de 2023.

Sentencia de la Audiencia Provincial de Oviedo 1539/2022, del 25 de abril del 2022.

Sentencia de la Audiencia Provincial de León 43/2022, del 12 de enero de 2022.

Sentencia de la Audiencia Provincial de Vigo 2387/2021, del 21 de octubre de 2021.

Sentencia de la Audiencia Provincial de Zaragoza 2056/2022, del 24 de octubre de 2022.

Sentencia de la Audiencia Nacional 3186/2022, del 28 de junio de 2022.

Sentencia de la Audiencia Provincial de Pamplona 2273/2021, del 11 de noviembre de 2021.

Sentencia de la Audiencia Provincial de Madrid 7649/2022, del 27 de mayo de 2022.

Sentencia de la Audiencia Provincial de Santander 1593/2021, del 8 de octubre de 2021.

Sentencia de la Audiencia Provincial de Palma de Mallorca 2322/2021, del 7 de octubre de 2021.

Sentencia de la Audiencia Provincial de León 1632/2022, del 30 de diciembre de 2022.

Sentencia de la Audiencia Provincial de Pontevedra 2615/2022, del 15 de noviembre de 2022.

Sentencia del Tribunal Superior de Justicia de Palma de Mallorca 870/2021, del 5 de octubre de 2021.

Sentencia de la Audiencia Provincial de Madrid 5466/2023, del 14 de marzo de 2022.

Sentencia de la Audiencia Provincial de Pamplona 700/2022, del 30 de junio de 2022.

Sentencia de la Audiencia Provincial de Jerez de la Frontera 3073/2021, del 16 de diciembre de 2021.

Sentencia de la Audiencia Provincial de Palma de Mallorca 919/2021, del 24 de febrero de 2021.

Sentencia de la Audiencia Provincial de Zaragoza 739/2021, del 11 de mayo de 2021.

Sentencia de la Audiencia Provincial de Barcelona 1845/2022, del 1 de febrero de 2022.

Sentencia de la Audiencia Provincial de Santander 842/2022, del 14 de enero de 2022.

Sentencia de la Audiencia Provincial de Málaga 2156/2019, del 25 de octubre de 2019.

Sentencia de la Audiencia Provincial de Segovia 411/2022, del 27 de octubre de 2022.

Sentencia de la Audiencia Provincial de Logroño 359/2022, del 19 de agosto de 2022.

Sentencia de la Audiencia Provincial de Mérida 428/2021, del 6 de abril de 2021.

Sentencia del Juzgado de lo Penal de Zamora 905/2020, del 9 de junio de 2019.

Sentencia de la Audiencia Provincial de Santander 843/2020, del 27 de mayo de 2020.

Sentencia de la Audiencia Provincial de Barcelona 16826/2019, del 18 de octubre de 2019.

Sentencia del Juzgado de lo Penal de Logroño 817/2019, del 13 de febrero de 2019.

Sentencia de la Audiencia Provincial de Madrid 2779/2018, del 7 de marzo de 2018.

Sentencia de la Audiencia Provincial de Lleida 465/2017, 14 de julio de 2017.

Sentencia de la Audiencia Provincial de Barcelona 7133/2020, 22 de julio de 2020.

Sentencia de la Audiencia Provincial de Santa Cruz de Tenerife 1900/2018, 3 de octubre de 2018.

Sentencia del Tribunal Superior de Justicia de Las Palmas de Gran Canaria 1961/2018, 28 de septiembre de 2018.

Sentencia de la Audiencia Provincial de Madrid 10579/2020, 7 de octubre de 2020.

Sentencia de la Audiencia Provincial de Zaragoza 2107/2019, 21 de febrero de 2019.

Sentencia del Juzgado de lo Penal de Cartagena 2106/2019, 23 de mayo de 2019.

Sentencia de la Audiencia Nacional 3185/2022, 28 de junio de 2022.

Sentencia de la Audiencia Provincial de Málaga 2072/2021, 12 de mayo de 2021.

Rogaway, P. (2004). Nonce-based symmetric encryption. En Roy, B y Meier, W. (Eds.), *Fast Software Encryption* (p. 348-358). <http://dx.doi.org/10.1007/b98177>

Wicab, O. (2018). Las criptomonedas ¿son realmente dinero?: Una perspectiva marxista sobre las monedas digitales y el bitcoin. *Ciencia Económica*, 12. <http://www.economia.unam.mx/cienciaeco/pdfs/num12/01WICAB.pdf>

Zárate Hernández, M. (2023). La nueva era de la criminología. *Revista Mexicana De Ciencias Penales*, 6(19), 141-156. <https://doi.org/10.57042/rmcp.v6i19.606>